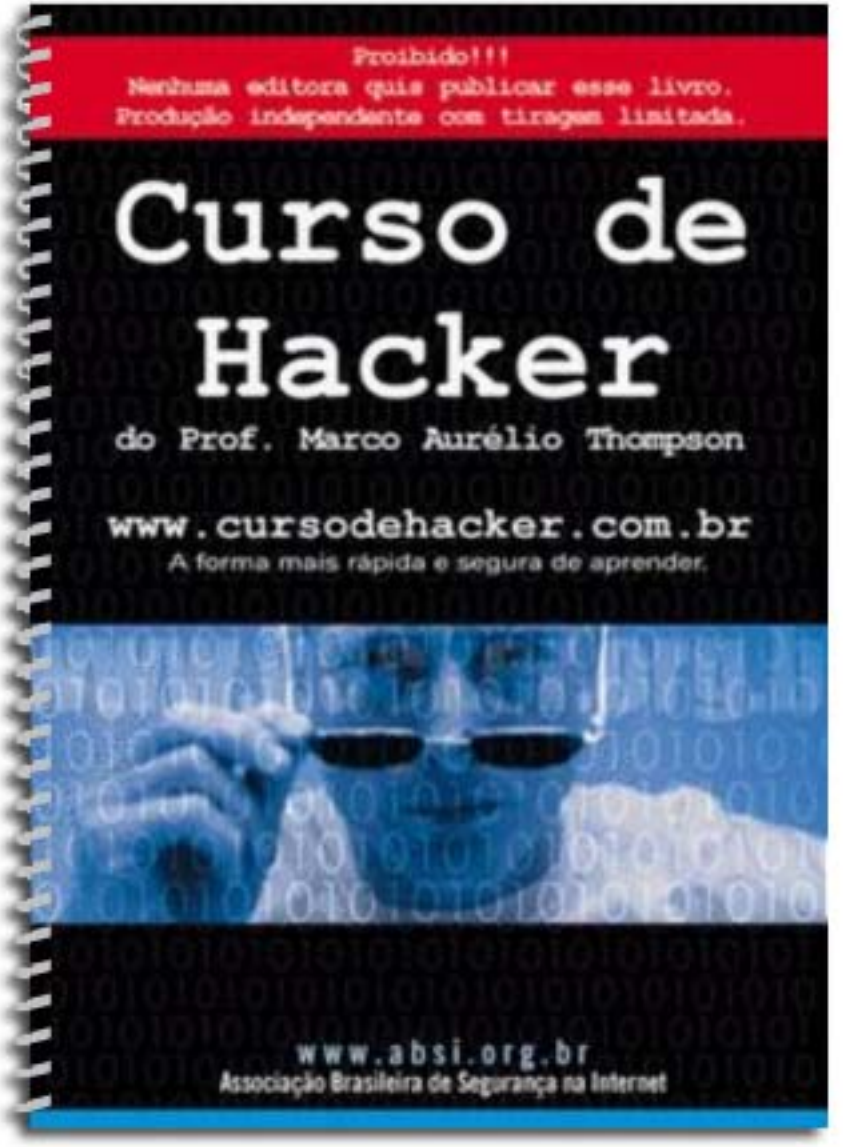

Proibido!!!
Nenhuma editora quis publicar esse livro.
Produção independente com tiragem limitada.
Curso de Hacker
do Prof. Marco Aurélio Thompson
www.cursodehacker.com.br
A forma mais rápida e segura de aprender.
www.absi.org.br
Associação Brasileira de Segurança na Internet

Apresentação da versão eBook

Este livro foi lançado em 2003 e fez um grande sucesso. Pela primeira vez alguém teve a coragem de mostrar como ocorrem as invasões de contas bancárias e desmistificar vários assuntos ligados ao tema. Este livro também popularizou o uso das máquinas virtuais. Antes de 2003, pouquíssima gente falava sobre isto.

Até hoje alguns assuntos deste livro não são abordados em nenhum outro e nem em sites. Mas é claro que três anos após o lançamento, o impacto não é o mesmo daquela época. Parecido com as cenas do filme Matrix, com ângulos de câmera em 360º. Este tipo de FX hoje não causa o impacto de antes.

Mas na época foi o que aconteceu. Editoras e gráficas se recusaram a publicá-lo. Tivemos que produzi-lo nós mesmos. E sem a ajuda de um revisor profissional, pequenos deslizes de revisão foram cometidos. Aproveito para pedir desculpas por esta pequena falha e conto com vocês para identificá-las e corrigi-las nas próximas edições.

Também quero aproveitar para dizer que este é um livro para iniciantes. Se você se acha *o fera* e coisa e tal, vou poupar seu tempo: procure outra leitura. Não vá fazer que nem os putos que nunca publicaram nada na vida e adoram desmerecer o trabalho dos outros. O mais comum que leio por aí é o tal do 'está tudo na Internet'. O problema é que nunca mostram onde encontrar na Internet. Eu desconfio de qualquer pessoa que faz críticas vagas e não tem sequer um projeto a apresentar. Despeito puro. Mas fico feliz quando recebo mensagens do tipo '*na página tal do livro tal você poderia ter explicado melhor/se aprofundado*'. Isto sim, contribui para a melhora do produto.

* 'putos' aqui no sentido carinhoso, como no título do livro 'Memórias de Minhas Putas Tristes' de Gabriel Garcia Márquez.

Mas como não tem jeito, vou ser elogiado e criticado, tudo ao mesmo tempo, vou lançar um desafio para o Volume 2, a ser lançado em 2007. Envie um e-Mail respondendo a seguinte pergunta:

'O que você gostaria de ler no Volume 2 do Livro Proibido, que seja tão impactante quanto foi na época, o lançamento do Volume 1?'

Envie para: atendimento@cursodehacker.com.br

Vocês sabem que atualmente sou quem mais entende de hacker no Brasil. Não há quem tenha mais cursos, livros, ebooks, textos, projetos, idéias, vídeoaulas, alunos, revistas digitais, que eu. E devo isto a vocês. Então quero aproveitar para agradecê-los:

Aos alunos, associados, bolsistas, clientes e amigos, obrigado pelo apoio e incentivo.

Aos despeitados, processados e invejosos, obrigado por mostrarem onde eu precisava melhorar. Continuem assim. Não há Mozart sem Salieri.

Realmente só tenho a agradecer. Poderia incluir a família, Deus e o anjo da guarda, mas ia parecer piegas, então fiquemos apenas com as coisas terrenas mesmo.

Boa leitura. Avise-me se achar algum erro. Fale sobre o que gostou e sobre o que não gostou. Faça críticas construtivas que é assim que eu cresço. Só me poupe da perfídia, caso tenha alguma, pois esta, eu dispenso.

* As ERRATAS que forem comunicadas ou constatadas serão publicadas em:

http://www.cursodehacker.com.br/erratas.htm

** Caso queira adquirir a versão IMPRESSA deste livro, com o CD-ROM que o acompanha, favor acessar:

http://www.absi.org.br/loja

(a) Prof. Marco Aurélio Thompson
atendimento@cursodehacker.com.br
Tel: +55 (71) 8108-7930

Sites interessantes:
http://MarcoAurelio.Net
http://www.cursodehacker.com.br
http://www.cursodephreaker.com.br
http://www.absi.org.br

“Você tem o direito de permanecer calado.
Tudo o que você fizer usando o conhecimento deste livro
poderá ser usado contra você no tribunal.”

Versão especial em formato eBook para ler na tela do computador. Não acompanha os CDs com programas citado no livro. Proibida a impressão, cópia e distribuição. As páginas em branco existentes na versão impressa foram removidas. Por este motivo você vai perceber pequenas ausências na numeração das páginas deste eBook.

Projeto Editorial, Revisão e Diagramação: *Marco Aurélio Thompson*
Capa: *Maurício S. de França*

O Livro Probido do Curso de Hacker

Prof. Marco Aurélio Thompson

Ano: 2007 2006 2005 2004
Edição: 9 8 7 6 5 4 3 2 1

Edições da ABSI

Dados Internacionais de Catalogação na Publicação (CIP)
(Câmara Brasileira do Livro, SP, Brasil)

Thompson, Marco Aurélio
O Livro Proibido do Curso de Hacker / Marco Aurélio Thompson. -- Salvador: ABSI, 2004

Bibliografia.
ISBN: 85-98941-01-8
1. Internet (Redes de computadores). 2. Internet - Programação. I. Título

CDD-004.678

Índice para Catálogo Sistemático:

1. Internet: Redes de computadores 004.678

O Autor e a Editora acreditam que todas as informações aqui apresentadas estão corretas e podem ser utilizadas para qualquer fim legal. Entretanto, não existe qualquer garantia, explícita ou implícita, de que o uso de tais informações conduzirá sempre ao resultado desejado. Os nomes de sites e empresas, porventura mencionados, foram utilizados apenas para ilustrar os exemplos, não tendo vínculo nenhum com o livro, não garantindo a sua existência nem divulgação. Eventuais erratas estarão disponíveis no site do Curso de Hacker (www.cursodehacker.com.br) para download.O autor também se coloca a disposição dos leitores para dirimir dúvidas e discutir quaisquer dos assuntos tratados nesta obra; por chat, E-Mail ou telefone.

ABSI - Associação Brasileira de Segurança na Internet
Caixa Postal: 2021, Salvador, BA, Cep: 40024-970
Site: www.absi.org.br
E-Mail: atendimento@absi.org.br

ADVERTÊNCIA

As informações contidas nesta obra se baseiam na minha experiência pessoal. Também foram feitas pesquisas na rede mundial de computadores (Internet) e consultas aos RELATÓRIOS RESERVADOS da ABSI - Associação Brasileira de Segurança na Internet. É um livro dedicado a iniciantes e as explicações foram dosadas, para não serem nem demasiadamente técnicas e muito menos superficiais. Enfatizei os aspectos práticos dos temas. A maior parte das técnicas aqui descritas, se colocadas em prática contra terceiros, poderá causar danos, com consequente interpelação judicial. Nosso objetivo ao divulgar estas informações, é tão somente o de contribuir para o aumento da segurança nas redes de computadores. Por mais paradoxal que possa parecer, acredito que só através da divulgação das falhas existentes nos sistemas de redes locais (LANs) e da rede mundial de computadores (Internet) é que os fabricantes de software, hardware e os profissionais de TI, se preocuparão em oferecer produtos e serviços comprovadamente seguros. Não concordo com a forma atual como somos tratados enquanto consumidores de software e hardware: empurram-nos programas, produtos e serviços ainda em fase de testes e nos cobram por isso. Esta é a minha bandeira. Em todo caso, me isento da responsabilidade pelo mal uso destas informações. Se em qualquer parte da leitura deste livro, alguma frase, palavra, parágrafo ou expressão, sugerir o incentivo a prática de delitos, por favor desconsidere. Embora a Constituição Federal, em seu Artigo 5º, me garanta a liberdade de expressão, nem por isso dá aos meus leitores e alunos, o direito de cometer atos ilícitos a partir das informações obtidas por meu intermédio.

Salvador, 10 de abril de 2004.

Prof. Marco Aurélio Thompson

Dedicatória

Aos meus alunos, clientes, leitores e colaboradores: os responsáveis permanentes pelo meu sucesso pessoal e empresarial.

Marco Aurélio Thompson é carioca, nascido no bairro de Magalhães Bastos no Rio de Janeiro, mas desde os quinze anos de idade reside em Nilópolis (RJ) com a sua família. Quando criança já demonstrava interesse e curiosidade pelas artes, ciências e tecnologia. Técnico em Eletrônica aos quatorze anos, foi naturalmente envolvido pela informática através da leitura das revistas técnicas que abordavam o assunto, como a extinta *Nova Eletrônica* e as, ainda nas bancas, revista *Eletrônica* da Editora Saber (*www.sabereletronica.com.br*) e *Antenna-Eletrônica Popular* (*www.anep.com.br*), quando ainda era dirigida pelo saudoso Gilberto Afonso Penna.

Começou a programar em Basic e Assembler em um TK-85 e mesmo antes da existência de cursos regulares de informática, já ensinava os primeiros passos aos seus companheiros de caserna, durante os dois anos em que prestou o Serviço Militar no 25º Batalhão de Infantaria Pára-quedista (RJ).

Após a baixa no Exército, ingressou no I Batalhão de Polícia Rodoviária (MG), iniciando na cidade de Ituiutaba (MG) o embrião de um projeto de democratização da informática, que mais tarde passou a ser conhecido como PROJETO INFO 2000 - INFORMÁTICA PARA TODOS.

De volta ao Rio de Janeiro, começou a colaborar com a revista *Antenna/Eletrônica Popular*, com artigos e programas sobre eletrônica e informática. Nesta época iniciou por conta própria estudos sobre PNL - Programação Neurolinguística, Gestalt, Eneagrama, técnicas de Pensamento Lateral e outras formas de autoconhecimento e aprendizagem acelerada.

Em 1989, projetou e operou com uma pequena equipe de colaboradores a *TV Fareua - Canal 3*, primeira TV comunitária a atuar no município de Nilópolis (RJ).

Em 1995, voltou a se dedicar à democratização da informática e implantou definitivamente o PROJETO INFO 2000 - INFORMÁTICA PARA TODOS, começando em Nilópolis (RJ) e depois expandindo para a capital. Foram mais de oito mil alunos formados nos quase seis anos do Projeto, inclusive nas cidades de Salvador (BA) e Coari (AM).

Pouco tempo depois foi eleito presidente da SBET - Sociedade Brasileira de Educação para o Trabalho (*www.sbet.org.br*), e assumiu também o cargo de Diretor do CET - Centro de Educação para o Trabalho.

Em 1997, tornou-se consultor pelo Sebrae (RJ) e desde então vem orientando empre-

sas e pessoas sobre como se adaptar e obter melhores resultados no mundo *on-line*.

Em 1999, organizou e fundou com duzentos de seus alunos e ex-alunos dos cursos de telecomunicações ministrados pelo CET, duas cooperativas de trabalho, tendo sido indicado e eleito presidente de uma delas. No mesmo ano, foi coordenador e instrutor dos cursos de *WebDesign* da ESTI - Escola Superior de Tecnologia da Informação e instrutor dos cursos de *WebDeveloper* da mesma instituição.

Em 2002 foi eleito presidente da ABSI - Associação Brasileira de Segurança na Internet (*www.absi.org.br*) e lançou pela Editora Érica (*www.editoraerica.com.br*), os livros Java 2 & Banco de Dados e Proteção e Segurança na Internet. Este último livro lhe valeu uma participação no programa "Sem Censura" especial sobre a Internet, exibido em 18 de novembro de 2002 pela TV Educativa (RJ) e reprisado algumas vezes.Também é autor, pela mesma editora, do livro Windows Server 2003 - Administração de Redes, lançado em 2003.

Em 2003 passou a se dedicar exclusivamente a projetos de minisites, criando em menos de duas semanas, quinze projetos de alto impacto a serem lançados sequencialmente até dezembro deste ano. O primeiro minisite (*www.cursodehacker.com.br*) foi um sucesso tão grande que obrigou a criação de uma equipe exclusiva para mantê-lo e a seus subprodutos.

Para 2004 tem na fila de espera o LIVRO VERMELHO do HACKER BRASILEIRO, a BÍBLIA do HACKER BRASILEIRO, vários roteiros, produção de DVDs, o livro MANUTENÇÃO DE MONITORES, IMPRESSORAS e SCANNERS pela Editora Érica e mais quatorze minisites, tão arrasadores quanto está sendo o Curso de Hacker do Prof. Marco Aurélio Thompson.

Atualmente o autor está concretizando um antigo sonho: o de poder trabalhar em qualquer lugar do mundo, bastando um computador com acesso a Internet e um cartão de crédito Internacional.

Prefácio

Conheci o Marco Aurélio quando ele ainda era criança. Já dava para notar que não era uma criança como as outras. Pelo menos eu nunca tinha visto uma que mantivesse no quintal da sua casa um cemitério de animais. E muito menos uma criança que aos onze anos de idade já houvesse feito curso de fotografia por correspondência.

Sua pequena biblioteca incluia coisas inusitadas, como uma coleção de revistas em quadrinho (*História da Ciência*), datada de 1950, muitos anos antes dele ter nascido. E também tinha a revista *Kripta*. Como é que alguém naquela idade se interessava por uma revista como aquela? Um misto de terror, ficção científica e realismo fantástico? Até hoje é de se estranhar um menino cujo vocabulário inclua palavras como *àbíkú*[1], *Lilith*[2] e *selenita*[3]. Eu mesmo, na época, tive que procurar o significado no dicionário para não parecer ignorante diante de uma criança. E nem sempre o dicionário ajudava (acho que até hoje estas palavras são de uso restrito).

Mas o tempo passou e eu perdi o contato com ele. Só fui encontrá-lo de novo quando estudava em colégio particular no bairro de Jacarépagua, a SUSE (*Sociedade Universitária Santa Edwiges*). O primeiro mico que paguei foi perguntar pelo 'cemitério'. Ele nem lembrava mais disso. Com o tempo fui vendo que ele é assim mesmo. Às vezes lembra de coisas do arco da velha. Às vezes não lembra da fisionomia de alguém que conheceu um dia antes.

Na SUSE, de novo me surpreendo com o Marco Aurélio: apesar de estar matriculado na sexta-série (atual Ensino Fundamental, antigo 1º Grau), o danado frequentava mesmo era as aulas de laboratório de química e eletrônica. Só que estas aulas eram destinadas aos alunos matriculados no 2º ano do 2º grau em diante. E lá estava o Marco Aurélio: explicando como usar a energia elétrica do corpo de uma rã para fazer funcionar um relógio digital e a sua paixão da época, as experiências com sódio metálico, máquinas eletrostáticas e ondas de radiofrequência. Não foram poucas às vezes que seus experimentos interferiram nos aparelhos de rádio e TV da vizinhança. Ficou tão estigmatizado que até quando não era ele a causa, sofria com os efeitos. Eu fico pensando como seria se já existisse a microinformática e a Internet...

Mas esta ausência na própria classe lhe custou caro, como a repetição de ano por duas vezes e um longo atraso na conclusão do 2º grau (atual Ensino Médio). Alias, sair depois e chegar antes já parece fazer parte da personalidade dele. Mesmo tendo ficado de fora na seleção para a Marinha do Brasil, onde se alistou por influência do pai, deu um jeito de servir como paraquedista do Exército, uma tropa de elite cuja entrada é das mais difíceis.

Depois de muito tempo sem contato, nos encontramos de novo. Dá até a impressão de que vamos nos ver esporadicamente até o fim dos nossos dias. Espero que sim, pois sempre há boas histórias para ouvir e você sempre sai de uma conversa com o Aurélio precisando rever conceitos.

Me foi pedido para prefaciar o seu 'LIVRO PROIBIDO'. Li. Gostei. Ri. Mas também me assustei. Tem coisas que eu pensei que não fossem fáceis e são. Tem coisas que eu pensei que fossem impossíveis e não são. Até sugeri que ele usasse um pseudônimo. Sei lá. Eu não teria coragem de me expor a frente de um assunto tão polêmico. Mas depois entendi que todos nós precisamos saber a verdade sobre a segurança nas redes e Internet. E se for o Marco Aurélio que vai nos mostrar estas verdades, melhor ainda.

M.·. Leonardo.·.

1. Àbíkú - Em país yoruba, se uma mulher dá à luz uma série de crianças natimortos ou mortas em baixa idade, a tradição reza que não se trata da vinda ao mundo de várias crianças diferentes, mas de diversas aparições do mesmo ser (para eles, maléfico) chamado àbíkú (nascer-morrer) que se julga vir ao mundo por um breve momento para voltar ao país dos mortos, órun (o céu), várias vezes.

2. Lilith - Segundo o Zohar (comentário rabínico dos textos sagrados), Eva não é a primeira mulher de Adão. Quando Deus criou o Adão, ele fê-lo macho e fêmea, depois cortou-o ao meio, chamou a esta nova metade Lilith e deu-a em casamento a Adão. Mas Lilith recusou, não queria ser oferecida a ele, tornar-se desigual, inferior, e fugiu. Deus tomou uma costela de Adão e criou Eva, mulher submissa, dócil, inferior perante o homem. Esse ponto teria sido retirado da Bíblia pela Inquisição.

3. Selenita - se na lua houvesse habitantes, estes seriam os selenitas. Há mesmo quem acredite na existência de tais seres. Os selenitas – em grego Selene significa a deusa Lua – são todos homens: os filhos "brotam" da perna de um adulto. Quando chega a hora de morrer, um selenita idoso simplesmente se dissolve no ar.

"Minha é a vingança e a recompensa,
ao tempo em que resvalar o seu pé;
porque o dia da sua ruína está próximo,
e as coisas que lhes hão de suceder
se apressam a chegar."

Deuteronômio 32.35

Indíce Analítico

Capítulo 1:

Lamer

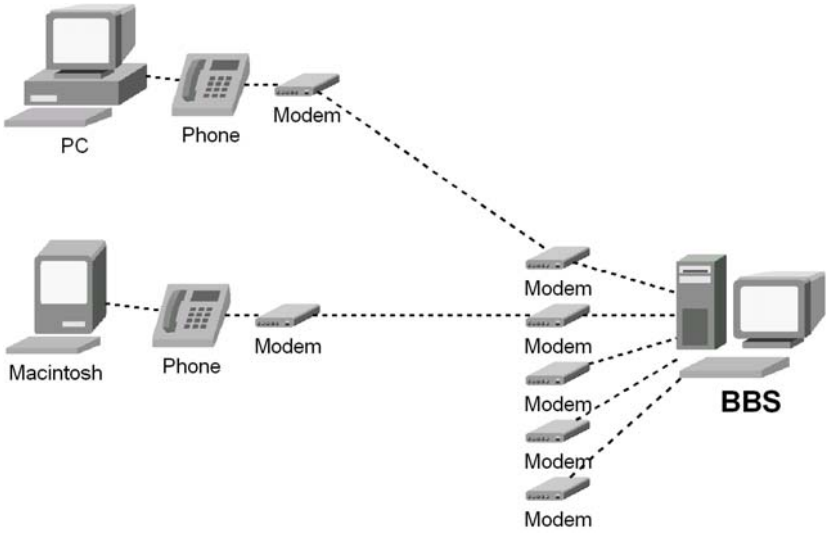
Capítulo 1:

Lamer

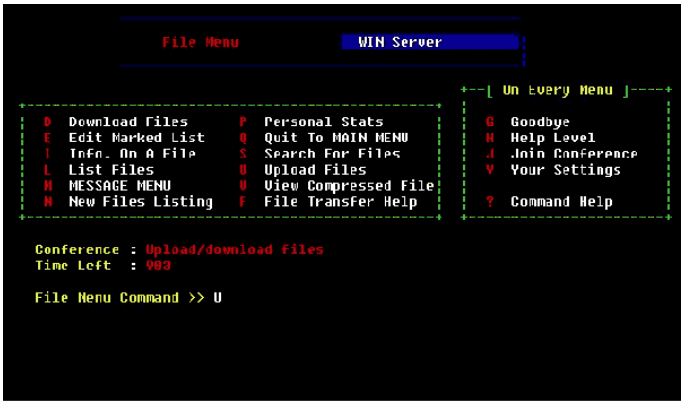
Objetivos Deste Capítulo:
Após concluir a leitura deste capítulo você deverá ser capaz de entender que o hacker tem uma forma de pensar própria. Que o verdadeiro hacker não depende exclusivamente de ferramentas (programas) para desenvolver suas ações. Que houve uma mudança na definição de *hacker* da década de 70 para cá. Que embora a justiça tenha dificuldade de lidar com os crimes de informática, o melhor é usar o conhecimento para ações lícitas e lucrativas. E que o conhecimento sobre hackerismo vai ser cada vez mais respeitado nos anos por vir.

Eu, Hacker

É comum me perguntarem como me tornei um hacker. Na verdade eu era hacker e não sabia. Só quando esta palavra se popularizou é que eu me reconheci como tal e também passei a ser tratado como hacker. Fui tudo muito natural.
Antes da Internet ser aberta ao público no Brasil, nós acessavamos algo parecido, chamado de BBS (*Bulletin Board System*). Antes do BBS ainda tinha o *Projeto Ciranda* que permitia conexões de 300bps a um serviço chamado de Videotexto. BBS é uma base de dados que pode ser acessada via telefone, onde normalmente são disponibilizados arquivos de todos os tipos, softwares de domínio público (freeware e shareware) e conversas on-line (chat). Muitos BBS ofereciam o correio eletrônico interno e também o da Internet. Os BBS são os precursores da Internet. Os computadores se conectavam ao BBS, onde se podia trocar mensagens localmente ou até mesmo conhecer pessoas em chats. Com a Internet, os BBS sumiram. Existem poucos ainda em funcionamento. Se quiser saber mais sobre BBS, visite o site *www.dmine.com/bbscorner/history.htm*.
De forma simplificada, o BBS funcionava assim: alguém disponibilizava um computador com várias linhas telefônicas e vários modens. As pessoas pagavam uma taxa mensal para acessar este computador. Mas o que havia neste computador que interessasse as pessoas? Como já disse, os BBS ofereciam áreas de download, fórum, salas de chat, listas de discussão e E-Mail (na maioria das vezes restrito ao



grupo, ou seja, você só poderia enviar E-Mail para alguém do próprio BBS). Alguns BBS disponibilizavam também serviços de Telnet, jogos on-line, consulta a banco de dados (Detran, companhia telefônica, etc...) e troca de pacotes entre BBS. Com o Telnet nós conseguiamos acessar BBS de outros países e através da troca de pacotes era possível participar de listas de discussão e enviar E-Mails para os BBS associados. Reparem que a área de atuação do BBS era local, até devido aos custos da ligação telefônica. BBS de outro estado ou país, só via Telnet. Se o BBS não possuísse muitos membros cadastrados, os chats e troca de E-Mails ficavam mais limitados do que já eram. Todo o acesso era feito em telas de texto. Às vezes criativamente enfeitadas com ANSI. Muito depois chegaram os BBS baseados em Windows. Mas aí já foi junto com a liberação da Internet no Brasil e os BBS acessados pelo Windows tiveram vida curta.



Outra limitação do BBS era o tempo diário de conexão. O plano de acesso popular permitia apenas UMA HORA DE CONEXÃO DIÁRIA. Planos mais caros permitiam no máximo DUAS HORAS de conexão diária. Não existia, na época, o ACESSO ILIMITADO. Isto só veio depois, como forma de competir com a Internet.

A maioria dos atuais colunistas do *Caderno Internet* do Jornal "O DIA" (Rio de Janeiro) eram frequentadores assíduos do mesmo BBS que eu, o Centroin. Inclusive o Gabriel Torres, que até hoje me deixou na dúvida ter sido ele ou não o autor de uma apostila que ensinava a fazer bombas caseiras. A autoria desta apostila foi atribuída a ele pelo próprio Jornal "O DIA".

Eu fiquei viciado em acessar BBS. Me cadastrei em vários, incluindo dois grandes, o Centroin (*www.centroin.com.br*) e o Digital Highway (*www.digitalhighway.com.br*). Os outros em que me cadastrei eram muito ruins. Meu sonho de consumo era o Mandic. Mas ficava em São Paulo e não dava para bancar o interurbano. Eu não possuía recursos para bancar mais do que isso. Sem falar que as contas de telefone eram altíssimas. A cidade onde moro, Nilópolis (RJ) era muito precária em matéria de telefones. Havia muitos anos que a companhia telefônica não abria novas inscrições. Até 1999 uma linha em Nilópolis custava cerca de 5 mil reais. Meu telefone era alugado a 200 reais por mês e a conta oscilava entre 400 e 600 reais só com ligações locais.

Já possuía alguma experiência com phreaking. Na época do quartel eu fabricava um circuito a base de diodos e resistores para fazer ligação direta de telefone público. Até o sub-comandante do quartel onde servi me pediu um. E o pior é que quando fui chamado pensei que era pra ser preso ou coisa assim. Segue a reprodução do diálogo (de memória):

Sub: _*"Soldado Thompson. Chegou ao meu conhecimento que o senhor possui um apetrecho que faz o telefone público discar sem ficha. Isto é verdade?"*

Eu: (fiz uma pausa, mas achei melhor abrir o jogo) _*"Sim senhor."* (já esperando pelo pior)

Sub: (agora com a voz doce como queijo) _*"Então providencie um para mim. Minha família é do Rio Grande do Sul e eu não quero gastar todo o meu soldo em fichas* (naquela época o telefone usava fichas e também era comum os gaúchos servirem na Brigada Pará-quedista, aqui no Rio de Janeiro).*"*

Eu: _*"Então fique com o meu..."*

Deste dia em diante as coisas foram muito boas para mim no quartel. Engajei, pedi baixa antes do tempo para ir para a polícia, me livrei da campanha da dengue para fazer o curso de cabo, mudei de Cia. quando a que eu estava mudou de comandante para um boçal. Como me ajudou aquele simples diodo.

Mas voltando ao BBS, eu estava com um grande problema: não aguentava ficar APENAS UMA HORA POR DIA conectado. Todos os dias, à meia-noite, lá estava eu aguardando minha conta ser zerada para poder acessar... por apenas mais uma hora. E depois ter que aguardar de novo até a meia-noite do dia seguinte.

Pensando Hacker

No BBS as pessoas deixavam uma ficha completa preenchida. Nome, apelido, o que gostava ou não de fazer, data de nascimento, endereço, telefone e tudo o mais. O nome de usuário era fácil de ser obtido. Podia ser pela ficha, listagem de nomes de usuários (havia esta opção no MENU do BBS) ou na sala de chat. Então pensei: _*"Será que vou ter problemas se tentar entrar como se fosse outro usuário?"* - E em seguida comecei a fazer uma tabela com os dados de cada usuário. Minha senha era a minha data de nascimento. Pensei que outras pessoas também tivessem a mesma idéia de senha (e tratei logo de mudar a minha). Não deu outra. De cada cinco tentativas, em uma eu conseguia usar a conta do outro usuário. Logo na primeira semana já havia conseguido mais quatorze horas de acesso. Um absurdo se comparado as sete horas a que tinha direito.

Como todo vício fui querendo mais do que o meu BBS podia oferecer. Passei a usar a mesma técnica em outros BBS e passei também a usar Telnet para conectar aos BBS americanos, que possuiam mais recursos e mais softwares para download. Meu modem de 9.600bps gemia feito um louco de tanto que era exigido naqueles dias (os modems atuais são de 56.000bps e uma conexão de banda larga das mais furrecas é de 128.000bps).

Minha fonte de renda vinha de um curso de informática que eu mantinha no centro de Nilópolis(RJ). Durante o dia eu dava aulas e administrava o curso e a partir da meia noite, hackeava contas de BBS para ter mais que UMA HORA de acesso por dia. Não tinha a menor idéia do que era HACKER ou PHREAKER e nem buscava este tipo de informação (nem sei se existia ou se existia com este nome).

Como o melhor do feito é que as pessoas saibam do fato, comecei a contar vantagens quanto a conseguir acessar por mais de uma hora, usando contas de outros usuários. Enquanto eu me gabava de ter conseguido 'até' seis horas em um único dia, fui avisado, não tão gentilmente, que o bom mesmo era conseguir uma conta de *Sysop* (corresponde ao *root* hoje em dia) e ter acesso irrestrito durante as 24 horas por dia. Inclusive podendo remover ou adicionar usuários.

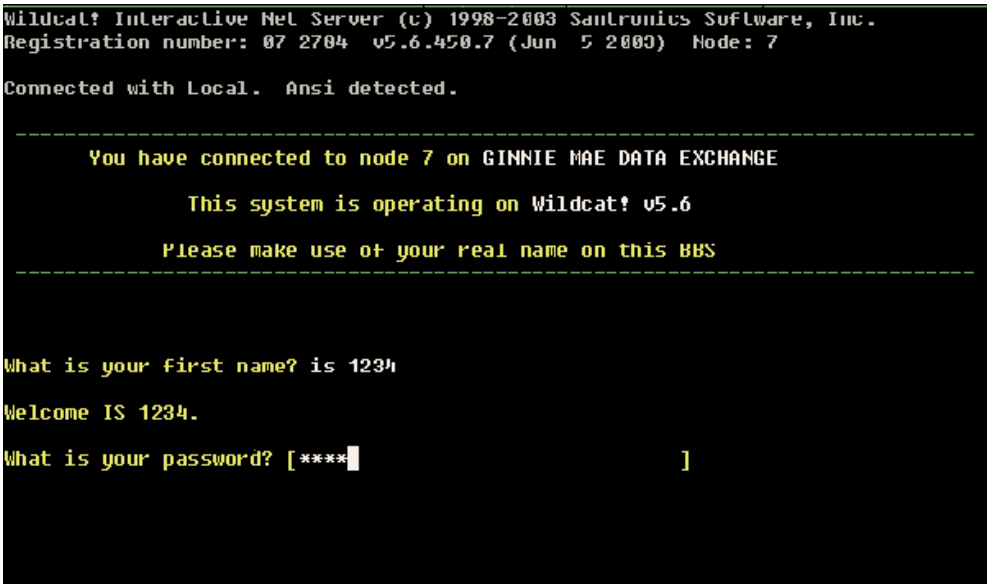
A primeira pergunta que veio a mente foi *"Como? Será possível? Mas... como?"*. Partindo de algumas pistas (ninguém entregava o ouro), descobri que o segredo era instalar na própria máquina o mesmo programa que o BBS usava para gerenciar o sistema. Estudando e analisando o programa eu descobriria falhas que me permi-

tiriam o acesso irrestrito, como *Sysop* (operador do sistema). E estas falhas eram divulgadas entre os grupos (clãs), mas eu não tinha a menor idéia do que se tratava. Não até aquele momento.
Com muito custo, consegui uma cópia funcional do programa PCBoard e em menos de uma semana já sabia administrá-lo. Entrei em listas de discussão de sysops e obtive muita ajuda por parte deles. Tive até que criar um nome fictício de BBS, dando a entender que estava para abrir um em breve. Foi uma das primeiras experiências com engenharia social. Ninguém desconfiava que eu estava para invadir os BBS em busca das contas com status de sysop. E na própria lista de discussão eles falavam sobre as brechas e ensinavam a correção. Mas... e os sysops que não frequentavam as listas de discussão ou não corrigiam o problema? Estavam todos vulneráveis.
Marquei para um sábado minha primeira tentativa de invasão. Já sabia como fazer desde quinta-feira, mas tinha que ser algo especial. A taquicardia se manifestava toda vez que eu pensava no assunto.

Minha Primeira Invasão

O que eu tinha que fazer era o seguinte: me conectar a um BBS que oferecia o serviço de Telnet. A partir daí eu deveria me conectar por Telnet ao BBS que estivesse usando o programa de administração que possuía a vulnerabilidade. Acessar por determinada porta, e executar alguns comandos UNIX. Daí era só baixar a lista de usuários, incluindo o(s) sysop(s). A lista de usuários poderia estar criptografada, mas seria uma situação atípica, pois naquela época não havia esta preocupação por parte da maioria dos sysops. Talvez não houvesse nem conhecimento para isso. Era uma época em que o que havia de melhor em matéria de PC era um 486. O primeiro 486 comprado para o curso custou dois mil e quinhentos dólares e veio por contrabando. Existia uma Lei de reserva de mercado que impedia a entrada de computadores domésticos no Brasil. O presidente Collor serviu ao Brasil de uma forma inusitada: devemos a ele o fim da reserva de mercado (que permitiu a entrada no país de computadores, carros e outros produtos importados) e o maior controle das ações presidenciais. Deus escreve certo por linhas tortas.
Feito. Estava eu com a lista de usuários do meu primeiro ALVO. Mudei a extensão e abri no meu editor de textos preferido, o Carta Certa na versão 3.3 que cabia em um disquete de 5 1/4" com 360k e trazia um corretor ortográfico de quebra (veja minha homenagem a este programa na página 83 do livro *Proteção e Segurança na Internet*). A lista baixada trazia o nome do usuário, a senha, qualificação e muitas outras informações sobre cada usuário, além da identificação de quem era operador (sysop) ou não. Escolhi aleatóriamente um dos operadores e comecei a conexão. Linha ocupada. Mais uma tentativa e... linha ocupada. Na terceira tentativa, de-

pois do modem implorar pelo meu perdão e gemer mais do que o normal, consegui visualizar a tela de "Boas Vindas" do meu ALVO. Entrei com *User*. Entrei com *Pass* e... pronto. Eu era o *Sysop*.



Eu, Sysop

A sensação é indescritível. Acredito que foi aí que eu me contaminei de vez com o vírus do conhecimento. Nunca foi tão claro para mim como naquele dia a expressão 'a verdade te libertará'. Comemorei com vinho *Sangue de Boi* bem gelado e castanha de caju. Hoje não sei como consegui beber aquela mistura que chamam de vinho. Mas naquele dia eu era Rei. Eu era o *Sysop* de um sistema invadido. Até se a comemoração fosse com água *Perrier* e torradas francesas levemente adocicadas, teria ficado na história. Pelo menos na minha história.

Tratei logo de criar uma outra conta com status de *sysop* e mais duas contas de usuário comum. Desconectei. Aguardei umas duas horas e voltei usando a nova conta. Uma inquietação tomou conta de mim daquele momento em diante. Algo como: *"O que mais posso fazer? Até onde posso ir? Existem outras formas de se fazer isto? É proibido? Corro algum risco?"* - Sim. Existiam outras formas que eu fui conhecendo aos poucos. Em uma delas era só se conectar ao BBS e quando fosse exibida a tela de *Boas Vindas*, bastava entrar com alguns comandos para conectar como usuário 'fantasma' ou roubar a sessão de alguém on-line. Outras formas incluiam o uso do Telnet. Era até melhor usar o Telnet pois em uma conexão direta você poderia ser detectado por algum BBS com BINA (uma raridade na época).

Tudo ia bem. Eu conectado até dez horas por dia (das 22 horas, quando termina-

vam as aulas, até às três horas da manhã, além de umas picotadas durante o dia). Tudo ia bem. Eu já estava craque em invadir BBS e obter contas de usuários, incluindo operadores do sistema. Já não achava difícil. Fazia isto com muita naturalidade. A palavra *hacker* ainda não fazia parte do meu mundo. A necessidade me levou a fazer o que fiz. A curiosidade me mantem fazendo o que faço.

Tudo ia bem: chat, telnet, download, E-Mail, listas de discussão, fórum, era a minha rotina diária. Só usava a invasão para ter acesso ao que eu queria poder pagar para ter acesso. Tudo ia bem, até chegar a conta do telefone... no valor de 850 reais.

Eu, Phreaker

Foi aí que eu dei conta de que havia relaxado com a empresa. Quase não esquentava mais a cabeça com o número de alunos ou com o marketing do curso. Estava mal das pernas financeiramente e, pior ainda, com uma conta de telefone daquelas. E de telefone alugado ainda por cima. Com o susto, tentei me controlar e limitar meu acesso a no máximo duas horas por dia. Mas depois que você consegue usar o tempo que quiser, não se contenta com menos. É como sair com a Viviane Araújo e depois ter que ficar com uma mulher 'genérica'.

Estava eu atormentado com a possibilidade de ficar até sem o telefone, pois não suportaria outra conta daquele quilate, quando fui visitado por uma amiga que havia comprado um aparelho telefônico e queria testá-lo na minha linha. Disse que não haver problemas. Sai um pouco da sala e voltei quando o meu telefone tocou. Atendi a ligação e percebi que ela também estava falando no aparelho que havia comprado. Pensei que ela estava de brincadeira (muito boba por sinal) ao fingir que falava em um telefone sem linha. Terminei minha ligação. Em seguida ela 'terminou' a dela e eu perguntei:

Eu: _*"Você não vai testar seu aparelho? É só tirar o meu da tomada."*

Ela: _*"Já testei. Esta tomada está funcionando."*

Eu: _*"Para de brincadeira. Esta tomada é do pessoal da sala ao lado. Eles também alugavam esta sala. Agora estão só com uma. Não acredito que ele tenha deixado a extensão ligada..."*

Mas deixou. A extensão estava ligada e funcionando. Não sosseguei enquanto o relógio não bateu sete da noite, hora em que eles iam embora, para que eu pudesse conferir minha tábua da salvação. Passei a usar um pouco a minha linha. Um pouco a dele. Até que chegaram nossas contas. Da minha sala dava pra ouvir o gerente reclamar com os funcionários por estarem abusando do telefone. Dei uma maneirada e comecei a procurar outras alternativas.

Um dos cursos que eu ministrava era o de instalação de antenas parabólicas.

Possuía o maior curso de instalação de antenas parabólicas do Brasil, principalmente depois que a fábrica Almo Gama em Nova Iguaçu(RJ), que também dava o curso, parou de ministrá-lo depois de uma situação prá lá de suspeita, envolvendo troca de tiros entre os Almo Gama e a polícia civil. O incidente resultou na morte de um policial, na internação do Almo Gama, que também foi baleado, e os alunos dele vieram quase todos fazer o curso comigo.
Durante a instalação de uma antena parabólica para servir ao curso, constatei que os fios de telefone de todo o prédio passavam por dentro do forro. Era um prédio velho que só agora em 2003 ganhou reforma e laje. A noite, com uma pequena lanterna, comecei a fazer a sangria de várias linhas para ir revezando e não onerar a conta de ninguém.

Deu no Jornal: *"Grampo no Telefone do Político"*

No mesmo prédio havia um político tradicional. Ex-*um-cargo-qualquer* e pessoa bastante influente. Um certo dia, ao chegar para mais um dia de trabalho, notei que se encontrava no prédio alguns funcionários da Telerj (atual Telemar) falando com o político: _*"Seu telefone está com indícios de grampo. Parece que a pessoa não sabia qual das linhas era a sua e grampeou várias no prédio todo."* Foi um bafafá danado. Saiu até no jornal. Todo mundo tratou de proteger suas linhas, fazendo a instalação embutida na parede. Eu mesmo, assim que 'soube', tratei de ver se a minha linha também não estava 'grampeada' (ou se eu não havia esquecido nenhum pedaço de fio apontando para a minha sala). De uma só vez perdi todas as minhas linhas alternativas, pois até a extensão esquecida na minha sala foi desligada.

E Chegou a Internet

A fase do deslumbramento já havia passado. Também já estava melhor financeiramente. Juntando a menor necessidade de permanecer conectado e o aumento dos meus rendimentos, não procurei mais linhas 'alternativas' para conectar-me a BBS. Foi quando o jornal "O Globo" do Rio de Janeiro, trouxe uma reportagem de página inteira no Caderno de Informática falando sobre umas contas de acesso a Internet que a Embratel iria liberar. Pouca gente tinha idéia exata do que era a Internet. Eu não dei muita importância, até começarem os comentários no BBS de que a Internet é que era a boa. E não eram só comentários. As pessoas estavam sumindo do BBS e indo para a tal da *Internet*. No chat: _*"Cadê fulaninho?"* _*"Está na Internet."*
Eu não havia conseguido (e nem tentado) obter uma das contas de acesso à Internet oferecidas pela Embratel (1995), pensei em usar a mesma técnica de experimentar nome e senha. Foi um pouco mais difícil pois eu não tinha acesso a lista de usuários. O que fiz foi usar nomes comuns e repetir o nome como senha. Depois de umas 40 tentativas, consegui o acesso. Para o acesso era necessário baixar um kit com

programas: browser (Mosaic, o Internet Explorer simplesmente não existia), FTP, Telnet, Gopher e E-Mail, além de alguns arquivos necessários ao Windows 3.11 (ui!) para a conexão com a Internet.
Não achei muita graça naquelas páginas com fundo cinza e em sua maioria em inglês. Mas o pessoal do BBS estava em polvorosa. Por falar nisso, os BBS também passaram a incluir a opção de acesso a Internet. As mesmas limitações de UMA ou DUAS horas por dia. Daí em diante ficou fácil: invadia o BBS e usava uma conta com acesso a Internet. Geralmente a do próprio sysop. Os BBS começaram a tomar dois rumos: ou viravam PROVEDORES DE ACESSO A INTERNET ou deixavam de existir. Com a chegada da Internet ninguém queria mais saber das limitações dos BBS. Limitações de interface, de serviços e de tempo de conexão.

Eu, Defacer

Com o tempo fui encontrando coisas interessantes para fazer na Internet. Nada se igualou aos primeiros tempos de BBS. Mas a Internet cresceu muito rápido e pouco tempo depois resolvi criar uma página pessoal na Geocities, que atualmente pertence ao grupo Yahoo! (*www.yahoo.com*).
Não sei como aconteceu, mas a minha senha na Geocities não entrava. Na mesma página que negou o acesso havia instruções de como pedir uma nova senha. Bastava enviaer um E-Mail. Fiz o pedido em em menos de 24 horas recebi uma nova senha. Foi aí que me passou pela cabeça: _*"Será que se eu pedir a senha de outro endereço eles mandam também?"* E mandaram. Não sabia o que fazer com a senha de acesso ao site dos outros. Daí, meio por acaso, entrei para o mundo dos *defacers* (hackers que fazem alteração na página principal de um site). Criava uma página com o texto: ***Estive aqui e lembrei de você*** e fazia o upload para a Geocities. Com o tempo isto também foi perdendo a graça.

Eu, Cracker

Devido a novas limitações, agora de tempo, para dar conta de tantos alunos, passei a usar nos cursos de informática o método americano CBT (*Computer Based Training*) e depois desenvolvi o meu próprio TBT (*Tasks Based Training*). Cada CBT custava cerca de cem reais. A moeda nem era o real. Como eu precisava de um CBT por computador e um CBT por curso que ministrava (Introdução a Microinformática, MS-DOS, Wordstar, Lotus 1-2-3 e dBase), não dava para adquirir tudo. Era imposto daqui, funcionário ladrão dali, baixa temporada acolá e dinheiro pra investir não sobrava.
Eu precisava descobrir um jeito de instalar aqueles programas em mais de um computador. Naquele época eu não sabia usar programas de cópia e edição de setores. Mas a solução que encontrei foi bem simples. Como após instalado o

programa não permitia uma nova instalação e nem permitia ser instalado com o disquete de 360k, $5^{1/4}$" protegido contra gravação, verifiquei as datas dos arquivos no disquete, instalei e voltei a verificar as datas dos arquivos no disquete. Apenas um arquivo estava com a data alterada.
Desinstalei. Copiei aquele arquivo com a data alterada para o disco rígido. Instalei novamente. Copiei o arquivo que estava no disco rígido para o disquete de instalação e pronto. O programa já podia ser instalado em qualquer micro, quantas vezes eu quisesse. Fiz até um arquivo de lote (.BAT) que automatizava a tarefa de copiar o arquivo de proteção para dentro do disco rígido e trazê-lo de volta para dentro do disquete.
...
Infelizmente eu não posso contar aqui tudo o que aconteceu daí por diante. Nem é este livro uma autobiografia. Já estou correndo riscos ao assumir estes atos e por publicar este livro. Seria uma confissão de culpa que poderia me levar facilmente aos tribunais. Só me permiti fazê-lo para que você entenda que ser hacker é um modo de pensar, que leva a um modo de agir. Não depende só de conhecimento, mas de raciocinar de certa maneira. Mas continue a leitura e verá não o que eu fiz, e sim o que você poderá fazer. Só não esqueça de que com o poder vem a responsabilidade. Nem tudo o que PODE ser feito DEVE ser feito.

Pequena História da Internet

A Internet nasceu em 1969, nos Estados Unidos. Interligava originalmente laboratórios de pesquisa e se chamava ARPAnet (ARPA - *Advanced Research Projects Agency*). Era uma rede do Departamento de Defesa Norte-Americano. Era o auge da Guerra Fria, e os cientistas queriam uma rede que continuasse funcionando em caso de um bombardeio. Surgiu então o conceito central da Internet: "Uma rede em que todos os pontos se equivalem e não há um comando central". Assim, se B deixa de funcionar, A e C continuam a poder se comunicar.

O nome Internet propriamente dito surgiu bem mais tarde, quando a tecnologia da ARPAnet passou a ser usada para conectar universidades e laboratórios, primeiro nos Estados Unidos e depois em outros países. Por isso, não há um único centro que "governa" a Internet. Hoje ela é um conjunto de mais de 40 mil redes no mundo inteiro. O que essas redes têm em comum é o protocolo TCP/IP (*Transmission Control Protocol/Internet Protocol*), que permite que elas se comuniquem umas com as outras. Esse protocolo é a língua comum dos computadores que integram a Internet.

Então, a Internet pode ser definida como:

- uma rede de redes baseadas no protocolo TCP/IP;
- uma comunidade de pessoas que usam e desenvolvem essa rede;
- uma coleção de recursos que podem ser alcançados através desta rede.

Durante cerca de duas décadas a Internet ficou restrita ao ambiente acadêmico e científico. Em 1987 pela primeira vez foi liberado seu uso comercial nos Estados Unidos. Mas foi em 1992 que a rede virou moda. Começaram a aparecer nos Estados Unidos várias empresas provedoras de acesso à Internet. Centenas de milhares de pessoas começaram a colocar informações na Internet, que se tornou uma mania mundial.

A Internet no Brasil

A Rede Nacional de Pesquisas (RNP) foi criada em julho de 1990, como um projeto do Ministério da Educação, para gerenciar a rede acadêmica brasileira, até então dispersa em iniciativas isoladas. Em 1992, foi instalada a primeira espinha dorsal (back bone) conectada à Internet nas principais universidades e centros de pesquisa do país, além de algumas organizações não-governamentais, como o Ibase.

Em 1995 foi liberado o uso comercial da Internet no Brasil. Os primeiros provedores de acesso comerciais logo surgiram. O Ministério das Comunicações e o Ministério da Ciência e Tecnologia criaram um Comitê Gestor Internet, com nove representantes, para acompanhar a expansão da rede no Brasil.

Adaptado do Texto de Maria Ercília "O que é a Internet"

A Vítima

Eu estava na padaria. Eu e mais quinze pessoas. Todos esperando a primeira fornada de pão. Tem padaria que merece este sacrifício. Não sei se é só a receita da massa ou se é o padeiro que dá vida e sabor a receita. Mas aqui o pão é muito gostoso e vem gente de longe comprar. Mesmo tendo padaria perto das suas casas.

A fila da padaria é uma das mais democráticas. Não sei se você também já percebeu. Onde mais vamos encontrar um juiz esperando a vez na fila depois de uma empregada doméstica? Nesta que eu estava por exemplo, a primeira da fila era uma faxineira que trabalha como diarista. Depois dela tinha um médico, um pedreiro, um juiz, um advogado, um aposentado, uma doméstica, uma senhora de idade como cara de 'madame', um policial militar e eu. Quase o último da fila. E o pior era ter que aturar um pastor que estava pouco depois de mim. A todo

custo ele queria converter um pai-de-santo que estava logo a sua frente. Por mais que tentasse, não dava para ficar alheio a peleja dos dois. Cada qual defendendo a sua fé. De repente um grito. Mas não era de gente não. Era de um pneu chorando alto no asfalto. Em seguida uma batida surda. Parecia bate-estacas de obra em tarde de ócio. Mas não era. Era um carro que atravessou o sinal e foi pego por um outro que bateu em sua lateral. Ainda estavamos todos paralisados pelo susto. Foi quando ouvimos o grito. Agora sim de gente. Era uma mulher que ficou presa entre as ferragens do carro atingido. Como se ensaiados, todos deixamos a fila da padaria ao mesmo tempo e corremos para o local do acidente. A verdade é que estavamos diante do local do acidente. Apenas uma banca de jornais impedia nossa visão do cruzamento onde os carros estavam batidos. No grupo que se formou ao redor do acidente, cada um assumiu uma posição diante da cena. (...) Agora é com você:

Qual foi o pensamento e o comportamento do policial militar?
R:

Qual foi o pensamento e o comportamento do pastor?
R:

Qual foi o pensamento e o comportamento do médico?
R:

Qual foi o pensamento e o comportamento do pai-de-santo?
R:

Qual foi o pensamento e o comportamento do juiz?
R:

Qual foi o pensamento e o comportamento do advogado?
R:

Qual foi o pensamento e o comportamento do hacker?
R:

Você já parou pra pensar o que é o SER? O SER existe a partir do PENSAR. O PENSAMENTO gera SENTIMENTO que gera COMPORTAMENTO. Penso como POLICIAL, sinto como um POLICIAL, vou agir como um POLICIAL. Só que neste caso, para ser polícia é preciso uma autorização dada por órgão

público. Ninguém é policial por conta própria. A não ser a lendária polícia mineira. Mas aí já é outra história.
Outro exemplo do SER: para SER uma FAXINEIRA só é preciso PENSAR como tal e FAZER o que uma faxineira faz. Não precisa da autorização de ninguém. Mas é preciso demonstrar competência na função, caso contrário não será aceita como faxineira.
Da mesma forma o hacker. Qualquer um pode se tornar HACKER. Basta PENSAR e AGIR como um HACKER. Não precisa de autorização de ninguém. Mas da mesma forma que a faxineira, para ser aceito como HACKER, você vai precisar PROVAR que é capaz de executar as tarefas que se espera de um HACKER: você vair precisar AGIR como um HACKER. O PENSAR vem antes do SER.
Existem algumas formas do SER em que a situação é mais complexa. Alguém que tenha dirigido um carro uma única vez, pode ser considerado motorista? Um adolescente que dirija desde os seus doze anos de idade e até de 'pegas' já tenha participado, é um motorista? Mesmo sem ter a carteira de motorista? E um adulto que comprou a carteira e dirige a mais de dez anos? É um motorista?
E mais duas para você pensar na cama: Alguém que tenha experimentado algum tipo de droga ilícita uma única vez na vida, pode ser considerado usuário? E um homem ou mulher que tenha experimentado a cópula com pessoa do mesmo sexo apenas uma vez na vida. Pode ser considerado homossexual?
Também vamos encontrar situações deste tipo no mundo HACKER. Alguém que invada e piche o site da Microsoft por exemplo, poderá até ser considerado hacker pela maioria das pessoas que tomarem conhecimento do fato. Mas se esta pessoa não possuir um histórico de ações hacker, não será aceita como hacker pela elite.
Aí temos um dilema. Suponha que o hacker em questão apareça na imprensa mundial como o 'hacker que invadiu o site da Microsoft'. Não importa se a 'elite' não o considere. A mídia o 'fez' hacker e até que esta pessoa não queira, já estará sendo lembrada e tratada como hacker. E quanto mais negar pior.
Então as formas de ser aceito como HACKER podem ser resumidas em: ou você apresenta o resultado das suas ações ou você é 'apresentando' como hacker. E quando eu falo de 'ações' não estou me referindo a meia dúzia de invasões de E-Mail e distribuição de trojans. As ações precisam ser ações respeitáveis. Coisas difíceis como invadir o site da Receita Federal, criar um vírus de fama mundial, tirar os servidores da Fapesp do ar, pichar o site da Casa Branca (sede do Governo Americano), etc...

Na verdade não são apenas duas as maneiras de ser reconhecido como hacker. Se você criar algo novo e revolucionário, como o fez Linus Torvalds ao criar o Linux,

você será respeitado e tido como o 'verdadeiro hacker'. Embora passe o resto da vida negando isto.

Manifesto Hacker

O Manifesto Hacker circula na Internet e foi supostamente publicado em 1986 por um hacker que atendia pelo apelido (nick) de *Mentor* ou *The Mentor*. Esse hacker, muito famoso na década de 80, foi preso época por invadir o sistema de um banco. Depois disso, ninguém mais teve notícias dele, pelo menos não com esse nick... E ninguém nunca soube o seu nome verdadeiro. Na época da prisão, Mentor era menor de idade...

Não há como saber ao certo até que ponto esta história é verdadeira e se esse Mentor existiu mesmo. Mas já dá para se ter uma idéia de nosso atraso tecnológico. Enquanto a Internet e os hackers já existiam antes de 1986 nos EUA, no Brasil a Internet só chega DEZ anos depois. É muito tempo. Em todo caso, lenda ou verdade, fiquem agora com as últimas palavras de Mentor:

"Mais um foi pego hoje, está em todos os jornais: "ADOLESCENTE PRESO EM ESCÂNDALO DO CRIME DE COMPUTADOR!", "HACKER PRESO APÓS FRAUDE EM BANCO!". Moleques danados! Eles são todos iguais!

Mas você, com sua psicologia e sua mente tecnológica dos anos 50, alguma vez olhou atrás dos olhos de um hacker? Você já imaginou o que o impulsiona, que forças o moldaram, o que o tornou assim? Eu sou um Hacker, entre no meu mundo...

Meu mundo começa na escola... Eu sou mais esperto que os outros, esta besteira que nos ensinam me aborrece... Droga de fracassados! Eles são todos iguais! Eu estou no ginásio. Eu ouvi os professores explicarem pela qüinquagésima vez como reduzir uma fração. Eu entendo como. "Não, Sra. Smith, eu não colei meu trabalho. Eu o fiz de cabeça...". Moleque danado! Provavelmente ele colou! Eles são todos iguais! Eu fiz uma descoberta hoje. Eu encontrei um computador. Espere um pouco, isso é demais! Ele faz o que eu quero que faça. Se ele comete um erro é porque eu errei. Não porque ele não goste de mim... Ou se sinta ameaçado por mim... Ou pense que eu sou um CDF... Ou não gosta de ensinar e pensa que não deveria estar aqui... Moleque danado! Tudo o que ele faz é jogar jogos! Eles são todos iguais! E então acontece... uma porta se abre para um outro mundo... fluindo pela linha telefônica como heroína nas veias de um viciado... um comando é enviado... uma fuga da incompetência do dia-a-dia é procurada... um BBS é encontrado. "É isso aí... é de onde eu venho! Estou onde gosto! Conheço todo mundo aqui... mesmo que eu nunca tenha conversado com eles e até mesmo nunca os tenha visto... Eu conheço todos vocês!". Moleque danado! Usando a linha telefônica de novo! Eles são todos iguais! Pode apostar que somos todos iguais... Nós fomos alimentados com comida de bebê na escola quando queríamos bifes... Os pedaços de carne que você deixou escapar estavam pré-mastigados e sem gosto. Nós fomos

dominados por sádicos ou ignorados por apáticos. Os poucos que tiveram algo a nos ensinar quando éramos crianças, acharam-nos dispostos a tudo, mas eram poucos, como "gotas d'água no deserto". Este é o nosso mundo agora... O mundo de elétrons e de botões, da beleza da transmissão. Nós fazemos uso de um serviço já existente sem pagar por ele (que seria bem barato, se não fosse manipulado por gananciosos atrás de lucros) e vocês nos chamam de criminosos. Nós exploramos... e vocês nos chamam de criminosos. Nós procuramos por conhecimento... e vocês nos chamam de criminosos. Nós existimos sem cor de pele, sem nacionalidade, sem religião... e vocês nos chamam de criminosos. Vocês constroem bombas atômicas, vocês fazem guerras, matam, trapaceiam, mentem para nós e tentam nos fazer crer que é para o nosso próprio bem... mesmo assim, nós somos os criminosos. Sim, eu sou um criminoso. Meu crime é o da curiosidade. Meu crime é o de julgar as pessoas pelo que elas dizem e pensam, não pelo que elas parecem. Meu crime é o de desafiar vocês, algo que vocês nunca me perdoarão. Eu sou um hacker e esse é o meu manifesto. Vocês podem parar esse indivíduo, mas não podem parar todos nós, afinal... somos todos iguais."

Os 21 Mandamentos do Hacker

Sem data definida, encontramos também outro texto lendário da Internet, os 21 Mandamentos do Hacker. Percebe-se tanto nesse texto como no anterior o espirito adolescente e traços da ingenuidade da segunda geração de hackers americanos:

1- Descobriu algo novo, olhe!
2- Não apague nada! É melhor ter acesso a um provedor do que destruí-lo.
3- Não modifique nada, ao menos que queira ser descoberto.
4- Nunca tente um su root direto. Isso fica logado!
5- Não fique dando telnet, pegando e-mail ou utilizando o acesso dos outros.
6- Nunca subestime um sysop.
7- Para atacar, escolha um horário entre 00:30 e 06:00.
8- Uma vez dentro, tente dominar o lugar. É claro: com muita cautela!
9- Não confie em ninguém.
10- Se pegar a senha do root de algum provedor e não souber o que fazer, mate-se!
11- Não teste vírus no seu próprio HD.
12- Tenha uma estratégia pronta antes de atacar.
13- Se possível, use os computadores de sua universidade. É mais seguro!
14- Não distribua, para ninguém, informações ou dados sobre o que você pegou.
15- Não obedeça a regras (claro que essas devem ser cumpridas...).
16- Não tenha pena de ninguém.
17- Você usa MS-DOS ou o Windows? Não conte a ninguém...
18- Você usa UNIX ou LINUX? Certifique-se de que está bem seguro...
19- Não crie laços afetivos com a vítima.
20- Aprenda o máximo que puder com quem sabe mais!

21- Você deve sempre aprimorar sua técnica. Lembre-se: "Os hackers são as pessoas mais inteligentes e estudiosas do planeta".

Hierarquia Hacker

A famosa 'hierarquia hacker' é pouco praticada no Brasil. Não temos 'grupos organizados' ou 'clãs' hacker tão atuantes como os que existem e exitiram nos EUA. Mesmo o *Legiao*, grupo de pesquisa criado e mantido por mim, possui entre os seus membros aqueles que se dedicam a pichar sites nas horas vagas. Como não podem usar o nome *Legiao* nestas babaquices, inventam o nome de algum grupo. Ás vezes pedem até a minha sugestão. Como eu já disse antes neste mesmo capítulo, a Internet pública no Brasil não tem nem oito anos. Ao contrário dos EUA, cuja Internet pública vai completar dezenove anos no ano que vem. O que temos de clãs são os que se reunem para jogos estilo RPG e Counter Strike. Também temos aqueles que alegam pertencer a determinado grupo (grupo de um homem só). O Brasil está entre os primeiros lugares no ranking do hacking mundial, mas não significa que possua esta quantidade absurda de grupos ou de hackers. São muitas as ações, mas partindo de grupos reduzidos e até mesmo uma pessoa em nome de um grupo imaginário. A (má) fama do Brasil é mais por conta de pichações de sites e não de invasões espetaculares ou criação de vírus e ferramentas de segurança.

Entre os 'grupos' com conhecimentos hacker, já identifiquei os seguintes:

- profissionais de rede em busca de conhecimentos hacker para a própria defesa ou de seus clientes e valorização do currículo;
- pessoas querendo abrir contas de E-Mail para ver se pegam alguma traição do companheiro;
- adolescentes que se exibem em salas de chat e canais do IRC;
- professores de informática e proffisonais de informática farejando um novo filão: o curso de segurança ou anti-hacker.Fora estes, identifiquei um grupo que está se tornando cada vez mais atuante. São quadrilhas em busca de hackers ou conhecimentos hacker para a prática de crimes de informática. Algumas já foram pegas, mas existem outras em ação. É um crime limpo, sem qualquer risco de confronto policial durante sua execução e, se bem executado, indetectável. A tendência é que este tipo de 'grupo' cresça bastante nos próximos anos.

Eu mesmo recebi convites prá lá de suspeitos durante o ano de 2002 e 2003. Se você também ficar em evidência, como foi o meu caso, talvez receba convites deste tipo. Só espero que resista à tentação do dinheiro fácil e use sua inteligência para atividades honestas e produtivas. Se você se acha inteligente, use esta inteligência para coisas boas, incluindo ganhar dinheiro. Você não precisa ser um hacker do crime. O mundo vai valorizar o hacker ético. E pagará muito bem por este serviço.

Não há organização no hackerismo brasileiro. Algumas revistas especializadas no assunto teimam em tentar fazer-nos acreditar que estes grupos altamente organizados existem, se comunicam por código do tipo usado para escrever a palavra *h4ck3r*, e estão neste exato momento planejando seu próximo ataque. Devaneio puro. O grupo que realmente deve estar planejando o próximo ataque é o de criminosos que estão usando técnicas hacker para aplicar golpes na Internet.
Nosso Brasil não é um país de ideologia e ideologismos. A reforma na educação cuidou disso muito bem.
Queremos mudar um pouco este cenário. Temos em nossos planos a realização de vários encontros hacker pelo Brasil, a realização da DEFCON nacional e a vinda do Kevin Mitnick para algum evento. Quase o trouxemos agora em abril de 2004. Infelizmente os 60 mil reais que ele cobra para ficar duas horas em um evento ainda é mais do que podemos dispor.

Nomeclatura Hacker

Embora a palavra hacker da forma que é usada atualmente, tenha sentido diferente do original, não há como negar que a imprensa é a culpada por ter enfiado lamer, wannabe, hacker, cracker, phreaker, warez, aracker, newbie, defacer, carder, hacker tudo no mesmo saco. A palavra hacker, da forma que é usada atualmente, engloba QUALQUER AÇÃO HACKER. Só a imprensa especializada é que tenta, em vão, separar o joio do trigo, diferenciando entre hacker e cracker. Mas mesmo a imprensa especializada e até escritores de livros hacker e sites, insistem na besteira de dizer que dá prá dividir o hacker em lamer, wannabe, aracker e outras baboseiras do tipo. Na prática a situação é esta:
IMPRENSA ESPECIALIZADA - *hacker* (o bom) / *cracker* (o mau)
IMPRENSA EM GERAL - *hacker* e *pirata de computador* (para qualquer ação hacker)
EMPRESAS E PROFISSIONAIS DE SEGURANÇA - *hacker* / *hacker ético* / *black hat* (o mau) / *white hat* (o bom) (estes termos são os mais usados atualmente nos EUA)
Outras definições de 'hacker' incluem:
Script Kiddie - adolescentes e nem tão adolescentes que por preguiça ou incompetência, se utilizam de programas prontos e 'receitas de bolo' para realizar ações hacker.
Hacker Ético / Ethic Hacker - está surgindo um movimento com a finalidade de formar 'hackers do bem' ou 'hackers éticos'. Isto também está ocorrendo nos EUA com o desejo do governo americano de que os hackers de lá sejam 'white hats' e usem seus conhecimentos para ajudar a indústria local. Como toda onda - está é apenas mais uma e vai passar, acreditem; já surgem as empresas interessa-

das em explorar este filão. No Brasil, o SENAC/RJ (*www.rj.senac.br*) em parceria com a Secnet (*www.secnet.com.br*), em uma atitude prá lá de oportunista, montou um laboratório com máquinas totalmente vulneráveis (Windows 2000 sem Service Pack) e quer fazer crer que ensina por setecentos reais, alguém a ser hacker em duas semanas (Curso de Técnicas de Invasão, Exploits e Incidentes de Segurança). No exterior, temos a EC-Council que emite uma CERTIFICAÇÃO HACKER (a do tal do hacker ético). Parece ser um puco mais séria. Saiba mais visitando o link:

www.eccouncil.org/ceh.htm

Lamer - A palavra lamer é usada para designar aquele que ainda está iniciando e que ás vezes faz papel de bobo.
No Brasil não é comum o uso dos termos *Phreaker*, *Wannabe*, *Defacer*, *Carder*, *Warez* e tantos outros que podem ser encontrados por aí, nos livros e Internet. A palavra HACKER ou PIRATA DE COMPUTADOR são as usuais ao se referir a qualquer ação de quebra de segurança de redes. Seja feita por um iniciante ou iniciado. Para saber o significado original da palavra *hacker*, consulte o link:

http://catb.org/~esr/jargon/html/H/hacker.html

Algumas pessoas podem discordar de mim quando afirmo que não tem grupo hacker organizado. Não tem mesmo. O que vocês verão por aí em forma de eventos, cursos e encontros, são de profissionais de segurança querendo ganhar algum. Os hackers que 'fazem e acontecem' não mostram a cara.
A partir de agora e durante todo este livro eu vou me referir ao hacker como hacker, independente da sua 'classificação' na 'hierarquia'.

A Um Passo do Crime

Ser hacker, para quem gosta, pode ser legal. Muitas das ações hacker podem ser feitas sem infringir uma só linha do Código Penal. O problema é que estamos no Brasil, onde o sistema judiciário, quando quer, cria todas as condições para que um cidadão seja condenado em uma acusação, independente da sua inocência. Estamos em um país em que, se por um lado é exigido o curso superior para alguém se tornar delegado, o mesmo não ocorre nas cidades mais isoladas, onde o delegado pode ser até analfabeto. Basta ser homem de coragem e ser indicado por político local. Nosso país é um país de extremos e de situações inusitadas. Não é difícil encontrar um engenheiro sendo mandado por alguém que mal concluiu o ensino primário, mas que é o dono da empresa. Uma das minhas teorias é a de que todo o sistema educacional, incluindo o ensino superior, preparar operá-

rios para o trabalho. E ser empregado não dá dinheiro, só dá dívidas. São vários os casos do empregado com anos de dedicação aos estudos, sendo mandado e mal pago por patrões ou políticos semi-analfabetos. No meu site *http://Prosperidade.Net*, tem um artigo com o título *"Quer ficar rico? Então pare de trabalhar"*. Não será esta aberração social que está incentivando as pessoas inteligentes a usarem o computador para o crime?

Mas voltando as idiossincrasias do nosso sistema judiciário, é recente o caso de um cidadão que denunciou à ouvidora da ONU ter sofrido violência física nas mãos de policiais e apareceu morto poucos dias depois. Também fiquei perplexo ao ver no programa Fantástico da Rede Globo o caso de um juiz que manteve a pensão alimentícia de uma criança, mesmo quando o exame de DNA provou que o acusado não era o pai biológico.

Com estas e outras fica difícil confiar cegamente na justiça brasileira. Aquele lema 'a justiça é cega', parece querer dizer 'a justiça é cega para a verdade'. Não dá pra confiar na justiça brasileira. É impossível prever se uma ação hacker vai dar em nada ou será o início de uma grande caça as bruxas. Então, embora a maioria das ações hacker não seja explicitamente prevista no Código Penal, aos olhos da Lei, uma ação hacker poderá ser 'enquadrada' em algum outro artigo, incluindo os do Código Civil e do Código de Defesa do Consumidor.

As maiores chances de ter problemas com a justiça será se for pego envolvido com FRAUDE NO SISTEMA FINANCEIRO (bancário, bolsa de valores, operadoras de cartão de crédito, grandes sites de e-commerce), PIRATARIA, PEDOFILIA (hospedagem ou divulgação de fotos de menores mantendo relações sexuais ou despidos), DISCRIMINAÇÃO (contra judeus, gays, negros e qualquer outro grupo com representatividade) ou se o alvo escolhido for PESSOA ou EMPRESA influente. No Brasil, há casos em que a polícia é omissa. E há casos, principalmente os que têm repercussão na imprensa, que o delegado acompanha pessoalmente as investigações e diligências. É só acompanhar o noticiário especializado para conferir o que estou dizendo. Além do mais, 'delegado' é cargo político. Basta uma indisposição com o governador ou prefeito para o policial ir prestar serviços na pior delegacia que o Estado tiver. Se o feito do 'hacker' der voto ao político, ele vai mandar o delegado se virar para solucionar o caso. É capaz do governador em pessoa posar ao lado do 'hacker', quando preso.

Para que você tenha uma idéia do 'risco' que estará correndo caso decida aprontar alguma, tenha em mente o seguinte:

1. A julgar pelo noticiário nacional, a impressão que se tem é de que a maioria dos crimes comuns ficam impunes. Que dirá os crimes de informática que são dificeis de de qualificar, enquadrar (já dei as áreas de risco) e condenar.
2. O fato de haver uma condenação não implica em uma 'prisão'. Pelo menos não

em regime fechado. A pena mais comum é a prestação de serviços comunitários. É bem capaz do hacker ser obrigado a ensinar informática de graça em alguma favela.
2. Pessoas e empresas vítimas de crimes virtuais, em sua maioria, não dão queixa. Preferem evitar o desgaste, a burocracia e a desinformação dos funcionários e dos órgãos competentes. Também não fica bom para a imagem da empresa a divulgação de ter sido vítima de ação hacker.
3. São poucas as delegacias especializadas em Crimes de Informática. Creio que só exista uma no Rio de Janeiro e outra em São Paulo (não confundir com delegacias virtuais). E se depender do que lemos sobre a falta de recursos nas outras especializadas, que dirá nesta, que é novidade.
4. No Brasil as pessoas não vão presas por cometerem crimes. Vão presas por não terem um bom advogado.
5. Você não precisa se assumir culpado. Pode e deve negar qualquer acusação até que possa ser assistido por um advogado. Principalmente sobre pressão.
6. Não esqueça que os advogados não estão ali para defender inocentes, eles estão ali para defender.
7. Quem tem que provar que você é culpado é quem o acusa. Não você provar que é inocente. Mas vão fazer com que você pense exatamente o contrário.

Sondagem de Consequências

A melhor maneira do hacker sondar quais os riscos que estará correndo durante o preparo de um PLANO DE ATAQUE e até corrigir detalhes do seu plano antes de colocá-lo em prática, é através da SONDAGEM DE CONSEQUÊNCIAS. Consiste em simular que o plano foi colocado em prática e verificar quais consequências decorreriam dali. A sondagem também poderá ser feita junto às pessoas. Como elas reagiriam diante de determinada situação? Como elas reagiriam se tivessem o E-Mail invadido? Como uma empresa reagiria se o site fosse desfigurado? Você pode ligar para diversas empresas como se estivesse fazendo uma pesquisa.
Eu liguei para o Procon do Rio de Janeiro e fiz o seguinte teste: aleguei ter sido enganado por uma loja virtual falsa, onde fiz o pagamento para receber determinado produto e o mesmo não me foi enviado. A atendente pediu os dados da loja, incluindo nome do responsável e endereço. Aleguei não ter nada disso, pois a loja é 'virtual' e eu não me preocupei em verificar se havia endereço físico da loja no site. A atendente disse então que nada o Procon poderia fazer, pois eu não possuía nenhuma informação da loja que permitisse a eles tomar as providencias cabíveis. E o Procon não vai em busca das provas materiais para o reclamante. Quem tem que apresentar estas provas é quem entra com a queixa.

Fiz outra experiência ligando para uma delegacia de bairro e contando a mesma história. O policial que me atendeu perguntou se o prejuízo era alto. Eu disse ter feito um depósito de duzentos reais. Ele sugeriu que eu deixasse isso pra lá, pois seria muito difícil reaver esse dinheiro ou localizar os responsáveis.

Liguei para mais uma delegacia, que me indicou a Especializada em Crimes de Informática. Mas também me alertou para ter mais cuidado da próxima vez, pois são crimes em que a polícia ainda tem dificuldades para coibir.

É claro que não liguei para a Especializada em Crimes de Informática. primeiro por que conheço o pessoal de lá. E também por que eles saberiam quais providencias tomar e eu poderia me complicar e ser enquadrado em falsa comunicação de crime, se levasse adiante minha 'pesquisa'.

Também consultei o Fórum (Juizado Especial de Pequenas Causas) de Nilópolis. Depois de muitas consultas a colegas e até a alguns advogados que se encontravam presentes no local (formou-se uma roda para discutir a questão), o funcionário pediu que eu conseguisse pelo menos o endereço do provedor. Sem o qual não teria como dar entrada no processo. De nada adiantou eu falar que o provedor era fora do Brasil. Também me orientou a procurar a delegacia de polícia e deixou bem claro que seria praticamente impossível conseguir o dinheiro de volta.

Vamos analisar duas situações hipotéticas:

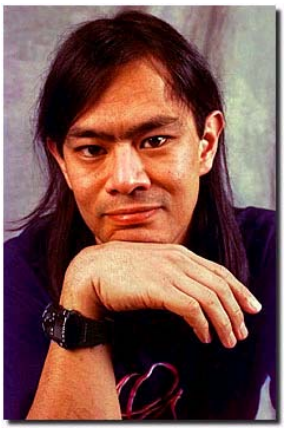
CASO 1: o hacker invadiu a conta de E-Mail do senhor X. Como forma de gozação ativou o recurso de resposta automática com um xingamento a ser enviado a cada E-Mail recebido.

DESDOBRAMENTO UM - o cidadão foi a delegacia, que por não ter meios nem o conhecimento necessário para lidar com o episódio, apenas orientou o senhor X para entrar em contato com o provedor. Caso não resolvesse, voltar a delegacia com o maior número de informações possível.

DESDOBRAMENTO DOIS - o cidadão é pessoa influente. Entrou em contato diretamente com um político local, que pressionou o delegado. Este, por sua vez, intimou o provedor a fornecer os dados da conexão. Devido a falta de meios e conhecimento da polícia para lidar com o caso, foi chamado um especialista (eu por exemplo) para ajudar na identificação e forma de ação para se chegar ao hacker. O hacker foi enquadrado no mesmo artigo que trata da violação de correspondência, mais danos morais e mais falsidade ideológica. E se não fosse a presença da imprensa, teria levado a mesma injeção que matou por infecção generalizada o sequestrador da filha do Sílvio Santos.

Neste exemplo hipotético do segundo desdobramento, o hacker foi tão azarado quanto o foi Kevin Mitnick ao inva-

dir o computador do Tsutomu Shimomura. Era uma ação que tinha tudo para dar em nada, mas a realidade foi outra. Sugiro que assista o filme *Caçada Virtual* para ter uma idéia de como foi a captura do Kevin Mitnick.



No Brasil, uma empresa ou pessoa, ao ser invadida, não pode contar muito com a polícia para chegar ao 'culpado'. E mesmo que encontre este elemento, é preciso que existam provas concretas. Nosso sistema judiciário ainda está longe de poder obter provas de crimes de informática que possa incriminar alguém.

Buscando na Internet você vai encontrar vários artigos escritos por advogados de renome, dissertando sobre os crimes de informática e de como um hacker poderá ser preso se invadir um computador. Tudo isto é besteira. A teoria é uma. A prática é outra. Advogado defende (ou acusa) tanto o culpado, como o inocente (Ôpa!). A decisão final compete ao juiz. É o juiz quem manda. Ganha quem convencer o juiz e não quem estiver certo ou errado. É triste mas é a verdade e temos que lidar com ela. E a polícia? A polícia prende até sair a decisão do juiz.

Um caso...

O editor do TI Master (*www.timaster.com.br*) fez a besteira de me azucrinar na lista de discussão Jornalistas da Web devido a uma DICA DA SEMANA que foi parar no E-Mail dele. Na lista formou-se uma calorosa discussão, incluindo a sugestão do editor do Infoguerra (*www.infoguerra.com.br*) para que o indivíduo me processasse pela prática de SPAM (o infeliz achou mesmo que um processo destes fosse possível). No fim das contas o processado foi ele - o editor do TI Master, conforme pode ser visto no site do judiciário na Internet ou no Fórum de Nilópolis. O editor do Infoguerra, quando soube do processo contra o amigo de farda, calou-se como uma moça.

Não quero que pensem que estou desfazendo do judiciário e nem dizendo que uma ação hacker não vai dar em nada. Também não estou incentivando meus leitores a hackear indiscriminadamente. O que quero deixar claro é que tem muito teórico de salto alto, incluindo advogados, juristas e pseudoespecialistas, que aterrorizam os hackers com o alardeamento de supostas punições que na verdade não existem. Ou por inexistência ou por inaplicabilidade ou por brechas na legislação em vigor. Faça um *clipping* (coleção de notícias sobre determinado assunto) de casos envolvendo hackers e confirmem o que eu estou dizendo. Mas tome cuidado para não virar o bode expiatório que nem o foi Kevin Mitnick.

A demonstração de falta de conhecimento por parte de alguns profissionais de Direito já começa no uso equivocado da expressão *crime virtual*. Se é virtual não existe e se não existe não é crime. O virtual não é real. A expressão correta, ao meu ver, é *crime de informática* ou algo do tipo. Muitos já utilizam esta forma de expressão. Mas vamos encontrar 'crime virtual' em várias publicações e sites. Busquem no Google por esta palavra e poderão comprovar o que digo. Até a Módulo, uma das mais antigas empresas na área de segurança na informática, comete este deslize em vários de seus artigos.
Em meu livro *Proteção e Segurança na Internet* eu falo mais um pouco sobre a legislação pertinente aos crimes de informática, incluindo um apêndice com o que existe na legislação vigente ou Projetos de Lei e que se aplica a este tipo de crime. No site da empresa de segurança Módulo Security você encontra artigos e coletâneas de legislação, incluindo os mais recentes Projetos de Lei sobre crimes de informática. Vale a pena consultar o seguinte link:

www.modulo.com.br/pt/page_i.jsp?page=2&tipoid=16&pagecounter=0

Se este link estiver quebrado, acesse a página principal do site e procure pelo título **Documentos -> Leis**:

www.modulo.com.br

Você precisa conhecer o tipo de punição para o que pretende fazer, até pra ver se vale a pena. Em certa ocasião, em uma destas confusões de trocar e renovar o título de leitor, soube que se não o fizesse no prazo pagaria uma multa de seis reais. Preferi ficar em casa...

Lei Comum Aplicada aos Crimes de Informática

No site da Delegacia de Repressão aos Crimes de Informática (RJ) podemos ver quais artigos a serão usados contra o hacker, caso seja pego. O link para consulta é:

www.policiacivil.rj.gov.br/artigos/ARTIGOS/drci.htm

Na página seguinte você encontra uma tabela com os artigos, a maioria do Código Penal, que podem ser usados para enquadrar um crime de informática. Criar uma avatar para fazer compras e não pagar, por exemplo, provavelmente será enquadrado como Falsa identidade (Art. 307 do Código Penal) e Estelionato (Art. 171 do Código Penal). Procure conhecer como a Justiça funciona, tenha noções de direito e conheça a Lei.

Delegacia de Repressão aos Crimes de Informática - DRCI

Conforme o Decreto Nº 26.209 de 19 de Abril de 2000, é incumbência especial desta D.R.C.I., prevenir e reprimir as infrações penais, cometidas com o uso ou emprego de meios ou recursos tecnológicos de informação computadorizada (hardware, software e redes de computadores), contra a propriedade intelectual da tecnologia da informação computadorizada, consoante a legislação vigente.

Entre as várias modalidades ilícitas que são objeto de investigações nesta especializada, observa-se tipificações penais elencadas abaixo:

Calúnia	Art.138 do C.P.
Difamação	Art.139 do C.P.
Injúria	Art.140 do C.P.
Ameaça	Art.147 do C.P.
Divulgação de segredo	Art.153 do C.P.
Furto	Art.155 do C.P.
Dano	Art.163 do C.P.
Apropriação Indébita	Art.168 do C.P.
Estelionato	Art.171 do C.P.
Violação ao direito autoral	Art.184 do C.P.
Escárnio por motivo de religião	Art.208 do C.P.
Favorecimento da prostituição	Art.228 do C.P.
Ato obsceno	Art.233 do C.P.
Escrito ou objeto obsceno	Art.234 do C.P.
Adultério	Art.240 do C.P.
Incitação ao Crime	Art.286 do C.P.
Apologia de crime ou criminoso	Art.287 do C.P.
Falsa identidade	Art.307 do C.P.
Inserção de dados falsos em sistema de informações	Art.313-A do C.P.
Adulterar dados em sistema de informações	Art.313-B do C.P.
Falso testemunho	Art.342 do C.P.
Exercício arbitrário das próprias razões	Art.345 do C.P.
Jogo de azar	Art.50 da L.C.P.
Crime contra a segurança nacional	Art.22 / 23 da Lei 7.170/83
Preconceito ou Discriminação Raça-Cor-Etnia-Etc.	Art.20 da Lei 7.716/89
Pedofilia	Art.247 da Lei 8.069/90 "ECA"
Crime contra a propriedade industrial	Art.195 da Lei 9.279/96
Interceptação de comunicações de informática	Art.10 da Lei 9.296/96
Interceptação de E-mail Comercial ou Pessoal	Art.10 da Lei 9.296/96
Crime de lavagem de dinheiro	Art.1º da lei 9.613/98
Crimes Contra Software "Pirataria"	Art.12 da Lei 9.609/98

Praticados especialmente pelos responsáveis legais dos Provedores.

Favorecimento pessoal	Art.348 do C.P.
Desobediência	Art.330 do C.P.

Todas com graves conseqüências àqueles atingidos.

Como Nascem os Hackers?

No início dos anos 60, um grupo de programadores do MIT - Massachusetts Institute of Technology (*web.mit.edu*) se autointitulou hacker em alusão as suas competências pessoais em lidar com computadores e sistemas. Neste sentido, o hacker era alguém especialista em lidar tanto com o software quanto com o hardware, incluindo os sistemas operacionais. Era alguém que conhecia como a palma da mão os sistemas de informática da época. Esta autodenominação era uma forma de autoreconhecimento por serem realmente bons no que faziam. Sem falar que a cultura americana incentiva a autopromoção. Por lá a humildade não é bem vista. No Brasil ocorre justamente o contrário. Se alguém se diz bom em alguma coisa é mal visto. Este excesso de humildade pode, de certa forma, atrapalhar o desenvolvimento humano. Mas este não é o assunto deste livro.

Voltando ao MIT, a situação se complicou quando alguns destes cérebros brilhantes resolveu ir para o lado negro da força e criar alguns programas com vida própria para testes: os vermes e vírus. A confusão entre hacker do bem ou do mal (cracker) começou na década de 80 quando surgiram os primeiros virus e presenciamos a criação da *Legion of Doom* em 1984. Foi lamentável essa confusão entre quem cria e quem destrói. Por outro lado, ao associar em excesso o "hackerismo" à informática, fez com que esta palavra fosse associada quase que exclusivamente aos especialistas em sistemas de informática que usam este conhecimento para cometer algum ato condenável. Se não houvesse este vínculo com a informática, teriamos hackers nas várias áreas de atuação humana: o hacker escritor, o hacker médico, o hacker jornalista, o hacker transformista, etc...

De forma resumida, em um primeiro momento (décadas de 60 e 70), hackers eram os especialistas em software e hardware. Muitos desses hackers contribuiram para o atual estado da tecnologia da informação. Como exemplos dos primeiros hackers, temos gente do quilate de Vinton Cerf ('pai' da Net), Tim Berners-Lee ('pai' da Internet), Steve Wozniak (criador do primeiro computador pessoal do mundo), Bill Joy (criador do Unix) e Linus Torvalds (criador do Linux), entre outros.

Na segunda geração de hackers (iniciada entre as décadas de 80 e 90) começamos a ter os problemas de vírus e invasão. O hacker passa a ser visto como o PIRATA DA INFORMÁTICA e tratado como criminoso. O melhor representante desta geração é o Kevin Mitnick, cuja fama mundial se deve ao excelente trabalho jornalistíco-para-vender-jornal do *The Washington Post*. Não custa lembrar que o site do Mitnick foi pichado, em uma 'homenagem' a sua libertação da prisão.

Ainda estamos na segunda geração de hackers, quase entrando na terceira. Não temos ainda alguém tão famoso quanto os pioneiros.

Faça o teste: *Você é Um Hacker?*

Elaborei um questionário para você conferir se tem aptidão para ser hacker. Responda com SIM ou NÃO, baseado na primeira impressão que lhe vier a mente. Confira o resultado no final:

1. Quando criança seus brinquedos incluiam video games, peças de armar (tipo Lego), brinquedos eletrônicos, kits de mágica ou jogos de estatégia do estilo War e Banco Imobiliário?
2. Você costuma se perguntar como as coisas são feitas?
3. Você já virou a noite fazendo algum trabalho no micro?
4. Você gosta de ler?
5. Você usa o computador mais de quatro horas por dia?
6. Você tem facilidade em fazer as pessoas acreditarem em mentiras?
7. Seus pais têm (ou tiveram) dificuldade para manter você na linha?
8. Você ouve mais a palavra NÃO do que SIM?
9. Você consegue se lembrar de pelo menos três encrencas em que tenha se metido?
10. As pessoas te pedem ajuda em assuntos que você acha simples, mas elas acham complexos, como programar um videocassete por exemplo?
11. Existe mais de três assuntos que você aprendeu por conta própria e domina bem (assuntos que normalmente as outras pessoas só aprendem em cursos, como idiomas, informática e preparação para concursos)?
12. Você acha que ao seu redor existem mais pessoas 'burras' do que 'inteligentes'?
13. Você se considera uma pessoa excêntrica (com gosto e comportamento diferentes da maioria das pessoas)?
14. Você costuma ser chamado para opinar sobre a compra de aparelhos eletrônicos, como computadores, videocassetes e telefones celulares?
15. Você tem uma biblioteca só sua?
16. Seus amigos o consideram uma pessoa inteligente?
17. Se você fosse um hacker e alguém lhe perguntar isto, você confirmaria ser hacker?
18. Você usa o computador a mais de dois anos?
19. Você gosta de filmes de ficção científica?
20. Quando assiste a shows de mágica você costuma descobrir o truque ou pelo menos pensar a respeito?

Agora conte UM PONTO para cada SIM e confira o resultado:
Se você fez de 1 a 18 pontos você é LAMER - Sinto muito. Você ainda é um Lamer e de vez em quando as pessoas se aproveitam da sua ingenuidade. Não sei se um dia vai conseguir se tornar um hacker. Mas se está lendo este livro, já é um bom começo.

Se você fez 19 pontos você é HACKER - Mas eu sei que não adianta te dizer isto por que você vai negar. Não é mesmo?
Se você fez 20 pontos você é ARACKER - Quase me enganou, hein!?

Como Se Tornar Um Hacker

Já dei a pista de como se tornar um hacker quando descrevi, neste mesmo capítulo, a condição do SER. Faça o que um hacker faz e será o que um hacker é: um hacker. Mas para FAZER temos que SABER. O grupo de conhecimentos necessários ao hacker de hoje, inclui:

conhecimento de lógica e linguagens de programação: não tem jeito. Se você não souber programar, vai depender sempre dos programas feitos pelos outros, correndo o risco de instalar trojans e vírus na sua máquina. E não se contente com a programação ensinada em cursos. Tem que saber programar sockets.

Quanto a qual linguagem aprender, tem as que não podem faltar: C, Delphi, Perl, Visual Basic, PHP, SQL, JavaScript e ASP. Mas a lista correta vai depender do tipo de hacker que você quer ser. Se pretende atacar plataformas Microsoft, vá de Visual Basic, VBA, VBScript, Delphi, ASP, SQL, C, C++ e Java Script. Se pretende atacar plataformas Unix/Linux, vá de Delphi, PHP, C, Perl e SQL. Se pretende focar suas ações na Internet, poderá ficar com C, Perl, PHP, ASP, SQL, VBScript, ActionScript (Flash) e JavaScript. Se bem que as últimas versões do Delphi e Visual Basic também vão ajudar bastante. Se pretende se aventurar na nova área de programação para celulares, conheça principalmente a linguagem Java e ActionScript (Flash). Se pretende ser um phreaker, vai precisar saber Assembler, C, Delphi e eletrônica analógica e digital.

conhecer o sistema operacional do alvo: um hacker precisa, no mínimo, saber mais sobre o sistema operacional do alvo que o administrador da rede. Seja ele Windows 2000, XP, 2003, Unix ou Linux e suas várias distribuições.

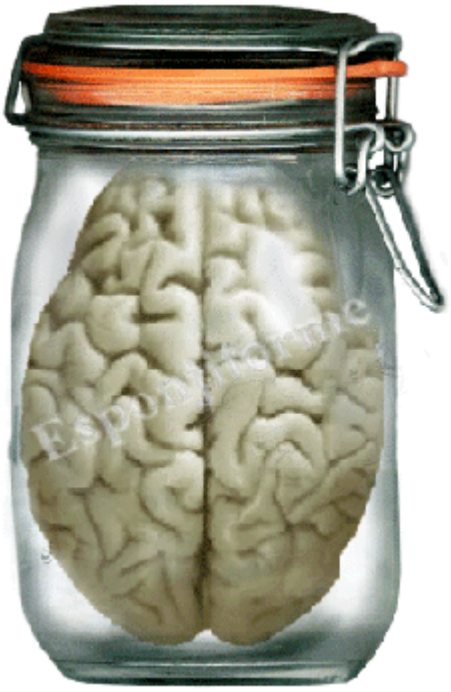
conhecer todos os aspectos que envolvem o funcionamento das redes: isto inclui rede física e lógica; protocolos, principalmente o TCP/IP e telecomunicações.

conhecer hardware: lembre-se de que o software é quem põe o hardware para trabalhar. Então você precisa conhecer também e a fundo todos os componentes usados para montar um micro e as redes de computadores.

conhecer pessoas: não no sentido de redes de relacionamento, se bem que também vai precisar disso. Mas conhecer como as pessoas pensam, como se comportam e, principalmente, como reagem a determinadas situações. Conforme a tecnologia vai tornando mais difícil a ação hacker ser bem sucedida do lado da máquina (software e hardware), o lado mais fraco da corda passa a ser o fator humano. Leituras na área de psicologia, vendas e programação neurolinguística vão ajudá-lo neste ponto.

saber se comunicar: qual ação de engenharia social vai dar certo se feita por um

hacker que gagueja na hora de pedir a senha de um E-Mail, supostamente esquecido? Você precisa ter controle sobre sua expressão vocal para que possa se beneficiar das formas de ataque que utilizam a engenharia social. Também precisará de voz firme para ser convincente quando interrogado por ser suspeito de alguma ação hacker.



saber raciocinar: o maior dom de um hacker é o seu modo de pensar característico. Empresas dos mais diversos tipos aumentariam enormemente os seus lucros caso contassem com a mente hacker para melhorar seus produtos ou processos. Caso você não saiba, o governo brasileiro da época da ditadura, retirou do currículo escolar todas as matérias que educavam o raciocínio. Nossos pais e avós, foram os últimos a terem a educação com ênfase ao pensamento. Estudavam latim e filosofia, mesmo em escolas públicas. Alguns dos idosos de hoje, só com alguns anos de estudo pelo programa educacional antigo, fazem cálculos melhor que muitos estudantes secundaristas. Justamente por raciocinarem, estas pessoas se rebelaram contra a forma de governo da época. Como consequência muitos foram perseguidos, mortos ou tiveram que deixar o Brasil. Artistas como Gilberto Gil e Caetano Veloso encontram-se entre os que foram expulsos do país (exilados). As pessoas da geração atual, da anterior e da próxima, estão com o raciocínio comprometido. São em sua maioria, pessoas que não sabem pensar. É diferente pensar e ter pensamentos. O cérebro destas pessoas está tão desacostumado a pensar que quando é submetido a algum problema que exija raciocínio, costuma reagir CONTRA a solução do problema.

A intenção do governo militar era criar operários para as fábricas que começavam a se instalar no Brasil. Não precisavam pensar. Só que o sistema atual exige que o trabalhador pense. Mas isto não foi ensinado. Estamos tão castrados mentalmente que o ex-presidente Collor confiscou a poupança de milhões de brasileiros e isto foi aceito de forma natural e passiva. Se você souber usar melhor o raciocínio, estará em vantagem em relação aos funcionários da empresa alvo. Um teste simples para sabermos se você usa bem o raciocínio é o seguinte. Sem o uso da calculadora, dê o resultado da operação 4 x 0,5 (resultado na página seguinte). Se você sentiu um bloqueio no pensamento, é mal sinal. se você desistiu e correu

para a calculadora, pior ainda. Além de preguiça mental, possui a principal característica do fracassado: falta de persistência. O normal seria o cérebro ACEITAR o desafio, se sentir MOTIVADO pelo desafio e encontrar a resposta SEM GRANDE ESFORÇO. Afinal, é um problema simples de matemática.

Uma ação hacker bem sucedida é fruto de planejamento. E planejar é pensar em tudo o que diz respeito a um problema e fazer um plano para alcançar o objetivo. Repito: o sistema educacional vigente não ensina a pensar. Nem os professores formados pela Nova Escola sabem pensar direito. Existe um movimento tentando mudar isto e construir o conhecimento a partir das experiências de cada cidadão e sua comunidade. Mas ainda está longe de ser o ideal. Cérebros questionadores não são bem vindos em um país de corrupção.

Não conte com terceiros para melhorar a qualidade do seu pensamento. Aprender programação, eletrônica, trabalhos manuais, música, xadrez, jogos de estratégia, simuladores de vida, tangran, culinária, todos estes conhecimentos vão ajudar seu cerébro a se desenvolver por inteiro. Tem muito neurônio a espera de uso na sua cabeça. Em nenhuma época esteve a disposição do cidadão comum tanta tecnologia com tão pouco investimento. Se não acredita, conheça o trabalho que o jovem Gemerson Sander está fazendo na *Parasan Filmes* (*www.parasanfilmes.com.br*).

Como sugestão de leitura, recomendo os livros: *Introdução a Filosofia*, *A Arte de Pensar*, *E Se...*, *Um Toc na Cuca* e *A Técnica dos Seis Chapéus*. E se você vir com a desculpa de que são quase duzentos contos de livro e já foi um sacrifício adquirir o LIVRO PROIBIDO, é mais um motivo para você melhorar sua capacidade mental. Aproveite para visitar também o meu outro site: *http://Prosperidade.Net*.

Resposta: 4 x 0,5 = 2

Capitão Crunch (*John Draper, The Captain Crunch*)

Um dos grandes ídolos dos hackers, da época em que eles deixaram de ser programadores do MIT e passaram a adolescentes descobrindo o potencial dos primeiros computadores pessoais, é a lenda viva John Draper, o Capitão Crunch. Em 1972, John Draper - que era técnico em eletrônica - conheceu Denny, um rapaz cego que havia percebido que um pequeno apito distribuído com a caixa de cereais *Cap`n Crunch* (*Captain Crunch*) da Quake, poderia ser utilizado para burlar o sistema telefônico e fazer ligações interurbanas gratuitas.

Naquela época, o sistema telefônico americano era analógico, sendo que determinadas funções eram operadas a partir de sons específicos transmitidos ao longo da linha telefônica.


Década de 70

Com o tempo, Capitão Crunch acabou por desenvolver um dispositivo denominado Blue Box (caixa azul) que reproduzia diversos sons utilizados pelas companhias telefônicas, liberando o acesso a serviços específicos.

As caixas azuis foram copiadas por vários membros dessa comunidade, até que Denny e alguns amigos foram entrevistados pelo jornalista Ron Rosenbaum da revista Esquire. Nessa ocasião, eles relataram a Rosenbaum tudo o que era possível fazer com uma Blue Box e como ela funcionava.

Ao ler a reportagem, Captain Crunch, que não havia sido entrevistado por Rosenbaum, ficou muito preocupado com a divulgação dessas informações e como isso poderia ser utilizado para paralisar as operações telefônicas em todo os EUA. Em plena Guerra Fria, existia o temor que esse tipo de informação poderia ser utilizado pela antiga União Soviética, paralisando o sistema telefônico americano.

As investigações realizadas por agentes das companhias telefônicas e pela polícia acabaram por descobrir John Draper, o que fez com que ele passasse algum tempo em uma prisão federal. Naquela época, suas atividades já não eram tão intensas, possivelmente pelo tempo que passava ocupado com o curso de engenharia eletrônica e com um emprego de meio período.

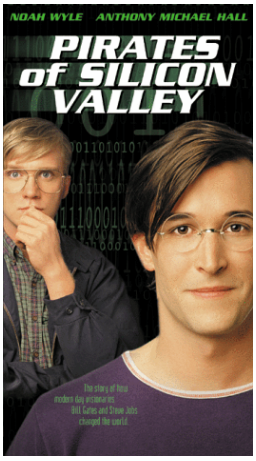

Foto atual

Na prisão de segurança mínima de Lompoc, uma de suas primeiras providências foi comprar um rádio. Ele modificou o aparelho de rádio e passou a

ouvir as conversas que os guardas na prisão mantinham através de seus *walkie-talkies*.

Posteriormente ele conseguiu fazer ligações telefônicas para números não permitidos dentro da prisão, utilizando as técnicas que o levaram para Lompoc. Esses conhecimentos atraíram outros presos e Draper logo começou a difundir suas técnicas dentro da prisão.

Após algum tempo, ele passou a trabalhar no *Receiving Studios* durante o dia, retornando apenas durante a noite para dormir na prisão. Em seu emprego ele obteve permissão para utilizar um computador e passou a desenvolver o *EasyWriter*, o primeiro processador de textos para o Apple e IBM PC. Ele digitava os códigos de programação durante o dia e os revisava a noite na prisão.



Atualmente, Draper comercializa um sistema firewall e de detecção de invasões de redes denominado *CrunchBox* (*http://shopip.com/index.html*). Segundo Steve Wozniak (*www.woz.org*), um dos fundadores da Apple, a CrunchBox está muito perto da perfeição, afinal foi desenvolvida por um hacker!

Curiosamente, Steve Wozniak foi um dos usuários das caixas azuis, ainda no tempo em que estudava em Berkeley, tendo sido instruído pelo próprio John Draper. É célebre a história de que Wozniak, ao utilizar uma Blue Box pela primeira vez, ligou para o Vaticano, junto com Steve Jobs (que posteriormente fundaria a Apple com Wozniak) e o próprio Draper.

Ele desejava confessar-se com o Papa. Do outro lado da linha ele recebeu a informação de que, devido ao fuso horário, o Papa já estava dormindo. Esta cena faz parte do filme *Pirates of Silicon Valley* que é enviado gratuitamente aos alunos do Curso de Hacker.

O hackerismo como o conhecemos hoje, voltado a quebra de sistemas, começou com fraudes no sistema telefônico (*phreaking*), depois é que passou a ser feito em computadores e redes. Principalmente com a chegada dos primeiros computadores pessoais. É esta capacidade em descobrir falhas que torna o hacker temido e perigoso.

A Máquina Hacker

Outra pergunta comum do iniciante é sobre qual a melhor máquina para hackear. Antes de responder a esta pergunta, deixe-me dizer uma coisa. Quando eu era criança em João Pessoa, na Paraíba, jogavamos bola em um campo abandonado. Ao lado do campo de futebol improvisado, dividido por um tapume de madeira,

estava sendo tocada uma obra luxuosa e o filho do dono, de vez em quando, aparecia com o pai e ficava olhando a gente jogar. Hoje dificilmente esta cena se repetiria: o campo estaria infestado de traficantes e usuários de drogas e este menino estaria correndo o risco de ser sequestrado. Os tempos mudaram. Mas

como eu ia dizendo, o filho do dono ficava olhando a gente jogar bola. E a gente ficava olhando para ele, bem vestido, pele sem nenhum arranhão. Com o motorista do lado: quepe e luvas brancas. Pareciam saídos de um filme americano. Um dia o *Ganso* (apelido de um amigo de infância, cujo nome verdadeiro eu não lembro), convidou este menino para jogar bola conosco. Ele ficou eufórico e foi logo falar com o pai dele. O pai não autorizou por já estarem de saída, mas ficou de trazê-lo em outra ocasião e dar uma bola nova para o time. A nossa estava com uma parte tão gasta que exibia um estufado do miolo. Um chute naquela bola era imprevisível. Eu só fui descobrir que não jogo nada de futebol quando pela primeira vez usei uma bola perfeitamente redonda. Chutava torto do mesmo jeito.

Um belo dia em que estavamos jogando despreocupadamente, o *riquinho* chegou. Era assim que o chamavamos, em alusão ao personagem das histórias em quadrinho *Riquinho*, que depois virou *Macaulay Culkin* no cinema. O menino estava todo emperequetado: uniforme do Flamengo, chuteira novinha com trava, apito e uma bola nova, oficial, ainda na embalagem. Foi a primeira vez que vimos uma trava de chuteira. Antes só em gibis. Depois de fechar a boca, começamos o jogo. De nada adiantou a bola nova e todos aqueles acessórios. O menino jogava mal pra caramba. Eu não ficava muito atrás, mas ele era pior. O melhor do time era um negrinho, o mais pobrinho do grupo, chamado *Bilico*. Este fazia o que queira com a bola. Era imbatível na embaixadinha.

O jogo correndo e o pai do riquinho gritando o tempo todo. Ás vezes para incentivar o filho (_*"Vai filho, vai"*). Ás vezes para intimidar a gente, principalmente o Bilico (_*"Ô moleque! Cuidado com o meu filho. Se ele se machucar você vai se ver comigo."*). E todo mundo com medo de chegar perto do riquinho. Mas nem assim ele fazia gol. Já no fim do jogo, pra ver se a gente ficava com a bola, deixamos ele fazer um gol. Terminada da partida soubemos que a bola realmente seria nossa. Nossa não, do time. E que ficaria guardada com o riquinho que a traria sempre que viesse jogar conosco. Nossos jogos nunca mais foram os mesmos.

Conto este pequeno 'causo' da minha infância para que vocês percebam que o que importa é o talento do hacker e não a máquina. Cuidado para você não se ligar muito em melhor configuração como forma de compensar sua menor qualificação. O notebook do Kevin Mitnick foi leiloado e era um 486. Isto mesmo, o hacker mais famoso do mundo fez o que fez com um 486.

É claro que uma máquina potente e de boa qualidade vai travar menos, trabalhar melhor, permitir o uso de vários programas de uma só vez, instalação de máquinas virtuais, demorar menos tempo para carregar os programas e todas aquelas vantagens que você já conhece. Uma conexão de boa qualidade também vai permitir o uso de algumas técnicas que são impossíveis de serem bem sucedidas em uma conexão discada. Mas não podemos colocar como CONDIÇÃO para desenvolver nossas ações hacker, a posse de uma máquina *top* de linha.

Windows ou Linux?

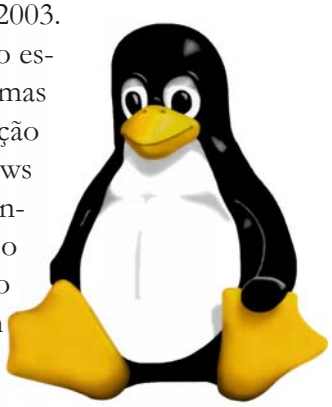
Os dois podem ser usados para hackear. A vantagem do Linux é possuir o maior, melhor e mais atualizado grupo de ferramentas de ataque e defesa. Muitas destas ferramentas não foram feitas para hackers, mas acabaram sendo usadas por eles. Quem está começando pode e deve começar pelo Windows. É mais fácil para aprender e as ferramentas são mais fáceis de usar No nosso Curso de Hacker a distância, só abordamos Linux nos módulos mais avançados. Mas mesmo usando Windows, algumas técnicas exigirão uma segunda máquina com Linux. Nada que uma máquina virtual com o RedHat ou FreeBSD não resolva.

Qual é a melhor máquina para o hacker?

Quem está começando e quer usar uma máquina antiga para as práticas, pode muito bem usar um PC entre 100 a 500MHz rodando o Windows 98 SE. Trata-se de um sistema com vários recursos de rede. Muito fácil de usar e excelente para o iniciante. Mas esta longe de ser o ideal para quem pretende alçar vôos mais altos. Para ataques mais ambiciosos, sugiro o Windows 2000 Server em máquina acima de 500MHz com generosa quantidade de memória RAM (256 ou 512 MB), que servirá para o uso de máquinas virtuais. Mas se você quiser tirar onda mesmo, instale o Linux Red Hat ou o FreeBSD na máquina de ataque.

Os sistemas que eu não recomendo para montar a MÁQUINA DE ATAQUE são o Windows Me, o Windows XP ou o Windows 2003.

O Windows Me tem um sistema de auto-recuperação especialista em reviver desastres. O XP não instala algumas das ferramentas hacker mais comuns e limita a atuação de outras. Ou seja, protege os outros de você. O Windows 2003 é recente no mercado e não foi testado o suficiente para ser aprovado como máquina hacker. Então o que posso sugerir é, tem competência para usar o Linux? Não? Então comece com o Windows. Mas com um pé no Linux.

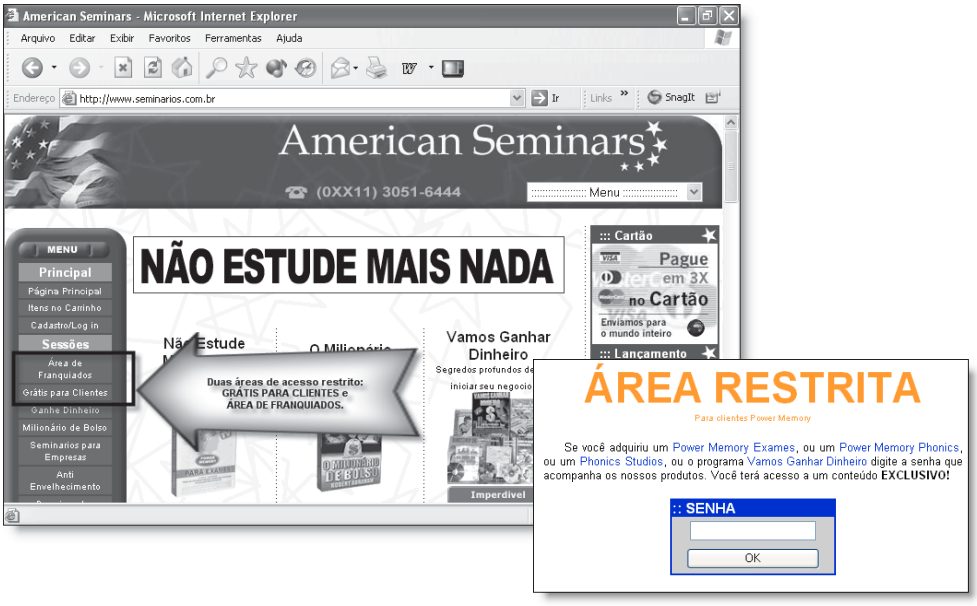


Hackeando Sem ferramentas

Um hacker deve ser capaz de hackear sem a necessidade de ferramentas. Um hacker deve ser capaz de hackear a partir dos recursos existentes no sistema operacional usado como plataforma de ataque. Um hacker deve ser capaz de hackear usando os recursos presentes na Internet. Um hacker deve ser capaz de hackear usando apenas o cérebro.

Para provar que podemos hackear sem ferramentas, só com o raciocínio, vamos usar como o exemplo o site *www.seminarios.com.br*. Não temos vínculo algum com o referido site e nem garantimos que as falhas aqui apresentadas continuem lá caso você decida repetir o teste. A importância deste tópico é provar minha afirmação: de que um hacker pode hackear sem ferramentas.

Entrando no site, percebemos na coluna da esquerda áreas de acesso restrito a clientes. Se nós soubermos a senha ou descobrirmos alguma vulnerabilidae, vamos ter acesso a esta área de acesso restrito. Antes de experimentar usar injeção de SQL, vamos ver qual página do site receberá a senha digitada. Se você não



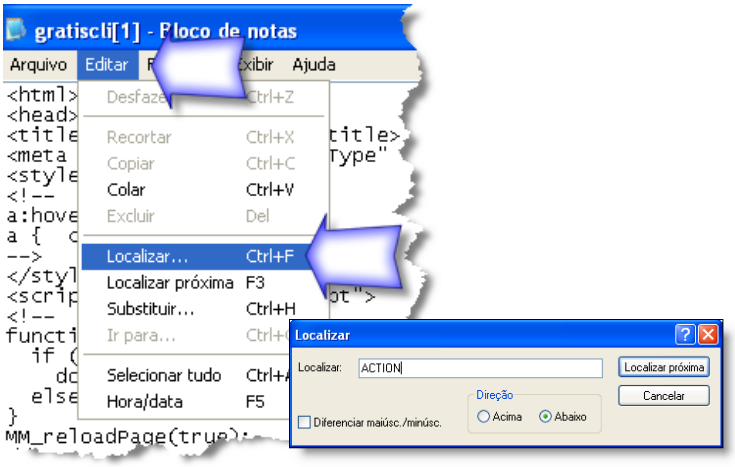
conhece programação, vou explicar melhor. As páginas com formulário chamam outra página, passando-lhe parâmetros (troca de informações entre uma página e outra). Se você digitar a senha correta, vai ser redirecionado para a página exclusiva dos clientes. Se a senha digitada estiver errada, você vai ser redirecionado para uma página de aviso. A primeira coisa que precisamos saber é qual página será chamada após clicar no botão OK ou ENVIAR.

Vamos visualizar o **CÓDIGO FONTE** em busca desta informação. O código

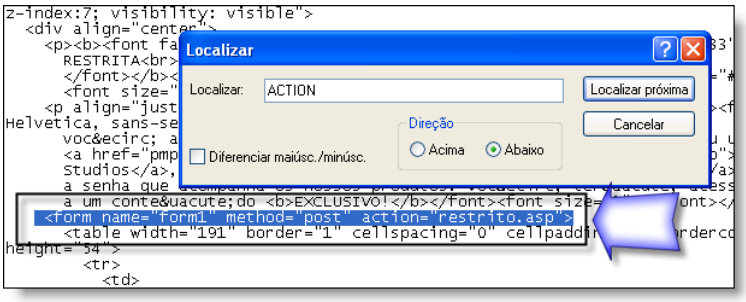
fonte de uma página na Internet pode ser visualizado acessando o menu do Internet Explorer **Exibir -> Código Fonte**:

Ou então, clicar com o botão direito do mouse sobre a página a ter o código fonte exibido e acessar a opção **Exibir Código Fonte**. Talvez o botão direito do mouse esteja desabilitado pelo programador. Uma forma de quebrar esta proteção contra o uso do botão direito é clicar com o botão esquerdo do mouse sobre a página e, sem soltá-lo, clicar também com o botão direito.

O código fonte será exibido no **Bloco de Notas** do Windows. No bloco de notas, vá ao menu **Editar -> Localizar** ou pressione as teclas de atalho **CTRL+F**.



O que estamos procurando é a linha onde consta a página a ser carregada depois que o botão OK (ou ENVIAR) for pressionado. O que você precisa fazer agora é digitar na caixa de pesquisa a palavra **ACTION**, para ver qual AÇÃO será realizada pelo formulário após envio.



Em nosso exemplo, o comando **Localizar** chegou ao seguinte resultado:

```
<form name="form1" method="post" action="restrito.asp">
```

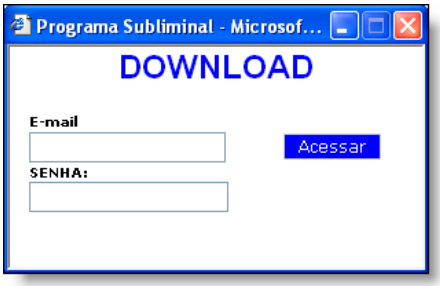
Já podemos ver que a o nome da página a ser chamada após clicar no botão OK ou ENVIAR é **restrito.asp**. Vamos digitar o endereço completo do site, incluindo no final o nome da página. A URL ficará assim:

*http://www.seminarios.com.br/**restrito.asp***

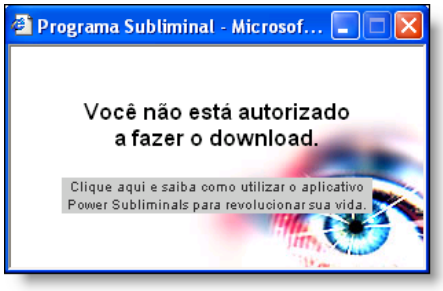
Acredite ou não, basta digitar o endereço acima e você terá acesso a ÁREA RESTRITA. O erro que o programador cometeu foi criar uma única página de autenticação e não se preocupou em validar a entrada quando feita diretamente na página restrita. Este é um erro muito comum: validação na página de entrada e sem validação na página restrita. Então se você chamar direto a página restrita, vai conseguir o acesso. O Google também pode ser usado para localizar estas páginas restritas e vamos ver como fazer isto posteriormente.

Ainda no site do exemplo, procurando, encontramos a opção de download para alguns programas. Um deles é o *Power Subliminals* que, segundo o autor, auxilia no processo de reprogramação mental, através da exibição de mensagens subliminares na tela do micro enquanto você trabalha. Isto realmente funciona e eu recomendo que você 'adquira' este programa.

Ao tentar fazer o download nos deparamos com uma nova janela de autenticação, pedindo E-Mail e senha para termos acesso ao programa. Vamos experimentar entrar com qualquer E-Mail e senha. Também podemos experimentar apenas clicar no botão ACESSAR, sem digitar nada. O resultado é uma tela informado que não estamos autorizados a fazer o download.



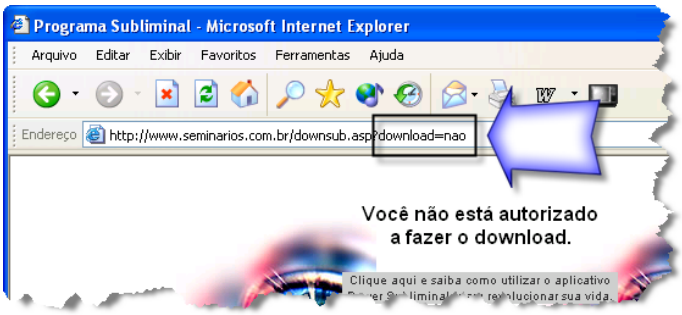
Neste caso a janela não exibe a barra de menus do Internet Explorer. Isto não é problema. Vamos usar o botão direito do mouse para exibir o código fonte e de novo procurar pela ação (ACTION) que este pequeno formulário vai executar (a página a ser chamada).



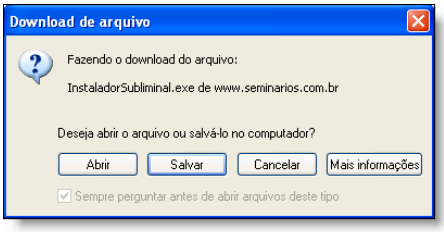
Como resultado encontramos a linha:

```
<form name="form1" method="post" action="downsub.asp?acessar=sim">
```

É só copiar e colar em uma outra janela do Internet Explorer. Só que... aconteceu um problema. O acesso foi novamente negado. Nesta página o programador foi mais experto. Mas repare no que está escrito no final da URL **download=nao**.



Mas... e se mudarmos para *sim*? Eu não quero estragar a supresa. Mas acho que a imagem diz tudo.



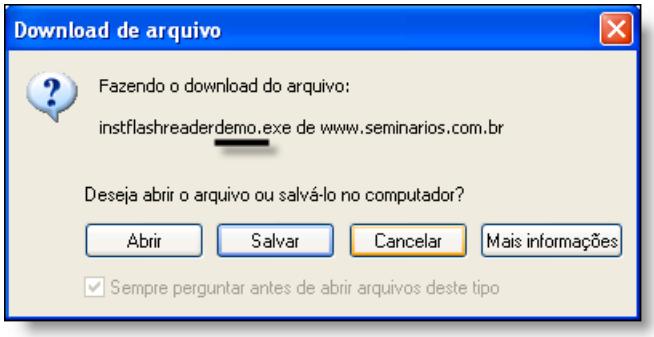
Este programa custava R$ 35 reais em abril de 2004, quando este livro foi lançado. Mas não pense que acabou. No mesmo site é vendido por R$ 60 reais um programa que promete dobrar a velocidade de leitura em 30 dias. Deve ser bom. Ainda mais para nós que temos tanto coisa pra ler. A página deste programa é:

http://www.seminarios.com.br/flashreader.asp

No final da página tem a opção de fazer o donwload do programa. É óbvio que este download só será autorizado depois de pagarmos os sessenta reais. Não é mesmo? É o que veremos...

Na página onde é feito o download (www.seminarios.com.br/baixarflashreader.asp) chegamos ao seguinte link:

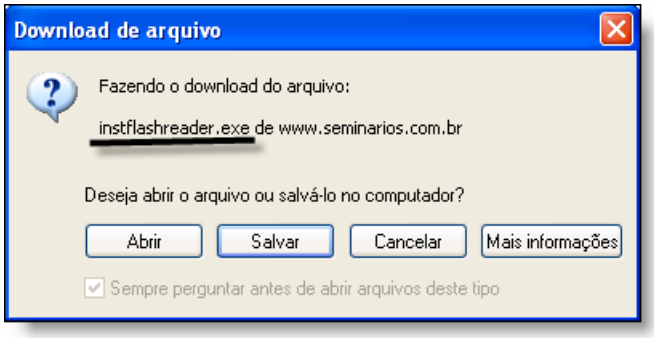
*http://www.seminarios.com.br/programas/instflashreader***demo***.exe*



Esta é uma versão de demonstração com algum tipo de limitação. Talvez eu nem encontre o crack para liberar o programa. Mas... será que se eu tirar a palavra demo do nome do programa eu consigo fazer o download? Será que o programador foi ingênuo o suficiente a ponto de deixar no mesmo local o programa completo? Não custa nada tentar o seguinte link:

*http://www.seminarios.com.br/programas/***instflashreader.exe**

Mais uma vez não quero estragar a surpresa. A imagem fala por si.

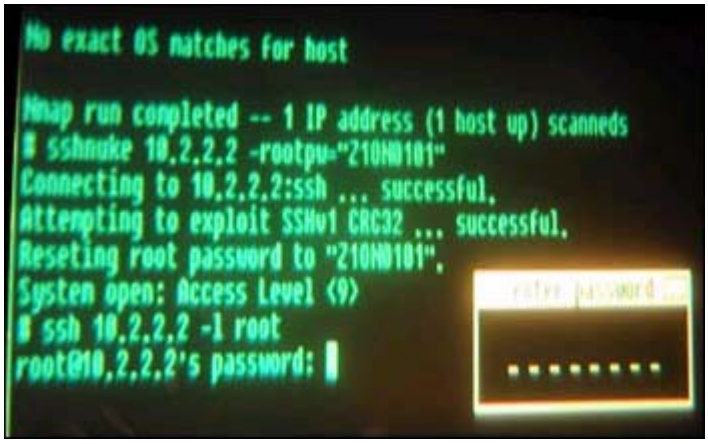


Como foi possível perceber, uma pessoa que pensa como um hacker, explora vulnerabilidaes sem o auxílio de qualquer ferramenta. É claro que existem casos em que o uso da ferramenta é imprescindível, porém de nada adianta a melhor ferramenta nas mãos de alguém que não pense apropriadamente. Já a união da ferramenta a uma mente preparada, é o que mais teme a indústria da informática. Por favor não me olhe com essa cara achando que eu saio por aí em busca de

programas que eu possa baixar sem pagar nada. Entenda esta demonstração como um exercício de curiosidade quanto ao nível de segurança implantado neste site. E não faça a besteira de procurar falhas e depois se oferecer para trabalhar na empresa invadida. Este truque é velho e não cola. Perceba que ao demonstrar as falhas de um sistema, estamos ajudando a empresa a tornar sua rede mais segura e a buscar por profissionais competentes.

Trinity: A Hackergirl

No filme *The Matrix - Reloaded*, o personagem *Trinity* interpretado pela atriz Carrie-Anne Moss, invade a *Matrix* usando o scanner de portas *Nmap* no Linux e um *exploit* de *ssh-server* descoberto em 2001 (SSH1 CRC32-exploit). Ambos existem no mundo real e o Nmap você vai aprender a usar mais a frente neste livro. Esta é a primeira vez que um filme com hackers exibe de forma fidedigna o uso de uma ferramenta existente no mundo real. Até agora o que se via era um show de efeitos visuais, muito longe do que realmente encontramos durante a ação hacker do mundo real.



Instalação e Uso de Máquinas Virtuais

A máquina virtual é um verdadeiro achado para o hacker. Veja algumas das possibilidades:

- rodar programas antigos, que só funcionam em MS-Dos ou Windows 95;
- estudar linguagens antigas de programação que rodam em ambiente MS-Dos;
- ter no mesmo computador uma máquina hacker separada da máquina de uso;
- testar programas suspeitos antes de trazê-lo para a máquina de uso;
- praticar o funcionamento das redes, criando uma rede virtual de máquinas virtuais;

- estudar o funcionamento de sistemas operacionais diferentes, sem a necessidade de particionar discos ou lidar com os problemas de boot simultâneo;
- praticar ataques a sistemas operacionais específicos, em forma de máquina virtual;
- usar uma máquina virtual como servidor de apoiso, necessário para a realização de algumas técnicas;
- criar um computador fantasma na rede da empresa, configurado com os programas que você não pode ter na sua máquina de trabalho. Esta máquina 'fantasma' também pode ser usada para acesso a Internet, caso exista alguma restrição neste sentido;
- criar uma máquina de captura de senhas, através do *fake login*.

Estas são apenas algumas das coisas que podem ser feitas com a máquina virtual. A sua imaginação dará conta do resto.

O Que é a Máquina Virtual?

A máquina virtual é um programa de computador, um software, que simula (faz de conta) que é um computador independente. Só que isto ocorre dentro do seu computador, em uma janela do Windows.

Vou explicar de novo: a máquina virtual é um programa que cria dentro de uma janela do Windows um computador virtual. Você poderá criar quantos computadores virtuais quiser. O limite de criação será o espaço no disco rígido e o limite de execução simultânea será a capacidade do processador e a quantidade de memória RAM que você tiver.

Um computador virtual tem praticamente tudo o que o computador real tem: placa de vídeo, rede, som, setup. Inclusive você vai precisar instalar o sistema operacional em cada uma das máquinas virtuais criadas.

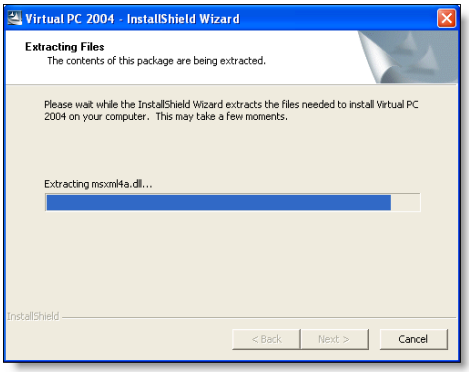
Os dois programas de criação de máquinas virtuais mais usados no mundo são o Virtual PC (agora da Microsoft) e o VMWare da empresa do mesmo nome. Ambos podem ser baixados da Internet:

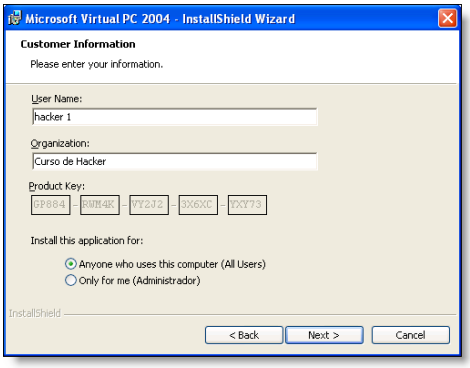
Virtual PC - http://www.microsoft.com/windowsxp/virtualpc/
VMWare - http://www.vmware.com

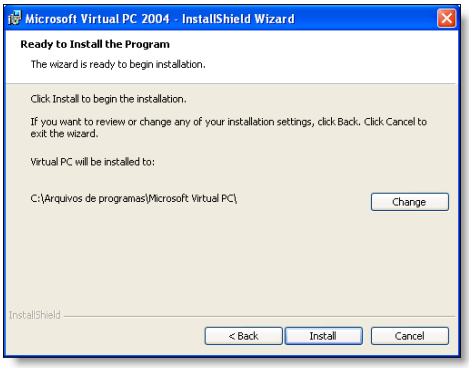
Para poupar seu tempo já incluimos no CD que acompanha este livro, uma cópia de cada uma destas máquinas virtuais, em versões para Windows 98, XP, 2003, 2000 e Linux.

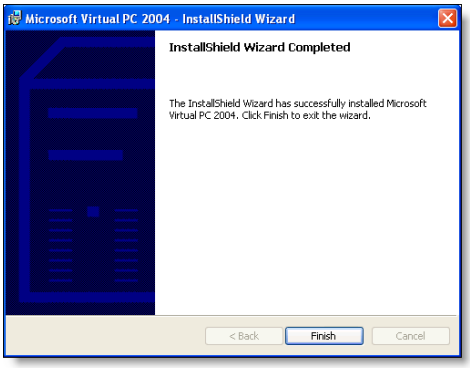
Vamos mostrar o uso do Virtual PC. A instalação, uso e funcionamento do VMWare não é muito diferente.

A instalação não é nenhum mistério, bastando seguir a sequência das telas:





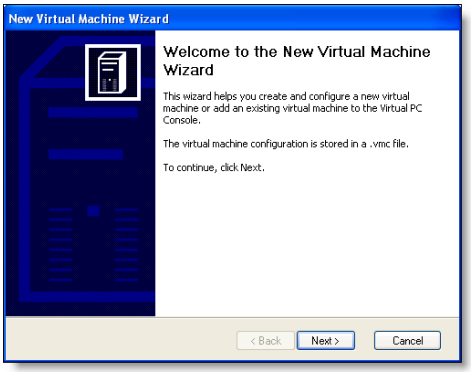


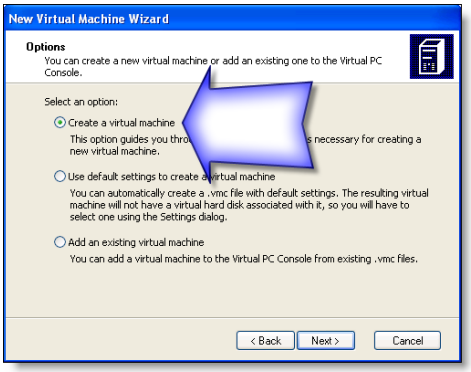


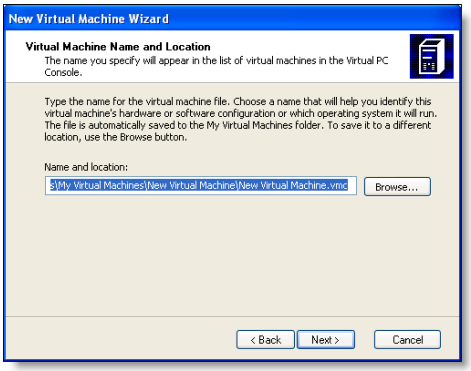
VMWare ou Virtual PC?

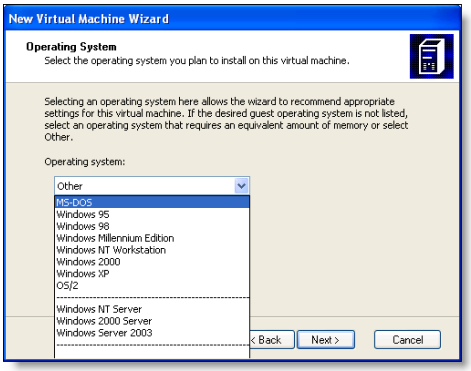
Os dois produtos são bons. O VMWare é mais respeitado quando se trata da criação de estrutura de servidores virtuais. Muitos servidores de hospedagem usam servidores virtuais alocado exclusivamente para um cliente. O Virtual PC é mais fácil para quem nunca mexeu com máquinas virtuais. Se puder, experimente uma e outra e veja qual se comportou melhor.

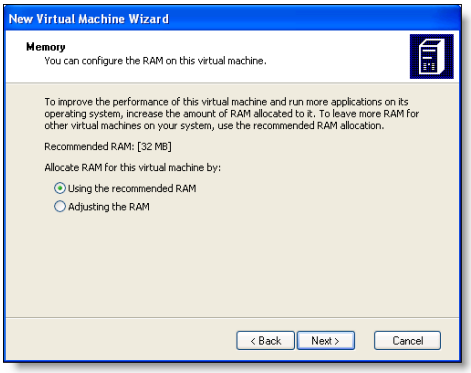
Executando o Virtual PC e criando uma máquina virtual com o assistente:

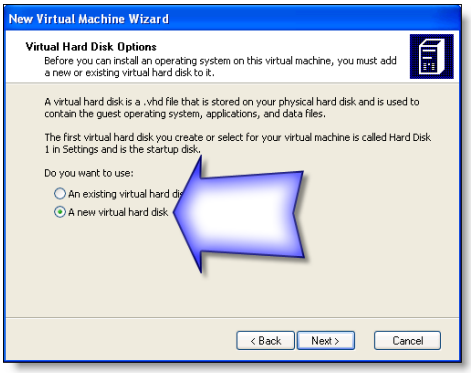








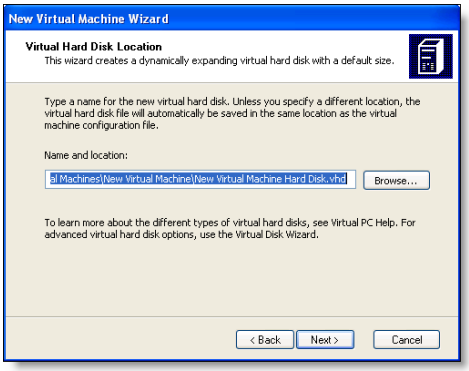


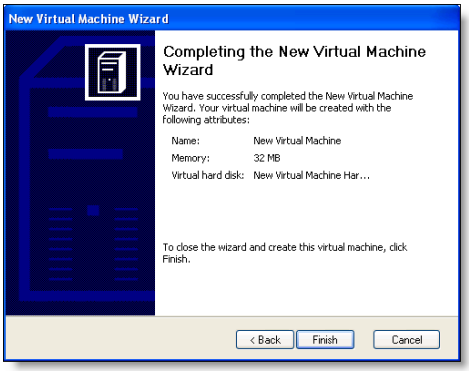


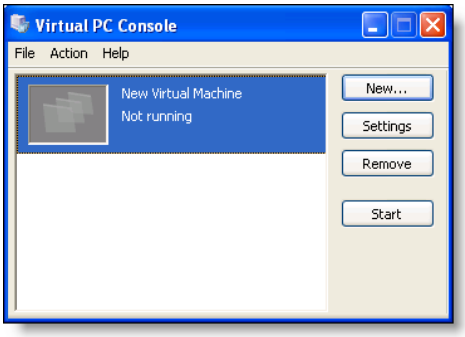
Fica claro que a Microsoft não tem o menor interesse na criação de máquinas virtuais Linux. Na aba de opções pré-configuradas, não há sinal das opções para emulação de sistemas que não sejam os da Microsoft.

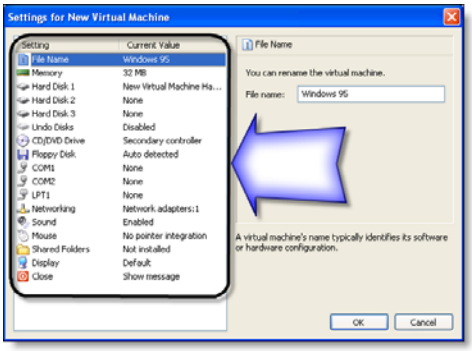
Se você estiver instalando o Linux use *Outer* ou prefira a VMWare que tem opções pré-configuradas para sistemas não Microsoft.

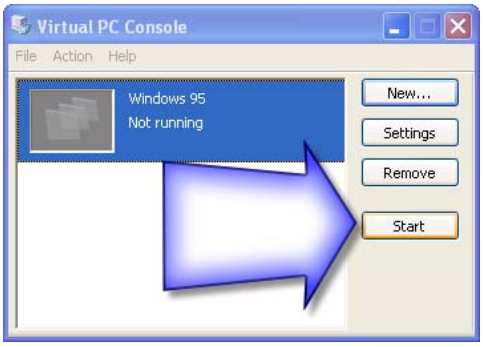
Ao concluir a instalação você vai precisar fazer alguns ajustes na máquina virtual:

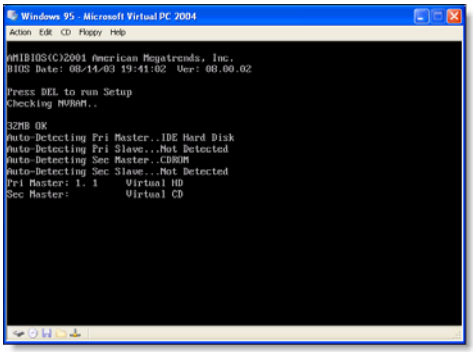








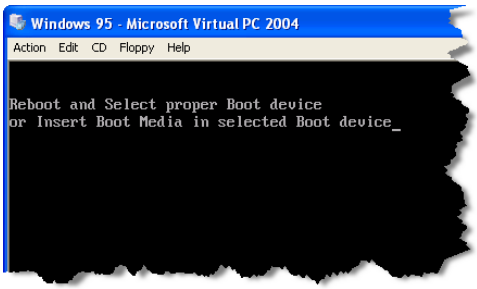




As principais opções do Virtual PC são as seguintes:

New - inicia a configuração de uma nova máquina virtual
Settings - ajusta a configuração da máquina virtual selecionada
Remove - apaga todos os arquivos da máquina virtual selecionada
Start - Inicia a execução da máquina virtual. Quando você inicia uma máquina virtual, é como se pressionasse o botão LIGAR do computador.

A máquina virtual começa com um HD vazio. Você vai precisar instalar o sistema operacional pretendido. Nesta hora não importa se é um Windows XP que vai rodar dentro do Windows 98 ou se é o Linux que vai rodar dentro do Windows 2000. Será bastante útil se você memorizar as teclas de atalho do Virtual PC:

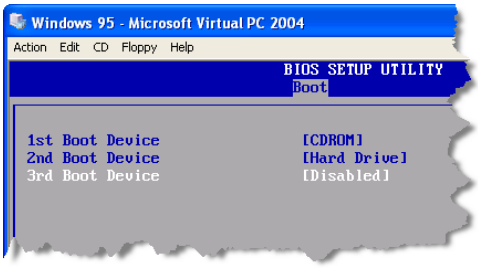


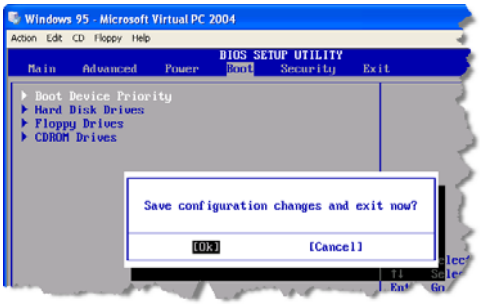
Full-Screen Mode	Right Alt+Enter
Ctrl+Alt+Del	Right Alt+Del
Pause	Right Alt+P
Reset	Right Alt+R
Close...	Right Alt+F4
Install or Update Virtual Machine Additions	Right Alt+I
Properties	

Tecla **ALT direita** + **ENTER** = executa a máquina virtual em TELA CHEIA.

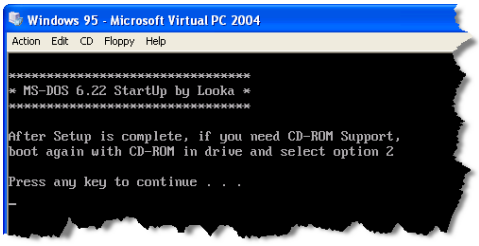
Tecla **ALT direita** + **DEL** = é o mesmo que pressionar CTRL + ALT + DEL no PC real.

A máquina virtual também possui um SETUP virtual com opções resumidas. Para dar o boot inicial por disquete ou CD-Rom e instalar o sistema que pretende usar na máquina virtual, você vai precisar ajustar as opções de BOOT no SETUP virtual, da mesma forma que precisa fazer isto no SETUP de um computador real. Entramos no SETUP mantendo a tecla DEL (ou F2) pressionada durante o processo de BOOT e saimos do SETUP, salvando as alterações, após pressionar a tecla F10:

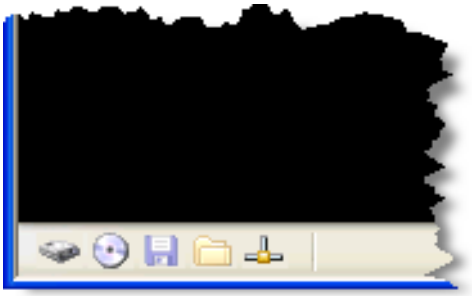




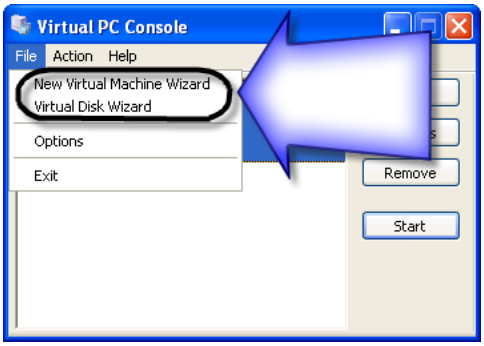
Na figura abaixo podemos ver o início da instalação do MS-Dos 6.22 em uma máquina virtual que está sendo preparada para receber o Windows 95:



Na parte inferior esquerda da máquina virtual você confere o *status* e o funcionamento do disco rígido, CD-Rom, drive de disquete, pastas compartilhadas e placa de rede, respectivamente. Estes periféricos são ajustados e ativados no menu *Settings* (configurações) do Virtual PC.



O disco rígido virtual é um arquivo que vai ocupar bastante espaço no seu disco rígido real. Este HD virtual pode ser criado na inicialização da máquina virtual, ou posteriormente, através do *Virtual Disk Wizard*.
O HD virtual pode ser movido a seu critério. Desta forma você pode criar uma máquina virtual do jeito que você quiser. Depois de pronta, faça uma cópia do arquivo e sempre que tiver problemas com a máquina em uso, basta removê-la e usar uma cópia da máquina inicial. Este procedimento é muito oportuno quando estamos testando vírus, worms, trojans e badcons.



Para criar uma nova máquina virtual usando o assistente, clique na opção *New Virtual Machine Wizard*.
Esta é a melhor forma de trabalhar com duas ou mais máquinas ao mesmo tempo. Também é ótimo para despistar possíveis auditorias. Supondo que você use o Windows XP e invada um micro usando o Linux, causará uma grande confusão no tribunal:

Advogado: *"_A auditoria constatou que a máquina usada no ataque rodava Linux. A perícia assinou um laudo dando como Windows XP o sistema operacional usado pelo meu cliente no dia do crime..."*

Não entrarei em detalhes quanto a instalação do Windows, pois foge ao escopo desta obra. Já estou me obrigando a divagar o mínimo possível sobre os temas, pois são muitos assuntos para caber em um livro só. Dicas sobre a instalação do Linux, serão vistas no capítulo do mesmo título.
Um só sistema operacional leva uma vida para aprender e ainda fica faltando alguma coisa. Sugiro que você use a máquna virtual para conhecer um pouco de cada um dos principais sistemas operacionais em uso atualmente e escolha um para se dedicar e se especializar em descobrir vulnerabilidades.

Um Mini Curso de Redes

Você vai precisar conhecer MUITO de rede e TCP/IP para se dar bem como hacker. Quem faz o Curso de Hacker recebe em forma de brinde, logo no primeiro módulo, farto material de redes para complementar o aprendizado: curso interativo para aprender a parte lógica, curso em vídeo para aprender a parte física, mais de duas mil páginas de material especialmente selecionado, em formato DOC e PDF.

Aproveite que você já sabe criar máquinas virtuais para criar uma rede CLIENTE x SERVIDOR virtual. É muito comum encontrarmos máquinas vulneráveis na Internet e não conseguirmos a conexão, por não termos as configurações de rede do nosso computador feitas corretamente. Por isso é importante que você tenha bons conhecimentos da estrutura das redes, principalmente as redes CLIENTE x SERVIDOR.

Instale em uma máquina virtual o Windows 2000 Server, por exemplo, pratique a invasão, ao mesmo tempo em que aprende também a aumentar a segurança das redes que rodam este sistema operacional.

Máquinas virtuais também podem ser usadas como *honeypot*. Basta criar uma máquina virtual com portas abertas e serviços rodando com a configuração de fábrica, para assistir os *Kiddies* fazendo a festa. Já um hacker, ao encontrar um servidor muito esburacado, pode desconfiar da armadilha.

Só não esqueça de um detalhe. Para que duas ou mais máquinas acessem a Internet ao mesmo tempo, você vai precisar de um servidor proxy. No CD-Rom que acompanha este livro incluimos um servidor proxy simples, eficaz e gratuito.

Segue agora um curso introdutório de redes e TCP/IP. A finalidade deste curso é ajudar quem não fez o curso a distância e também serve como revisão para os que fizeram.

Quem Precisa de Rede?

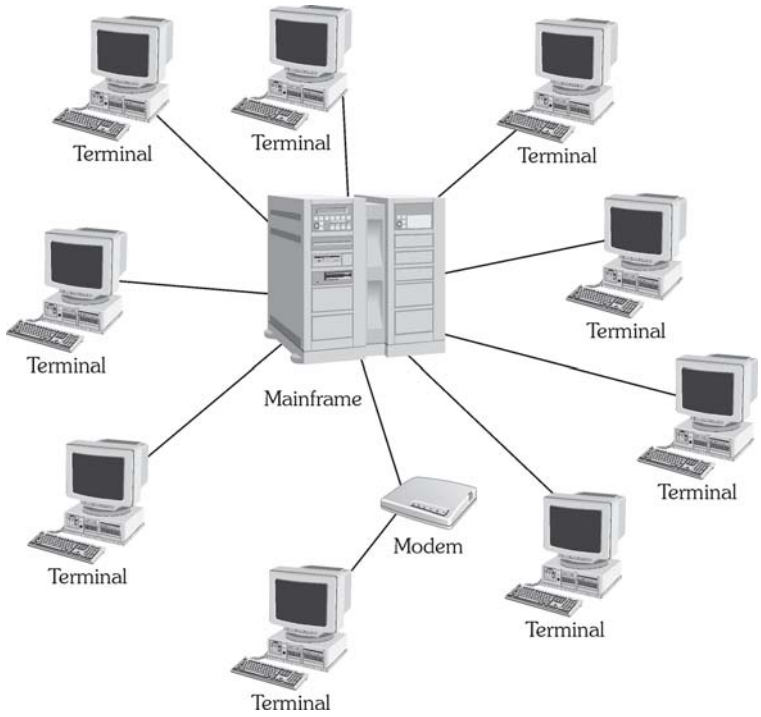
O mundo não funciona mais sem as redes. Redes telefônicas, redes de rádio e TV, redes de computadores. Todas estão convergindo para uma única rede, que ainda não possui nome próprio, mas que dela farão parte sua geladeira, aparelho de TV, telefone celular, automóvel e até o microondas. As principais tecnologias que tem tornado isto possível é a *Bluetooth* e a *Wi-fi*. Realmente, o futuro é das redes.

O incrível é que até pouco tempo atrás, apenas grandes empresas possuíam computadores ligados em rede. Atualmente, empresas de todos os portes e até residências com dois computadores apenas possuem seus micros ligados em rede.

O que aconteceu de lá para cá? Quais são os fatores que levaram a esta necessidade vital de conectar os micros das empresas e residências em rede?

Para entender estas mudanças, é interessante relembrar os motivos que levaram ao surgimento das primeiras redes. Naquela época os computadores eram caros e imensos - os *mainframes*. Não havia como disponibilizar um computador para cada funcionário. A solução encontrada foi o compartilhamento de tempo (*time-sharing*). Terminais sem poder de processamento ou armazenamento (terminais burro) eram interligados ao computador central (*mainframe*).

Os usuários tinham a impressão de serem os únicos a utilizar o computador, quando, na verdade, dezenas, centenas e até milhares de usuários simultâneos poderiam estar conectados ao mesmo tempo. Alguns desses usuários podiam, inclusive, acessar o mainframe de outras cidades através de um modem.

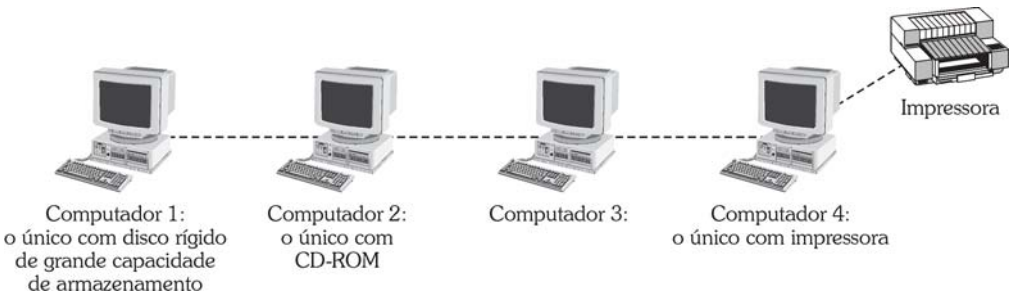


Time-sharing - "terminais burro" acessam o mainframe.

Assim, as primeiras redes surgiram devido à impossibilidade de disponibilizar um computador para cada filial, departamento, setor ou funcionário. Computadores eram caros e ocupavam muito espaço. Era a época em que reinavam mainframes e minicomputadores.

Com a popularização dos microcomputadores na década de 80, o perfil das redes mudou. Já era possível cada filial, departamento, setor ou funcionário possuir um micro exclusivo. Porém, alguns periféricos eram extremamente caros, como unidades de disco rígido, CD-ROM e impressoras. Nesta fase, as redes eram necessárias para o compartilhamento de periféricos e armazenamento em disco rígido.

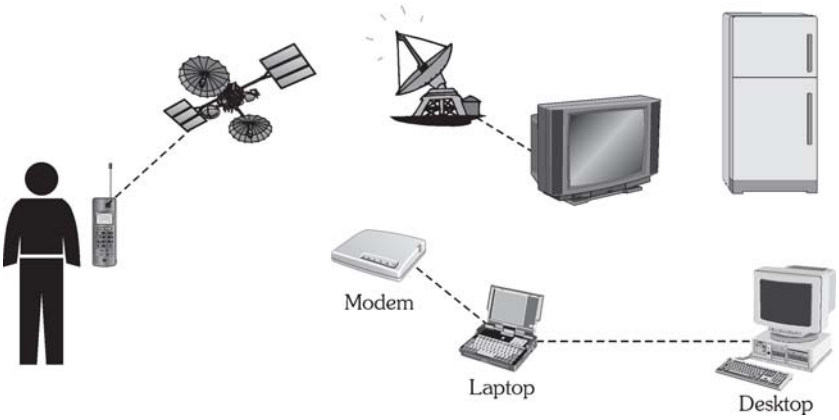
Embora um dos motivos para a escolha de uma rede ainda seja o compartilhamento de alguns periféricos caros, como impressoras laser e conexões com a Internet, por exemplo, o principal objetivo das redes atuais é o compartilhamento de dados entre os mais diversos dispositivos. As redes têm sido solução para os mais diferentes perfis de consumidor. Desde a empresa que precisa disponibilizar informações de clientes a todos os seus funcionários, onde quer que estejam, ao jovem que procura apenas diversão, como os jogos em rede, a coqueluche deste início de século.



Uma única impressora, CD-ROM e disco rígido de

alta capacidade de armazenamento são compartilhados por todos.

E já não é mais privilégio do computador a ligação em rede. Aparelhos dos mais diversos tipos têm sido projetados visando à interconectividade.



As redes atuais visam à interconectividade.

A expansão e popularização das redes se tornou possível graças aos seguintes fatores:

Barateamento do hardware - computadores, periféricos e componentes eram raros e caros. Um 486 (o melhor micro por volta de 1993) custava dois mil e quinhentos dólares e precisava ser contrabandeado para entrar no país. Atualmente, um computador trinta vezes melhor, custa oito vezes menos.

Sistemas operacionais de rede amigáveis - os primeiros sistemas operacionais de rede eram difíceis de ser configurados. A escassa documentação era em inglês. Atualmente temos sistemas traduzidos para o português, farta literatura traduzida ou produzida por autores nacionais e a tecnologia plug-and-play, que reconhece a maioria dos periféricos dos principais fabricantes.

Globalização - pela primeira vez na história da economia, empresas passam a ter como concorrentes não só as empresas locais. Empresas distantes, algumas sediadas em outros países, conseguem mesmo concorrer com as empresas locais. As facilidades de comunicação, transporte e transferência de dinheiro do mundo globalizado fazem com que um fornecedor de Singapura possa atender a clientes no Brasil sem grandes dificuldades e talvez até com menos burocracia. O empresário que só se preocupava com o concorrente do mesmo bairro, cidade ou estado precisa aumentar sua vantagem competitiva. A rede é uma das formas de conseguir isto.

Expansão da Internet - a Internet, a rede das redes, está se consolidando como a nova forma das pessoas fazerem negócio. Algumas empresas só

disponibilizam seus produtos ou serviços pela Internet. Muitos dos serviços públicos federais e estaduais, principalmente os destinados às pessoas jurídicas (empresas), só estão disponíveis na Internet.

Banda larga - se a tarifação e escassez de linhas telefônicas impedia as empresas de ligarem suas redes locais à Internet, isto é coisa do passado. Com o surgimento, expansão e barateamento da banda larga, possuir um link de 128 ou 256 K está ao alcance de qualquer pessoa.

Como podemos observar, cada um destes fatores contribuiu para a evolução, expansão e popularização das redes. Até mesmo um pequeno escritório com dois ou três computadores se beneficia da interligação em rede. Seja para compartilhamento da impressora, da Internet, troca de arquivos ou trabalho em grupo. Muitas residências já usam redes locais com esta finalidade, principalmente para o compartilhamento da Internet e impressora, além dos já citados jogos em rede.

Como não há como saber com exatidão qual o grau de conhecimento sobre redes que cada leitor possui e para evitar que leitores menos experientes se percam no decorrer dos próximos capítulos, foram incluídos conceitos de rede nesta parte do livro. Se você já é um expert no assunto, sinta-se à vontade para ir direto ao capítulo de seu interesse.

O Que É uma Rede?

É um conjunto de hardware e software que permite que computadores individuais estabeleçam comunicação entre si. Essa comunicação permite, não só a troca de informações, mas também o compartilhamento de recursos. Mas não é por estar em rede que todos os arquivos e recursos de seu micro pessoal estarão disponíveis aos demais usuários indiscriminadamente. Isto só ocorre quando não são adotados procedimentos de segurança para controle do acesso físico e lógico ao micro em questão.

A lista seguinte é um resumo dos objetivos e benefícios de uma rede:

Compartilhamento de recursos;

Compartilhamento de informações;

Redução de custos;

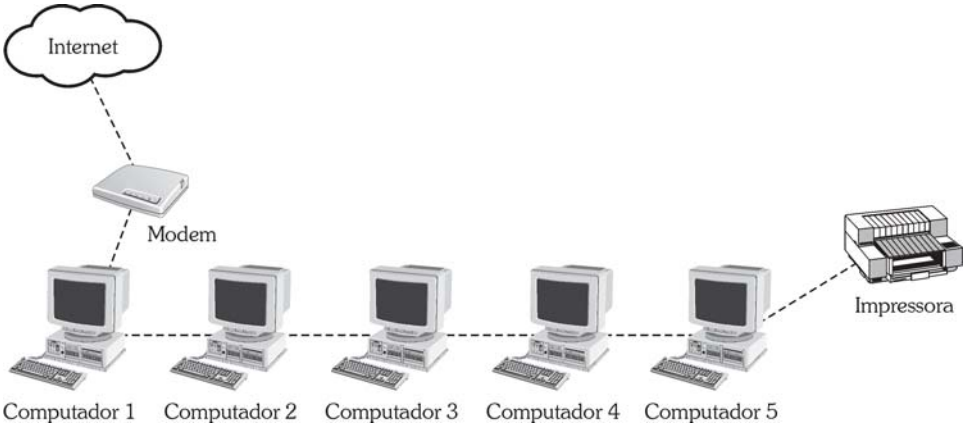
Segurança.

Como se Classificam as Redes?

As redes possuem classificação quanto à distância entre os hosts (pontos da rede), à forma de gerenciamento (hierarquia) e quanto à forma de ligação dos hosts (topologia).

Classificação das Redes quanto à Distância entre os Hosts

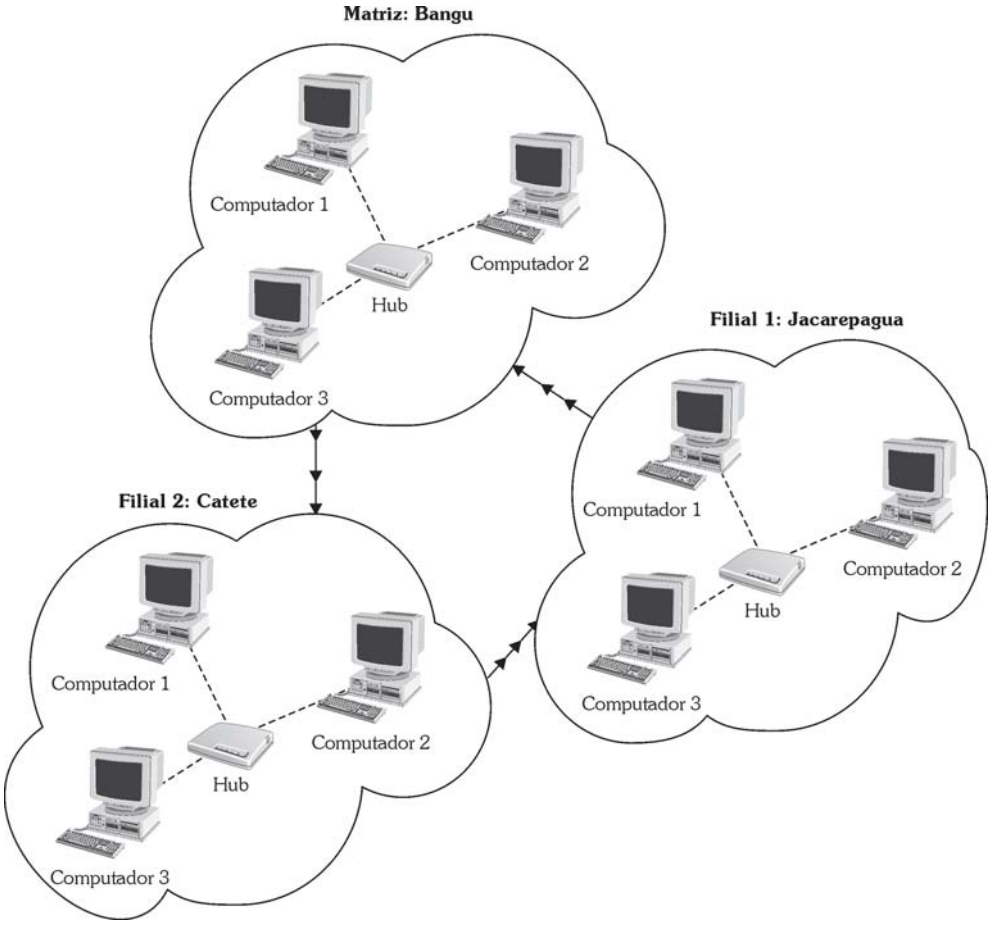
LAN (Local Area Network/Rede de Área Local) - são as redes cuja área de abrangência é limitada a um prédio. Uma rede em uma residência, escritório ou empresa é uma LAN.



Uma LAN formada por cinco micros. Todos

compartilhando a conexão com a Internet e uma impressora

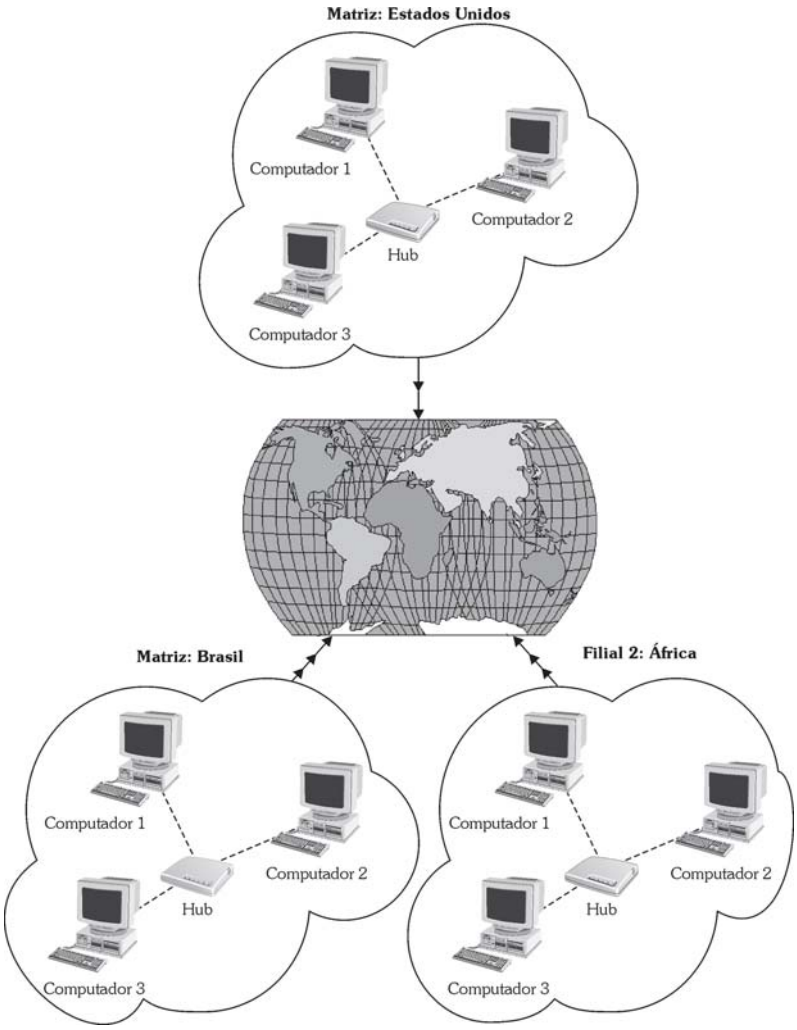
MAN (Metropolitan Area Network/Rede de Área Metropolitana) - são redes que abrangem o perímetro de uma cidade. São mais rápidas e permitem que empresas com filiais em bairros diferentes se conectem entre si. Este termo é pouco usado e às vezes é usado WAN (veja em seguida). A figura na página seguinte exibe um exemplo de MAN.



Três filiais se conectam através de uma MAN

(Rede de Área Metropolitana).

WAN (Wide Area Network/Rede de Área Global ou de Área Ampliada) - são redes que abrangem todo um estado, região, país ou até mesmo um continente. O exemplo mais comum de uma WAN é a Internet.

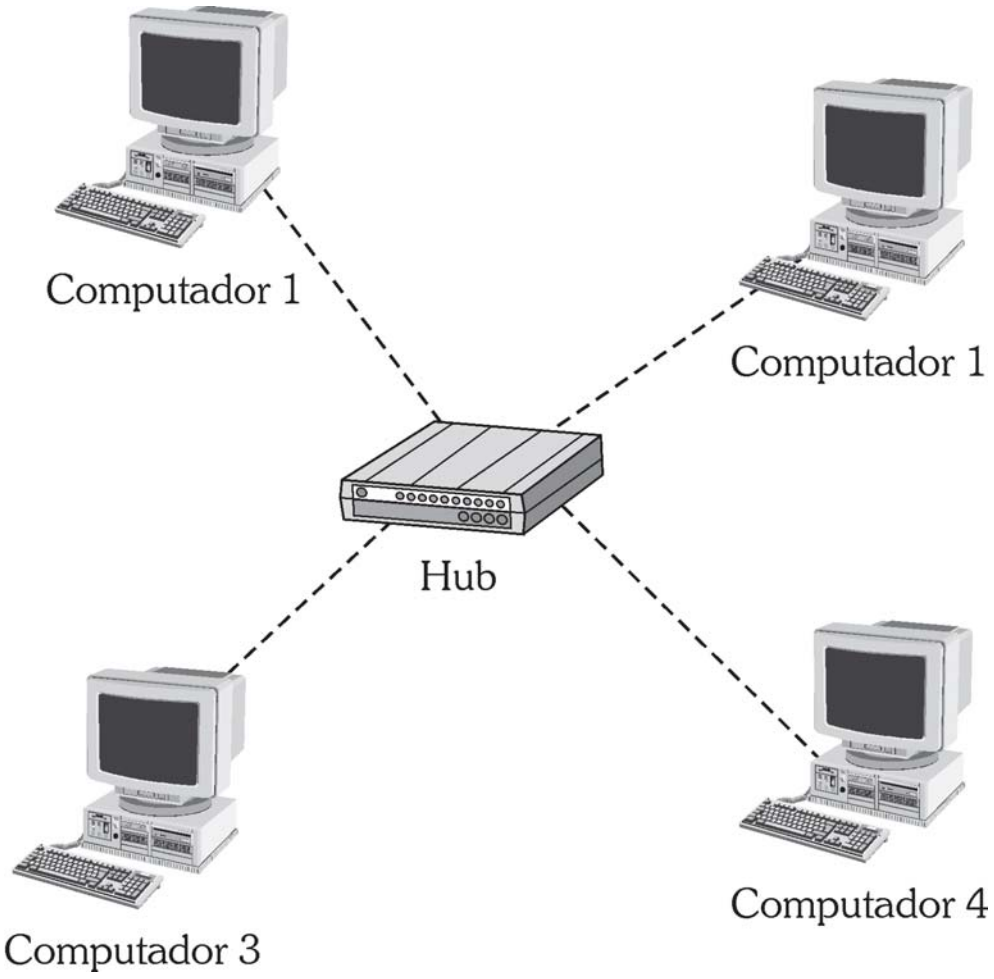


A Internet é um exemplo de WAN (Rede de Área Global).

*Não confunfir com WLan (*Wireless Local Area Network*) que designa as redes locais sem fio (*Wi-fi*).

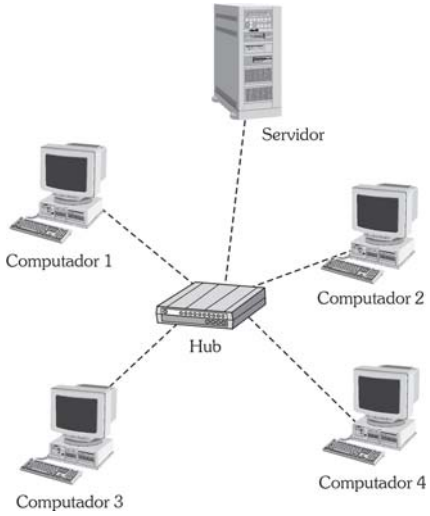
Classificação das Redes quanto à Hierarquia

Uma rede pode ser hierarquizada ou não. Redes não hierarquizadas são conhecidas também como redes ponto a ponto.



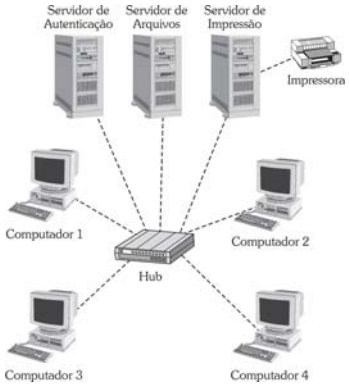
Rede não hierarquizada (ponto a ponto).

Uma rede ponto a ponto não utiliza o Windows Server como sistema operacional. O Windows Server é destinado a redes hierarquizadas, conhecidas também como redes cliente servidor.



Uma rede hierarquizada (CLIENTE x SERVIDOR)

Nas redes cliente servidor, um ou mais computadores são configurados como servidores de rede. Essas máquinas não são destinadas ao uso. São mantidas em local seguro e com acesso restrito. Podemos ter um único computador desempenhando o papel de vários servidores, mas também podemos usar computadores separados.



Computadores destinados a atuar como servidores devem ser dimensionados adequadamente. É um desperdício usar um Pentium IV de 3 GHz e 512 MB de RAM apenas como servidor de autenticação em uma pequena ou média empresa. Da mesma forma, é inadmissível usar um Duron 1.2 e 128 MB de RAM para hospedar o site de uma empresa que vive do comércio eletrônico. Cada caso é um caso e deve ser anali-sado dentro do contexto, além de prever as necessidades futuras da rede empresarial.

Às vezes é difícil convencer a diretoria da empresa a investir em um servidor de maior capacidade. Mesmo com o argumento de que o tempo em que o servidor fica fora do ar custa dinheiro.

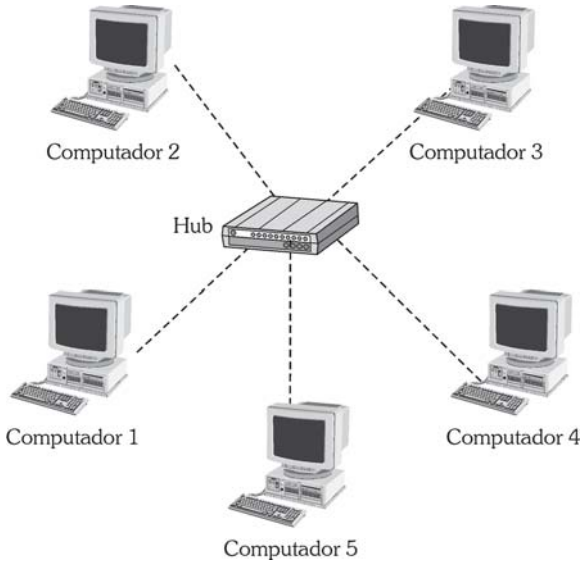
Classificação das Redes quanto à Topologia

De forma simplificada, topologia é o modo como os computadores da rede são conectados entre si. Os dois tipos mais comuns são a de **BARRAMENTO** e em **ESTRELA**.

Topologia de Barramento - cada um dos dispositivos da rede é conectado a um cabo principal conhecido por backbone (espinha dorsal). Este tipo de topologia tem sido descontinuado, pois apesar da simplicidade de sua instalação, possui sérias limitações de desempenho, e caso haja interrupção em algum ponto, toda a rede se torna inoperante. Isto torna a manutenção cara e demorada.

Topologia de barramento.

Topologia em Estrela - cada um dos dispositivos da rede é conectado a um ponto central. Esse dispositivo, geralmente um hub ou switch, se encarrega de distribuir os sinais entre os demais micros. A manutenção deste tipo de rede é rápida e bastante simplificada. Havendo problema em um dos segmentos, somente ele ficará inoperante. Se toda a rede ficar inoperante, muito provavelmente o concentrador (hub ou switch) é o componente problemático.



Topologia em Estrela.

Partes de Uma Rede

Uma rede típica é formada por:

computadores;

placas de rede;

cabos;

conectores;

concentradores;

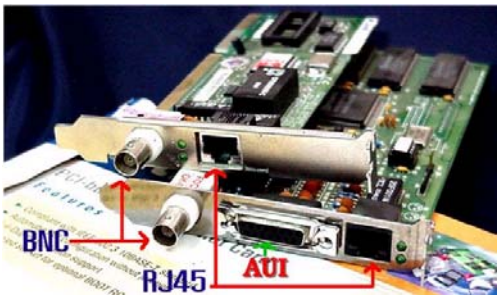
softwares.

Computadores em Rede

Um micro conectado a uma rede também é conhecido por host, nó ou workstation (estação de trabalho). Para que um micro possa se conectar a uma rede, ele necessita de uma placa de rede. Impressoras podem ser adquiridas com uma placa de rede embutida, assim não precisarão de um computador para se conectar à rede. Os aparelhos telefônicos celulares estão incorporando as funções dos PDAs (assistentes digitais portáteis) e já se conectam a rede empresarial através da Internet.

Placa de Rede

A placa de rede ou NIC (Network Interface Card) é a responsável pela comunicação entre os nós da rede. Atualmente todos os micros populares já saem de fábrica com uma placa de rede. Os modelos atuais de placas de rede só dispõem de conectores do tipo RJ-45. Modelos mais antigos possuíam dois ou mais conectores diferentes.



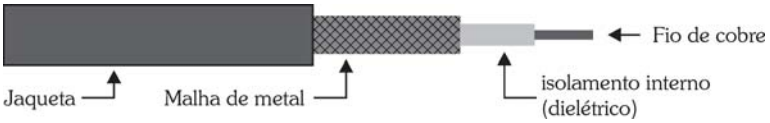
Placa de rede antiga com conectores BNC, AUI e RJ-45

Placa de rede atual: somente conector RJ-45

Placa de rede sem fio: não há conectores

Cabos

Os tipos mais comuns de cabos de rede são: o coaxial, o de par trançado e o de fibra óptica. O coaxial está sendo descontinuado. O mais usado é o de par trançado. O de fibra óptica é de uso restrito em redes corporativas e de longa distância. É o que oferece maior qualidade, porém com o maior custo. Temos também as redes sem fio em que os sinais trafegam por ondas de rádio.



Cabo coaxial.

Cabo de par trançado.

Conectores

Servem para fazer a ligação da placa de rede ao concentrador. É óbvio que o tipo de conector adotado deve ser o mesmo que estiver disponível na placa de rede e, caso a placa de rede seja de um modelo antigo, com vários conectores diferentes, apenas um tipo de conector pode ser usado por vez. A escolha do cabo segue o mesmo critério. As redes atuais utilizam conectores RJ-45, fibra óptica ou ondas de rádio (sem fio).

Conector RJ-45 usado em redes com cabos de par trançado (figura 1.16).

Uma rede formada por apenas dois micros não necessita de concentrador para funcionar. Basta um cabo do tipo cross-over, montado conforme as seguintes especificações:

Um cabo cross-over para interligar apenas

dois micros em rede, sem a necessidade do hub.

Para três ou mais computadores precisamos de um dispositivo concentrador. Então o cabo deve ser montador com a seguinte especificação:

Cabo de rede para interligar computadores através de hub ou switch.

Embora qualquer ordem de cores permita o funcionamento da rede com mais de dois micros, o ideal é que o padrão T568B mostrado na figura 1.19 seja mantido ou então o T568A (tabela seguinte), cuja diferença é a posição dos fios dos pinos 1, 2, 3 e 6.

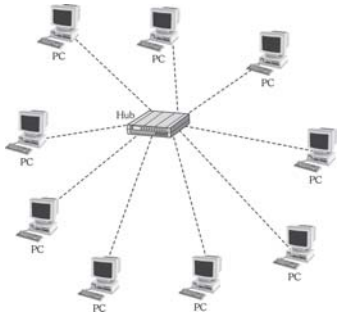
Organizações e associações internacionais de indústrias e profissionais, estabelecem padrões para a construção e funcionamento de dispositivos dos mais diversos tipos. Já pensou se cada fabricante de lâmpada adotasse seu próprio diâmetro e formato de rosca? E era exatamente isto o que acontecia antes que os fabricantes e profissionais criassem os comitês de regulamentação. Cada fabricante seguia suas próprias normas.

Pino	**Cor**
1	Branco mesclado com verde
2	Verde
3	Branco mesclado com laranja
4	Azul
5	Branco mesclado com azul
6	Laranja
7	Branco mesclado com marrom
8	Marrom

Atualmente, os dois órgãos responsáveis pela maioria das normas e especificações da informática são o IEEE (*Institute Electrical and Electronics Engineers*/Instituto de Engenharia Elétrica e Eletrônica) americano e a européia ISO (*International Standards Organization*/Organização Internacional de Padrões).

Concentradores

O concentrador, também conhecido como hub, é o dispositivo responsável pela ligação dos micros a uma rede. Hubs podem ser passivos ou ativos, que incluem funções de filtragem, reforço de sinais e direcionamento de tráfego.

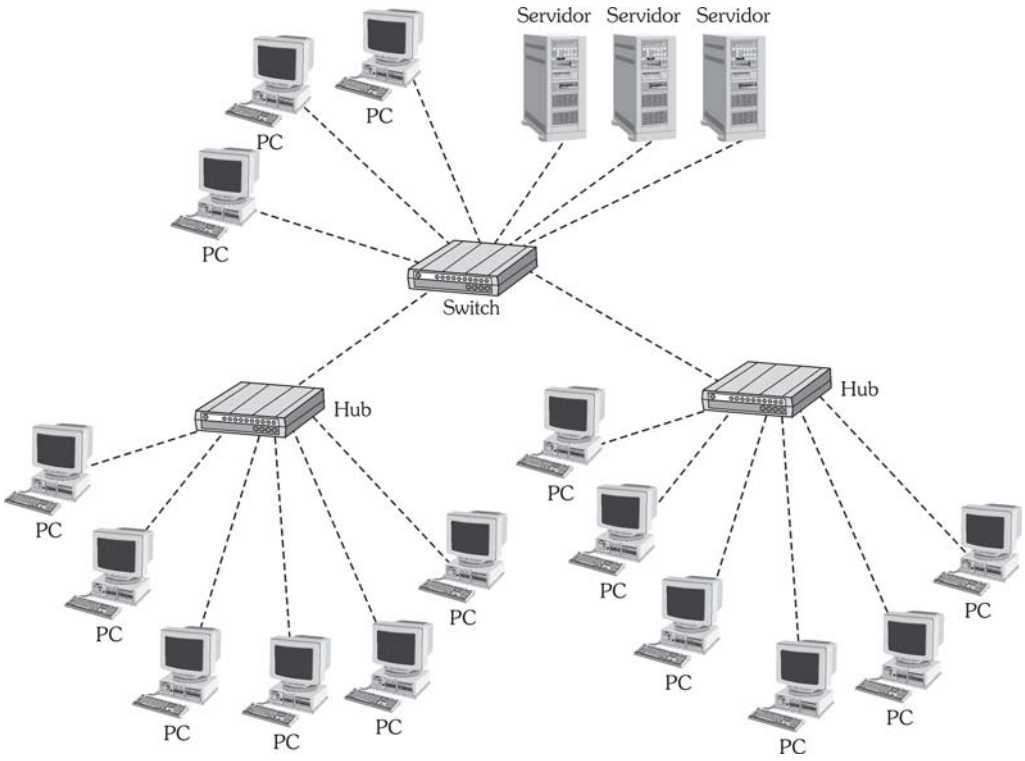


Um hub interligando todos os micros da rede.

Hubs são mais que suficientes para pequenas redes e mesmo redes de médio porte. Eles podem ser ligados entre si (cascateamento), porém quando as redes tornam-se maiores ou a distância entre as estações é grande, elas passam a necessitar de outros componentes, que oferecem melhor desempenho e mais recursos para o controle do tráfego na rede.

Switch

Funciona de forma similar ao hub e costuma ser um pouco mais caro. Em alguns casos substituem os hubs com vantagens, ao distribuir o sinal mais uniformemente. Tornam-se um desperdício em redes domésticas e em pequenos escritórios. São uma necessidade em redes empresariais de médio e grande portes, bem como nos laboratórios de informática. Também são utilizados para agrupar redes menores, como podemos ver no exemplo.



Exemplo de uso do switch em uma LAN.

Repetidor

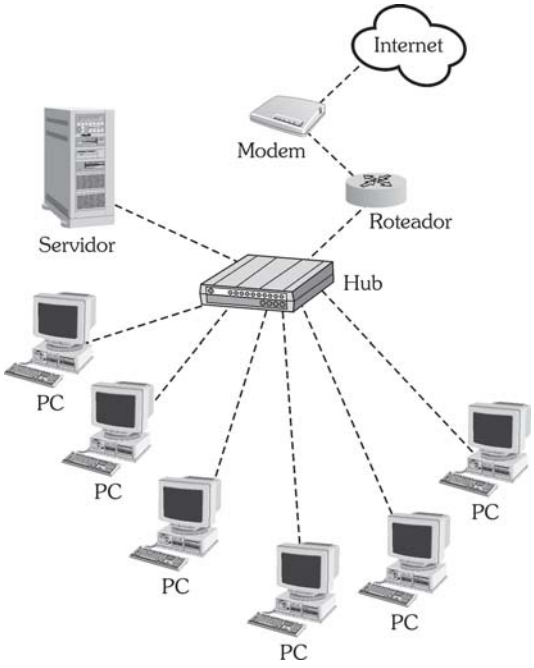
Realiza a ligação de duas redes de forma direta, usando a camada física do modelo OSI. Não possui qualquer tipo de tratamento no sinal.

Ponte ou Bridge

Uma ponte é um dispositivo que permite interligar duas redes idênticas, mas separadas por uma distância considerável, como entre prédios, bairros ou cidades. Pontes também são usadas para reduzir o fluxo de tráfego entre redes.

Roteador ou Router

O roteador funciona de forma muito semelhante à ponte, porém com mais recursos. Nos últimos meses têm se tornado cada vez mais populares, devido à expansão da banda larga e dos números IPs fixos cada vez mais baratos e acessíveis.



Exemplo de uso do roteador.

A lista seguinte descreve o uso mais comum dos roteadores:

- Interligar duas ou mais LANs distantes, formando uma WAN;
- Interligar uma LAN a uma WAN, como, por exemplo, a rede local da empresa à Internet;
- Interligar diferentes redes a uma rede principal;
- Em substituição às pontes (bridges);
- Controle de fluxo de tráfego entre redes.

Roteadores são como computadores sem teclado, mouse e monitor. São acessados via Telnet (um protocolo de acesso remoto) de qualquer terminal da rede. Um hacker que consiga acesso ao programa de configuração do roteador pode ter acesso a todo o tráfego de dados da empresa.

Softwares

Todas as versões atuais do Windows funcionam em rede. Este cenário é muito diferente do encontrado quando o Windows chegou ao Brasil. Conectar à rede um micro rodando Windows naquela época exigia bons conhecimentos de hardware e de programação. Só a partir do Windows for Workgroups ou 3.11 é que as coisas melhoraram (nem tanto).

Uma falha de interpretação muito comum é pensar que qualquer programa, ao ser instalado na rede, poderá rodar em qualquer um dos micros que estiver conectado. Para que isso ocorra, é necessário que o software tenha sido desenvolvido com esta funcionalidade. O mais comum em rede não é o compartilhamento de software e sim o compartilhamento de arquivos.

As novas tecnologias de computação distribuídas têm permitido aos fabricantes desenvolver softwares totalmente compartilhados. Já podemos encontrar no mercado empresas que oferecem aplicativos, como processadores de texto, planilhas e banco de dados, on-line. Já é possível entrar em um cibercafé e continuar a digitação de um texto que se encontra armazenado em um disco virtual. E o processador de textos não precisará estar instalado, já que pode ser disponibilizado on-line pelo fabricante.

Não foi nossa intenção o aprofundamento nos conceitos sobre hardware e instalação física das redes. Esta abordagem se destina aos que têm pouco ou nenhum conhecimento sobre redes (parte física) e também como uma rápida revisão para os que já estão há mais tempo na estrada. Isto fará com que todos, sem exceção, possam compreender os demais capítulos.

O administrador, teoricamente, não tem que se envolver com a parte física da rede (função do técnico em manutenção de hardware). Mas na prática, as pequenas e médias empresas esperam que ele se encarregue de todos esses pormenores, ainda que como supervisor.

O Que São Protocolos?

Protocolos são como idiomas e os responsáveis pela comunicação entre máquinas diferentes entre si. Um computador rodando Linux, por exemplo, pode se comunicar com outro rodando Windows, graças aos protocolos. Inclua nessa rede um Macintosh e a comunicação continuará possível. A função do protocolo é tornar possível essa comunicação entre redes e computadores diferentes.

O protocolo é um conjunto de regras que permite a conexão, roteamento, transferência e alguns serviços nas redes.

Pacotes

Uma das funções do protocolo é a divisão do arquivo a ser transmitido em pedaços menores, chamados de pacotes. Um pacote possui, além do fragmento da informação original, outras características: **CRC**, **Comprimentodo Pacote**, **Endereço do Emissor**, **Endereço do Receptor** e **Dados**.

Dividir os dados em pacotes foi a solução que os projetistas encontraram para otimizar o uso da rede. Se não houvesse esta divisão em pacotes, toda a rede teria seu funcionamento comprometido, a cada vez que um arquivo maior fosse transmitido. Cada máquina só poderia enviar seus dados após a primeira ter concluído a transmissão.

Cada pacote possui, além do fragmento da informação principal, os endereços do emissor e do receptor do pacote, seu comprimento e controle de erro, como o checksum e o CRC (*Cyclical Redundancy Check*).

Protocolos

Os principais protocolos de rede usados atualmente são:

IPX/SPX - os pacotes de dados IPX e SPX foram desenvolvidos para redes Netware (Novell®). Se você precisa se comunicar com redes Novell, habilite esse protocolo.

NetBEUI/NetBIOS - NetBEUI é um protocolo simples e eficaz usado principalmente em pequenas redes. Por não suportar o roteamento, não serve para uso em redes de grande porte, como a Internet por exemplo. Nos últimos anos, tem sido alvo de vírus e outros tipos de pragas virtuais. O NetBIOS é uma interface que faz parte do protocolo NetBEUI. Já foi o protocolo mais usado nas redes Microsoft.

TCP/IP - é o protocolo adequado a redes de médio e grande porte. Devido as suas características e robustez, é o protocolo ideal para uso na Internet. É o que oferece a maior compatibilidade quando precisamos conectar dispositivos diferentes entre si. Na verdade trata-se de um conjunto de protocolos que formam atualmente a base das conexões em rede.

1) Telnet - FTP - SNMP - SMTP
2) TCP
3) IP
4) UDP
5) NFS

1. **a) Telnet** - permite a conexão e controle de computadores a distância.
   b) FTP *(File Transfer Protocol/Protocolo de Transferência de Arquivos)* - permite a troca de arquivos entre computadores.
   c) SNMP *(Simple Network Management Protocol/Protocolo de Gerenciamento de Rede Simples)* - permite o gerenciamento de dispositivos de rede, coleta de informações de diagnóstico e o controle da configuração dos dispositivos da rede.
   d) SMTP (*Simple Mail Transfer Protocol/Protocolo de Transferência de Correio Eletrônico Simples)* - permite que os programas enviem e recebam mensagens de e-mail.
2. **TCP** (*Transmission Control Protocol*/Protocolo de Controle de Transmissão) - estabelece a comunicação confiável entre dois computadores.

3. **IP** (Internet Protocol/Protocolo Internet) - é o responsável pelo endereçamento e roteamento dos pacotes que irão trafegar pela rede. Trabalha em parceria com o TCP: um estabelece a conexão segura e o outro providencia a distribuição dos pacotes aos seus destinatários.
4. **UDP** (*User Datagram Protocol*/Protocolo de Datagrama do Usuário) - recebe informações do IP e as repassa a protocolos de nível superior, como o NFS.
5. **NFS** (*Network File System*/Sistema de Arquivos de Rede) - permite o uso de discos remotos e arquivos, como se estivessem no computador local. Aumentam a segurança e confiabilidade no acesso aos dados gravados em disco.

O TCP/IP permite ligações entre sistemas operacionais (MacOS, Windows 9.x, NT, Me, 2000, 2003, XP, OS/2, BSD, Linux, Unix, Netware, etc.) e arquiteturas diferentes (micros, mainframes, dispositivos portáteis com e sem fio, eletrodomésticos, etc.).

O TCP/IP é um conjunto de protocolos diferentes, mas relacionados entre si e que continuam a mudar e a ser definidos quase que diariamente.

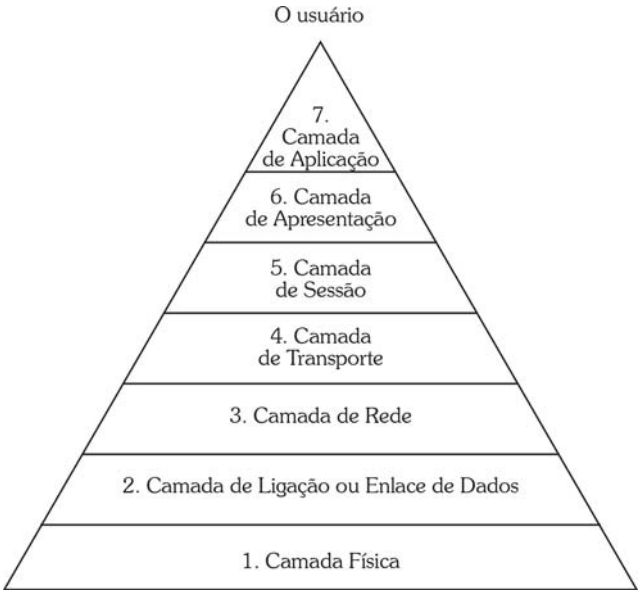
Conhecimentos de programação e do conjunto de protocolos TCP/IP é o que torna um hacker potencialmente perigoso.

O Que É o Modelo OSI?

Na década de 70, a ISO formou um comitê para desenvolver uma arquitetura mundial de comunicação de dados que permitisse a comunicação entre computadores de diferentes fabricantes.

O modelo OSI (*Open System Interconnection*/Sistema Aberto de Interconectividade) foi concluído em 1980 e aprovado em 1983, tanto pela ISO como pelo IEEE.

Atualmente o modelo OSI é a base para quase todos os protocolos de dados atuais, apesar das críticas que vem recebendo. Consiste em um modelo de sete camadas, cada uma representando um conjunto de regras específicas. Cabe a cada fabricante implementá-las em seus produtos e é o que tem sido feito. Com isto se garante a compatibilidade entre sistemas, independente do fabricante.



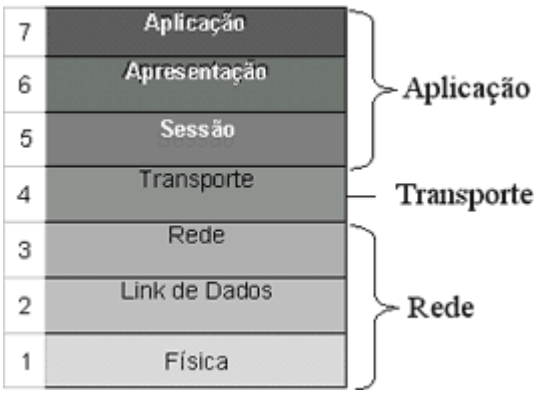
As sete camadas do modelo OSI.

Cada uma das camadas do modelo OSI, apesar de se comunicar com a camada adjacente, possui funcionamento e características próprias.

1. **Camada Física** - trata do hardware e demais dispositivos de rede, incluindo cabos, conectores, hubs, etc.
2. **Camada de Ligação ou Enlace de Dados** - é a responsável pelo recebimento dos dados da camada física e sua entrega à camada seguinte. Não sem antes serem devidamente identificados e passarem por um processo básico de correção de erros. De forma simplificada, podemos dizer que essa camada recebe os dados em seu estado bruto, identifica-os, corrigi erros e envia para a próxima camada, após inserir alguns caracteres de controle, necessários para que o sinal prossiga até seu destino final.
3. **Camada de Rede** - essa é a camada responsável pelo controle, distribuição e colocação das informações na rede. O protocolo IP faz parte dessa camada.

Nota: *As três camadas que acabamos de conhecer são as responsáveis pela remessa de pacotes através da rede. Elas controlam a remessa física de dados e normalmente estão reunidas no conjunto placa e driver de rede.*

4. **Camada de Transporte** - essa camada é a fronteira entre os dois grupos de camadas. Realiza o controle de fluxo entre a origem e o destino do pacote. A camada de transporte também é a responsável pela identificação de cada computador da rede como único e pela divisão das mensagens em partes menores, que são enviadas em seqüência e remontadas no destino. O TCP é um protocolo dessa camada.
5. **Camada de Sessão** - é a responsável pelo estabelecimento das sessões entre os micros da rede. Uma sessão deve existir antes que os dados sejam transmitidos. Podemos comparar uma sessão a uma conexão telefônica. Os interlocutores só podem estabelecer conversação após a ligação ter se completado. A camada de sessão também identifica alguns problemas que podem ocorrer, como ausência de papel na impressora ou falta de espaço no disco rígido.
6. **Camada de Apresentação** - é a responsável pela conversão de um tipo de representação de dados em outro. Um exemplo seria a compressão de dados ou criptografia.
7. **Camada de Aplicação** - esta é a camada que representa a interface com o usuário. Não são programas como o Word e o Excel que usam essa camada e sim o próprio sistema operacional. Outras aplicações que usam essa camada são: correio eletrônico, transferência de arquivos, login remoto, emulação de terminal, banco de dados distribuídos, etc.



Na página seguinte, temos a comparação do modelo OSI com um diagrama simplificado.

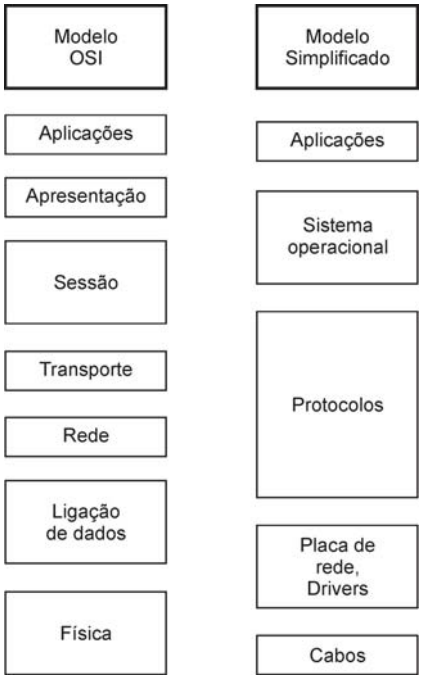


Diagrama OSI x Modelo Simplificado.

Tarefa Proposta

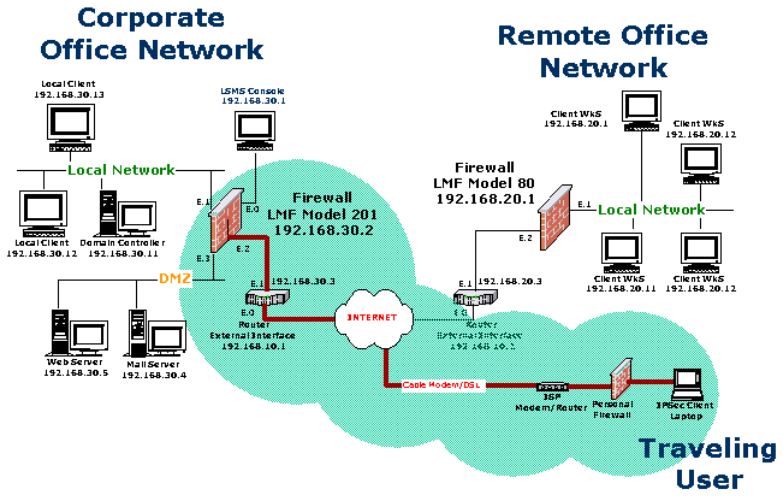
A tarefa proposta para melhor aproveitamento deste capítulo é a seguinte: manuseie os componentes de rede citados neste capítulo, principalmente se você nunca teve contato com placas de rede, cabos, conectores e hubs. Aproveite para verificar se o seu computador possui uma placa de rede. Todos os micros populares atuais contam com uma placa de rede. Basta verificar na traseira de seu micro se existe um conector RJ-45 fêmea.

Atenção para não confundi-lo com os conectores do modem que são semelhantes, mas um pouco menores. São do tipo RJ-11 e ficam lado a lado na placa de modem (LINE e PHONE).

Tem uma maneira de você ter contato com esse material sem precisar comprá-lo só para esta finalidade. Faça visitas a lojas especializadas em material de rede. Pergunte ao vendedor o que é cada peça. Solicite catálogos. Mostre-se interessado,

mesmo que não vá comprar nada. Um lojista de visão terá o maior interesse em ajudá-lo. Afinal, você é um cliente em potencial; e dos mais promissores.

Outra forma de realizar a tarefa do capítulo é pedir a alguém que trabalhe com redes para mostrar-lhe cada um dos componentes citados. Se você pretende invadir uma rede, precisa saber exatamente do que se trata.



Agora vamos aprender um pouco sobre TCP/IP. Eu sei que este capítulo ficou imenso. Prometo que os outros capítulos serão menores. Mas esta base é importantíssima para que você se torne um hacker de verdade. Nesta última parte do primeiro capítulo vamos saber:

1. Como funciona o TCP/IP.

2. Que são e como são formados os números IP.

3. Quem fornece os números IP.

4. Diferença entre IP estático e IP dinâmico.

5. As classes de endereçamento IP.

6. Identificar a rede e a máquina na rede através de seu número IP.

7. O que é IPv6.

8. O que é máscara de sub-rede.

9. A definição de resolução DNS.

10. O que é a resolução WINS.

11. O conceito de DHCP.

12. O que é um *gateway*.

13. A definição de *proxy server*.

Como Funciona o TCP/IP?

O TCP/IP foi desenvolvido nos anos 70 para conectar tipos diferentes de redes e computadores. O dinheiro que financiou a pesquisa do TCP/IP era público. Por isso ele se tornou um padrão aberto (não proprietário), o que permite que qualquer empresa o implemente em seus produtos de rede. Embora toda implementação do TCP/IP funcione, existem diferenças entre os protocolos TCP/IP de empresas diversas. Um exemplo é o NetBIOS embutido no TCP/IP da Microsoft e que não existe nas implementações UNIX.

O TCP/IP é o idioma da Internet e na verdade é um conjunto de protocolos que dá suporte a três aplicativos essenciais: acesso remoto (Telnet), transferência de arquivos (FTP) e e-mail (SMTP).

Rede Comutada de Pacotes

As informações trafegam por uma rede através de pacotes. Esses pacotes são enviados, não importando a ordem em que chegam ao seu destino, reorganizados e remontados. Caso algum pacote esteja corrompido ou mesmo não seja recebido, ele será solicitado novamente.

O TCP (*Transmission Control Protocol*/Protocolo de Controle de Transmissão) faz a coleta dos dados e seu particionamento em pacotes. Cada pacote recebe caracteres de controle de erros do tipo soma de verificação (*checksum*).

O IP (*Internet Protocol*/Protocolo Internet) é o responsável pelo endereçamento dos pacotes. Se você considerar cada pacote como se estivesse dentro de um envelope, é o IP que faz o endereçamento, lembrando que todos os pacotes com a mesma informação seguirão para o mesmo endereço de destino.

Os roteadores que, como já vimos, também servem para interligar redes, ao receber os pacotes, determinam o melhor caminho até o destino final. Não importa o caminho que cada pacote tomou nem a ordem em que chegam. No destino, o TCP se encarrega de reuni-los novamente, a fim de obter a informação original. O extravio ou a corrupção de algum pacote faz com que ele seja requisitado novamente.

O Endereçamento IP

Para que o pacote chegue ao seu destino, é necessário o endereço do destinatário. Enquanto em nosso dia-a-dia usamos endereços formados por nomes e números, os computadores utilizam um endereçamento numérico, chamado de endereçamento IP. O endereço IP ou número IP é um conjunto de quatro números separados por pontos.

207 . 234 . 129 . 65

Exemplo de endereço IP ou número IP.

Quem Fornece o Endereço IP?

Em nosso mundo os endereços são criados pelos nossos governantes. Você passa a ter um endereço quando ganha ou adquire um imóvel, quando aluga ou se hospeda, ou ainda, quando se acoita com alguém.

Os endereços IP são administrados pela InterNIC que os distribui aos órgãos e empresas ligados à Internet, como as concessionárias dos serviços de telecomunicações, provedores de grande porte, etc.

Em uma rede particular, como de uma empresa ou residência, é possível usar qualquer endereço IP válido. Quando você acessa a Internet através de um provedor, ele "empresta" um número IP durante todo o tempo que durar a sua conexão. Se a conexão é desfeita, ao ser refeita, seu número IP muito provavelmente terá mudado.

Empresas que queiram hospedar o próprio site necessitam de números IP fixos. Esses números são comercializados como parte dos serviços de conexão ao *backbone*.

IP Estático x IP Dinâmico

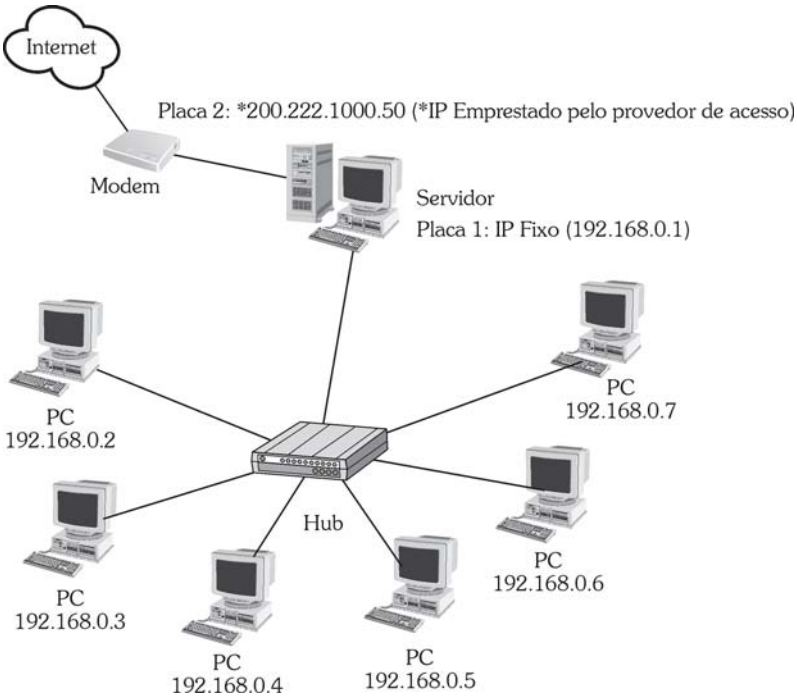
Os IPs estáticos ou IPs fixos são usados em redes locais para identificar os servidores da rede. Nada impede que toda a rede seja formada por máquinas usando IP fixo, sendo o mais comum adotá-lo apenas para os servidores.

Os IPs dinâmicos são usados nos clientes da rede e também quando pretendemos acessar a Internet através de uma conexão discada ou dedicada, do tipo banda larga.

Computadores podem ter mais de um número IP. Um exemplo do dia-a-dia é um servidor que necessita de um IP fixo para a rede interna, mas também utiliza um IP dinâmico, emprestado pelo provedor, para o acesso à Internet.

Na figura abaixo temos um exemplo de servidor com duas placas de rede, sendo uma com IP fixo para a rede interna e a outra configurada com "obter o IP automaticamente" para se conectar à Internet. O IP será "emprestado" pelo provedor de acesso e pode mudar a cada conexão.

Ainda sobre o exemplo da figura, fixamos o IP de todas as máquinas cliente da nossa rede interna. Não haveria problema se os clientes fossem configurados para "obter o IP automaticamente".



Servidor usando IP fixo para a rede interna e IP dinâmico para a Internet.

Classes de Endereçamento

Não é só saber como são distribuídos os endereços IP. Também precisamos saber as regras para a sua composição. O IP é um número de 32 bits, formado por quatro grupos de números de 8 bits, que varia entre 0 e 255 (2^8).

Existem cinco classes de endereçamento IP, identificadas pelas letras de **A** a **E**. As classes D e E são de uso específico. Provavelmente a mais usada por você é a classe C.

Classe	Endereço Mais Baixo	Endereço Mais Alto
A	1.0.0.0	127.0.0.0
B	128.1.0.0	191.255.0.0
C	192.0.1.0	223.255.255.0
D	224.0.0.0	239.255.255.255
E	240.0.0.0	255.255.255.254

Faixas de endereçamentos IP distribuídos por suas classes.

Identificação da Rede e da Máquina na Rede

Uma parte do endereço IP identifica a rede e a outra parte representa o nó da rede ou host. Lembre-se que nó e host são palavras usadas para definir qualquer computador de uma rede.

Na classe A apenas o primeiro número identifica a rede e os demais representam a máquina. Na classe B os dois primeiros números identificam a rede e os dois últimos representam a máquina. Finalmente na classe C, os três primeiros números identificam a rede e apenas o último representa a máquina.

O IPv6

A expansão da Internet vai fazer com que não haja números IPs suficientes para todos se conectarem. Ainda mais se levarmos em conta que a conexão não se restringe mais a computadores PC: telefones celulares, geladeiras, microondas e até câmeras de vídeo já saem de fábrica com conexão à Internet. Para solucionar essa limitação do protocolo atual de 32 bits, foi desenvolvido um novo sistema

de numeração IP, chamado IPv6, com números de 128 bits. Foge ao escopo da obra detalhar o IPv6, mas você não encontrará dificuldades para obter informações pormenorizadas na própria Internet.

Como Escolher a Numeração IP da Rede

Você só pode escolher números IP para redes internas. As conexões com a Internet usam o número IP atribuído automaticamente pelo provedor de acesso.

Teoricamente você pode escolher qualquer número IP válido para uso em uma rede interna, mas na prática usamos um grupo de números especialmente destinados às redes internas. Com o uso dessa faixa de endereços obtemos a vantagem de os roteadores reconhecerem-na como sendo de uma rede interna e as chances de conflito com outros endereços ficam bastante reduzidas.

Classe	Endereço mais Baixo	Endereço mais Alto
A	10.0.0.1	10.255.255.254
B	172.16.0.1	172.31.255.254
C	192.168.0.1	192.168.255.254
D	Não Usar	
E	Não Usar	

Sugestão de faixas de endereçamento IP para uso em redes particulares.

Máscara de Sub-Rede

Outro termo que você vai encontrar quando estiver configurando dispositivos de rede é a MÁSCARA DE REDE ou MÁSCARA DE SUB-REDE. São vários os motivos pelos quais os endereços de sub-rede devem ser utilizados:

Quando interligamos redes de tecnologias diferentes;

Para exceder o número de máquinas por segmento físico;

Para reduzir o tráfego de pacotes.

A tabela seguinte exibe números padrões para MÁSCARA DE SUB-REDE:

Se você estiver usando esta classe	Usar este número como máscara
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0

Números padrões para MÁSCARA DE SUB-REDE,

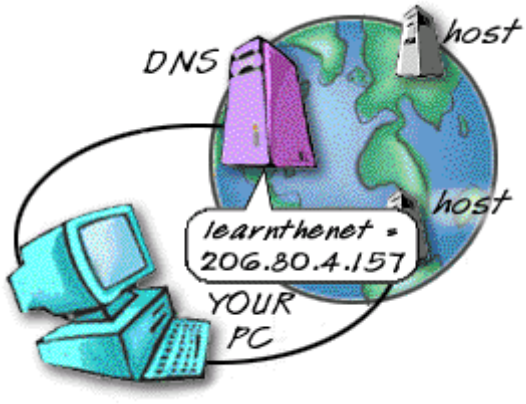
conforme a classe de endereçamento IP adotada.

DNS (*Domain Name System*/Sistema de Nomes de Domínio)

Cada micro na Internet possui um número IP, próprio ou emprestado. Mas você deve concordar que lembrar de números como 207.234.129.65 ou 65.251.83.54 para acessar o site *www.cursodeflores.com.br* e *http://Prosperidade.Net*, respectivamente, não é nada agradável.

Na verdade é inviável a memorização de números IP. A Sun encontrou uma solução amigável para a questão: manter computadores com listas de nomes e a devida identificação de seu número IP. Esta tecnologia é chamada de DNS e é a responsável pela conversão do nome *www.microsoft.com* em seu IP correspondente: 207.46.249.27.

Logicamente, mais de um nome pode ser atribuído a um IP. O serviço DNS faz a leitura do cabeçalho e identifica o nome que foi digitado na área de endereço do navegador, exibindo a página correta. É dessa forma que os provedores de hospedagem trabalham. A partir de um par de números IP hospedam dezenas, centenas e até milhares de sites na mesma máquina.



Resolução WINS (*Windows Internet Name Service*/ Serviço de Nomes Internet do Windows)

A resolução WINS é o serviço de nomes do protocolo NetBIOS. Através da resolução WINS os clientes de uma rede local podem ser localizados a partir do nome da máquina.

Número IP	Identificação amigável da máquina
192.168.0.1	\\Matriz

A resolução WINS torna a identificação da máquina mais amigável.

Podemos perceber que é muito mais fácil gravar o nome da máquina do que seu número IP. Outro problema na memorização do número IP é que, caso esteja habilitada a opção "obter IP automaticamente", a cada conexão o IP pode ser alterado. Já com o nome isso não ocorre.

O NetBIOS usa um servidor chamado Windows Internet Name Service (WINS). Já o Winsock (TCP/IP) usa o servidor Domain Name System (DNS). O mesmo "nome" é visto de maneira diferente pelo WINS e pelo DNS:

DNS	WINS
alunos.cursodehacker.com.br	\\Alunos

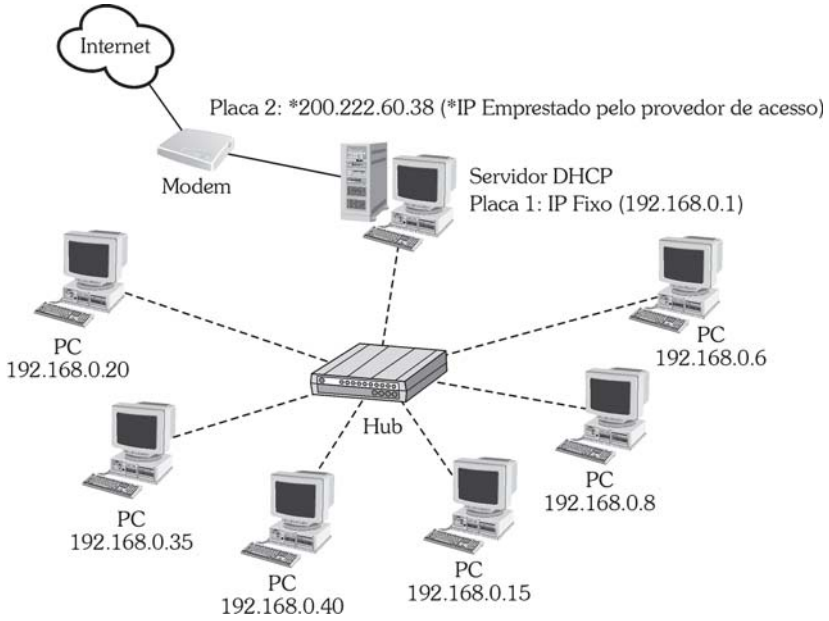
Como o DNS e o WINS enxergam os nomes na rede.

Uma rede totalmente baseada em Windows Server 2000 ou 2003 não necessita ter habilitada a resolução WINS. O *Active Directory* a substitui com vantagens.

DHCP (*Dynamic Host Configuration Protocol*/ Protocolo de Configuração Dinâmica de Máquinas)

Podemos configurar os computadores de uma rede com IP fixo ou não. Vimos que só os servidores necessitam obrigatoriamente do IP fixo. Quando não usamos o IP fixo, necessitamos de um sistema de distribuição automática de números IP. O serviço DHCP faz essa distribuição.

Quando precisamos compartilhar uma conexão à Internet, configuramos o computador que possui o modem como servidor DHCP. Podemos usar soluções de terceiros, ás vezes com mais recursos e facilidade de uso.



Neste exemplo, as máquinas clientes receberam seus IPs do servidor DHCP.

Gateway

Gateway é o dispositivo (software ou hardware) que permite a conversão de protocolos entre redes e computadores diferentes. O Windows 2003 pode ser configurado como gateway, conforme veremos nos capítulos posteriores.

Proxy Server

O *proxy server* ajuda a impedir que usuários não autorizados da Internet se conectem à rede da empresa. Ele permite ao administrador controlar quem acessa a rede da empresa e quais serviços essas pessoas utilizam. A Microsoft possui o Microsoft Proxy Server que, uma vez instalado, funciona como uma barreira (*firewall*) entre a rede da empresa e a Internet. Além disso, o *proxy server* pode manter armazenada uma cópia das páginas visitadas (*cache*), tornando mais rápida a navegação pelos endereços mais acessados na Internet.

Capítulo 2:

Security

Capítulo 2:

Security

Objetivos Deste Capítulo:
Após concluir a leitura deste capítulo você deverá ser capaz de identificar quais são os principais problemas de segurança na Internet e como evitá-los. Também saberá como tornar o seu micro uma fortaleza. Como ter uma atitude que impeça ou dificulte ações hacker. E se recuperar de desastres, ficando imune as consequências de qualquer ataque ou invasão.

Segurança na Internet

A cada dia, mais e mais pessoas se conscientizam da necessidade de segurança e proteção na Internet. E se depender do tipo de E-Mail que eu recebo aqui no Curso de Hacker, também tem gente interessada em descobrir como se aproveitar dessas falhas.

Quando pensamos que a estratégia de defesa é forte o bastante para conter qualquer ataque ou invasão, lá vem um hacker qualquer provando que não é bem assim. Veja o caso da indústria de software. Aparentemente tudo estava sob controle. Principalmente após as experiências com os vírus *Melissa*, *I Love You*, *Nimda*, *Code Red*, *Sircam*, *Klez*, *Bug Bear*, *Blaster*. Mas eis que surge o *MyDoom*, explora falhas ingênuas no código do Windows e voltamos a estaca zero. A pergunta é: _*"Qual será a próxima falha a ser explorada?"*

A massificação dos telefones celulares GSM, a popularização das redes sem fio (*Wi-fi*), a chegada da TV digital que entre outras coisas, permitirá o acesso a Internet via TV, a obrigatoriedade das empresas de telefonia implantarem pontos públicos de acesso a Internet, a adoção em massa da plataforma Linux por empresas e órgãos públicos. Tudo isto já acontecendo. Entre agora e 2008.

Acompanhe meu raciocínio: celulares GSM permitem download de programas e navegação na Internet. Um campo aberto para vírus, trojans e *phishing scam*. Os pontos de acesso público a Internet e a Internet via TV digital, permitirão a população que nunca teve acesso a um computador, navegar na Internet.

O governo federal pretende transferir para a Internet o máximo de serviços

que conseguir. Tudo para que o cidadão não precise se deslocar até o posto de atendimento. Há cidades onde não existe posto de atendimento. Ou o cidadão se desloca até a cidade mais próxima que tenha posto ou aguarda a ida de um posto móvel até a cidade onde mora. Todas estas pessoas estarão a mercê dos golpes que podem ser praticados pela Internet.

Os empresários já sentiram estas mudanças na pele faz algum tempo. Vários procedimentos que uma empresa precisa cumprir no seu dia-a-dia só estão disponíveis na Internet. Um contador que se estabeleça atualmente, se não tiver acesso a Internet, não consegue atender todas as solicitações dos seus clientes. Talvez não consiga nem se manter, já que vai depender de alguém para executar operações importantes.

A moda Linux vai trazer vários benefícios. Além de boas oportunidades de trabalho, em um primeiro momento, será uma tragédia quando o assunto for segurança. Não quero defender a Microsoft, mas parte da má fama que seus produtos tem é devido a usuários despreparados. É muito fácil instalar um programa da Microsoft. São programas que se instalam praticamente sozinhos. O difícil, e é aí que a porca torce o rabo, é configurar um servidor corretamente, tornando-o seguro. O pessoal do Linux, dada as exigências do sistema, são em sua maioria profissionais com conhecimento profundo do sistema e de redes também. Não é qualquer um que coloca uma rede linux para funcionar. Só que com a adoção indiscriminada do Linux, não haverá no mercado tantos profissionais para dar conta da demanda. Vai acontecer como ocorreu na telefonia. Um bando de curiosos vai fazer curso de fim de semana e se apresentar como autoridade em redes Linux. Com certificação e tudo. Aí nos veremos que o Linux também não é isso tudo que dizem dele e vamos nos deleitar com invasões Linux, talvez em pé de igualdade com as invasões Windows.

Então não pense que o problema de segurança já é caso encerrado e as ondas de vírus, trojans e scams acabou. Ainda tem muito trabalho pela frente e neste mar de possibilidades, você poderá dar grandes contribuições para tornar a Internet mais segura.

Comentários Sobre Este Capítulo

Como a maioria dos leitores deste livro também são leitores do meu outro livro que só trata da segurança na internet; e como sei, pelos comentários que antecederam o lançamento deste livro, que o maior interesse é por conhecer as técnicas de ATAQUE e INVASÃO. Não me estenderei muito nos assuntos sobre segurança. Neste capítulo abordarei os aspectos práticos da defesa, deixando o embasamento teórico de cada assunto por conta do site da ABSI (*www.absi.org.br*) e do livro *Proteção e Segurança na Internet* (*www.editoraerica.com.br*).

O Primeiro Problema de Segurança: Vírus

O primeiro problema de segurança com o qual se depara o usuário é o vírus. E basta estar com o antivírus instalado. Sabemos de casos e mais casos em que mesmo com a presença do antivírus, o vírus ou outra praga virtual se alojou no computador.

Um vírus, como você já deve saber, é um programa de computador. Programas de computador são feitos por programadores. Por que alguém vai dedicar horas, semanas ou meses estudando um sistema só para criar um programa que é nocivo e destrutivo? Só por diversão? Creio que não.

Os supostos motivos são vários. Vai desde a intenção deliberada de prejudicar a concorrência, passa pela suspeita dos vírus fabricados pelos mesmos fabricantes dos programas antivírus, até a pura maldade. Estes motivos são apenas suposições. Em alguns países vírus dá cadeia. Então não vamos ver com frequência programadores expondo abertamente a autoria de suas crias. Digo o mesmo das estatísticas hacker. Não dá prá ter certeza se no Brasil a maior parte dos hackers é formada por adolescentes. Acreditamos que seja, por ser uma faixa etária em busca de limites e sem compromisso com casa ou trabalho. Basta um coleguinha na escola dizer que 'hackeou' para a turma toda querer fazer o mesmo. Também acreditamos serem jovens de classe média, pelo simples fato de ser este o perfil do adolescente que tem computador e acesso a Internet. Quem mora nos grandes centros não percebe, mas menos de 10% da população brasileira tem acesso regular a Internet.

Especula-se que os prováveis motivos da criação de vírus seja:

. desacreditar a concorrência e seu produto, seja ele um software, um antivírus ou um sistema operacional

. pura maldade

. experiências, incluindo novas formas de marketing. Não tem a ver com o termo marketing viral, mas as empresas tem interesse em uma forma de divulgação que possa se aproveitar da eficácia do vírus em varrer o globo em poucas horas.

. obter proveito financeiro mediante fraude. Alguns vírus tem por propósito roubar senhas e enviar ao seu criador.

. se tonar uma celebridade. Acredite se quiser, mas tem gente que não se importa em ser presa pela distribuição de vírus), desde que isso a torne famosa. São apenas suposições sem condições de comprovação, a não ser pela intenção implicita de cada novo vírus que aparece.

As primeiras gerações de vírus se alojava no setor de boot dos discos rígidos e disquetes, tornando impossível iniciar a máquina infectada até a remoção do código viral.

Depois tivemos a onda de vírus de arquivos, cujo principal propósito era corromper os arquivos infectados.
Em seguida surgiram os vírus de macro que infectavam os documentos gerados pela suíte de aplicativos da Microsoft, como os do Word e Excel.
Devido a popularização das redes locais, se tornou comum o vírus especialistas em atacar vulnerabilidades de redes. Esta fase teve o seu auge durante o ano 2000.
Atualmente, os vírus dedicados a redes locais passaram a não conhecer limites, se propagando a partir do aproveitamento de antigas falhas nos programas de E-Mail da Microsoft.
Supõe-se que a próxima grande fase dos vírus sejam ataques aos sistemas de telefonia celular com tecnologia GSM. Isto está previsto para os primeiros meses de 2005.
Embora tenham causado grandes prejuízos a alguns setores, devemos agradecer aos criadores de vírus pela sua parcela de contribuição para o aumento da segurança na Internet. Empresas passaram a ter políticas mais austeras em relação ao uso do E-Mail corporativo e as pessoas passaram a ter mais cuidado na hora de abrir um arquivo anexado a um E-Mail.

Removendo Vírus

Até uma criança já sabe que para remover um vírus precisamos do programa antivírus, que antigamente era chamado de vacina. A dificuldade dos usuários atuais é confiar no antivírus, já que não são poucos os casos de vírus alojados em sistemas, mesmo com a presença de antivírus. Aqui mesmo neste livro vamos ver como tornar um trojan invisível a antivírus. Então, diante disto, o que fazer para aumentar a confiança no antivírus?
Algumas regras devem ser seguidas:

1ª REGRA - TER o antivírus
2ª REGRA - MANTER o antivírus ATUALIZADO
3ª REGRA - MANTER a BASE DE VÍRUS atualizada

Você pode até não acreditar, mas tem muito usuário doméstico que usa seu micro sem qualquer tipo de proteção contra pragas virtuais. Recentemente uma baiana se espantou por eu ter tanta coisa no HD e não perder nada. Segundo ela, seu micro só vivia perdendo arquivos. Depois de uma olhadinha, constatei a presença de vírus de todos os tipos, incluindo trojans e spywares. Não é a tôa que vivia perdendo tudo. Assim como ela (Ôpa!), deve ter muita gente na mesma situação.
Mas não basta cumprir a primeira regra. O antivírus deve ser atualizado. Não estou falando só da base de dados de vírus, mas da versão do antivírus também. A tecnologia do Norton 2004 é superior a do Norton na versão 2002. As versões

mais recentes dos programas antivírus são melhor preparadas para as inovações dos vírus atuais. E finalmente, a parte mais vilipendiada no que diz respeito a proteção antivírus, é a falta de atualização da base de dados de vírus. Já foi tempo que podiamos contar com as atualizações de base de dados que eram distribuidas nas revistas com CD-Rom. A defasagem de dois a três meses não interferia na eficácia da vacina. Atualmente, os antivírus já se programam para buscar por atualizações para a base de dados semanalmente.

Qual Antivírus Usar?

Não vou indicar indicar nenhum antivírus como sendo melhor ou pior que o outro. Esta escolha terá que ser sua. Não fiz testes comparativos o suficiente e que me permitam recomendar com lisura um antivírus em particular. Segue abaixo a lista dos principais antivírus para que você possa tirar suas próprias conclusões:

ANTIVÍRUS GRATUITOS

AVG 6 - *www.grisoft.com/us/us_dwnl_free.php*
Avast! - *www.avast.com*
eTrust (com firewall integrado) **-** *www.my-etrust.com/microsoft/*

ANTIVÍRUS PAGOS

Norton Anti Vírus - *www.symantec.com.br*
McAfee VirusScan - *http://br.mcafee.com/*
NOD 32 - *www.nod32.com.br/*
Panda - *www.pandasoftware.com/com/br/*
AVG 7 - *www.avgbrasil.com.br/*
PC-Cillin - *www.trendmicro.com/br/home/personal.htm*

ANTIVÍRUS ON-LINE

Symantec - *www.symantec.com.br/region/br/ssc/*
Panda - *www.pandasoftware.com/com/br/*
McAfee - *br.mcafee.com/root/package.asp?pkgid=113*
Trendmicro (PC-Cillin) - *http://housecall.trendmicro.com/*
Zone Labs (mesmo fabricante do Zone Alarm):
www.zonelabs.com/store/content/promotions/pestscan/pestscan3.jsp

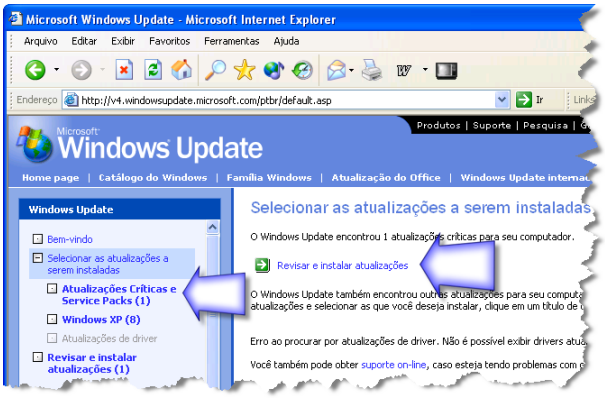
Atualização do Sistema e Windows Update

O risco que corremos na Internet não se limita aos vírus. Antes fosse. Algumas das correções que o antivírus faz em seu computador, são correções de falhas no

sistema operacional. Ou seja, você deve se preocupar também em baixar as ultimas atualizações disponíveis para o seu sistema operacional.

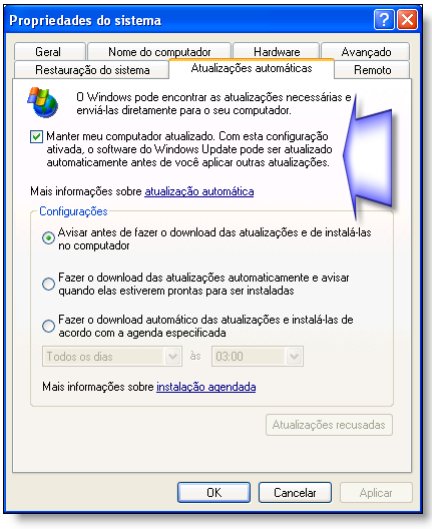
Para os usuários do Windows podemos contar com o *Windows Update* que pode ser acessado como opção disponível ao clicar no botão **INICIAR**. O próprio sistema operacional costuma avisar que existem atualizações a serem baixadas. O mais comum, principalmente para os usuários de conexão discada, é deixar essa atualização para depois. Só que o depois nunca chega e fica mais um micro vulnerável na rede.

Existem casos que o usuário nem pode se dar a este luxo. O Windows 2000 e XP por exemplo, caso se conectem a Internet após a primeira instalação, não duram nem dez minutos sem baixar um vírus que os impeça de funcionar a partir de então.



Mesmo com todas as críticas que a empresa recebe, o serviço de Windows Update prestado pela Microsoft pode livrar o usuário do Windows de muitas dores de cabeça.

A frequência necessária depende da sua atividade on-line. Os usuários de banda larga e *hard user* devem deixar esta opção no automático. O antivírus também pode e deve ser programado para buscar por atualizações automaticamente.



Configurações da Rede

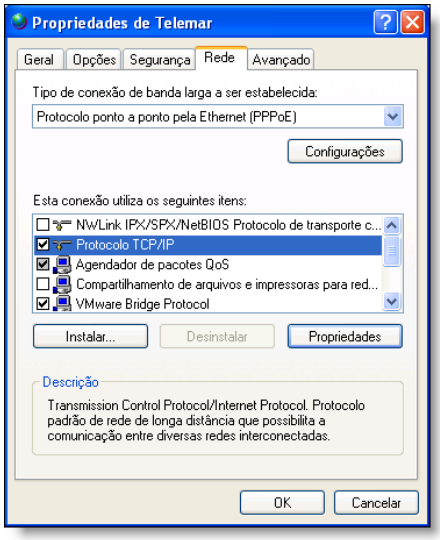
Uma vez trabalhei em uma empresa onde o responsável pela rede, o Samuca, habilitava em cada máquina, todos os protocolos possíveis. E para 'facilitar', também compartilhava o disco rígido inteiro. Com isto, segundo ele, não só era mais fácil as máquinas da rede se enxergarem, como as pessoas poderiam guardar seus documentos em qualquer lugar do HD e recuperá-los de qualquer máquina.

Tudo ia bem até que chegar os vírus que se aproveitavam das falhas em alguns protocolos de rede para a empresa parar por quase uma semana. Até eu que só cuidava da programação fui chamado para ajudar a resolver os problemas da rede. Só que além do vírus, também havia o problema da configuração da rede que estava bastante vulnerável. Este é um daqueles casos em que técnicos em manutenção viram gerentes de rede e metem os pés pelas mãos.

Pouco tempo depois Samuca foi demitido. Um parêntesis: Samuca é gay assumido. Isto é um particular dele. Acho que cada um faz o que quer e o que tem vontade com seus recursos biológicos. Mas o chefão não pensava assim e não via com bons olhos a amizade que o Samuca tinha com seu próprio filho, este sim, gay não assumido (pelo menos aos olhos do pai). Abri este parêntesis para que você perceba que a demissão não foi pela incompetência. Profissionais despreparados, fruto dos baixos salários, são os maiores aliados do hacker. Depois que o Samuca foi mandado embora eu fui convidado para reorganizar a rede.

Um dos problemas que você vai encontrar ou talvez o esteja vivenciando sem ter consciência disso, é o uso de protocolos, ligações e compartilhamentos desnecessários em sua máquina. Mesmo que seja um computador único, ele acaba fazendo parte de uma rede quando você se conecta a Internet.

Na maioria das vezes o protocolo TCP/IP é suficiente para a rede funcionar adequadamente. Redes heterogeneas talvez necessitem do NetBIOS e IPX. A escolha do procolo em uma rede CLIENTE x SERVIDOR depende também de como este servidor está configurado. Quanto a compartilhamentos, usuários do Windows 98 não tem qualquer tipo de proteção, mesmo quando colocam senha no compartilhamento. O melhor é não compartilhar nada, ou só compartilhar no momento em que for usar o compartilhamento e logo em seguida, descompartilhar.



O que você deve se perguntar para verificar a segurança da sua máquina ou rede é:

_Tenho compartilhamentos de discos, pastas ou impressoras?

_Se houver compartilhamentos, estes compartilhamentos são mesmo necessários?

_Meu sistema de arquivos é FAT ou NTFS (mais seguro)?

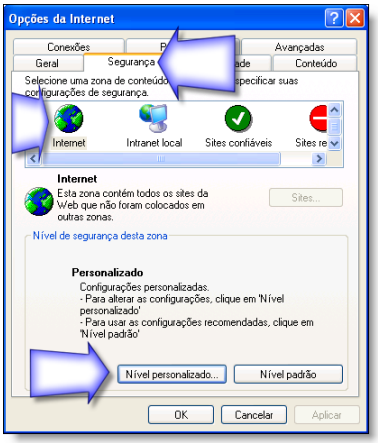
_Preciso de todos os protocolos que estão instalados em minha máquina? Porque?

_Existe alguma ligação entre protocolos e recursos que seja desnecessária?

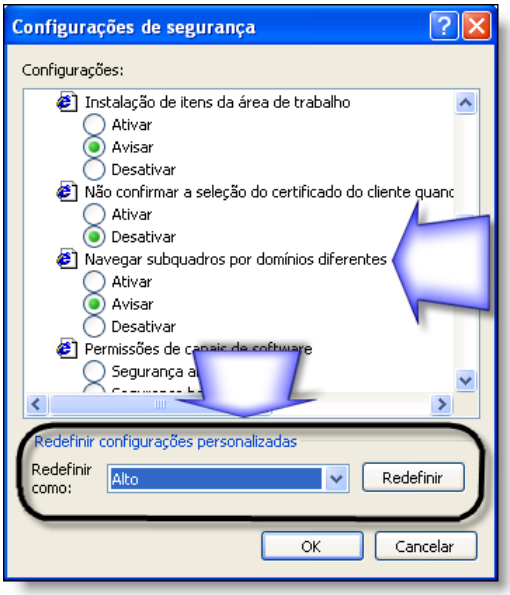
Configuração do Internet Explorer e Outlook

A configuração padrão do Internet Explorer e do Outlook Express, os dois mais usados programas para navegação na Internet e leitura de E-Mails respectivamente, pode ser melhor ajustada para fornecer maior segurança ao usuário.

No caso do Internet Explorer, acesse na **BARRA DE MENUS** as opções **Ferramentas -> Opções da Internet -> Segurança**:

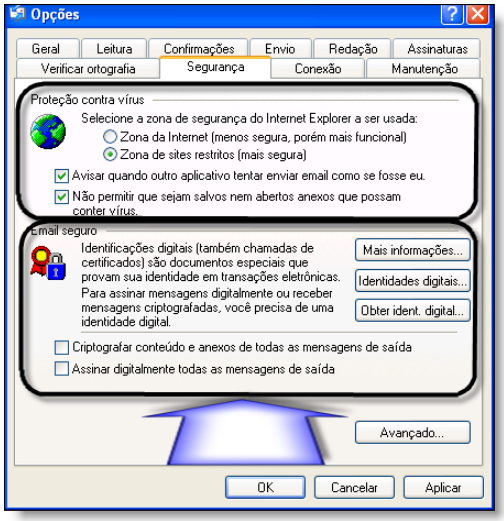


Vários ajustes podem ser feitos para aumentar o nível de segurança. Estude cada um deles e veja qual se aplica ou não ao seu grau de risco:

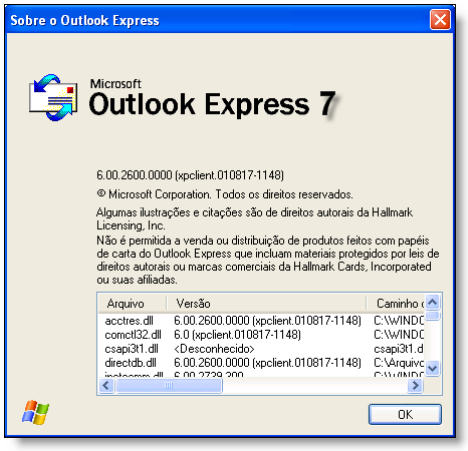


O Outlook Express também possui opções de configuração que permite o aumento da segurança na recepção e envio de E-Mails. É altamente recomendável que você escolha um antivírus com integração ao E-Mail. Os principais antivírus do mercado possuem este recurso.

As opções de configuração do Outlook Express podem ser acessadas pela **BARRA DE MENUS** usando a sequência **Ferramentas -> Opções -> Segurança**:



Entre os ajustes que podem ser feitos, está o que permite barrar todos os arqivos anexados a uma mensagem automaticamente. Se houver algum anexo que realmente seja do seu interesse receber é só voltar a esta opção e desmarcá-la. Os anexos ficam presos a mensagem, porém inacessíveis. Outra opção igualmente útil é a que não permite a programas enviar E-Mails sem o seu conhecimento.



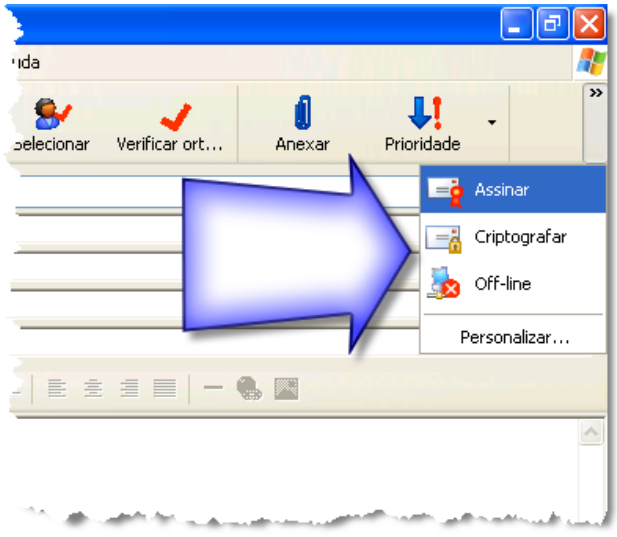
De nada adianta todos esses cuidados se a sua versão do Internet Explorer e Outlook Express for antiga. Não aceite em seu micro menos que a versão 6. Para saber qual versão está instalada, vá a opção *Ajuda* na barra de menus e clique em Sobre.

Na parte de baixo da janela com as opções de segurança, podemos assinar digitalmente e criptografar todas as mensagens enviadas. Para obter uma assinatura digital, clique no botão *Obter Identidade Digital*. Você será redirecionado a uma página da Microsoft com várias empresas autorizadas a distribuir assinaturas

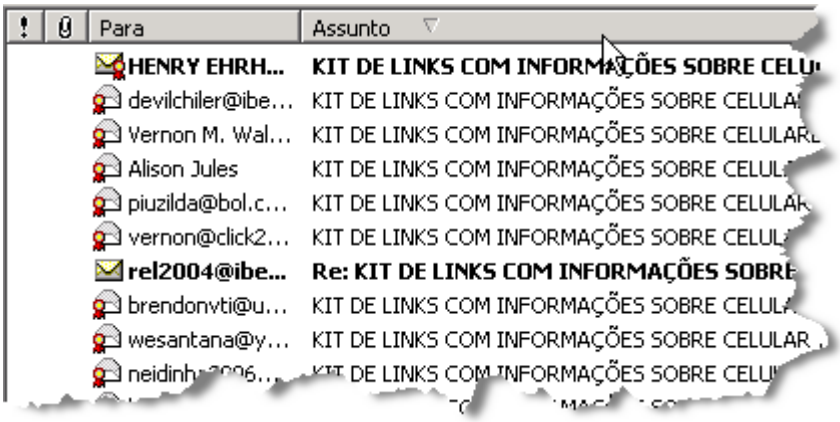
digitais. Não temos no mundo real os cartórios que reconhecem a sua assinatura em títulos e documentos? Também na Internet temos empresas que atestam ser a sua assinatura ou site, realmente pertencentes a você.
A maioria destes serviços é pago. Mas encontramos uma empresa que oferece o serviço de assinatura digital para E-Mail gratuitamente:

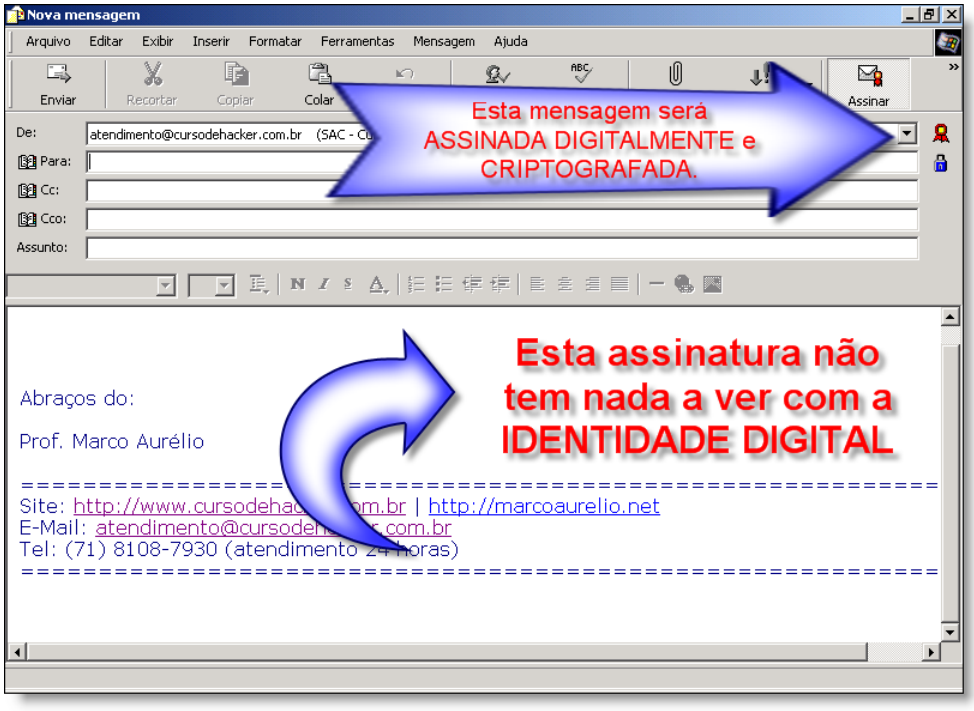
www.thawte.com

Para obter um certificado gratuito para ser usado com seu E-Mail, faça assim:
1. Acesse o endereço *www.thawte.com/email/*
2. Clique no link que aparece no primeiro parágrafo da página com o título ***Click here***
3. Será aberta uma janela *pop-up* com os termos e condições de uso.
4. Após aceitar as condições de uso do serviço (se é que alguém lê estes contratos), será aberta a janela *Novo Registro no Sistema de Certificados Pessoais Thawte* para que você preencha com seus dados. Não se preocupe que, apesar do site estar em inglês, a página identificará o idioma do seu sistema operacional e exibirá as informações em português.
5. Siga com o preenchimento dos seus dados pessoais até concluir o cadastro.
6. Feito estes procedimentos, você receberá um E-Mail o qual lhe permitirá ativar a certificação em todas as mensagens enviadas por você. Para assinar digitalmente as mensagens a partir daí, basta clicar no botão *Assinar* da *barra de ferramentas* do Outlook Express.



Não confunda assinatura de E-Mail com ASSINATURA DE IDENTIDADE DIGITAL. A assinatura de E-Mail é aquela que entra ao final de cada mensagem. Já a assinatura de identidade digital é aquela que garante a procedência do E-Mail. Muitos de vocês já devem ter recebido uma das minhas mensagens assinadas digitalmente. As mensagens assinadas digitalmente exibem no ícone do envelope um símbolo parecido com o de honra ao mérito.





Proteção do Micro Local

A proteção e segurança de um sistema não se restringe a softwares e configurações. O roubo, furto ou avaria também deve ser motivo de preocupação e precaução. Não são poucos os casos de computadores e notebooks esquecidos perto da janela em dias de chuva. Também não são poucos os casos de micros no ambiente de trabalho que ficam acessíveis a qualquer pessoa na hora do almoço. Naquela empresa em que o Samuca era o gerente de redes, uma vez ao entrar no CPD a faxineira estava lendo o E-Mail no servidor da empresa. Quando eu perguntei se o Samuca sabia disso, ela disse que sim e que foi ele quem a ajudou a criar uma conta de E-Mail. Basta uma criatura destas receber um trojan anexado e adeus servidor.

Pausa: quando assumi a rede da empresa, tive que acabar com estes e outros hábitos nocivos e arriscados. Só que a galera não gostou muito quando eu coloquei ordem na casa. Estavam acostumados com a bagunça. Foi preciso muito jogo de cintura e uma paciência de Jó.

A precaução contra roubo e furto é a de sempre: atenção, proteção física e até seguro, se achar que vale a pena. A proteção para não usarem o computador na sua ausência é senha no protetor de tela, senha no setup e o uso de programas que configuram a proteção do computador, escondendo os recursos que você não quer que fiquem expostos, como painel de controle e acesso a discos, por exemplo.

Para esta finalidade temos o *System Mechanics* e os *Protect Me* e *Protect XP* em português. Não são os únicos programas do genero, mas são os que oferecem o maior número de recursos e facilidades.

No segundo módulo (SECURITY) do Novo Curso de Hacker você assiste a vídeoaulas completas sobre este programa.

Protect Me - *www.quartzo.com/novo/pmereg.htm*
Protect XP - *www.quartzo.com/protectxp/*
System Mechanics - *www.iolo.com/sm/4/index.cfm*

Apesar de ser um software em inglês, O System Mechanic possui vários recursos úteis para eliminar rastros no PC local. Vale a pena investir algum tempo aprendemdo a usar este software. E uma dica. Softwares de segurança, são bastante eficazes em descobrir se você está tentando burlar o registro do programa sem o pagamento devido.
Proteções locais por software podem ser burladas se o hacker conseguir dar o boot por disquete ou CD-Rom. Portanto fique atento a forma em que o *setup* do

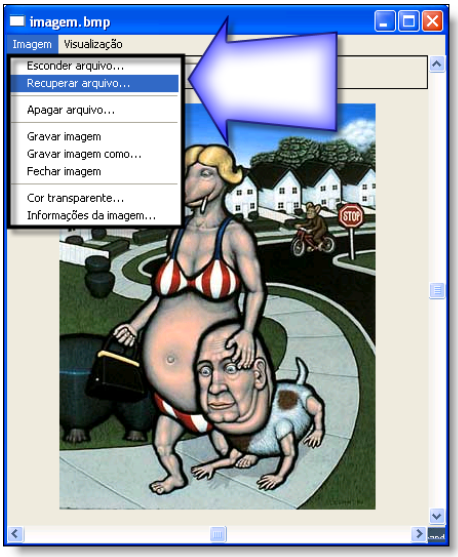
micro está configurada para o boot. O ideal é o boot exclusivamente pelo disco rígido.

Criptografia e Esteganografia

Arquivos locais podem ser criptografados (codificados) e esteganografados (escondidos dentro de uma imagem ou outro arquivo). Mas você deve ter algo de extremo valor para querer tanta segurança. Criptografar e esteganografar arquivos dá trabalho e envolve riscos. Risco do arquivo se corromper depois de tanta manipulação digital. Risco de você não lembrar mais da senha. Risco de apagar o arquivo acidentalmente em caso de arquivos com nomes dissimulados.
Uma dica simples que ajuda a manter os arquivos pessoais longe dos curiosos é criar dentro da pasta **C:\Windows** ou **C:\Windows\System32** uma pasta com um nome que confunda o curioso, por ser parecido com o de uma pasta do sistema. Exemplos: ***shel***/*shell*, ***drive***/*driver*, ***tempor***/*temp*, ***bkp***, etc...
Só que estamos esquecendo uma coisa, o comando ***Pesquisar*** do Windows. Uma opção é manter as extensões mascaradas, como **.do_** em vez de **.doc**. Ou então manter a pasta inteira criptografada.

Acho que já deu para você perceber o dilema de quem tenta defender um sistema de informática. Quanto mais fundo você vai na segurança, quanto mais você busca soluções de proteção e segurança, mas você complica a sua vida, mais você corre o risco de não conseguir acessar o recurso protegido. E sempre existirá um SE em cada etapa de aumento da segurança. Sempre existirá alguém que pensou exatamete na estratégia que você bolou para se proteger. Então vale o bom senso. Proteção sem paranoia. Proteção sem complicação. Proteção sem risco para você mesmo.

No CD-Rom que acompanha este livro você encontra programas de criptografia e esteganografia.



Apagando o Próprio Rabo

Um PC rodando Windows armazena muito mais sobre você do que você pensa. Veja a lista:

- Processadores Pentium possuem um número de identificação único que permite rastrear o seu computador pela Internet. Esta opção pode ser desabilitada no Setup e gerou protestos nos EUA. Acredita-se que algumas placas mãe não possuam na BIOS a opção de desabilitar o número de identificação dos processadores Pentium.

- O Windows, ao ser instalado pergunta pelo nome do usuário e empresa. Estes nomes serão usados depois de várias maneiras, inclusive para nomear alguns recursos da rede. Verifique se você não forneceu informações que permitam a sua localização.

- Aplicativos da suíte Office da Microsoft (Word, Excel, etc...) armazenam em

cada documento criado informações sobre o autor e a máquina.
- Quando você navega na Internet, todos os sites visitados formam uma lista de atalhos chamada ***Histórico***.
- Os últimos arquivos abertos por você formam uma lista de atalhos chamada ***Documentos Recentes***. A maioria dos programas que gera algum tipo de arquivo, também possui a uma lista de *histórico* ou *arquivos recentes*.
- A maior parte dos sites que você visita armazena arquivos em seu computador, sem o seu conhecimento ou consentimento. Estes arquivos são conhecidos por cookies e podem ser localizados na pasta *c:\Windows\Cookies* ou *c:\Documents and Settings**Usuario***\Cookies* dependendo do sistema operacional e navegador utilizados. Nada que o *Pesquisar* do Windows não resolva. *Cookies* são simples arquivos de texto que podem (e devem) ser eliminados periodicamente.
- Os programas que você instala, usa ou apaga, deixam rastros em diversas partes do sistema. Informações sobre programas podem ser encontradas nos arquivos do sistema, no registro ou na forma de pedaços de arquivos e pastas armazenados no disco rígido.
- Mensagens deixadas por você em listas de discussão (grupos), livros de visita, fóruns, sites que pedem cadastros, área de opinião em sites de vendas de livros, blogs e até E-Mails, podem ser localizados na Internet até muitos anos depois de terem sido enviados. Algumas destas informações ficarão armazenadas indefinidamente. No Google por exemplo, podemos encontrar as primeiras mensagens trocadas entre as pessoas no início da Internet. Provavelmente estas mensagens não serão apagadas nunca. Então muita atenção quanto ao que você coloca na rede, pois pode ser impossível apagar depois. Foi desta forma que uma revista de fofocas descobriu que a Big Brother Juliana, tinha um cadastro em um site *pega-marido*. Ela estava a procura do homem dos sonhos, o que incluia um salário mensal entre 5 e 15 mil reais. Numa ficha como esta, de site de encontros, é possível saber muita coisa da pessoa. E por se tratar de um tipo de cadastro feito sem o uso da razão, quase que só da emoção, um *phishing scam* direcionado a este publico será muito bem sucedido.
- Arquivos apagados não são removidos do HD. Vão parar na lixeira, uma pasta do sistema de fácil acesso. E mesmo que você remova os arquivos da lixeira, eles podem ser recuperados. Veremos como fazer isto ainda neste capítulo. Também veremos como apagar definitivamente um arquivo que não queremos que seja localizado posteriormente. Mesmo com o uso deste recurso, é bom saber que o FBI afirmou conseguir recuperar em laboratório, arquivos sobrescritos mais de vinte vezes. Não sei a quantas anda a polícia brasileira. Todo cuidado é pouco.
- Empresas de telefonia fornecem seus dados pessoais a qualquer um que ligar perguntando. E não adianta assinalar a opção de que não permite que seu

número não conste da lista telefônica. As operadoras possuem acesso a base de dados das concorrentes. Se você não conseguir a informação que procura em uma operadora, poderá tentar em outra, inclusive de telefonia celular. Aqui também podemos usar um pouco de engenharia social. Ligar para o setor de cobrança e perguntar se existe algum débito em nome de fulano de tal. Você pode inventar que está comprando o celular dele ou dizer que achou o aparelho e precisa devolver. Se você for convincente vai conseguir qualquer informação disponível. Um exemplo ocorreu em 2003 quando uma repórter simplesmente ligou para a Embratel e pediu o telefone do Senor Abravanel (o Silvio Santos) que estava no exterior. Segundo o próprio Silvio, o telefone mal acabara de ser instalado e nem ele sabia o número. A repórter acabou conseguindo a sua matéria. Só que o Sílvio resolveu tirar um sarro com a jornalista e dizer que ia vender o SBT. O motivo é que os médicos o alertaram de que ia morrer do coração em no máximo cinco anos. O resultado da brincadeira foi uma queda de 15% nas ações da Televisa que, segundo o Sílvio Santos, seria uma das compradoras do SBT.
- micros em rede CLIENTE x SERVIDOR mantêm o registro da sua conexão. Nos servidores Windows, o nome de usuário da última pessoa logada no servidor será exibido na tela de login.
- Conexões remotas a servidores, bem intencionadas ou não, são registradas em arquivos de *log* bastante minuciosos.

Existem muitos outros locais onde você deixa rastros. Tanto no computador local, como nos micros promíscuos e nas suas conexões em rede. Além disso, os sites governamentais nos três níveis: municipal, estadual e federal, possui alguma informação a seu respeito. Órgãos como INSS, Detran, SERPRO, Ministério do Trabalho, Receita Federal, serão boas fontes de consulta. Até o seu local de trabalho pode ser consultado em busca de alguma informação que leve até você ou que possa ser usada contra você.

Até agora vimos como estes rastros podem ser usados para nos localizar ou contribuir para provar nossa autoria em uma ação hacker. Da mesma forma podemos usar as dicas acima para localizar um ALVO.

Uma pausa...

O ALVO é a pessoa ou empresa que futuramente será VÍTIMA de uma AÇÃO HACKER. Enquanto a AÇÃO não for bem sucedida o que temos é um ALVO. Com o sucesso da ação passamos a ter uma VÍTIMA.

Depois de ter assustado você, ao mostrar a quantidade de rastros que você deixa a partir do momento em que liga o computador, vamos ver como podemos reduzir as chances de sermos localizados, seja por um hacker, seja por 'alguém' em busca de um.

Criando Avatares

A primeira precaução é não vincular o seu nome a bens e serviços. O problema é que na maioria das vezes isto não será bem visto pela justiça comum. Transações comerciais exigem a discriminação das partes. Mas existem algumas situações em que o uso de pseudônimo é aceita e até incentivada.

Vamos a alguns exemplos:

- nos cadastros em serviços de E-Mail gratuitos você pode usar a frase NÃO AUTORIZO, NÃO DISPONÍVEL, NÃO FORNECIDO ou algo similar, sem qualquer preocupação.
- contas de telefone, luz e água obrigatoriamente devem vir no nome de alguém. Se você usar o nome de uma pessoa sem o seu consentimento estará cometendo o crime de falsa identidade. Se houver o consentimento da pessoa, como o conjuge por exemplo, tudo bem.
- algumas empresas enviam a mercadoria antes do pagamento, juntamente com um boleto bancário. Outras exigem o primeiro pagamento e enviam o boleto dos pagamentos seguintes. É fácil encontrar empresas deste tipo assistindo aos canais de TV pela manhã e na parte da tarde. Iogurteiras, mini máquinas de costura, utilidades domésticas, livros e coleções. Tudo isto pode ser adquirido parceladamente. Ao usarmos o nome de outrem, mesmo que tenhamos que pagar a primeira parcela, pela falta do restante do pagamento, o nome a ser negativado é do laranja.

Uma Pausa...

LARANJA é o nome dado a quem serve involuntariamente a alguém ou organização, que comete algum ato ilícito em seu nome. O fato de você pegar os dados de uma pessoa na Internet e fazer compras como se fosse ela é um crime. Embora seja muito difícil provar a autoria.

No Brasil é muito fácil criar um laranja. Uma das formas e verificar nos obituários dos jornais alguém que tenha mais ou menos a sua idade. De posse do nome completo, ir ao cartório e tirar uma segunda via da certidão de nascimento. Com a certidão de nascimento, você poderá pedir uma segunda via da identidade. So que neste caso as impressões digitais não vão bater. Uma opção é tirar a identidade em outro estado, pois os sistemas não são integrados. De posse da identidade e da certidão de nascimento, pedir uma segunda via do CPF nos correios, transferir o título e pedir uma segunda via e já dá até para abrir conta em banco. A preferência é por abertura de contas nas agências dos correios que possuam o

Banco Postal, pois os funcionários não são tão bem preparados como os da agência tradicional.
Quem não quiser ter todo este trabalho, basta procurar nos jornais os anúncios suspeitos do tipo "*abro sua conta bancária mesmo que você tenha nome no SPC e SERASA*". Por trás destes anúncios estão quadrilhas especializadas na criação de documentos falsos.
Você também poderá conseguir documentos dos mais diversos tipos nas empresas que trabalham com cópias do tipo Xerox, principalmente as que ficam próximas ao Fórum, onde é comum a necessidade de cópia de vários documentos para anexar a processos.
Quem não tem a cara de pau de dizer que esqueceu um documento lá e nem quer correr o risco de pedir documentos perdidos, poderá simplesmente revirar o lixo destas empresas. Muitas cópias com defeito são jogadas no lixo. E ali tem de tudo: cartões de crédito, certidão de nascimento, CPF, tudo mesmo.
Uma outra forma de transferir para oura pessoa a responsabilidade dos seus atos é criando um AVATAR. Avatares já são conhecidos das pessoas que frequentam as salas de bate-papo (*chat*). Não consideramos avatar a simples escolha de um apelido (*nick* ou *nickname*). O avatar é mais que isso. É uma personalidade completa, incluindo nome, endereço, números de documentos, aparência, conta de E-Mail, hábitos e tudo o mais que uma pessoa real possa ter que a identifique no mundo real. A diferença do avatar para o laranja é que o avatar não existe no mundo virtual. Nenhuma das informações vinculadas ao avatar existem ou são tiradas de pessoa real. O avatar é totalmente virtual. O laranja é alguém do mundo real.

Para que serve um avatar?

Um avatar serve para proteger sua identidade real. Serve para você andar sem deixar rastros. Um avatar deve ser memorizado a ponto de você poder descrever de memória todos os dados relacionados a ele. Um avatar é a sua representação no mundo virtual. Um avatar será sua sombra usada na batalha. Quando ele tiver muito ferido ou visado, deve ser eliminado sem dó nem piedade. Nunca ressuscite um avatar. Você nunca sabe o que ele pode trazer do mundo dos mortos.
O avatar nunca será motivo de problemas ou preocupação se for usado para cadastros em serviços pouco confiáveis. Isto inclui os serviços de E-Mail gratuitos, cadastros em sites dos mais diversos tipos e registros de programas pós ou pré-instalação. Você pode informar explicitamente no cadastro, que as informações não são verdadeiras. Você não é obrigado a despejar seus dados pessoais na Internet, caso não queira. O serviço de loja virtual do HPG, o BPG, foi invadido e milhares de usuários tiveram seus dados expostos na Internet. É isto que que-

remos evitar. Veja um exemplo de informações explicitamente falsas que podem servir a um avatar:

Nome: Chacrinha
Endereço: Rua, A s/nº
Bairro: Qualquer
Cidade: Rio de Janeiro
Estado: BA

Outro exemplo:

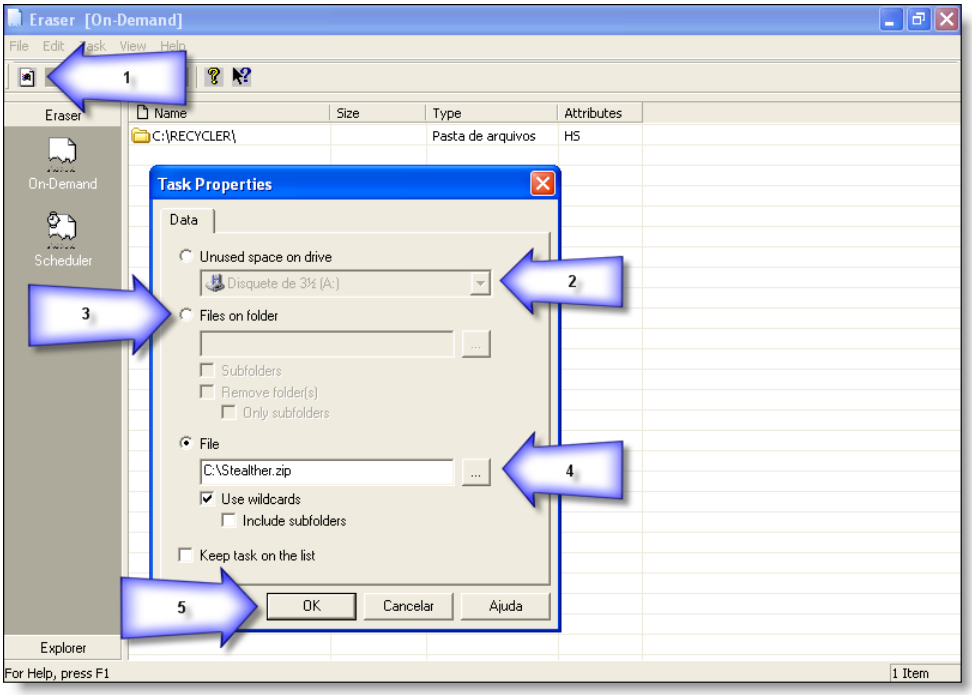
Nome: Não Fornecido (ou Não Autorizado)
Endereço: Não Fornecido
Bairro: Não Fornecido
Cidade: Não Fornecido (ou uma cidade qualquer em formulários com caixa de seleção)
Estado: Não Fornecido (ou um estado qualquer em formulários com caixa de seleção. De preferência a um estado em que a cidade selecionada não exista)

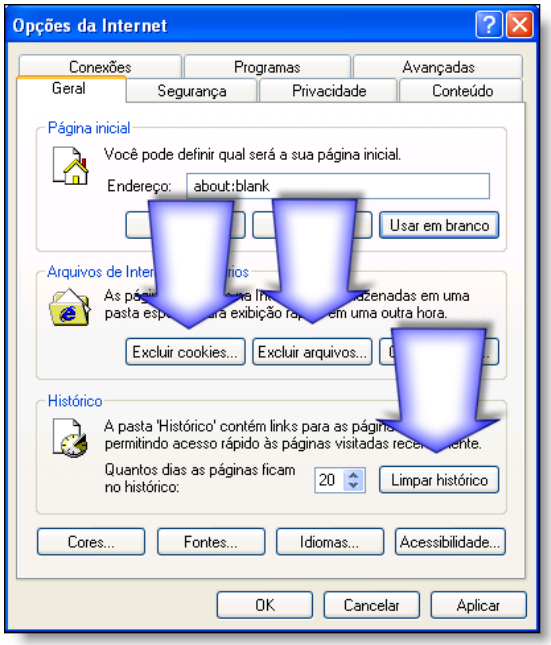
O avatar será ilegal e considerado delito se for usado para qualquer tipo de fraude. Use o avatar para aumentar sua privacidade. Não cometa fraudes na Internet. Não podemos negar que alguns hackers usaram o avatar como laranja. E aí o céu é o limite. Um avatar transformado em laranja pode causar muita dor de cabeça as empresas escolhidas como alvo.
Experimente você procurar o próprio rastro na Internet. Use tudo o que sua imaginação permitir: nome, apelido, eventos relacionados a você, número de documento, ICQ, telefone, E-Mail, empresas nas quais trabalhou; procure também em órgãos do governo.

Apagando Arquivos Definitivamente

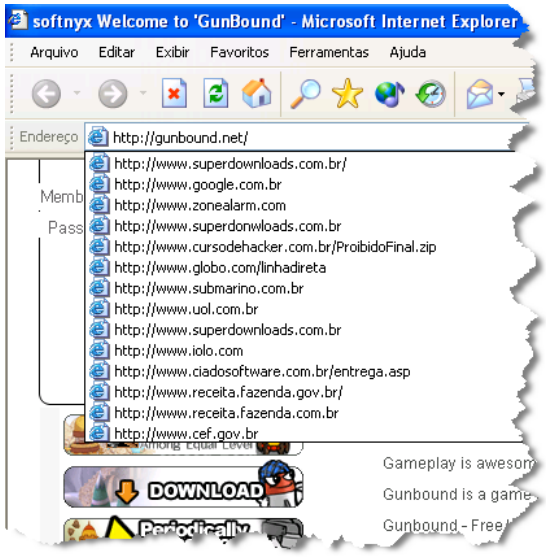
Já sabemos que um arquivo ao ser apagado do micro vai para lixeira. Se a lixeira for esvaziada, o arquivo ainda estará em algum lugar do disco rígido. Porém invisível. Na verdade ele continua no mesmo lugar em que estava. Só que agora o sistema operacional tem permissão para, se necessário, gravar qualquer outra informação sobre ele.
O apagamento definitivo de um arquivo ou programa do disco rígido ou disquete, pode ser obtido com o uso de programas que sobrescrevem várias vezes o arquivo apagado.
O programa Eraser é um freeware que apaga definitivamente um determinado arquivo, todos os arquivos de uma pasta, incluindo subdiretórios e também o espaço não utilizado do disco rígido. Como sabemos, o espaço 'não utilizado' no disco rígido está cheio de programas que podem ser recuperados.

O uso do programa é muito simples. **(1)** Crie uma nova tarefa (new task) e escolha entre **(2)** apagar definitivamente todo o espaço livre do seu disco rígido ou disquete, **(3)** apagar definitivamente todos os arquivos presentes em determinada pasta do disco rígido, como a lixeyra (recycled) por exemplo ou **(4)** apagar definitivamente um arquivo específico. Clique em **(5)** OK quando terminar.
O Eraser também tem a opção de agendamento. Você pode deixá-lo programado para apagar definitivamente tudo o que for para a lixeira (pasta recycled).
Só não vale instalar este programa no computador do seu primo e agendar para apagar tudo o que ele tiver no disco rígido. Não esqueça de que estamos falando de um apagamento definitivo.





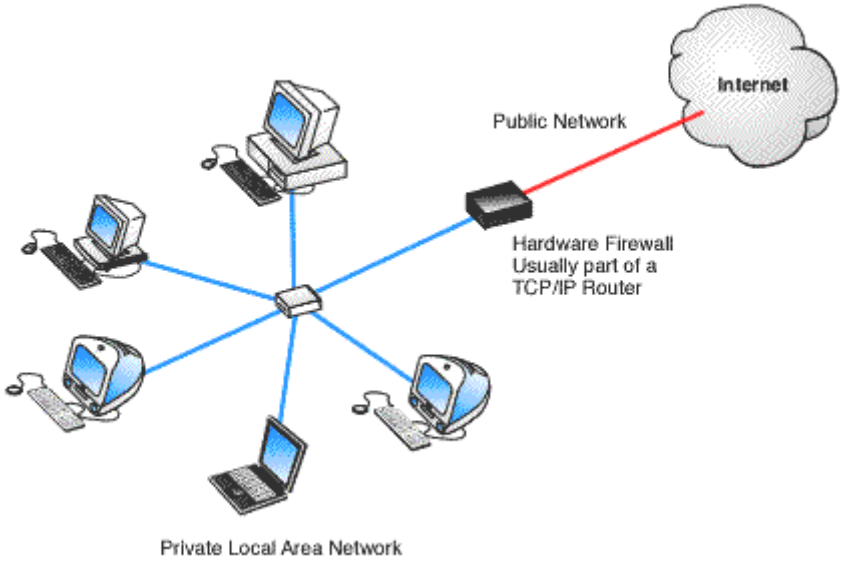
Algumas opções do Internet Explorer podem ser úteis na hora de apagar alguns rastros. Muitas das vezes peguei funcionários meus navegando sem autorização em sites de encontros e pornografia. Bastou uma olhadinha na BARRA DE ENDEREÇOS do Internet Explorer. Uma operação simples como esta que acabamos de ensinar, eliminaria as evidencias da navegação.



Firewall

O firewall é um tipo de programa que só despertou o interesse do usuário comum de uns dois a três anos pra cá. Antes disso o uso deste tipo de software era restrito ao ambiente corporativo, em redes CLIENTE x SERVIDOR.

Um firewall pode existir em forma de hardware. Também pode ser um computador totalmente dedicado a função de firewall, rodando um sistema operacional configurado para esta finalidade. Como também pode ser um software que desempenha as funções do firewall no micro pessoal. Daí o nome: *personal firewall* ou firewall pessoal.



A principal função do firewall é controlar a entrada e saída de dados da rede. Um firewall pode ser usado para proteger uma rede inteira ou apenas a máquina do usuário que acessa a Internet.

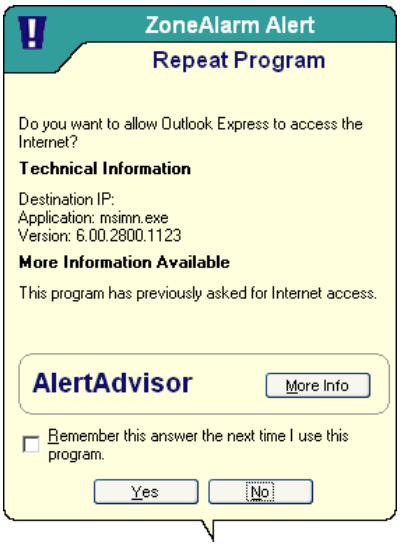
Vamos encontrar o firewall com diversas opções de preço e performance. Tanto é possível encontrar firewall gratuito, em forma de software, como dispositivos de hardware com preço de venda acima de 10 mil reais.

O leque de possibilidades de configurações também varia muito de um firewall para outro. O firewall ideal deve permitir a configuração das seguintes formas:

- controle de tráfego por portas
- controle de tráfego por protocolo
- controle de acesso por programa

O usuário comum pode sentir-se bastante incomodado com o uso de um firewall

em seu computador. Nem sempre os alertas emitidos pelo firewall pessoal são claro o suficiente para permitir uma decisão acertada por parte do usuário. Se você nunca usou um firewall, este programa funciona assim: monitora as conexões ao seu computador, de dentro para fora e de fora para dentro. Quando um programa inicia uma conexão com a Internet, o firewall assume o comando e passa a decisão para você. Permitir ou não o acesso? Alguns programas são fáceis de identificar. Outros não. E aí é que mora o perigo. Um trojan bem feito pode ter o acesso a Internet autorizado, ao se fazer passar por um programa conhecido. Na tela abaixo vemos o firewall perguntando se deve permitir ou não que o Outlook Express acesse a Internet. Mas não dá para saber isto só olhando as informações que o firewall apresenta.



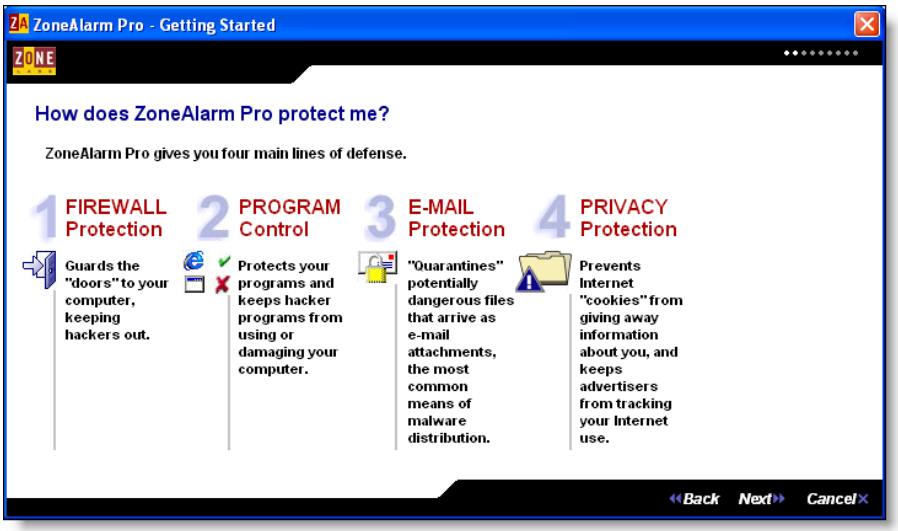
O Norton Personal Firewall versão em língua portuguesa parece ser o mais indicado ao usuário pouco experiente. Usuários mais avançados podem querer programas que não sobrecarreguem tanto o sistema operacional e que permitam ajustes mais precisos.

Estes são os firewalls mais usados atualmente (pesquisa feita entre os alunos do Curso de Hacker). Com exceção do Norton, os demais tem versão gratuita:

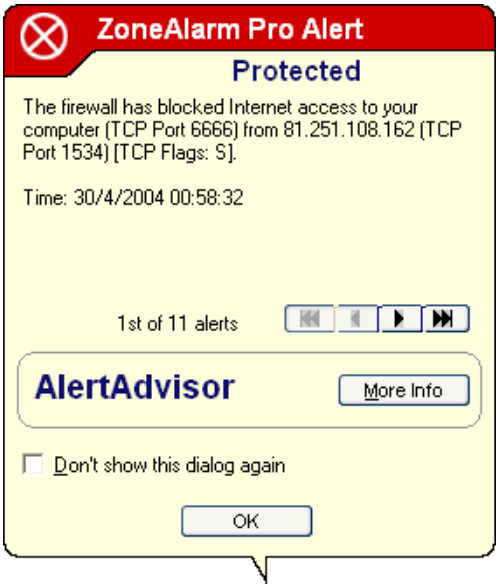
Zone Alarm - *www.zonelabs.com*
BlackICE PC Protection - *http://blackice.iss.net/update_center/index.php*
Kerio Personal Firewall (atenção à porta 25) **-** *www.kerio.com/kerio.html*
Norton Personal Firewall - *www.symantec.com.br*
McAfee Personal Firewall - *http://br.mcafee.com*
Sygate Personal Firewall (insiste na versão paga) **-** *www.sygate.com*
Outpost Firewall - *www.agnitum.com/download/outpost1.html*
Tiny Personal Firewall - *www.tinysoftware.com*
Coyote Linux (roda até em um PC 486 sem HD e sem monitor, basta um drive de disquete) - *www.coyotelinux.com*
eTrust (da Computer Associates e vem com antivírus) **-** *www.my-etrust.com/microsoft/*

Nota: o antivírus eTrust da Computer Associates (*www.ca.com*) vem com um firewall muito parecido com o Zone Alarm. Ambos são gratuitos.

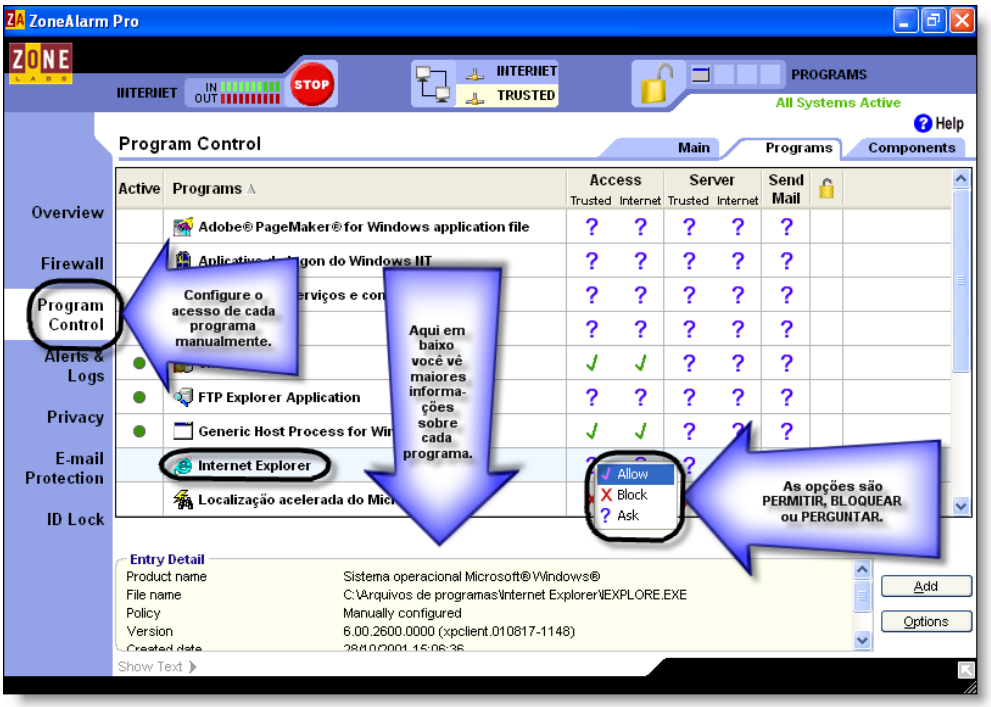
O Zone Alarm é um firewall que cada vez mais vem ganhando a confiança dos usuários. Após a instalação, permite ser usado com a interface simplificada ou não, atendendo assim, aos diversos tipos de usuário. Se o idioma inglês não for problema para você, vale a pena experimentá-lo, vcaso já não tenha outra opção:



Na figura abaixo podemos ver um alerta do Zone Alarm. Neste caso em particular, trata-se de um programa de troca de arquivos em plena execuçaõ. Não há como usar com eficácia um firewall se não soubermos o que temos, para que servem e como funcionam os programas instalados em nosso micro:



Na figura abaixo podemos ver como configurar o Zone Alarm para bloquear ou permitir o acesso a Internet:



Spam

A palavra spam é usada para descrever o recebimento de E-Mails indesejados e em grande quantidade. Na prática não é muito fácil punir uma pessoa por enviar E-Mail sem o consentimento do destinatário. É algo difícil até de provar, a não ser que você confesse ou seu computador seja apreendido e provas encontradas. É mais fácil punir o provedor ou a empresa por trás do spam do que o spammer. São os provedores os maiores interessados em bloquear o spam. Se por um lado as empresas tem o direito de divulgar seus produtos. Você tem o direito a privacidade. E a decisão continua sendo do juiz.

O usuário é apenas aporrinhado com o lixo eletrônico. Os verdadeiros prejudicados são os provedores. Por que? Porque os provedores pagam pelo tráfego que circula em suas redes. Se vários usuários de determinado provedor cismarem de enviar spam, isto

vai consumir a largura de banda e os demais serviços ficarão comprometidos: FTP, acesso aos sites hospedados no servidor, envio de E-Mail normal, etc...

E é daí que parte o grito mais forte. Os provedores sistematicamente insistem em nos fazer crer que spam é coisa do diabo. Spam é um incomodo, sem sombra de dúvidas. Mas não é este crime hediondo que tentam nos fazer acreditar. Pelo menos eu não caio nessa. O site AntiSpam (*www.antispam.org.br*) é mantido pela Associação Brasileira de Provedores de Acessso. Precisa dizer mais?

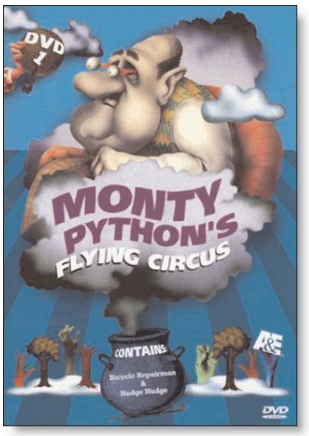
O protocolo responsável pelo envio do E-Mail é o smtp. É sabidamente um protocolo com falhas de segurança. Um E-Mail pode ser forjado com facilidade. Por isso eu não acredito que possa ser usado como prova contra alguém.

Fico admirado com a reação de pessoas que se acham 'inteligentes' como o Giordani Rodrigues do site Infoguerra (*www.infoguerra.com.br*), que confessou sentir urticária ao se aproximar de um spammer. Como é que é? Vai ficar se coçando todo? Conheço isto como viadagem.

Não sou a favor do spam. Mas também não aceito ser conduzido que nem gado e induzido a ver algo que não existe. Incomoda receber E-Mail indesejado, incomoda receber pelo correio impressos que não pedi, incomoda receber ligação da LBV pedindo doações, incomoda a interrupção da novela para exibição de comerciais e incomoda quando alguém tenta incutir na minha mente um pensamento que não é meu.

Já cansei de falar sobre o editor do TI Master que me acusou de spammer e teve que se retratar para não pagar 40 salários de indenização. Na Internet você vai ler muito sobre leis antispam (inexistente) e tudo o mais. Na prática a história é outra. A única punição que tem sido aplicada aos spammers é a perda da conta de E-Mail ou do serviço prestado pelo provedor (de hospedagem, E-Mail ou acesso).

A palavra "SPAM" surgiu em 1937, como marca registrada da empresa norte-americana Hormel Foods (*www.hormel.com*) ao criar a primeira carne suína enlatada (Spiced Ham ou Spiced Pork And haM (presunto temperado)). Esse produto é largamente consumido até hoje (*www.spam.com*), e emprestou seu nome para uma piada do grupo humorístico inglês Monty Python (*www.pythonline.com*), episódio que tornou o nome do alimento sinônimo de incômodo na Internet.



O grupo Monty Python, responsável por produções cinematográficas como "A Vida de Bryan" (1979), estreava um programa televisivo de humor nos anos setenta (Flying Circus), e em um dos episódios um casal entra em um "bar" e tudo que eles pediam para comer tinha SPAM (spam com spam, ou mesmo spam e spam com spam,spam de spam com spam e molho de spam) e um grupo de vikings que também estava no bar, começavam a gritar "Spam, Spam, Spam, Spam....." de maneira intermitente e irritante, simplesmente impossibilitando qualquer comunicação das outras pessoas presentes com a gritaria repetitiva. Leia o diálogo original no site: *www.detritus.org/spam/skit.html.*

Alguns anos mais tarde, nos primórdios da Internet, no meio de um grupo de discussão, alguém teve a infeliz idéia de enviar repetidas mensagens comerciais aos participantes de determinados chats, invadindo os grupos e atrapalhando a comunicação das pessoas.

Assim, surge o termo Spam no mundo digital, com a lembrança do episódio do Monty Python por um usuário de grupos de discussão equiparando o envio de mensagens não solicitadas nestes grupos com a gritaria ensurdecedora do programa cômico inglês, e essas mensagens migraram para os endereços de correio eletrônico que começavam a se difundir.

A partir de então, o termo Spam pode ser definido como o envio de mensagem eletrônica não solicitada e não autorizada por quem a recebeu. O spam deve se assemelhar ao nosso apresuntado em lata que tantas vidas já salvou em acampamentos e repúblicas universitárias.

O spam é um grande auxiliar do hacker para a técnicas como phishing scam, engenharia social, controle remoto, disseminação de vírus, homem no meio, entre outras.

Eliminar o spam, pelo menos por enquanto, tem se tornado uma tarefa impossível. Para reduzir o número de mensagens indesejadas, podemos tomar as seguintes atitudes:

- manter pelo menos duas contas de E-Mail. Um a ser divulgado em situações realmente importantes e o outro para todas as outras ocasiões.
- ao instalar um programa que pede registro ou se inscrever em grupos de discus-

são, o ideal é ter um E-Mail só para esta finalidade.

- Evite comprar os produtos ou serviços divulgados. Além de confirmar a eficiência do spam, você fornece dados pessoais a desconhecidos.

- Não repasse e-mails sem conhecer o remetente ou checar a veracidade das informações. Boatos e correntes são formas importantes de spam.

- Jamais responda aos spams. Tampouco clique na opção 'remover'. Isso dá a certeza de que sua conta pertence a um usuário ativo.

- não deixe o seu E-mail na Internet. Como assim? Existem programas que varrem as páginas da Internet (robôs) em busca de endereços de E-Mail para geração de listas de envio. Fóruns, página de opinião sobre produtos, blogs, páginas pessoais, todas estas situações podem e serão usadas pelo spammer para montar sua lista de endereços.

- não use nomes comuns para contas de E-Mail. É que spammers usam programas para gerar listas de endereço, a partir da combinação de nomes e endereços de provedores. Um spammer pode simplesmente pegar um gerador de dicionários e depois combinar as palavras geradas com cada um dos principais provedores de E-Mail. Exemplo: ana + @globo.com, ana + @bol.com.br, ana + @zipmail.com.br e assim sucessivamente.

Experiência Pessoal...

Como eu tenho o meu próprio dominio, qualquer E-mail enviado para um_nome_qualquer@marcoaurelio.net chegará a minha conta principal de E-Mail. Assim, quando faço algum cadastro, escrevo antes o nome do site ou programa e se chegar algum spam neste endereço, saberei de onde surgiu. Isto me ajudou a descobrir que o site www.Superdownloads.com.br não é muito ético. Bastou cadastrar um programa lá para começar a receber spam no E-Mail sd@marcoaurelio.net. A solução foi bem simples, bastou bloquear as mensagens para este E-Mail.

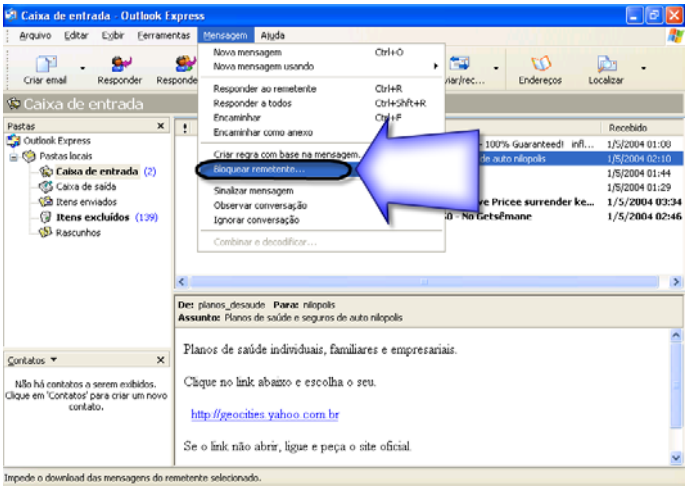
Usando esta dica você poderá usar o filtro do Outlook para barrar as mensagens destinadas aos endereços sabidamente usados pelo spammer.

Programas anti-spam

Existem alguns programas anti-spam. Não recomendo nenhum. O sistema de inteligência artificial destes programas é precário e você pode perder mensagens importantes que não são spam. O melhor é adotar o que eu chamo de atitude antispam e gerenciar o lixo do dia-a-dia configurando regras para o Outlook Express.

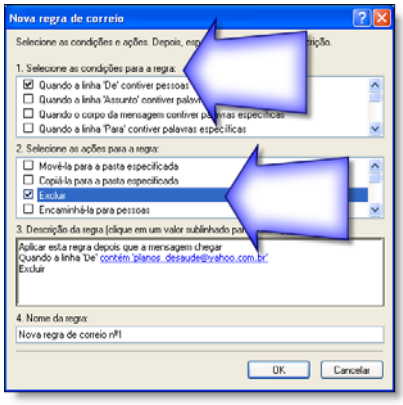
Configurando o Outlook Express para bloquear E-Mails indesejáveis

O Outlook Express pode ser configurado para bloquear E-Mails indesejados tendo como referência o endereço do remetente. Basta selecionar a mensagem de remetente indesejado e acessar na **BARRA DE MENUS** a opção ***Mensagem -> Bloquear Remetente***:



Configurando Regras para Mensagens no Outlook Express

Existem programas que mascaram o endereço de E-Mail do remetente. Nestes casos, os mais comuns, o método acima não vai adiantar. Podemos configurar regras mais sofisticadas acessando na BARRA DE MENUS do Outlook Express as opções Mensagem - Criar Regras a Partir da Mensagem:

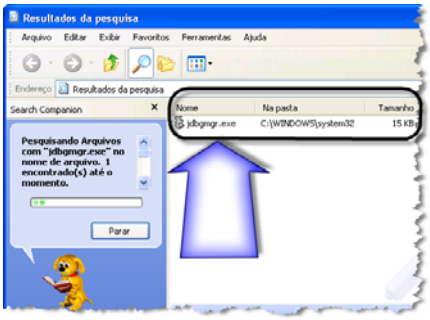


Hoax

Leia o seguinte texto:

Por favor verifique se você pegou este vírus de mim. Ele também me foi enviado acidentalmente e distribuido a todas as pessoas da minha lista. É provável que você o tenha.
Se você o tiver, distribua este E-Mail a todas as pessoas da sua LISTA DE ENDREÇOS porque O programa envia automaticamente a mensagem com o vírus. O nome do vírus é **jdbgmgr.exe** e não é detectado por nenhum antivírus. Ele permanece no seu computador por 14 dias antes de apagar todos os seus arquivos.Para deletá-lo e eliminá-lo completamente, faça o seguinte:
1. Vá em ***Iniciar -> Pesquisar -> Todos os Arquivos e pastas***
2. Digite **jdbgmgr.exe** e clique em Pesquisar Agora (tenha certeza de que você está procurando no Drive c)
3. Se aparecer o arquivo **jdbgmgr.exe** não clique nele, pois é o vírus *(o ícone dele é o de um ursinho de pelúcia)
4. Não abra. Apenas apague.
5. Após ele desaparecer, esvazie a lixeira para removê-lo definitivamente.
Se você encontrar o vírus em seu sistema, por favor envie essa mensagem a todos da sua lista de endereços, pois provavelmente eles também estão infectados.

Hoax são boatos, mensagens falsas, que também podem ser considerados spam feito involuntariamente por pessoas com certo grau de ingenuidade. Um hoax começa assim, alguém envia o primeiro lote de E-Mails sobre um assunto de interesse público e pede para que seja repassado ao maior número possível de pessoas. Estes E-Mails são bem bolados, com histórias convincentes, fotos, nomes de pessoas, enedereço e telefone. Quem recebe, na ânsia de ajudar, acaba fazendo justamente o que não deveria fazer: propagar o boato.



Os alertas mais comuns são os que envolvem vírus, crianças em hospital, promoções em nome de grandes empresas, pacientes terminais, bichos e pessoas desaparecidas, descobertas científicas, tudo falso.

Da mesma forma que o spam, o que o hoax tem de mal é apurrinhar quem recebe, às vezes várias mensagens sobre o mesmo assunto vindas de pessoas diferentes. Todos querendo ser o primeiro a propagar alguma 'descoberta'.

Da mesma forma que o apam, o hoax gera tráfego não lucrativo e não interessa aos provedores a rede sobrecarregada. Para o hoax só te um remédio: a informação.

Nota: o arquivo acima é parte integrante do Windows e não deve ser removido.

Spyware, Adware, Trojan, Track, Dialer, Malware, Hijacker e outras pragas virtuais

Se não bastasse os vírus, spam e hoax, temos também a nossa espera na Internet muitas outras pragas virtuais. São pequenos programas que se instalam sem o seu conhecimento ou consentimento. Estes programas tem as mais variadas formas de instalação e finalidade. Como formas de instalação temos:
- instalação simultânea com outro programa, geralmente shareware ou freeware. Exemplo: O Kazaa, programa de compartilhamento de arquivos, instala vários spywares em seu micro.
- ao visualizar uma mensagem de E-Mail em formato HTML ou ao abrir uma anexo.
- via programa de mensagem instantânea (MSN, Yahoo!, ICQ)
- ao visitar uma página na Internet
- ao baixar programas hacker de sites pouco confiáveis ou da rede P2P

E como objetivo destas pragas virtuais, temos:

MARKETING DE BAIXO NÍVEL
- propaganda em forma de janelas pop-up. Alguns programas, após a instalação, faz com que apareça um número de janelas pop-up maior do que você encontraria se não estivesse com ele instalado.
- inserção de links em páginas Web
- alteração do resultado nos sistemas de busca
- coleta de todas as informações sobre sua navegação e envio para o fabricante do programa. Isto inclui sites visitados, duração da visita, palavras pesquisadas, tempo on-line, dias e horários preferidos.
- substituição do discador padrão por outro que faz discagem internacional.

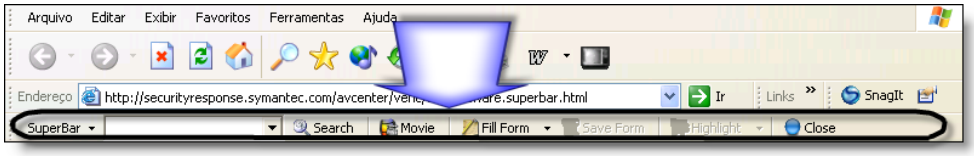
AÇÃO HACKER
- captura das senhas e informações a serem enviadas ao hacker
- abertura de portas para invasão

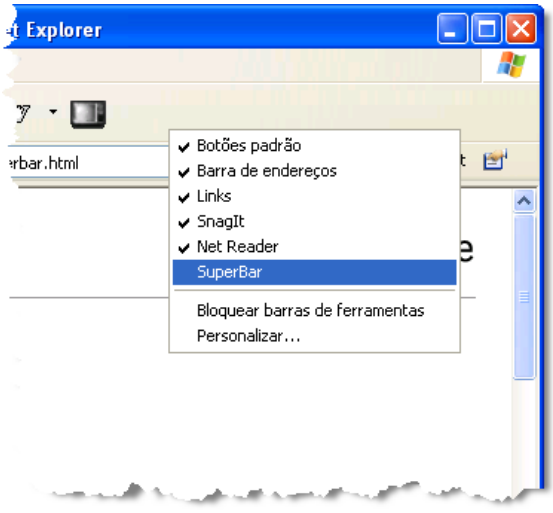
As pragas virtuais são tão ou mais perigosas que os vírus. A maioria não é detectada pelos antivírus, pois trata-se de um programa como outro qualquer. Não causa 'dano aparente' que faça o antivírus suspeitar e suspender suas atividades. Para você ter uma idéia do grau de nocividade destes programas, a maioria não possui desinstalador e quando tem, ao tentar desinstalar o programa avisa que foi desinstalado, muda de lugar e apaga o 'desinstalador'.

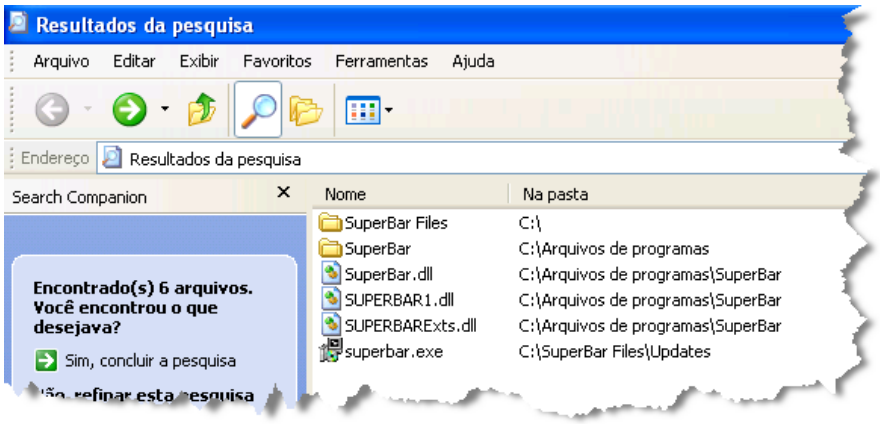
Estas são algumas das pragas virtuais disponíveis atualmente na Internet: AdBrake, Brilliant Digital, BrowserAidToolbar, DownloadWare, HighTraffic, Hotbar, HuntBar, IEAccess, INetSpeak, Lop, MoneyTree, OnlineDialer, PerMedia, RapidBlaster, Search-Explorer, SearchitBar, StripPlayer, TinyBar, Xupiter, StopSign, AdultLinks, Aureate Spy (vem numa grande quantidade de software), HXDL AL e Aveo Attune (muito software de marca, como CorelDraw, Dell Computer, GetRight, Hewlett-Packard, IBM, Logitech, Macfee, US Robotics, Xoom, HelpExpress, ect), HuntBar, PalTalk, StopSign, Wnad, CnsMin, CommonName, HuntBar, IGetNet, SuperBar, Cydoor, Cytron, DailyWinner , DialerOffline, HighTraffic, IEPlugin, IGetNet, Transponder.
A lista é muito maior. Conheça o que faz cada um destes programas ser considerado nocivo visitando o site:

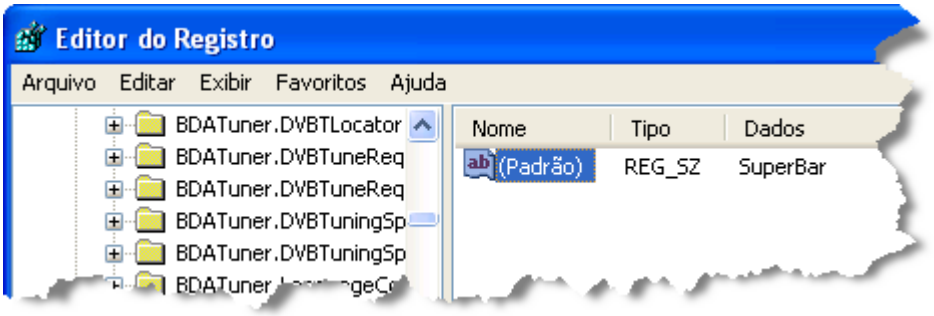
www.numaboa.com.br/informatica/spyware/intrusos.php

Nas figuras abaixo vemos o Super Bar. Caso o tenha consigo, provavelmente nem deve saber como ele foi parar no seu micro e muito menos como removê-lo, já que ele não se deixa apagar, não possui desistalador, não aparece na lista de programas do *Adicionar/Remover* e nem na lista de tarefas, ao pressionar **CTRL+ALT+DEL**:









Diante disso, começa a ganhar importância no cenário da computação doméstica os programas de detecção e remoção de pragas virtuais. Nesta categoria o Ad-Ware e o Spy Bot são os que mais se destacam. Por serem gratuitos. Por serem fáceis de usar. Por terem versão em português. Por realmente cumprirem o que prometem: remover as pragas virtuais que silenciosamente infestam o micro do usuário.

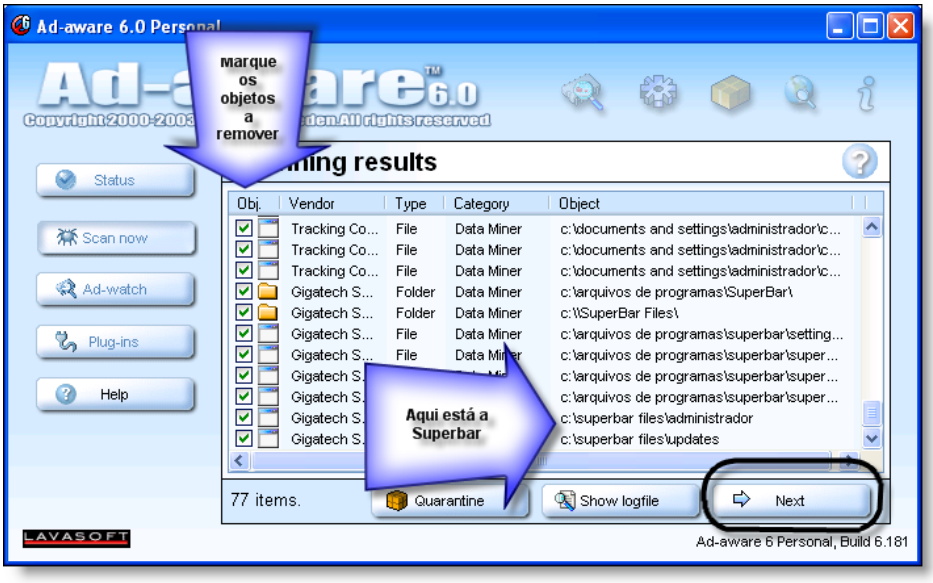
Apesar dos antivírus já detectarem também as pragas virtuais, eu prefiro deixar esta missão a cargo de um software especialista, como um dos dois que eu acabei de citar e que podem ser baixados dos links a seguir:

Ad-aware - *www.lavasoftusa.com*
Spy Bot Seach & Destroyer - *www.safer-networking.org/index.php?lang=pt*

Use um deles ou ambos. Não esqueça de atualizar a base de dados. Estes programas dependem da base de dados atualizada para que obtenham a máxima eficácia.

O Ad-aware é muito fácil de ser utilizado, mas precisa de uma pequena orientação para que você realmente remova as pragas virtuais do seu micro. Após fazer a varredura no sistema, o Ad-aware aguarda a sua autorização para remover os elementos suspeitos que foram localizados:

No exemplo a seguir podemos ver que a SuperBar foi localizada. Após selecionar os obejtos a serem eliminados ou postos em quarentena, basta clicar no botão ***Next*** para que a remoção seja efetivada:



Backup

O que de pior pode ocorrer em uma ação hacker dirigida contra nós, é o apagamento de todos os dados do HD. Se você mantiver um backup atualizado, isto não será problema. Já foi o tempo em que era uma tarefa complicada fazer o backup de nossos arquivos mais importantes. O backup ou cópia de segurança, independe de você ter ou não um micro a prova de hacker. Também devemos contas com os problemas físicos que podem atingir qualquer equipamento eletrônico. A frequência do backup vai depender de quanto agressivo você é no uso do micro.

Veja o meu caso. Eu crio do nada, cerca de 30 páginas de material impresso por dia. São roteiros, capítulos de livros, aulas, scripts, textos publicitários, projetos e tudo o mais que me cerca no dia-a-dia. Baixo quase 3 GB de material digital por dia e também recebo entre 200 e 300 E-Mails úteis, com pedidos, dúvidas, comprovação de depósito e tudo o mais que envolve o Curso de Hacker e meus outros negócios virtuais. Vamos comemorar um ano de curso de hacker. São mais de 10 mil mensagens trocadas e vocês nunca receberam comunicado meu avisando que perdi as mensagens ou arquivos importantes por conta de vírus, invasão ou pane no sistema. E com exceção da invasão e vírus, já tive que lidar com inúmeros panes no sistema, incluindo um HD de 80 GB perdido irremediavelmente. Mas todo o material e as mensagens sempre foram recuperados intactos e em pouco tempo. Algo em torno de 30 minutos a 90 minutos.

O segredo deste controle é manter o sistema protegido contra ataques e invasões e, no caso do pior acontecer, que é perder tudo por falha física, vírus, ataque ou invasão, possuir uma estratégia de recuperação.

Vou dar a receita do bolo. As dicas a seguir destinam-se ao usuário doméstico. minha estratégia de recuparação de disastres para redes corporativas é diferente e envolve conhecimentos de SCIS, RAID, cluster e sistemas operacionais de rede. Fora do escopo e da proposta desta obra.

Prevenção e Recuperação de Desastres

1. Mantenha em um mesmo local, podendo ser uma embalagem em formato de caixa com tampa ou porta CD, todos os CDs usados no seu micro;
2. Baixe e copie para um CD-Rom todos os drivers de dispositivo devidamente atualizados e service packs possíveis. Inclua uma cópia dos seus programas de uso geral: Acrobat, Winzip, Winamp, antivírus, WinRar, Kazaa, eMule, etc...
3. Se você não souber quais os drivers de dispositivo usados pelo seu micro, rode o programa AIDA. Um freeware excelente para revelar informações sobre drivers. Procure-o no CD-Rom que acompanha este livro.

4. Com todo o material em mãos, instale e prepare a máquina ao seu gosto, incuindo as personalizações. Supondo que você possua um computador atual, com disco rígido de 20GB ou mais, recomendo você crie pelo menos uma partição adicional.
5. Faça uma cópia da imagem do HD. Se você criou a partição adicional, o arquivo de imagem poderá ser copiado para a partição extra e depois copiado para um CD-Rom. Um ótimo programa para criar imagem do HD é o Norton Ghost da Symantec. Costuma vir de brinde nos CDs de placa mãe.

Até aqui você já tem como restaurar o sistema ao seu melhor estado de saúde. O que temos que fazer a partir de agora, é criar cópias de segurança para os dados que vão surgir no disco rígido. Estas cópias de segurança serão criadas em função da sua necessidade. Se você usa muito o micro, faça cópias semanais. Se você usa pouco, faça cópias mensais. Se você usa eventualmente, faça cópias eventuais. Mesmo que você mantenha um sistema de backup periódico, sempre que houver alguma alteração importante, crie uma cópia de segurança ANTES e DEPOIS da mudança. Exemplo: você está fazendo um trabalho para a faculdade. Não vai esperar uma semana para fazer o backup, a cada meia hora mais ou menos, já é recomendável salvar uma cópia de segurança em MÍDIA EXTERNA, seja disquete, servidor de FTP ou CD-RW (a melhor opção).

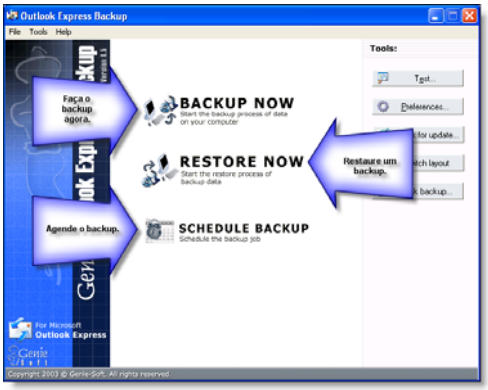
6. Supondo que já tenha passado um tempo desde que você criou a imagem do HD pós instalação e já tenha arquivos a serem salvos, em forma de cópia de segurança. A primeira opção é fazer uma cópia das seguintes pastas (pode variar o nome ou localização em dependendo da sua versão do Windows):

Meus Documentos
*C:\Documents and Settings**Usuario**\Meus documentos*
Arquivos Salvos na Área de Trabalho
*C:\Documents and Settings**Usuario**\Desktop*
Livro de Endereços do Outlook Express
*C:\Documents and Settings**Usuario**\Dados de aplicativos\Microsoft\Address Book*
Todas as Mensagens do Outlook Express
*C:\Documents and Settings**Usuario**\Dados de aplicativos\Identities*
Fontes do Windows (caso use fontes personalizadas)
C:\WINDOWS\Fonts

As pastas acima são as mais usadas pelo usuário comum. Se você tem por hábito gravar suas informações em locais diferentes dos citados acima, saiba que esta é

uma boa prática de segurança. Os locais acima (entre outros) são onde o hacker irá procurar por informação útil.

Mas supondo que você queira um backup mais sofisticado, que inclua todas as suas personalizações do Windows, incluindo assinaturas, remetentes bloqueados e regras para mensagens do Outlook, terá de recorrer ao registro ou usar um programa que automatize estas tarefas. Nossa sugestão é o **Genie Outlook Express Backup** (*www.genie-soft.com*), também em versões otimizadas para o Windows ou para o Outlook.



O processo de criação de backups com os softwares da Genie é muito simples e seguro.

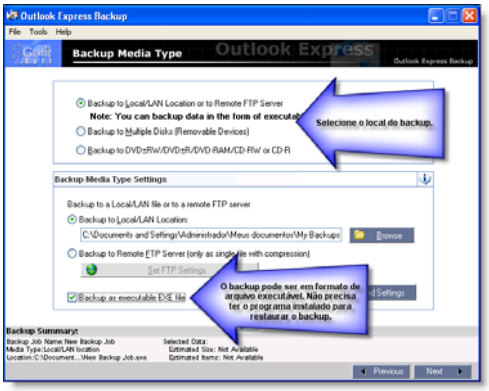
Na janela ao lado, você deve selecionar entre:

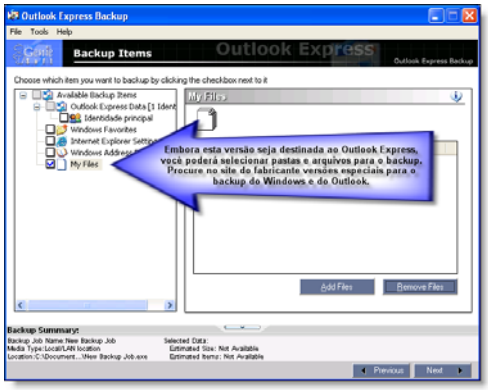
. CRIAR UM BACKUP AGORA
. RECUPERAR UM BACKUP AGORA
. AGENDAR UM BACKUP

Os programas da Genie oferecem várias opções de destino para o backup:

- **micro em rede local**
- **servidor de FTP**
- **CD-Rom**
- **disquete**

Incluindo a opção de multiplos arquivos, caso não haja espaço suficiente na mídia.





Embora neste exemplo eu esteja usando o programa de backup otimizado para o Outlook Express, podemos perceber que ele permite a inclusão de pastas e arquivos no backup.

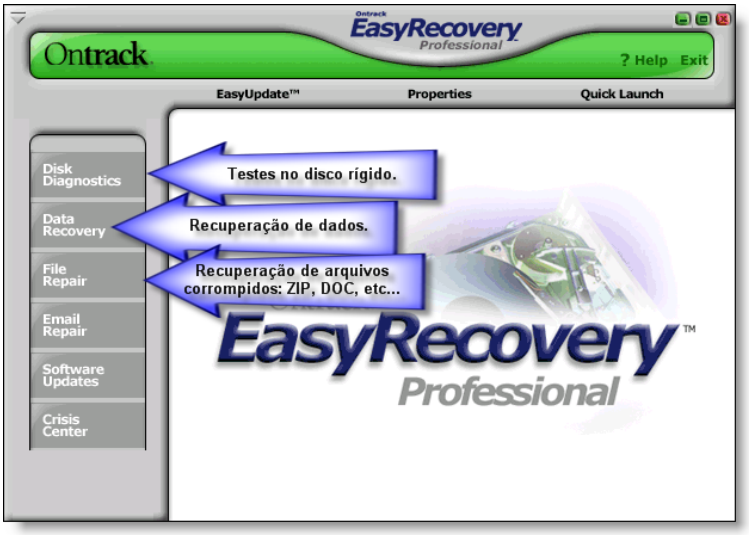
Sugiro a opção que gera um arquivo executável, pois não haverá necessidade do Genie instalado para recuperar os arquivos. Um hacker pode usar este programa para fazer um backup do alvo.

Usando estes dois procedimentos: ter uma imagem do seu HD pós instalação e manter um sistema de backup periódico, o pior que pode acontecer, a perda de todos os seus dados, não lhe causará grandes trasntornos já que a recuperação será POSSÍVEL, RÁPIDA e SEGURA.
Mas por favor, não mantenha o backup no mesmo HD ou a mídia junto ao computador. Backups ficam armazenados em local diferente. Nunca na mesma máquina ou no mesmo local. Quem não conhece a história dos dois backups da firma de contabilidade que estavam todos ao lado do computador que pegou fogo.
Antigos e ainda pouco usados, são os discos virtuais. Existem opções gratuitas que podem servir tanto para um backup como para o hacker que precisa de um local seguro para armazenar suas ferramentas. Em vez de ter um monte de ferramentas comprometedoras em sua máquina, mantenha as ferramentas hacker em um disco virtual e baixe-as conforme a necessidade. A maioria das ferramentas ocupa pouco espaço em disco.

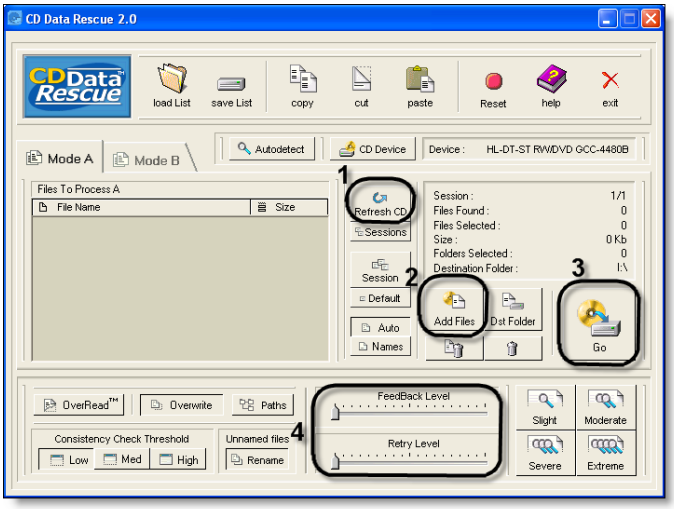
F.... tudo

O mais provável é que você seja como a maioria e não tenha imagem do HD pós instalação e muito menos um sistema de backup atualizado. Aí pode ocorrer de um vírus, uma experiência mal sucedida, uma falha no hardware ou uma ação hacker, sumir com todo o conteúdo do seu HD. E agora? Será que estamos amaldiçoados a partir daí? Nada disso. Não é a melhor opção, já que o melhor é a prevenção, mas tem jeito sim. Será um pouco demorado, mas tem jeito.
Existem programas que varrem o disco rígido em busca de arquivos apagados, inclusive da lixeira. Estes programas podem recuperar partições corrompidas, alteradas ou apagadas. Também podem recuperar dados de HDs formatados e até com algumas falhas físicas com baixo grau de comprometimento. São ferramentas usadas pela polícia, em um processo chamado de Forensic (análise para fins judiciais).
As ferramentas desta categoria podem ser simples ou sofisticadas e totalmente baseadas em linha de comando. Para o usuário pouco experiente, sugerimos o programa **Ontrack Data Easy Recovery** (*www.ontrack.com*) que se mostrou capaz de realizar as seguintes tarefas:
. diagnóstico de HDs
. correção de problemas em HDs
. recuperação de dados, mesmo em HDs formatados ou problemáticos
. reparação de arquivos corrompidos: ZIP, WORD, EXCEL, ACCESS, POWERPOINT, OUTLOOK. Ás vezes um arquivo se recusa a abrir. Nesta hora precisamos de um programa que corrija os arquivo corrompido.
O processo de recuperação de um HD com mais de 20 GB pode levar um dia

inteiro. Não tenha pressa caso precise recuperar um HD por este método. E se o HD estiver totalmente inacessível, você vai precisar de uma segunda máquina funcionando ou pelo menos de um segundo HD. Existem ferramentas que fazem esta verificação a partir de um disquete. Mas seu uso não é tão simples e foge ao escopo desta obra.



Concluindo esta lição sobre recuperação de dados, pode ser que você tenha algum CD-Rom ou DVD que apresente erro de leitura no drive. Neste caso você vai precisar de um programa apropriado a recuperação de dados armazenados em CD-Rom e DVD. Estamos falando do **CD Data Rescue** (*www.naltech.com*):



1. Clique em **1** para ler os dados do CD-Rom problemático
2. Clique em **2** para selecionar quais arquivos serão recuperados.
3. Clique em **3** para selecionar o destino dos arquivos e também para dar início ao processo de recuperação.
4. Em **4** você ajusta a profundidade da recuperação.

Dez mandamentos de segurança no PC

PCWorld.com/EUA
31/10/2003 15:34

Em algum lugar do passado recente, um sujeito chamado Bill Gates escreveu: Usarás PC com Windows para trabalhar e acharás ótimo. Mas computadores com Windows são vulneráveis a pragas em proporções bíblicas: vírus que derrubam redes inteiras, worms de e-mails que se replicam na velocidade da luz, cavalos de tróia que se escondem por trás de inocentes programas, hackers que dominam seu computador e muito mais.

Felizmente, arqueólogos desenterraram recentemente dois Tablets de pedra de uma garagem perto de Cupertino, na Califórnia, que podem ajudar a nos livrar dessa maldição. Apresentamos aqui algumas instruções de segurança com interpretações de nossos especialistas.

1) Lembrarás sempre do seu antivírus e sempre ficará atualizado. Não é suficiente apenas ter o software instalado (se você não tem um antivírus, pare de ler esse texto agora mesmo e vá arranjar um logo); você também precisa se manter informado sobre as novas pragas virtuais. "Seu antivirus só é bom se atualizado contra os mais recentes vírus" diz Kelly Martin, diretor sênior de produtos do Norton AntiVirus, Programas como o software da Symantec e o McAfee VirusScan da Network Associates atualizam automaticamente sua base de vacinas, com um custo adicional para assinaturas anuais.

2) Não invejarás o arquivo anexo do próximo. Você recebe uma mensagem com um arquivo anexo que você pensa que é de um amigo seu. Apenas clique, então. Você começará a enviar e-mails infectados para todos na sua lista de endereços. Foi assim que o worm Sobig.F se espalhou - e tudo aconteceu tão rápido que milhões de cópias começaram a se espalhar antes mesmo que as companhias de software pudessem atualizar seus bancos de dados. "Nunca confie no campo Endereço de um e-mail", aconselha Chris Wysopal, diretor de pesquisa para a consultoria de segurança @Stake. "E nunca abra um arquivo sem ao menos verificar se ele foi enviado por uma pessoa de confiança, e ele pretendeu lhe enviar essa mensagem".

3) Evitarás falsos downloads de arquivos. Desconfie de qualquer site que peça que você baixe algum tipo de arquivo para visualizar a página, a não ser que

o software seja familiar, como um plug-in Flash ou o Acrobat Reader. O arquivo pode conter vírus, um cavalo de tróia ou algum aplicativo que programa seu modem a fazer ligações frequentemente, aumentando sua conta de telefone. "Não instale software via Web a não ser que você esteja absolutamente certo sobre que programa é aquele ou confie demais na empresa que lhe oferece o aplicativo" avisa Wysopal.

4) Destruirás spywares e pop-ups. Como cavalos de Tróia, spywares se instalam secretamente quando você baixa algum software que compartilha arquivos pela Web, por exemplo; o spyware segue todos seus movimentos online e lhe mostra anúncios baseados naquilo que você procura pela Web. Anúncios pop-up podem também explorar falhas de segurança no Internet Explorer, como o recente Trojan Qhost que seqüestrava o navegador dos usuários após uma simples visita a um site do Fortune City. Felizmente, existem ferramentas que podem lhe proteger: por exemplo,o Ad-aware bloqueia Spywares gratuitamente e o StopZilla cuida dos anúncios pop-up. Alguns antivírus e pacotes de segurança também impedem spywares e pop-up personalizados na sua cola.

5) Frustrarás os spammers. E-mails comerciais não solicitados são muito mais que apenas chateações; são também uma das maiores fontes para vírus. Em fato, algumas versões de Sobig são programadas para transformar PCs infectados em máquinas zumbi que podem ser usadas para enviar spam. Um bom filtro como o Norton AntiSpam 2004 da Symantec, o McAfee SpamKiller 5, da Network Associates, ou o IHateSpam, da Subelt Software, ajudam a aprisionar essas maldições que escapam a alguns antivírus.

6) Manterás o sistema operacional atualizado pelos pacotes de correção. Worms de e-mail e outras pragas gostam de explorar falhas de segurança em seu software -- em outras palavras, o Windows e outros programas Microsoft. Atualmente a empresa de Bill Gates divulga tantos pacotes para correção de falhas que a maioria dos usuários apenas ignora os avisos. No começo do ano, um worm explorou uma vulnerabilidade que a Microsoft já havia consertado seis meses antes. Mas milhares de computadores infectados -- inclusive alguns dentro da Microsoft -- não tinham a correção instalada. Faça uma visita ao Windows Update pelo menos uma vez por semana e quando os avisos de segurança do Windows aparecerem.

7) Farás um disco de recuperação e o manterás sempre em mãos. Quando a coisa fica feia, um reboot ou um disco de recuperação são parte do primeiro

passo para a recuperação. No mínimo, você colocará os requerimentos básicos de seu sistema operacional em um disquete ou em um ZIP, para que você consiga evitar o disco rígido na inicialização. Uma idéia melhor: use seu antivírus para criar um disco de recuperação que você consiga usar quando o sistema estiver infectado. Cole uma etiqueta nele com a data em que foi feito e guarde-o perto de seu PC.

8) Não cairás em falsos alarmes. Existem mais impostores que hackers na Internet e mais e-mails de alerta sobre vírus falsos do que vírus de verdade. Até mesmo vírus reais são citados em excesso pela mídia. Um alerta falso pode fazer você deletar arquivos que não oferecem risco algum e passar a mensagem para todos seu endereços, entupindo servidores de mensagens e causando danos parecidos a vírus no processo. Quando você recebe um desses e-mails (ou encontra alguma nova notícia bombástica), investigue primeiro. Escreva o nome do suposto vírus em um algum sistema de busca para ver se alguma das maiores empresas de segurança online já tem algum antídoto ou alertas e visite páginas que listam pragas virtuais, como o F-Secure e o Hoaxbusters.

9) Honrarás seu firewall. Um firewall é como um guarda para seu computador - ele checa cada RG em suas portas e não deixa ninguém entrar ou sair se não aprovar. Com ele, um hacker não consegue acessar informações pessoais em seu HD e o logger de teclas (programa espião que monitora todas as teclas digitadas no seu PC) de um cavalo de tróia não conseguirá roubar suas senhas e transmitilas pela Internet. Tanto a Symantec como a Network Associates oferecem pacotes de firewall pessoais, enquanto o Zone Labs oferece uma versão gratuita de seu ZoneAlarm. Mas a melhor solução é um pacote de segurança online que combina antivirus, firewall, bloqueadores de anúncios e spam e outras aplicações extremamente úteis.

10) Farás backups constantemente e irás considerá-los sagrados. Simples: faça um backup de seus dados ao menos uma vez por semana (diariamente, se você estiver mexendo com negócios). Mesmo se você for vítima de um vírus ou um ataque de hacker, seus danos serão bem menores. Não faça esse backup constantemente e você irá direto pro inferno - pelo menos, foi assim que me senti na última vez que isso me aconteceu.

. . . . . .

Esta bem humorada versão dos DEZ MANDAMENTOS aplicadas a segurança do PC, é um resumo de tudo o que vimos anteriormente.

Capítulo 3:

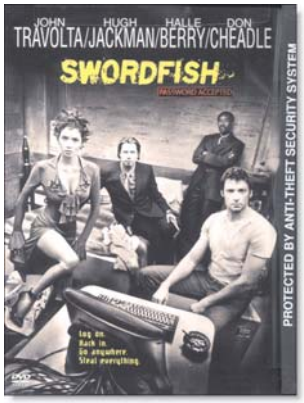
Cracker

Capítulo 3:

Cracker

Objetivos Deste Capítulo:
Após concluir a leitura deste capítulo você deverá ser capaz de quebrar os mais variados tipos de senhas, incluindo senhas de E-Mail. Também deverá ser capaz de definir qual a importância da engenharia social para o hackerismo.

O processo de quebra de senha é uma batalha que envolve TEMPO, CONHECIMENTO, PACIÊNCIA, PROCESSAMENTO, FERRAMENTAS, OPORTUNISMO, ENGENHARIA SOCIAL e TÉCNICA. Filmes tentam fazer crer que um hacker pode mesmo chegar na frente de um computador e quebrar qualquer tipo de sistema em frações de segundo. No filme *Swordfsih* (A Senha), JohnTravolta colocou uma p... para chupar o hacker durante uma cena de cracking. Na cena o hacker era testado quanto a sua capacidade de quebrar sistemas.



Já o filme *Caçada Virtual*, sobre a captura do hacker Kevin Mitnick, foi mais fiel a realidade. Para quebrar a criptografia de certo programa, Mitnick (segundo o filme) usou vários micros da rede de uma universidade, distribuindo a tarefa de quebrar a senha entre as máquinas (clustering). No filme o ator demonstra a impaciência característica antes de obter a quebra do sistema.

Não se deixe iludir pelas aparências. Às vezes uma empresa multinacional, onde se espera o melhor em segurança, possui várias brechas que permitem a descoberta de senhas e portas de entrada para um ataque e invasão. A Nestlê (*www.nestle.com.br*) se encaixa neste perfil. O Grupo Digerati (*www.digerati.com.br*), pioneiro em publicações hacker no Brasil, já teve o site invadido (defacement) por duas vezes.

Se você deixar de lado o medo e o derrotismo (achar que não vai conseguir antes mesmo de tentar), se surpreenderá com a fragilidades das instituições quando operam na Internet. Mas antes de ser um incentivo a baderna digital, é uma sugestão: use este conhecimento para proteção, e cobre por isso.

Sistemas

Entenda por sistema os programas, serviços e recursos presentes em uma rede. Como exemplo de sistemas podemos citar os softwares de qualquer tipo, incluindo os sistemas operacionais, serviços como o de E-Mail, autenticação de usuários em rede local, Internet Banking e muitos outros. O que muda no processo para obter acesso não autorizado a um sistema (cracking) são as estratégias.

Autenticação

Um sistema com restrição de acesso é um sistema cujos recursos só são liberados após a confirmação de se tratar de alguém autorizado. Este processo é chamado de AUTENTICAÇÃO. Um colégio por exemplo, usa a carteirinha escolar para IDENTIFICAR e AUTORIZAR ou NÃO o acesso dos alunos aos seus recursos: aulas, acesso aos professores, dependências, material didático de uso coletivo, etc...

Níveis de Acesso

Em muitos sistemas, além da AUTORIZAÇÃO ou NÃO de acesso (AUTENTICAÇÃO), temos NÍVEIS de acesso, com oferta de recursos diversificada. Por incrível que pareça, alguns sistemas são mais vulneráveis justamente nos níveis onde o acesso permite o uso de um maior número de recursos.

Ainda no exemplo do colégio, se eu quiser entrar como aluno, terei de conseguir um uniforme, falsificar a carteirinha e ainda por cima serei chamado à atenção caso esteja fora da sala no horário de aula (a maior parte do tempo).

Por outro lado, se eu passar por professor substituto ou em meu primeiro dia, não precisarei mostrar nenhum tipo de identificação e terei acesso a todas as dependências do colégio, mesmo no horário de aula.

Uma outra forma de obter acesso, seria me informando sobre o nome de algum funcionário da cantina e citando este nome para o porteiro ou zelador. Isto é a tão falada engenharia social e para obter o nome do funcionário da cantina, basta perguntar a algum aluno.

Um exemplo pessoal

Na Av. Presidente Vargas, principal via localizada no centro do Rio de Janeiro, tem sede de algumas faculdades (campus avançado ou 'caça níquel' se preferir). Estava eu esperando uma condução para Nilópolis (RJ) quando percebi uma baixinha bastante interessante me olhando. Como isto não é normal na minha vida de solteiro, fiz questão de olhar para os lados e para trás pra ver se não era

para alguém próximo que ela estava olhando. Já paguei esse mico e não queira repeti-lo nesta encarnação. Ela percebeu minha exitação e apontou pra mim. Me aproximei e ela manifestou o interesse em me conhecer, disse que era estudante de biologia e começaria um período naquele dia. Com poucos minutos de conversa fiquei bastante animado com as possibilidades a partir daquele encontro. Olhando para o relógio ela disse ter que ir e me deu o número do celular. Perguntei se poderia fazer-lhe uma surpresa. Ela não entendeu bem como seria esta 'surpresa', mas consentiu. Beijinho na boca (um tal de selinho) e foi-se a baixinha estilo Raimunda ou mignon (quem lê *Forum* saberá do que eu estou falando, e não se trata do *forum* da Internet).

Pois bem, a surpresa era assistir à aula ao lado dela. Quem freqüenta faculdade sabe que os mestres não nem aí para quem entra ou sai da sala. O problema era chegar na sala, pois havia uma catraca com cartão magnético. O primeiro passo foi observar como o sistema funciona:

1. O aluno passa pelo segurança do prédio sem qualquer controle.

Nota: Geralmente nestes prédios sempre tem um segurança que é a cara do *baby*. Para quem não sabe, o *baby* é o coleguinha do Luciano Hulk. Aquele que segura a mala (Ôpa!) com o dinheiro dos *Acorrentados* (*http://acorrentados.globo.com/*). Ele está ali só para intimidar com a aprência e porte físico. É como em *Matrix*. O guardião só vai se mexer se perceber algo *fora do padrão*.

2. O aluno passa o cartão magnético
3. O acesso é autorizado

O que poderia me impedir? O segurança nem tanto, já que a entrada até a catraca era livre. Mas a ausência do cartão sim. Notei que alguns alunos passavam antes pela secretaria. Também notei que nenhum deles havia entrado SEM O CARTÃO. Mas o segredo para a engenharia social funcionar é você ACREDITAR NO PRÓPRIO BLEFE.

Fiz assim. Cheguei na catraca e disse:

_*"Hoje é meu primeiro dia aqui e estou sem o cartão. Como eu faço?"*.

A moça simplesmente apertou um botão e liberou a catraca pra mim. E ainda perguntou:

_*"Sabe a sala?"* Eu disse: _*"Biologia. Segundo período!?"* Ela: _*"318, 3º andar."*

Sim. Foi fácil assim. E lá fui eu para o terceiro andar. Logo no caminho identifiquei um mestre pelo andar apressado, pouco cabelo e modo de falar esbaforido. E já foi logo perguntando qualquer coisa para dar mais autenticidade ao blefe. Meu coração estava bastante acelerado: tanto pelo blefe como pela surpresa que eu faria a lourinha. Mas o surpreendido foi eu: assim que botei a cara pra dentro da sala a primeira coisa que vi foi ela agarrada e passando a mão no peito de um colega de classe. Até hoje meu estado de espírito é alterado quando percebo certos olhares na rua.

A lógica por trás dos fatos é bastante simples: investe-se milhares de reais em sistemas e tudo é deixado nas mãos de pessoas que em média recebem 500 reais ou menos de salário. É o mesmo problema das nossas policias: muito poder e força nas mãos de pessoas que em sua maioria, tem que viver com mil reais por mês, às vezes até menos.

Quebrando Tudo

A forma de quebrar um sistema (CRACKING) segue três padrões:

- Cracking por clonagem
- Cracking por vulnerabilidade
- Cracking por adulteração ou engenharia reversa

O **cracking por clonagem** é quando você se passa por quem não é. Exemplos: se passar pelo dono da conta de E-Mail e ler os E-Mails da vítima; se passar como correntista do banco e movimentar a conta bancária da vítima; se passar pelo administrador da rede e usa os recursos da rede.
Na prática, a clonagem é obter uma cópia da autenticação, geralmente nome e senha. Não foi o meu caso ao entrar sem autorização no campus. Naquele exemplo vimos uma **vulnerabilidade do sistema**. No E-Mail por exemplo, se o webmail permitir injeção de SQL ou PHP, ou se o serviço puder ser exploitado, não foi clonagem, foi vulnerabilidade.
Um software que você abre em um editor hexadecimal e altera a autenticação na fonte já é exemplo de **sistema adulterado**. Mesmo se for usado um software que faça automaticamente esta alteração, ainda é um exemplo de cracking por adulteração. Já um software que você consegue o número de série, é mais um exemplo de cracking por clonagem.

Formas de Autenticação

A AUTENTICAÇÃO, como já vimos, é a parte do sistema responsável por verificar se quem PEDE O ACESSO é quem PODE TER O ACESSO. O mais comum é a autenticação pela dobradinha NOME + SENHA. Bancos adotam duas senhas diferentes (uma para usar com o cartão e a outra para usar on-line) e mais uma frase secreta ou grupo de letras ou datas pessoais, como dia, mês e/ou ano do nascimento. Ainda citando o exemplo dos bancos temos a autenticação por instrumento, como é o caso da combinação CARTÃO MAGNÉTICO + SENHA. Outras formas incluem o uso de partes do corpo (biometria), como a íris, impressão digital, formato do rosto e até mesmo o DNA. Fiquemos com as mais comuns: NOME + SENHA.

Como Quebrar Senhas

São várias as maneiras de se obter uma senha:

DEDUÇÃO + TENTATIVA E ERRO
FORÇA BRUTA com dicionário
FORÇA BRUTA sem dicionário
ENGENHARIA SOCIAL (FOOTPRINT) + PHISHING SCAM
BUG
REPOSITÓRIOS DE SENHAS
GERADORES DE SENHAS

Descobrindo Senhas por Dedução

Deduzimos quando chegamos a uma conclusão a partir de fatos ou eventos anteriores. Se ao puxar o rabo de um cachorro levamos uma mordida, podemos deduzir que ao puxar o rabo de uma cobra o mesmo ocorrerá. Já a tentativa e erro consiste em experimentar combinações de nome e senha, desde os mais óbvios aos não tão óbvios, até conseguir a autenticação. Para obter sucesso com esta técnica devemos levar um maior tempo na preparação do ataque (footprint). No livro de minha autoria ***Proteção e Segurança na Internet*** (*www.editoraerica.com.br*) vimos mais de 40 formas de senha fáceis de ser descobertas e que representam mais de 80% das senhas usadas no mundo todo. Embora no livro o objetivo tenha sido de ajudar na criação de uma senha segura, um hacker poderá experimentar cada sugestão de senha podre até conseguir êxito.

Descobrindo Senhas por Força Bruta com e sem dicionário

Existem programas projetados exatamente para quebrar senhas dos mais diversos tipos, tanto de programas e arquivos, como de serviços, o que inclui os E-Mails. Um programa de FORÇA BRUTA pode ou não usar um dicionário. Se a senha for somente numérica, dispensa-se o dicionário. Este método também é conhecido por BRUTE-FORCE ATTACK e DICTIONARY-BASED ATTACK. Alguns fatores devem ser levados em consideração por quem pretende empreender um ataque de quebra de senhas:

. A quebra de senha pode ser local (você está na máquina a ter a senha quebrada ou copiou o arquivo a ser quebrado para a sua máquina) ou remota (pela Internet).
. Dependendo do algoritmo de encriptação do arquivo, da velocidade do seu processador e da complexidade da senha, poderão se passar algumas horas ou dias até que você obter sucesso. Se ainda não assistiu, assista ao filme *Caçada Virtual* com a suposta história da captura do Kevin Mitnick, e poderá ver em uma das cenas, o sufoco que ele passou para poder quebrar uma determinada senha.

. Senhas quebradas remotamente tem a conexão sujeita a falhas e interrupções. Lembre-se que você estará 'forçando a barra' e o sistema pode tornar-se instável.
. Todas as senhas podem ser quebradas. O problema não é SE e QUANDO. A combinação CONFIGURAÇÃO x TÉCNICA determinará o tempo necessário a esta operação. Uma senha que inclua mais de oito caracteres e seja formada por letras maiúsculas, minúsculas, números e caracteres especiais, levará muito mais tempo para ser revelada. Ás vezes damos sorte de encontrar uma vulnerabilidade, como é o caso do Microsoft Access, cujas senhas são quebradas com rapidez e facilidade, independente de quão complexas sejam.
. No Brasil quase não temos bons dicionários para cracking a disposição do hacker. Um bom dicionário deve incluir nomes de times, nomes bíblicos, signos, cores, cidades, empresas, nomes de homens e mulheres, palavrões, apelidos, etc... Existem programas geradores de dicionários. Você paga um arquivo com texto, ele tira deste arquivo todas as palavras e elimina as palavras duplicadas.
. Usuários de conexão dedicada (banda larga) serão mais bem sucedidos em suas quebras de senha remota.

Descobrindo Senhas por Engenharia Social e Phishing Scam

Este tem sido o método preferido de algumas quadrilhas que se passam por hackers. Consiste em obter a senha através da fraude. A engenharia social pode ser combinada com a 'pescaria de senhas', que consiste em criar sites ou enviar E-Mails se fazendo passar por alguma empresa conhecida e com isso obter a senha de mão beijada, dada pelo próprio usuário.
As duas formas que tem sido usadas para fazer o phishing scam são:

. E-Mail falso que remete a uma página também falsa. A senha é capturada na página falsa.

. E-Mail falso que oferece um arquivo.

Este arquivo, se executado ou vai abrir a máquina a uma invasão ou vai capturar a digitação e enviar ao hacker por E-Mail ou vai usar o seu computador para um ataque, como foi o caso do recente vírus MyDoom. Os arquivos mais comuns oferecidos por estes E-Mails são: atualização de software, cartão virtual, jogo, vídeo com nudez, fotos pornográficas, vídeo de algum tema atual, etc...

Bug

Uma autenticação pode ser burlada através de uma falha no sistema. Um erro no código do programa (o Windows tem vários) ou uma falha no processamento. Como analogia temos a porta da frente da casa muito bem protegida e a da cozi-

nha, que usa fechadura gorges. Bugs são 'exploitados' e veremos mais sobre este assunto nos próximos capítulos deste livro.

Repositório de Senhas

Assim como existem os sites de busca de informações, como o Cadê?, Yahoo! e Google, encontramos na internet sites que buscam seriais e cracks. O mais famoso é o:

http://astalavista.box.sk

O inconveniente é que a maioria dos sites listados são armadilhas. Os perigos são:

Trojans – em vez do crack ou serial, poderá estar baixando programas que vão abrir sua máquina para uma possível invasão.

Dialers – programas que cancelam sua conexão local e fazem uma conexão internacional a provedores pagos.

Pop-Up Bomb – a partir da visite ao site suspeito, toda vez que você acessar a Internet aparecerão várias páginas de cassinos e pornografia.

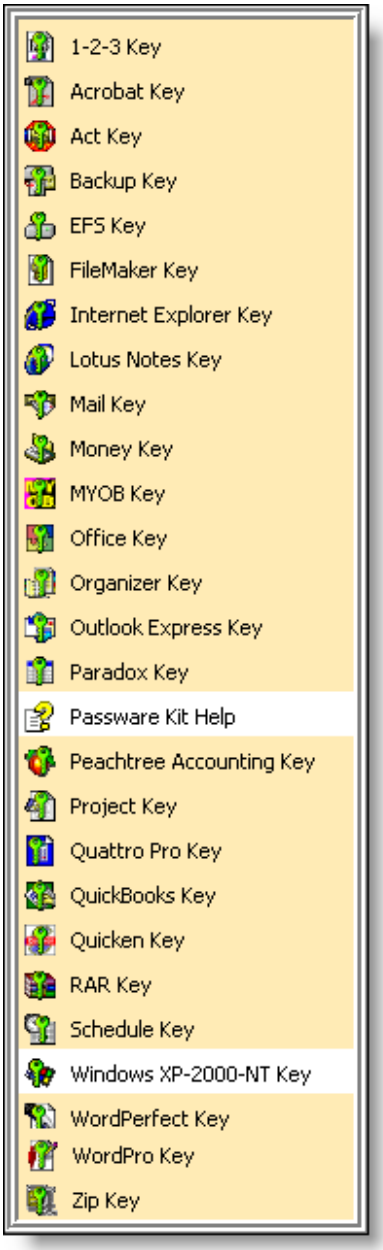
Vírus – em vez do crack ou serial, poderá estar baixando um vírus que vai destruir todos os dados do seu disco rígido.

Mas se você já leu o segundo capítulo deste livro, saberá como se proteger. Eu mantenho uma máquina virtual em meu computador de uso, exclusiva para testes de vírus e aferição de cracks e serials. Fica a sugestão.

Quebrando Senhas de Arquivos

Quando quebrar uma senha de arquivo? Geralmente precisamos quebrar senhas de arquivos cujas senhas esquecemos ou, em se tratando de hacking, quando precisamos abrir um arquivo com senha, sem que tenhamos autorização para isto. Também sabemos que ao usar o Google em suas opções de busca avançada, é comum encontrarmos arquivos que pedem senha para serem abertos. Também existem situações em que um arquivo com senha é disponibilizado para download e, após o pagamento de um valor pré-determinado, a senha é enviada por E-Mail. Para quebrar senhas de arquivos o método mais utilizado é o que faz uso de programas de quebra de senha de arquivos. Como o processo de quebra de senhas é idêntico, sendo a mudança apenas no arquivo a ter a senha quebrada e no programa que vai quebrar a senha, vamos exemplificar apenas a quebra de senhas dos arquivos mais comuns, como os do Microsoft Access (extensão .MDB), Microsoft Word (extensão .DOC) e arquivos zipados (extensão . ZIP).

Existem programas destinados a quebrar senhas de cada um dos principais arquivos existentes no mercado. Optamos pela suite da empresa **Passware** (*www.lostpassword.com*) que possui todas as ferramentas que você precisa para quebrar os mais diversos tipos de senhas de aqruivos. O difícil é achar na lista abaixo um tipo de arquivo cuja senha este programa NÃO QUEBRE:



O processo de quebra de senha usando o software de Passware é muito simples. Na maioria das vezes basta arrastar o arquivo para dentro da janela do programa. Como eu já disse, vamos exemplificar com alguns arquivos e depois passamos a bola pra você. É só repetir o processo para cada tipo de arquivo que desejar quebrar a senha.
Conforme os fabricantes dos programas que tem a senha quebrada identificam as falhas que levaram a quebra da senha, lançam versões ou correções que impedem a quebra de senha, pelo menos por aquele programa que conseguia quebrá-la.
A Microsoft por exemplo, ao atualizar o Windows via Windows Update, aproveita para corrigir falhas em seus outros produtos. Por isso é comum alguns programas de quebra de senha não funcionarem após a atualização do Windows ou mesmo em algumas versões do Windows, como o XP, por exemplo.
Uma das soluções é usar uma máquina virtual com o sistema Windows 98 sem atualizações. Mas só se você estiver tendo problemas de compatibilidade com o seu sistema operacional em uso atualmente, pois uma máquina emulada perde desempenho. Outra ação que deve ser tentada é a busca de atualizações para a versão do programa que você está usando para quebrar senhas.
Outras formas de descobrir senhas de arquivos incluem a engenharia reversa. Sobre este assunto veremos um pouco mais a frente, quando ensinaremos a desbloquear arquivos com limitação de uso (shareware).

Como Saber se o Programa Está MESMO Quebrando a Senha?
A melhor forma de descobrir se um programa está mesmo quebrando a senha do arquivo é criando um arquivo com senhas variadas e usá-lo para teste. Podemos testar arquivos sem senha, com a senha sendo a seqüência 123 ou abc e, obtendo sucesso, podemos passar para testes mais complexos, que incluam letras, números e caracteres especiais. É óbvio que se você criar uma senha para teste muito longa e difícil de ser quebrada, ela vai levar muito tempo para ser descoberta. Nesta hora o bom senso deve prevalecer.
Uma das dúvidas mais comuns dos alunos do Curso de Hacker é sobre a demora na quebra de senhas compactadas pelo Winzip. Dependendo da versão do Winzip e da configuração escolhida na hora de criptografar o arquivo, pode se passar de algumas horas a algumas semanas para obter sucesso na quebra da senha. Principalmente se for usado o método BRUTE FORCE ou um dicionário medíocre.

Quebrando Senhas de Arquivos Microsoft

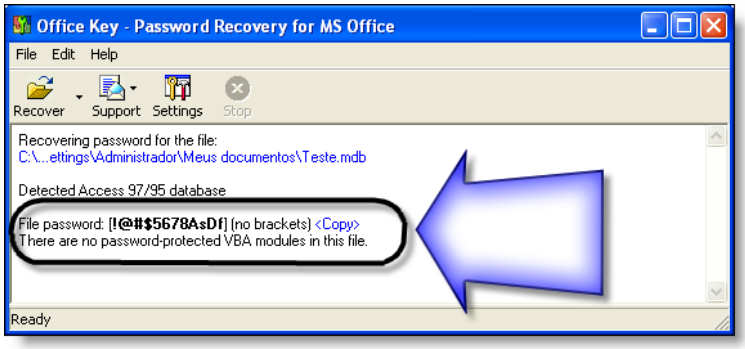
O MS Access é um dos arquivos mais rápidos de ter sua senha descoberta. Dependendo do seu processador, será quase instantânea a revelação da senha. E o

processo também, mesmo nas senhas mais longas e complexas. Já para os arquivos do MS Word e do MS Excel pode levar algum tempo. Na figura abaixo vemos o módulo usado para quebrar senha dos arquivos Microsoft:

O teste foi feito da seguinte forma. Crriamos um documento no Microsoft Acces versão 97, 2000 e XP. Colocamos uma senha de proteção bem difícil, com letras minúsculas, maiúsculas e caracteres especiais. A senha ficou assim:

!@#$%67890AsDfG

Depois arrastamos o documento para dentro da janela do programa. O resultado foi a quebra da senha quase instantâneamente:



Não espere um resultado tão rápido para todos os arquivos, principalmente se foram criados pelos softwares mais atuais.

Antes de iniciar o processo de quebra de senha de arquivos, principalmente dos arquivos que são mais demorados, como o .DOC, .XLS e .ZIP, é importante a configuração do programa (otimização). Esta configuração pode ser acessada através do botão Settings ou opção similar existente em praticamente todos os

programas do tipo. As telas de configuração são fáceis de serem entendidas e costumam ter as seguintes opções:

método de ataque: dicionário, força bruta ou força bruta otimizado
caracteres a serem utilizados: letras, caixa alta ou baixa, números, caracteres especiais, símbolos, espaços em branco.
localização do arquivo de dicionário
uso da CPU no processamento: pouco, médio, prioridade para a quebra da senha
faixa a ser testada: número mínimo e máximo de caracteres

Esta configuração é semelhante à de qualquer outro programa de quebra de senhas de arquivo. Às vezes as configurações deste programas oferecem mais ou menos recursos. Uma configuração mal feita pode fazer com que leve horas algo que poderia ser feito em alguns minutos. Mas ai não tem jeito, só com a prática você vai encontrar o melhor ajuste para cada arquivo que queira ver a senha revelada.

Meu segredo...
As pessoas que me contratam e presenciam como eu quebro senhas de E-Mails com rapidez ficam abismadas com a aparente facilidade. Na verdade o que está por trás desta 'facilidade' é um dicionário de senhas que já chega a 200 MB, uma mente analítica e uma afinada configuração do software. Os mesmos que vocês estão vendo no curso.

Quebrar senhas de arquivos não é mais uma questão de SE e sim de QUANDO. Mas não esqueça do segredo:

MENTE ANALÍTICA + OTIMIZAÇÃO + DICIONÁRIO

E não desista à toa. Tenho alunos que com dez tentativas já jogam a toalha. Chegam a enviar o arquivo para que eu quebre. Posso até fazê-lo, mas isto é um serviço que eu cobro, e caro.

Diálogos:
Lamer: _ *"Professor. Quebre a senha deste arquivo para mim que eu faço o curso."*
Professor: _*"OK. Faça um depósito no valor de mil reais pela quebra da senha e leve o MÓDULO 1 de brinde."*

Existe um campo de trabalho a ser explorado. Já sugerimos a recuperação de HDs formatados e arquivos apagados (ensinado no capítulo dois). Você poderá prestar mais este serviço aos seus clientes: a recuperação de senhas de arquivos e E-Mail.

Descobrir a senha do próprio E-Mail ou do E-Mail de outra pessoa com a autorização dela própria, se assemelha a chamar um chaveiro para abrir a porta da casa em que se perdeu a chave. Não é motivo de preocupação ou medo. Recebo E-Mails de pessoas que precisam da senha do próprio E-Mail. Perdida por esquecimento ou ação hacker. Já ajudei pessoas que esqueceram a senha dos arquivos armazenados no disco rígido. Já foi contratado para desbloquear servidores travados, cuja senha o funcionário demitido não revelou. Estes exemplos mostram que é possível ser um hacker, agir dentro da legalidade e ainda ganhar dinheiro com isso.

Descobrindo Senhas de E-Mail

Vamos aprender a criar nosso próprio dicionário e a quebrar senhas de Telnet, FTP, WWW e POP (E-Mail) remotamente. Ao quebrar senhas de Telnet você terá acesso a um servidor, podendo usá-lo como ponte de ataque se desejar. Ao quebrar uma senha de FTP você poderá baixar os arquivos de acesso restrito ou armazenar arquivos para distribuição ou recuperar posteriormente. Também poderá ter acesso a pasta onde ficam armazernadas as páginas de um site, podendo alterá-las se quiser (defacemente). Ao quebrar senhas de páginas Web você terá acesso a áreas restritas do site, como áreas de alunos ou áreas de assinantes por exemplo. Ao quebrar a senha do serviço POP você terá acesso a caixa postal de E-Mail da vítima.

Dicionários (Wordlists)

Um dicionário pode ser obtido de três formas:

- Baixando da Internet
- Com um programa gerador de dicionário ou 'lista de palavras'
- Com um programa compilador de 'listas de palavras'

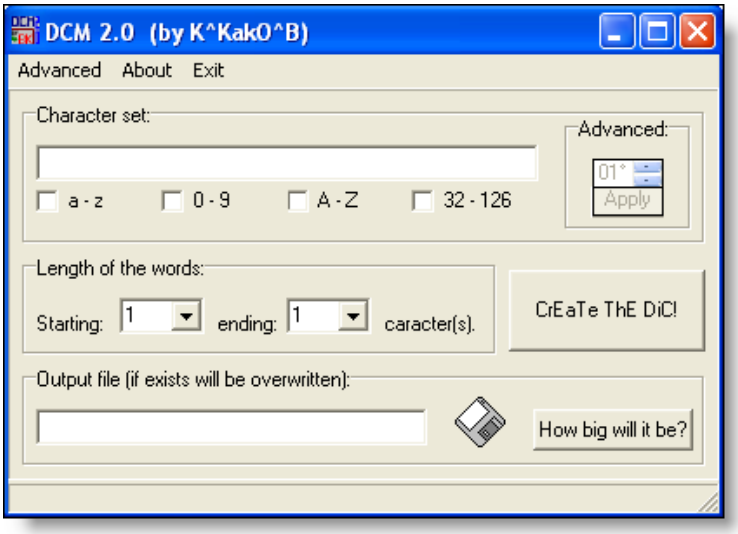
Para nós brasileiros, baixar da Internet é a pior opção. Enquanto os americanos e argentinos encontram dicionários com mais de 2 GB de tamanho, nos sites brasileiros é praticamente inexistente dicionários de qualidade em língua portuguesa. O meu é fruto de mais de cinco anos de palavras catadas sempre que a oportunidade apareceu.

Uma solução simples e eficaz é baixar um dicionário americano e usar um programa TRADUTOR, tipo o Power Translator. Depois é só salvar ou exportar a

wordlist traduzida. Ou então criar a própria wordlist. Os programas que fazem isto trabalham de duas formas: a primeira é combinar letras, números e caracteres para gerar palavras (na maioria das vezes sem significado algum), conforme podemos ver na lista abaixo (no exemplo definimos palavras com 3 caracteres):

```
aaa
aab
aac
aad
aae
aaf
aag
 .
 .
 .
zzz
```

Um programa deste tipo é o DCM 2.0 que pode ser encontrado no CD-Rom que acompanha este livro:



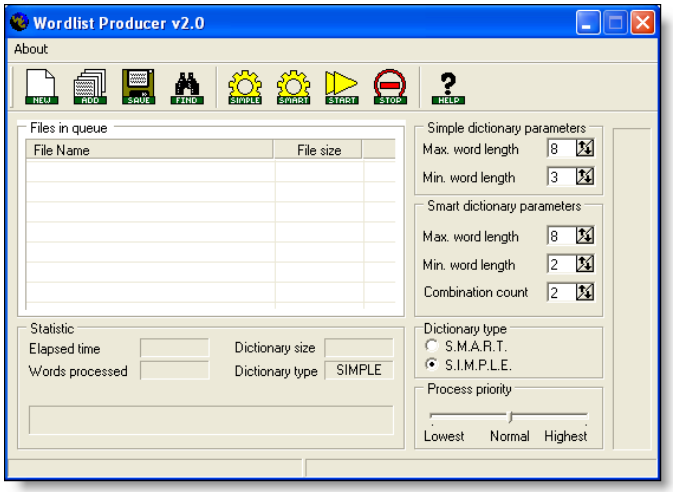
Outros tipos de geradores de listas, lêem um texto qualquer, compilam todas as palavras encontradas e removem as repetidas. No exemplo, a frase:

"Não perca nosso próximo lançamento: O LIVRO VERMELHO DO HACKER BRASILEIRO."

Vai gerar a seguinte wordlist:

```
BRASILEIRO
DO
HACKER
lançamento
LIVRO
Não
nosso
O
perca
próximo
VERMELHO
```

Você poderá usar qualquer arquivo de texto para gerar a wordlist. Minhas sugestões incluem: a Bíblia, compilação de páginas sobre esportes, signos, palavrões, medicina, informática, filmes famosos (Matrix por exemplo) e séries (Jornada nas Estrelas por exemplo), cidades, estados, nomes de bebês, listas de aprovados, listas de senhas padrão, etc...
Um programa que gera wordlist desta maneira é o Wordlist Producer v2.0 que pode ser encontrado no CD-Rom que acompanha este livro:



1) Clique em ***New*** para começar uma nova wordlist
2) Clique em ***Add*** para incluir um ou mais arquivos texto. Estes arquivos terão todas as suas palavras capturadas, com a exclusão das palavras repetidas.
3) Clique em ***Start*** para gerar a wordlist.
4) Clique em ***Save*** para salvar a wordlist.

As opções **SIMPLE** e **SMART** permitem gerar wordlists a partir da combinação de caracteres.

Brutus

O Brutus é um excelente programa para quem está começando a descobrir senhas de serviços como Telnet, FTP, WWW e POP (E-Mail). O Brutus pode ser baixado do site:

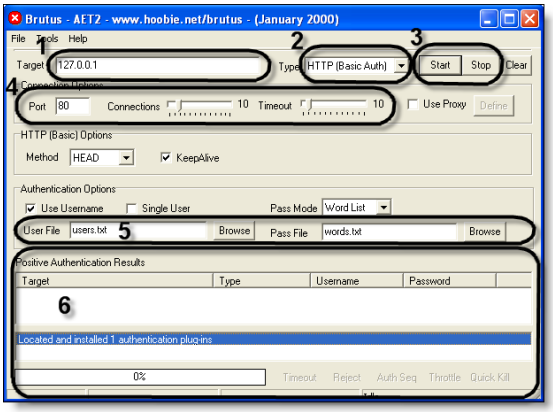
www.hoobie.net/brutus

Da mesma forma que os programas de quebra de senha local, o Brutus precisa ser configurado para que funcione corretamente. A maior parte dos problemas relatados com o uso do Brutus se deve a má configuração. Para cada alvo será necessário um ajuste fino nas configurações. Uma configuração pode ser SALVA e recuperada posteriormente. Basta acessar o menu *File -> Export Service* e recuperar com *File -> Import Service*.

Você pode inclusive salvar a sessão e recomeçar em outro dia e outra hora. Use o menu *File -> Save Session* e recupere com *File -> Load Session*. Se não ficou claro a importância deste recurso, vamos lá: suponha que eu queira obter a senha do alvo www.abc.com. Posso deixar o Brutus trabalhando durante toda à noite. Pela manhã salvo a sessão de ataque e na noite seguinte recomeço de onde parei. Seguindo assim até quebrar a senha. Eu já disse que quebrar senhas não é uma questão de SE e sim de QUANDO.

A configuração básica do Brutus inclui:

1. Selecionar o alvo (IP ou endereço)
2. Selecionar o protocolo (para E-Mail é o POP)
3. Iniciar ou Interromper o processo
4. Selecionar a porta (80 para WWW , 21 para FTP e 110 para E-Mail)
5. Selecionar a wordlist
6. Acompanhar o processo e visualizar o resultado.



Em *Target* você insere o domínio ou IP do alvo. Em *type* você seleciona o protocolo conforme o caso. A maior parte dos alunos que reclama de não conseguir sucesso com o Brutus, quando vem tirar dúvidas comigo, constatamos ser problema de configuração ou de paciência (falta de paciência para aguardar o programa fazer o serviço, como por exemplo depois de meia hora tentando já desistir e pedir ajuda).

Os provedores usam normalmente o endereço *pop.provedor.com.br* ou *pop3.provedor.com.br*. Verifique no próprio site do provedor o *help* sobre como configurar o E-Mail. ou então abra uma conta no provedor a ser atacado, que tenha senha rápida de ser quebrada, como 123 por exemplo e teste a configuração do Brutus. Alguns endereços de provedores de E-Mail:

BOL	pop.bol.com.br
BrFree	pop.brfree.com.br
Click 21	pop.click21.com.br
Embratel	pop-gw.embratel.net.br
Globo.Com	pop3.globo.com
iBest	pop.ibest.com.br
IG	pop3.ig.com.br
Matrix	pop.matrix.com.br
Rede Livre	pop.redelivre.com.br
Telecom	pop3.telecom.net.br
Telemar	pop3.Telemar.net
TERRA	pop.bnu.terra.com.br
Uai	pop.uai.com.br
Unisys	pop.unisys.com.br
UOL	pop3.uol.com.br
Yahoo!	pop.mail.yahoo.com.br
Zipmail	pop.zipmail.com.br

Os botões START, STOP e CLEAR servem para INICIAR o processo, PARAR o processo e LIMPAR as informações dos campos. Quero aproveitar para lembrar que os provedores mais populares, como os da lista acima, são os mais bem protegidos. Até por que sofrem ataques o tempo todo e obrigam a equipe de manutenção a cuidarem de todos os detalhes que possibilitem uma invasão. Não são a melhor opção para quem está inciando. Sugiro que comecem seus experimentos em servidores de pequeno porte, do interior por exemplo, e conforme ganharem cobfiança (e aprenderem a configurar o programa), passem para servidores maiores.

Digo isto por que é muito frustrante você aprender algo e quando tenta colocar

em prática não é bem sucedido. Quando eu comecei a consertar aparelhos de rádio e TV aos quatorze anos de idade, recebia para consertar aparelhos antigos 'encostados' pelos seus donos. Nasci antes da *Era Collor*. Uma época em que as pessoas levavam seus aparelhos para conserto tantas vezes quantas forem necessárias. Hoje em dia os aparelhos eletrônicos são semi-descartáveis. A tecnologia evoluiu tanto que um televisor tem garantia de até dez anos. Findo este prazo seu televisor já estará obsoleto devido a chegada da TV digital.

Mas voltando aos aparelhos que me davam para consertar, eu penava muito e quase não conseguia consertar nada. Eu fazia tudo certo, mas dava tudo errado. Persiti na profissão até que com o tempo eu percebi que aqueles aparelhos encostados os técnicos profissionais não pegavam para consertar. Eram aparelhos que até chuva já tinham tomado e ficava impossivel deteminar, no meio de tanta coisa estragada, quais componentes deveriam ser substituídos. Sendo iniciante, eu deveria começar a consertar os aparelhos mais modernos, de preferência com o primeiro defeito e só então partir para os abacaxis. Até os aparelhos com muitos defeitos deveriam ser evitados, devido aos gatilhos que alguns técnicos colocavam para o aparelho funcionar. Mas nunca, sendo um inciante, eu deveria receber um cacareco para consertar. Infelizmente só aprendi isto depois de perder muito tempo, dinheiro e parte das esperanças. O mesmo ocorrerá com você, ainda inexperiente, se escolher como primeiro alvo o site www.globo.com por exemplo. Primeiro começo pelos sites pequenos e depois que entender como as coisas realmente funcionam, passe a voar mais alto.

Voltando ao Brutus depois dessa pausa, podemos dizer que um outro erro muito comum na configuração do Brutus é informar a porta errada. Cada serviço possui sua porta padrão (que pode ser alterada pelo provedor). As portas mais comuns são:

POP3 (E-MAIL) 110

HTTP (para quebrar senhas de área protegida de sites, inclusive área de administração) 80, 81, 8080

TELNET (para acesso remoto, inclusive de roteador) 139

FTP (protocolo de transferência de arquivos que às vezes permite acesso à pasta de hospedagem do site. Podemos usar para defacement.) 21

Em *Port* você informa a porta adequada. Use o *Languard* para confirmar se a porta é a padrão ou se foi alterada(este programa está no CD-Rom que acompanha este livro e seu uso será ensinado posterioremente). Alguns administradores de rede mudam a porta padrão para dificultar ataques, principalmente os feitos por lamers e *scrip kiddies*.

Em *Connections* você informa quantas conexões serão abertas entre o seu micro e o alvo. Um número de conexões muito grande pode resultar em instabilidade e até perda de conexão. É questão de experimentar. O Brutus suporta até 60 conexões simultâneas e aproximadamente 2500 autenticações por segundo, dependendo da conexão.
Em *Timeout* você configura o tempo que o Brutus deve aguardar uma resposta do servidor alvo. É outro campo a ser experimentado, caso você receba sucessivos avisos de *Timeout*. Este é um dos campos mais críticos.
Em *Proxy* você informa o IP e porta do servidor proxy, caso esteja utilizando algum. Se você usar um servidor proxy público para permanecer anônimo, faça o ajuste fino do *Timeout* e esteja pronto para uma espera adicional devido ao percurso ter incluído uma passagem pelo servidor proxy público.
Se você não tem a menor idéia de como o servidor faz a troca de parâmetros, terá de experimentar diferentes opções de *Method* até obter sucesso. A configuração das opções HTTP só é necessária quando você está trabalhando na quebra de uma página protegida.
Finalmente as opções de autenticação, onde podemos fazer um ataque global ou a apenas um usuário (opção *Single User*). O modo de busca da senha poderá ser por *Word List* (você possui um dicionário), *Combo List* (você possui uma lista pequena, com palavras que poderão ser a senha) e *Brute Force* (o Brutus vai tentar combinações até conseguir a senha).
Em *User file* você informa a lista de usuários. Use o botão *Browse* para localizá-la.
Em *Pass file* você informa o dicionário de senhas. Use o botão *Browse* para localiza-la.

Nota: o nome de usuário tanto pode ser usuário como pode ser usuário@provedor.com.br. As duas formas são usadas, mas depende de como o provedor autentica seus usuários.

Como forma de proteção, os provedores de grande porte costumam restringir o número de tentativas de acesso a uma conta de E-Mail. Isto significa que a conta poderá ser bloqueada por algum tempo ou permanentemente, caso um ataque *brute force* seja detectado pelo provedor.

Um resumo dos problemas mais comuns ao usar o Brutus:

- SUCESSIVAS QUEDAS DE CONEXÃO – as conexões discadas são péssimas para uso em quebra de senha remota. Adote uma conexão decente (banda larga).

- O BRUTUS NÃO ENCONTRA A SENHA – as causa são várias sendo as mais comuns:

configuração mal feita
IP ou endereço errado
uso de firewall ou proxy

A solução é configurar o programa corretamente, verificar se o IP ou endereço é mesmo o do servidor alvo e desabilitar o firewall, mas somente se estiver interferindo no processo de busca da senha. Cada firewall funciona de forma diferente e alguns impedem o Brutus de funcionar.

- O MICRO CONGELA – programas de hacking e cracking rotineiramente fazem o micro congelar ou 'rebootar' (reiniciar sozinho). Use hardware de qualidade. Fuja das placas on-board e tenha uma excelente placa de comunicação (rede ou modem). Por que será que a placa 3Com custa 150 reais e a Genius custa apenas 20? Por que será que o modem US Robotics custa de três a quatro vezes mais caro que o Lucent? A qualidade do hardware também influencia na qualidade da ação hacker. Não determina, mas influencia.

- ESTÁ DEMORANDO – não tem como fugir do tempo. Só filmes de ficção mostram hackers sentando e quebrando senhas em minutos. Assista ao filme do Mitnick e verá que ele usou vários computadores em cluster para quebrar uma senha localmente. O tempo que leva para quebrar uma senha varia muito. Dependendo do servidor eu levo de dois minutos a dois dias. Você precisa ter PACIÊNCIA, CONEXÃO, HARDWARE, TÉCNICA, SOFTWARE e BRAIN.

- DURANTE A BUSCA DA SENHA A CONEXÃO CAI – alguns servidores são configurados para cortar a conexão depois de determinado número de tentativas. Também devemos levar em conta sua conexão, hardware e o sistema operacional em uso.

Nota: o Brutus tem um gerador de wordlists no menu *Tools*. Não use, este módulo tem bug e é muito ruim.

Como testar um programa de quebra de senhas?

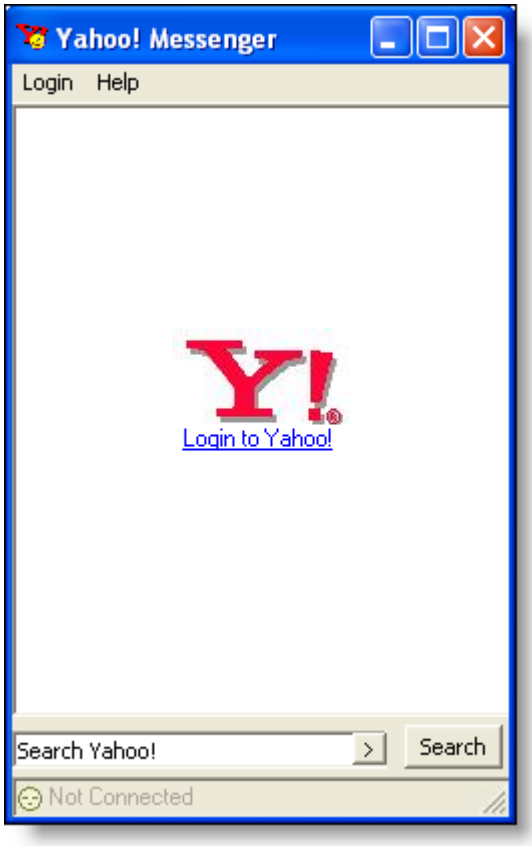
Já falei sobre isto, mas vou repetir. Antes de começar a quebrar senhas por aí, teste o programa. Já dei exemplos quando falei sobre quebra de senhas de arquivos: criar um arquivo com senha fácil de ser quebrada. Se o programa quebrar a senha fácil, quebrar a mais difícil (a que você quer realmente), será mesmo uma questão de TEMPO.

No caso da senha de E-Mail, se puder, crie uma conta de teste e coloque uma senha fácil de quebrar. Se o programa quebrar a senha, provou que funciona. A senha a ser quebrada será apenas uma questão de ter paciência.

Outros programas de quebra de senha POP3, Telnet, FTP e HTTP são o Entry 2.7 e o WWWHack, ambos disponíveis no CD-Rom que acompanha este livro.

Fake Login

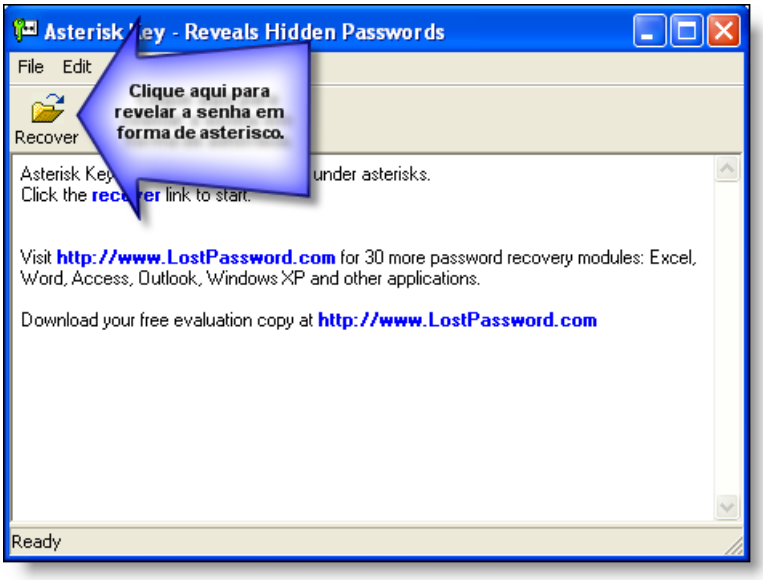
O fake login é simples de ser feito, mas seu uso depende do acesso a máquina local, seja da empresa, residência ou cybercafé. Fake login consiste em simular um LOGIN, para que o alvo entre com nome e senha sem perceber se tratar de uma cilada. Vamos encontrar fake login imitando ICQ, messenger, webmail, autenticação de servidor, etc... Na figura abaixo temos um exemplo de fake login:



Com o mínimo de conhecimentos de Visual Basic ou Delphi é possível copiar a tela de login de qualquer programa. Com um pouquinho mais de conhecimento é possível capturar os dados e gravá-los no disco rígido. E sabendo programação de sockets, você poderá criar um trojan.

Revelando Senhas Ocultas em Asteriscos

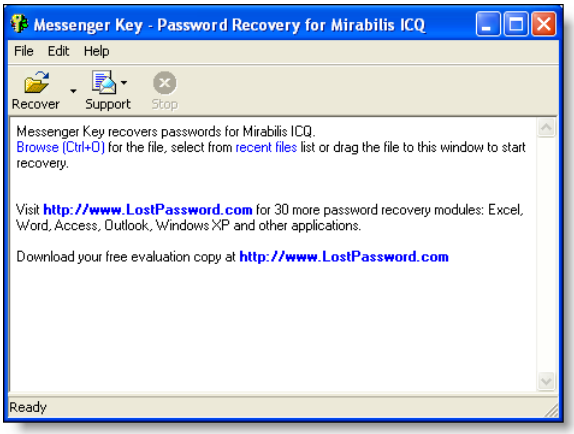
Também existem programas especializados em revelar senhas em forma de asteriscos. Nesta categoria, também da Passware temos o *Asterisk Key*:



Quebrando a Senha dos Serviços de Mensagem Instantânea

Existem duas formas de ação hacker: *inside* (o hacker tem acesso a máquina localmente) e *outside* (o hacker só tem acesso remoto). Alguém que tenha acesso a rede local da empresa, um técnico de empresa terceirizada ou um funcionário insatisfeito por exemplo, só não conseguirá fazer o que não quiser. A política de segurança é voltada para ataques de fora para dentro. Daí a proliferação dos trojans, que se comunicam com o hacker de dentro para fora e burlam as defesas proporcionadas pelo firewall.

Feito para uso local, o programa *Password Messenger Key* recupera senhas do ICQ. Funciona da maneira mais simples possível, arrastar e soltar.



Como Crackear Programas

Outra habilidade que todo hacker precisa desenvolver é a quebra de senhas de softwares. Existem diversas formas de quebrar a senha dos softwares. Para algumas você vai precisar de conhecimentos avançados de programação, o que foge ao objetivo deste livro. Para outras, basta saber procurar no lugar certo.

Quando quebrar senhas de softwares?

Usualmente vamos precisar quebrar senhas de programas quando não temos interesse ou condições para adquirir o produto pagando por ele. Às vezes o motivo é até nobre: a empresa não vende o produto em nosso país. Às vezes nem tão nobre, como quando adquirimos cópias alternativas de produtos facilmente encontradas no comércio formal, como os produtos da Microsoft, da Corel e da Adobe, que são os mais pirateados.

Antes de quebrar a senha, veja se alguém já não o fez

Seu tempo deve ser aproveitado ao máximo. Então, antes de começar a quebrar a senha de um programa, verifique se já não se encontra disponível o SERIAL ou o CRACK na Internet. Continue lendo para saber como se faz.

Como Procurar Cracks e Serials na Internet

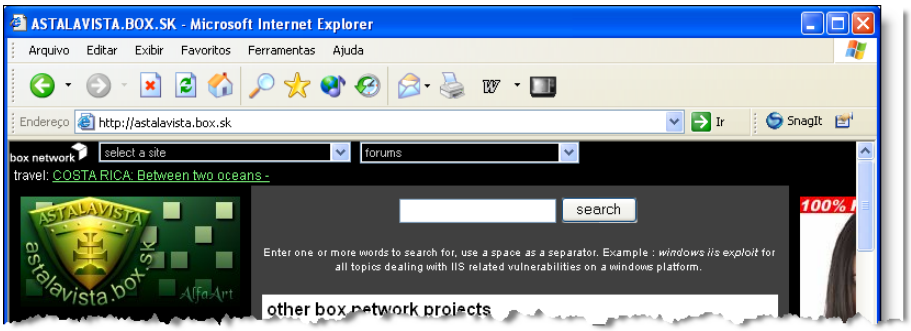
Assim como existem sites de busca de links, também existem sites especializados em buscar informações sobre determinado assunto: MP3, imagens, clipping de notícias e também CRACKS e SERIALS. O mais famoso é o portal de buscas do site Astalavista, que desde 1994 serve a comunidade:

http://astalavista.box.sk

Quando você digita o nome de um programa no campo de busca do Astalavista, vai receber de volta links para sites onde poderá ser encontrado o crack, serial ou keygen do programa procurado.

AVISOS IMPORTANTES:

1) Atenção quando for baixar o crack. A maioria dos sites vai tentar instalar trojans



em sua máquina . O segredo para se proteger é bem simples: NÃO ACEITE A INSTALAÇÃO DE NENHUM PROGRAMA EM SUA MÁQUINA, mesmo que no aviso indique que sem a permissão para instalar o tal programa você não poderá baixar o crack.

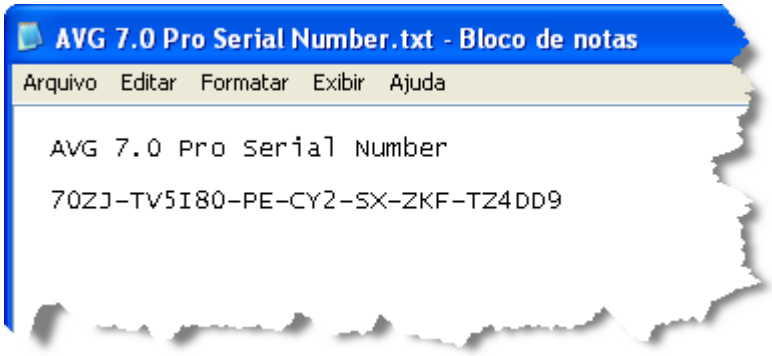
2) Outro problema com o qual você irá se deparar é a excessiva oferta de sites pornográficos e cassinos. Estas 'ofertas' se manifestarão através de múltiplas janelas abertas em seu navegador. Há casos em que o browser chega a travar devido ao excesso de processos simultâneos. Nada que um anti pop-up não resolva. Desconfie de algum um *malware* instalado, caso as janaleas pop-up se tornem frequentes durante a navegação na Internet.

CRACK – são pequenos programas que alteram o código do programa original, removendo ou adulterando a parte que bloqueia ou limita o produto. Cada programa possui um sistema diferente de proteção contra crackers (há há há). A proteção pode ser através de um arquivo .INI, inserção no REGISTRO, código embutido no arquivo executável, algum outro arquivo oculto para o controle do registro, proteção por hardware e diversas outras formas.

Na figura ao lado temos o CRACK do programa AutoPlay Menu. Este tipo de CRACK normalmente precisa ser executado na mesma pasta em que foi instalado o programa a ser crackeado. Alguns CRACKS consistem na substituição do arquivo original por outro já crackeado. E uma minoria exige que se faça algumas ações para efetivar a liberação do programa. Estas informações são encontradas no arquivo Leia-me que costuma acompanhar os programas crackeadores. Àntes de usar um crack, abra e leia o conteúdo dos arquivos com extensão .txt, .diz, .nfo e .doc.

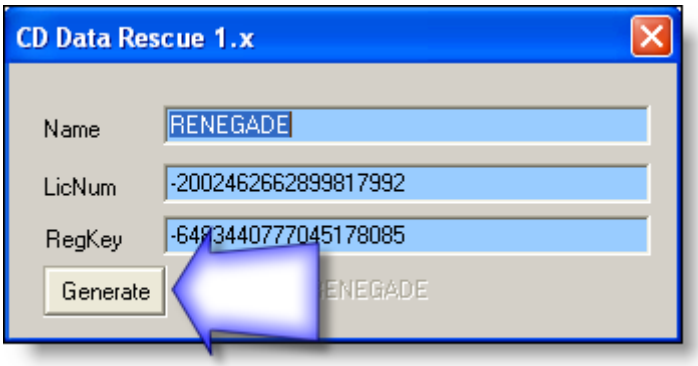
O perigo no uso de programas crackeadores é que, por se tratar de algo geralmente ilegal (crackear programas comerciais), estaremos lidando com pessoas cuja ética não será a maior virtude. Em resumo, é muito comum um TROJAN vir disfarçado de CRACK.
Pode ocorrer de um programa crackeado deixar de funcionar. Muitas empresas usam as facilidades da Internet para se comunicar com sua base de programas instalados e desativar programas adulterados.

SERIAL – a maioria dos softwares pede apenas um número de série para permitir o acesso completo ao programa. Isto quer dizer que qualquer pessoa que tenha este número de série vai poder usar o programa sem qualquer restrição. Buscar na Internet nos sites especializados em SERIALS será suficiente para fazer a maioria dos programas rodar sem limitações.

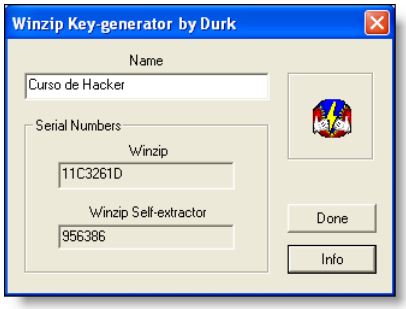


Existem programas que permitem a digitação de qualquer número como número de série, ou pelo menos, que seja digitado no formato da máscara aceita pelo programa. Geralmente o que se perde ao entrar com um número de registro qualquer é o suporte ao produto. Mas volto a repetir, uma MINORIA de programas aceita esta forma de desbloqueio. Versões mais antigas do Corel Draw aceitam sequencias de 1 a 9 como número de série.

KEYGEN – uma outra categoria de programas SERIALS é o gerador de SERIAL ou KEYGEN. Como o nome já diz, trata-se de programas que gera números de série, incluisve permitindo a personalização da sua cópia pirata do software. Alguns CRACKERS criam geradores de seriais (KEYGEN) e crackeadores com design arrojado.
Nesta categoria de crackeadores, vamos encontrar desde programas que se limitam a exibir um único número de série , até aqueles que geram o número de série com o mesmo algoritmo usado pelo software original.

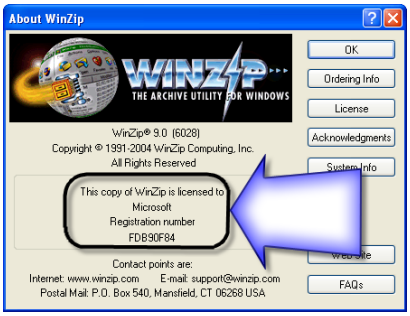


Outro KEYGEN, gerando o serial do Winzip, que serve para as versões de 6 a 9:



O CRACK acima gera números de desbloqueio para o Winzip, da versão 6 a 9 que é versão atual. Podemos observar que o mesmo programa também gera o código de desbloqueio para o Winzip Selfextractor.

Às vezes, ao procurar por um CRACK, não encontramos para a versão do programa que temos em mãos. Vale a pena experimentar cracks de versões anteriores ou posteriores. Em outras ocasiões precisamos nos contentar em usar uma versão mais antiga do programa (crackeada) até conseguirmos o crack da versão mais atual do mesmo programa. Alguns programas possuem diferenças irrisórias entre uma versão e outra.



MULTIKEYGEN, MULTISERIALS ou MULTIMAKER - os programas de geração de múltiplas licenças de uso são úteis quando usamos vários programas do mesmo fabricante, como é o caso da Microsoft e da Adobe. Funcionam da mesma forma que o KEYGEN, porém gerando números de licença para vários programas, geralmente do mesmo fabricante.

Pequeno Glossário do Cracking

SERIAL – número usado para controlar a quantidade e a distribuição de um produto. Supondo uma tiragem deste livro de cem exemplares, eu poderia numerá-los de 001 a 100. Se algum dia encontrasse alguma cópia tipo Xerox, saberia de onde partiu a cópia não autorizada. Os números de série incluem informações úteis aos fabricantes. No exemplo do livro, eu poderia incluir dados sobre região da compra, data, versão do livro e tudo o mais que julgar útil e oportuno.

Quando você compra um programa de computador, não está adquirino o programa e sim uma licença de uso. No contrato que costuma acompanhar este tipo de produto, os termos do licenciamento são definidos e geralmente proibe, entre outras coisas, a instalação em mais de um computador. Estes termos do licenciamento costumam ser exibidos durante a instalação do programa, mas a maioria das pessoas não dá importância a este contrato.

O número de série também pode ser usado para desbloquear o software e para rastrear a origem das cópias não autorizadas. Mais recentemente tem sido usado para bloquear a distância, softwares instalados irregularmente.

CRACK – é um programa, geralmente de tamanho bastante reduzido, usado para alterar o código de proteção dos softwares. Uma vez este código alterado, o programa poderá ser usado normalmente como sem qualquer restrição. Como se fosse o programa original.

PATCH - são programas com dois siginificados. Existem patchs que corrigem falhas (bugs) em outros programas. São os patchs de correção. Exemplo. O jogo XPTO não roda em placas com vídeo on-board. Aplicando o patch este problema é resolvido. Mas temos também os patchs que são cracks. Ao aplicar o patch a limitação do produto é removida.

KEYGEN - são programas que geram o número serial necessário ao desbloqueio de determinado software. A grande vantagem ao usar um KEYGEN no lugar do SERIAL é a possibilidade de personalizar a cópia crackeada.

PROGRAMA DEMO - são programas destinados a demostrar as características do produtos para ajudar o comprador a se decidir pela aquisição ou não do produto. Alguns programas do tipo demo são distribuídos incompletos. Não há como crackeá-los por que não existe a parte do código necessária ao funcionamento das opções bloqueadas. Mas também existem programas demo que são completos, dependendo única e exclusivamente de um número de série para funcionar sem qualquer limitação. Estes são os mais crackeados.

PROGRAMA BETA - algumas empresas liberam cópias de seus produtos a grupos de usuários, para que o avaliem, antes da distribuição da versão definitiva. Estes programas de avaliação restrito ao grupo de testes é chamado de BETA e seus testadores são conhecidos como betatesters. Embora o Windows 2005 (Longhorn) só esteja disponível no próximo ano, nós já estamos experimentando uma versão beta deste sistema operacional. Existe também a versão ALFA, geralmente restrita aos laboratórios do fabricante.

PROGRAMA DESBLOQUEADO – aquele em que se usou um número serial. Não houve alteração nas linhas de código do programa.

PROGRAMA CRACKEADO – aquele que foi desbloqueado a partir da alteração em suas linhas de código. Estas alterações podem ter sido feitas manualmente ou via software (CRACK).

CHAVE DE ATIVAÇÃO - trata-se de um sistema de controle de distribuição de software que teoricamente deveria por fim a pirataria. Na prática funciona desta forma: você adquire o programa e recebe um SERIAL válido por 30 dias ou mais. Até o fim deste prazo, você precisará entrar em contato com a representação do fabricante e confirmar seus dados: on-line, pelo correio ou por telefone. Caso contrário o produto deixará de funcionar. Ou seja, continua sendo aquele REGISTRO que todo programa pede. A diferença é que agora o produto passa a ter um duplo registro, deixando de funcionar se você não confirmar ser o legítimo dono. Como toda proteção, este sistema também foi adulterado e já é possível encontrar nos mecanismos de busca especializados em cracking, tanto o serial dos produtos com ativação, quanto a própria chave de ativação. Mas não confie cegamente na chave de ativação e mantenha o backup atualizado.

Um caso...
Fui chamado às pressas (como sempre) para resolver um problema que o administrador de redes da empresa não estava dando conta. O servidor estava bloqueado devido ao uso de uma cópia pirata do Windows Server 2003.
Em particular, o administrador da rede me confidenciou que usou uma CHAVE DE ATIVAÇÃO baixada da Internet via rede Kazaa e que aparentemente estava tudo certo... até terminar o prazo para a ativação.
Minha vontade era de dar um sermão no biltre por usar um programa pirata como servidor de redes de empresa. Mas depois de saber que a criatura ganhava menos de seiscentos contos por mês para manter a rede funcionando, pensei em como esta empresa era feliz por ainda encontrar gente que trabalha de graça, só por casa e comida.
Depois de fazer caras e bocas como se tudo estivesse perdido, saquei do bolso meu ...

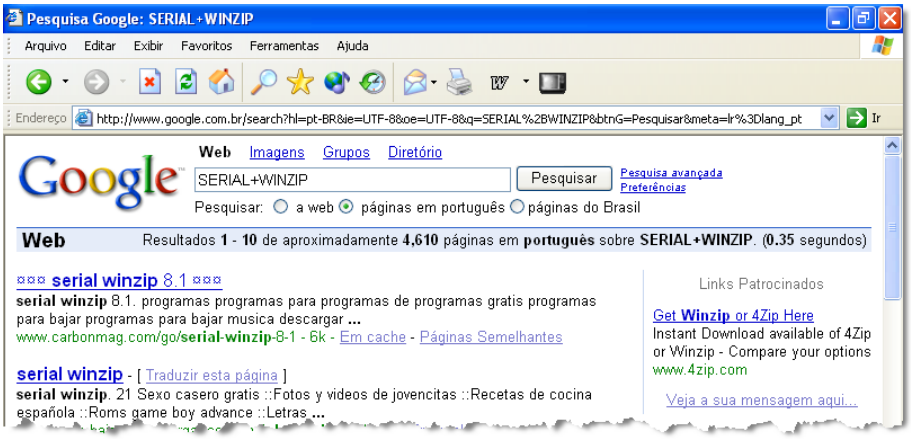
O que interessa na história acima é perceber que as chaves de ATIVAÇÃO baixadas da Internet não são 100% confiáveis. Como a quase totalidade das empresas e pessoas estão se conectando, os fabricantes estão desenvolvendo sistemas que, de tempos em tempos, verifica em sua base de programas instalados a existência de cópias piratas e simplesmente as desativa. Ano passado a Microsoft bloqueou milhares de cópias na Europa. Isto incluiu cópias adquiridas legalmente e gerou grande transtorno entre os usuários.
Atualmente, os usuários de cópias piratas do Windows XP, são impedidos de fazer o download do Service Pack 1. Incluimos no CD-Rom que acompanha este livro programas que alteram o registro do Windows XP e permitem o download do Service Pack 1 sem maiores problemas.
ENGENHARIA REVERSA - é a arte de descobrir como um programa foi construído. Exige bons conhecimentos de programação e das ferramentas usadas para 'desconstruir' o código. Hackers usam a engenharia reversa para copiar, modificar, desbloquear, personalizar ou criar scripts e programas que explorem as eventuais vulnerabilidades encontradas (exploits).
PROTEÇÃO POR HARDWARE - algumas empresas fornecem junto com a cópia original do programa, algum dispositivo de hardware como forma de combater a pirataria. Nesta categoria vamos encontrar programas que só funcionam com placas proprietarias ou com a instalação de dispositivo na porta serial, paralela, USB ou entre o teclado e a CPU. Estes são os métodos de proteção mais comuns entre os programas deste tipo. Os programas que costumam receber proteção adicional por hardware são os destinados a engenharia e uso industrial. São programas que custam entre 15 e 50 mil reais e tem mercado reduzido.

PROTEÇÃO POR ASSINATURA DE HARDWARE - Outra forma bastante eficaz de proteção, consiste na leitura das características do hardware do usuário, principalmente HD e processador, para a geração do número de série.

Usando o Google para Hackear

O portal de buscas Google (*www.google.com*) pode ser usado para buscar números de serials. Você pode procurar por softwares e números de série usando frases ou combinações de palavras. Ás vezes nem será necessário visitar o site apontado, bastando olhar na descrição do link para ver o serial. Veja alguns exemplos de buscas simples:

SERIAL + NOME_DO_PROGRAMA
CRCAK + NOME_DO_PROGRAMA
KEYGEN + NOME_DO_PROGRAMA
DOWNLOAD+FULL+NOME_DO_PROGRAMA



Além do Google, experimente os seguintes sites, especializados na busca por serials:

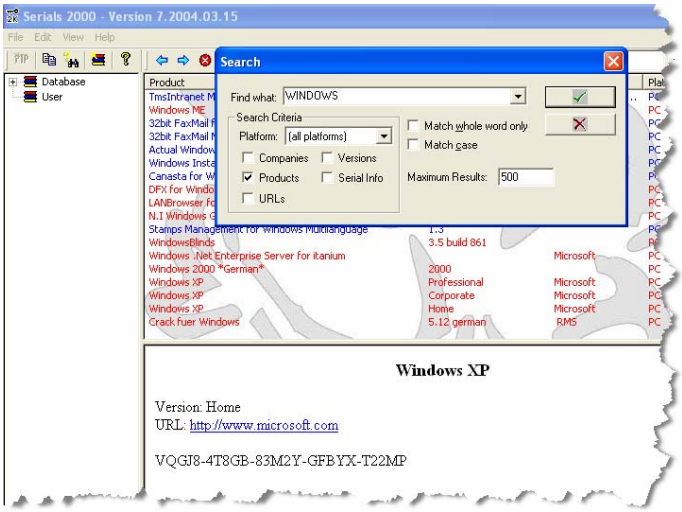
www.serials.ws
www.cracks.am (não autorize a instalação de programas em micro)

Banco de Dados de Senhas

Não poderíamos deixar de fora das nossas aulas sobre CRACKING os programas de banco de dados de senhas. Gamers já conhecem de longa data os programas que armazenam milhares de macetes e trapaças para jogos. Os hackers tam-

bém possuem um programa deste tipo: banco de dados de senhas. Um dos mais antigo é o OSCAR 2000, uma raridade. Infelizmente só servirá para quem procura por senhas de programas ultrapassados, tipo abandonware.
Atualmente você ainda pode contar com o SERIALS 2000 (www.serialz.to/serials2000.html). Não esqueça de atualizar a base de dados, no mesmo site em ue baixar o programa (www.serialz.to/s2kupdates.html):

Um exemplo de busca pelo SERIAL do Windows XP (pressione F3 para exibir a caixa de diálogo para busca):



Para atualizar o SERIALS 2000, baixe os arquivos de atualização a partir do site já citado neste capítulo, descompacte-os em uma pasta qualquer e clique em *File -> Update Database* para atualizar a base de dados. As atualizações não são cumulati-

vas e você terá de importar todos os pacotes, desde 2001, se quiser ter o software atualizado.

Crackeando de Verdade

Até agora você aprendeu a crackear usando material alheio. Se quiser ser considerado um hacker de verdade, você vai precisar fazer mais que isto. Procurar por cracks e serials qualquer um faz, não precisa ser hacker. Se pretende mesmo se tornar um hacker especializado em quebra de programas, vai precisar dedicar algumas semanas no estudo das principais linguagens. Nesta lista não poderá faltar as linguagens C e Assembler.

Neste final do capítulo três, darei um exemplo de como fazer o cracking de um software protegido. Não é a única maneira de se fazer isto e nem teriamos, nem com um único livro, como ensinar-lhe a arte do desassembler. Mas antes de entendermos como é que se quebra a senha de um programa, vamos relembrar alguns conceitos sobre sistemas de numeração.

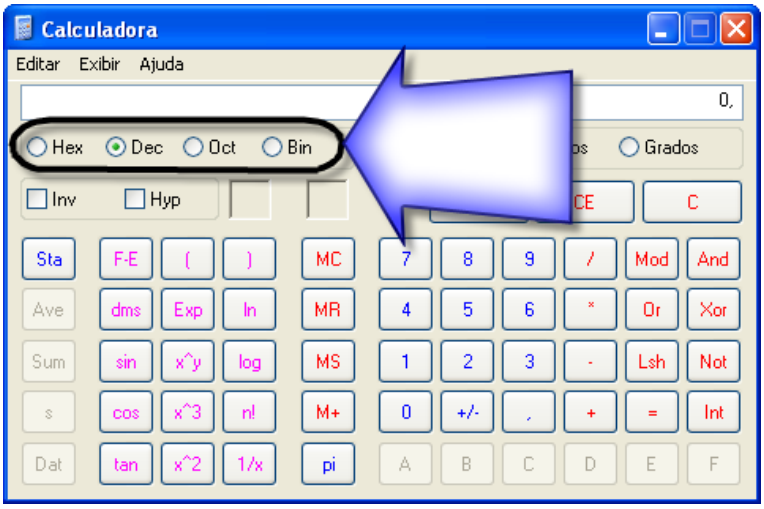
São várias as formas de representar os números. Entre nós, a mais comum é a DECIMAL, talvez devido ao fato de termos DEZ dedos nas mãos. Os computadores trabalham através de um sistema de chaveamento elétrico, onde se convencionou que, se há circulação de corrente, o estado lógico é UM. Se não há circulação de corrente elétrica, o estado lógico é ZERO. A esta notação damos o nome de BINÁRIA pois neste caso só DOIS símbolos para representam qualquer número. Os computadores na verdade só entendem esta linguagem: 0 (zero) e 1 (um).

	EM DECIMAL	EM BINÁRIO
ZERO	0	0
UM	1	1
DOIS	2	10
TRÊS	3	11
QUATRO	4	100

Existem outros sistemas de numeração, como o HEXADECIMAL que usa dezesseis símbolos para representar os números. Este é um dos sistemas de numeração usados para escrever códigos e programas. É uma forma de comunicação poderosíssima, pois estaremos nos comunicando com a 'alma' do programa. E quando você se comunica com a 'alma' de um programa você consegue descobrir e fazer coisas que não conseguiria usando outra forma de comunicação (outra linguagem).

	EM DECIMAL	EM HEXADECIMAL
ZERO	0	0
UM	1	1
DOIS	2	2
TRÊS	3	3
...		
NOVE	9	9
DEZ	10	A
ONZE	11	B
TREZE	13	C
QUATORZE	14	D
QUINZE	15	E
DEZESSEIS	16	F
DEZESSETE	17	A0

A calculadora do Windows, no modo de exibição calculadora científica, permite a conversão entre os sistemas binário, decimal, octal e hexadecimal:



Linguagens como Visual Basic e Delphi facilitam a criação de programas. Mas por outro lado, são limitadas quando queremos alterar a estrutura interna de um programa existente.

O que um editor HEXADECIMAL faz é exatamente isto: permitir que você olhe dentro de qualquer programa e faça alterações, como desbloqueá-lo por exemplo. E esta é a sua importância para o hacker, permite o acesso a partes do programa que não estariam disponíveis de outra forma.

Usando Editor Hexadecimal para Crackear

O uso de editores hexadecimais ou desassembladores vai exigir conhecimentos de linguagem assembler. No capírulo quatro vamos abordar o tema programação. Junto com o material extra que acompanha o CD-Rom do livro, voc~e poderá dar os primeiros passos por conta própria.

Para que você ter uma idéia de como funciona o cracking via desassemblador, vamos mostrar o roteiro para a quebra de senha de um programa. Infelizmente isto só vai dar a você uma noção deste tipo de cracking, pois cada programa tem sua peculiaridade na forma de ser crackeado. Mas já é alguma coisa. E como já demos o caminho das pedras, na maioria das vezes você não vai precisar quebrar a proteção do programa. Poderá usar as que encontrar prontas e usar seu tempo para se dedicar às técnicas de ataque e defesa, o que talvez seja o seu obejtivo principal.

Nos dias de hoje, adquirir programas caríssimos por menos de 2 dólares é muito fácil. No Rio de Janeiro e São Paulo este material é vendido nas ruas do centro comercial. Em todas as grandes capitais você encontra no jornal anúncios de softwares piratas. Nos jornais cariocas "O Globo" e "O Dia" você encontra páginas inteiras de anúncios de software pirata. Muitos com telefone fixo. Alguns de empresas que se dão ao luxo de contar com motoboys e emitir nota fiscal.

Mas supondo que você seja um(a) aficionado(a) por cracking e quer você mesmo desassemblar programas protegidos, sugiro que adquira o nosso CD AVULSO que trata do assunto CRACKING de SOFTWARE.

Mãos a Obra...

Vamos usar o programa OllyDbg v1.09d para crackear o programa WinConnection 3.5. Baixe o OllyDbg em:

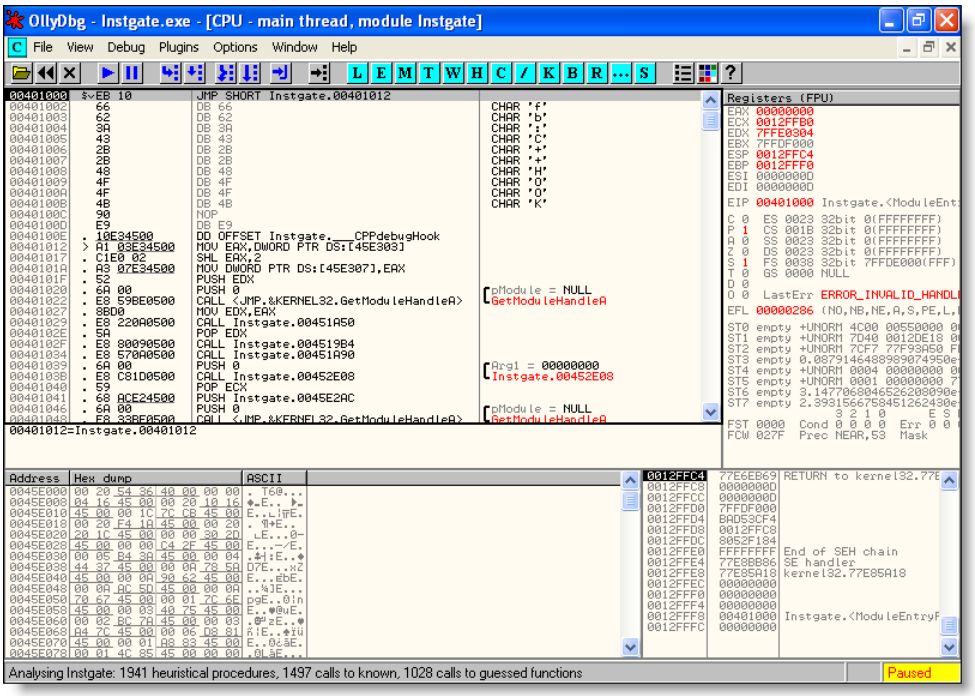
http://home.t-online.de/home/Ollydbg/download.htm

Baixe o Winconnection em:

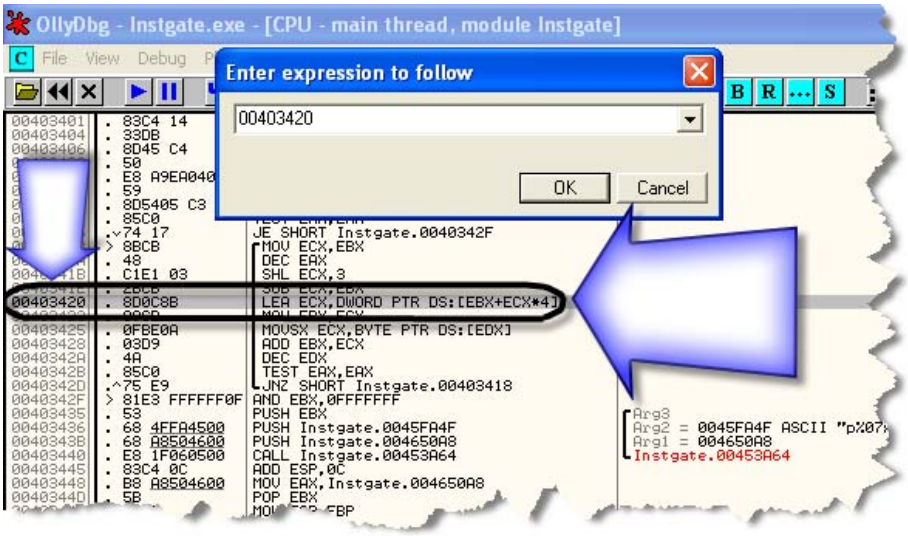
www.winconnection.com.br/download.php?versao=S35

1. Instale o Winconnection e abra o executável dentro do OllyDbg. Para fazer isto você deve acessar a barra de menus e clicar na opção **File -> Open** ou usar a tecla de atalho F3. O caminho completo para o executável é este:

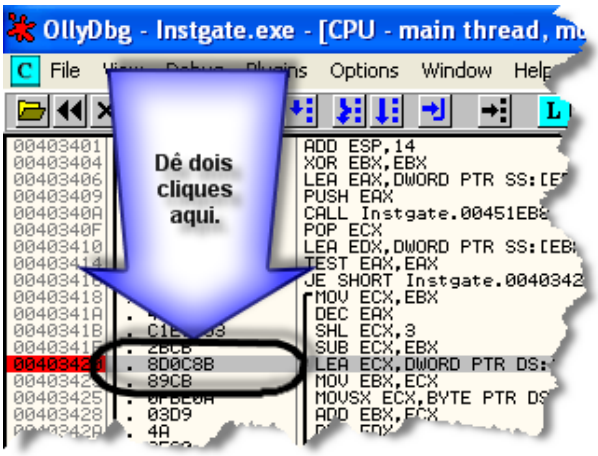
C:\Arquivos de Programas\Winco\WinConnection\Instgate.exe



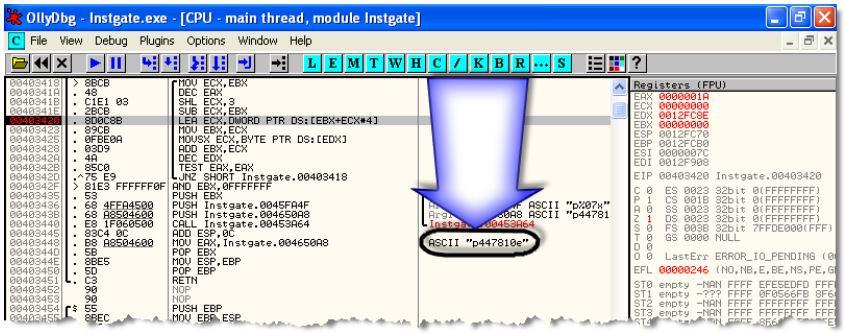
Eu sei que assusta, principalmente se for a primeira vez que você vê um programa por dentro. Não se preocupe que vamos guiá-lo em todos os passos. O objetivo é te dar uma visão geral do processo de cracking.



2. Agora pressione **CTRL+G** e localize o endereço **00403420**:
3. Dê dois cliques na segunda coluna da linha do endereço localizado, para inserir



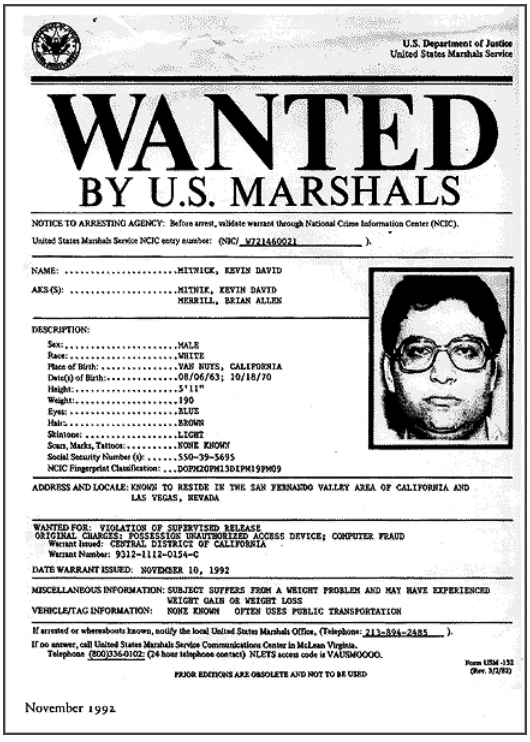
um *breakpoint*. O endereço deverá ficar marcado em vermelho:
4. Pressione **F9** para continuar a execução do programa. Talvez você tenha que



pressionar **F9** várias vezes até que apareça a *string* com o número de desbloqueio:
5. Feito isto chegamos a string **p4478810e** (sem as aspas mostradas na figura acima). Agora é só chamar o programa e entrar com o número da licença e o programa estará desbloqueado e pronto para uso.
Aparentemente tudo muito simples e fácil, não é mesmo? Se não fosse a pergunta que não quer calar: _*"Como o professor sabia que deveria selecionar o endereço 00403420?"* – Isto foi feito através da leitura do código do programa. Aprender programação é como aprender um novo idioma. Ao olhar para o código do programa usado como exemplo nesta aula, acredito que a maioria vai, no mínimo, torcer o nariz. Mas depois que se aprende a 'ler' um programa, vai encontrar tudo lá. Inclusive o local exato onde o programador guardou a 'chave' para desbloqueá-lo. Fica o convite para quem quiser se aprofundar no assunto, adquirir nosso CD AVULSO com programas e vídeoaulas ensinando a arte do desassembler (cracking de programas).

Capítulo 4:

Hacker



U.S. Department of Justice
United States Marshals Service

WANTED
BY U.S. MARSHALS

NOTICE TO ARRESTING AGENCY: Before arrest, validate warrant through National Crime Information Center (NCIC).

United States Marshals Service NCIC entry number: (NIC/ W721460021).

NAME: .....MITNICK, KEVIN DAVID

AKS (S): .....MITNIK, KEVIN DAVID
MERRILL, BRIAN ALLEN

DESCRIPTION:
Sex:.....MALE
Race:.....WHITE
Place of Birth: .....VAN NUYS, CALIFORNIA
Date(s) of Birth:.....08/06/63; 10/18/70
Height:.....5'11"
Weight:.....190
Eyes:.....BLUE
Hair:.....BROWN
Skintone:.....LIGHT
Scars, Marks, Tattoos:.....NONE KNOWN
Social Security Number (s):.....550-39-5695
NCIC Fingerprint Classification:...DOPM20PM13DIPM19PM09

ADDRESS AND LOCALE: KNOWN TO RESIDE IN TWE SAN FERNANDO VALLEY AREA OF CALIFORNIA AND LAS VEGAS, NEVADA

WANTED FOR: VIOLATION OF SUPERVISED RELEASE
ORIGINAL CHARGES: POSSESSION UNAUTHORIZED ACCESS DEVICE; COMPUTER FRAUD
Warrant Issued: CENTRAL DISTRICT OF CALIFORNIA
Warrant Number: 9212-1112-0154-C

DATE WARRANT ISSUED: NOVEMBER 10, 1992

MISCELLANEOUS INFORMATION: SUBJECT SUFFERS FROM A WEIGHT PROBLEM AND MAY HAVE EXPERIENCED WEIGHT GAIN OR WEIGHT LOSS
VEHICLE/TAG INFORMATION: NONE KNOWN OFTEN USES PUBLIC TRANSPORTATION

If arrested or whereabouts known, notify the local United States Marshals Office, (Telephone: 213-894-2485).
If no answer, call United States Marshals Service Communications Center in McLean Virginia.
Telephone (800)336-0102; (24 hour telephone contact) NLETS access code is VAUSM0000.

Form USM -132
(Rev. 3/1/82)

PRIOR EDITIONS ARE OBSOLETE AND NOT TO BE USED

November 1992

Capítulo 4:

Hacker

Objetivos Deste Capítulo:
Após concluir a leitura deste capítulo e com o estudo do materialo adicional que se encontra no CD-Rom que acompanha o livro, você deverá ser capaz de desenvolver pequenos programas em uma ou mais linguagens diferentes.

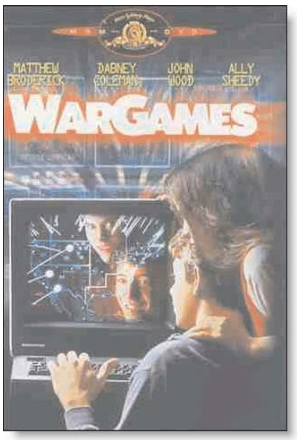
O Hacker Programador

Sinto desapontá-lo, mas você não será considerado um hacker se não souber programar computadores. Talvez também não seja considerado um hacker se não souber diferenciar um diodo de silício de um de germânio. Mas aí já achamos que é exagero.

Sem saber programar você estará dependendo do que já tem pronto. Suponha que você tenha uma ótima idéia sobre como produzir uma peça de *phishing scam* arrasadora, daquelas que aparecem na Info e na TV. Como levar a cabo a tarefa se você não souber criar teclados virtuais em java, javascript ou flash? E nem souber como fazer o micro do usuário se comunicar sozinho com a Internet?

O que diferencia o *script kiddie* do *hacker* é o conhecimento avançado de programação. E o que diferencia o *hacker* do *phreaker* é o conhecimento avançado de eletrônica e telecomunicações.

É perfeitamente possível (e é o que mais ocorre) hackear usando métodos e ferramentas descobertos por terceiros. Usá-los sem a menor idéia de como funcionam, mas obtendo todos os resultados esperados.



No filme *Jogos de Guerra,* um dos primeiros a falar sobre hackers*,* o personagem inicia um processo de *wardialing* e se conecta acidentalmente ao computador central do centro de defesa norte americano.

Se ele tivesse a intenção deliberada de conseguir este acesso, provavelmente não teria conseguido.

Riscos Que Corre o Hacker que Não Sabe Programar

O primeiro risco é passar vergonha. Hacker que não sabe programar é tão real quanto galinha com cinco dedos nos pés. Mas falando sério, o risco mesmo é usar um programa pensando que vai atacar, quando na verdade o atacado será você. Em outros casos o programa vai fazer o que se espera dele... para o criador do programa e não pra você. Alguns exemplos:

Vários programas do tipo trojans distribuídos na Internet, embora permitam que você configure o seu E-Mail ou ICQ para receber a notificação de quando o alvo está on-line, em vez de enviar pra você a notificação, envia para o criador do programa. Faça o teste. Se após seguir todas as instruções e ter certeza de que o alvo está on-line, um cybercafé ou 'amigo' por exemplo. E mesmo assim não receber a notificação, desconfie. Se puder (e souber) analise as linhas de código do programa.

Vários programas distribuídos na Internet como sendo programas hacker, incluindo *cracks*, *keygens*, geradores de números de cartão de crédito e geradores de créditos para celular, são na verdade, programas que vão abrir as portas do seu micro a um ataque ou invasão.

Quando o serviço Velox começou no Rio de Janeiro, tive uma penca de clientes hospedando sites pornô e MP3 no próprio micro, sem que tivessem a menor idéia de como aquele material foi parar lá. Um caso em particular, de um senhor que tem uma máquina excelente, na proporção da sua ignorância em lidar com ela, mas que recebeu um comunicado do provedor alertando-o sobre possíveis atividades hacker partindo daquele micro. Ele ficou desesperando pensando até que iam mandar a polícia na casa dele para averiguar alguma coisa.

Como Programar Computadores

No parágrafo anterior, espero tê-lo convencido da necessidade de saber programar para se tornar um hacker de verdade. Como bônus do conhecimento sobre programação, você poderá criar programas comerciais para vender ou aumentar suas chances de trabalho, incluindo em seu currículo mais esta qualificação: a de programador de computadores.

O poder obtido com o conhecimento de programação é assustador. Se manda no mundo quem domina o computador, manda no computador quem sabe programá-los. Pensa que eu estou delirando? Por acaso não é o homem mais rico e poderoso do mundo um programador? Se o Windows parar de funcionar de uma hora para outra, você tem idéia do caos que vai se instaurar? Você sabia que existem boatos do apagão que houve em Nova York ter sido causado por um programa

(vírus) ? Em que época da vida humana na terra houve a possibilidade de uma única pessoa causar tantos prejuízos ao redor do mundo, sem sequer sair do seu quarto de dormir!?
Eu gosto quando minhas idéias parecem ser um pouco estapafurdias. É sinal de que eu estou no caminho certo. Quando comecei o Curso de Hacker (www.cursodehacker.com.br) as pessoas ao meu redor acharam loucura. Esta loucura está para me comprar meu primeiro apartamento. Também percebi que estava no caminho certo com este livro quando mais de dez editoras (e até gráficas) se recusaram a produzi-lo ou publicá-lo. Já é fato que antes de 2010 toda a comunicação de telefonia fixa, celular e TV circulará pela Internet. Já é fato que antes de 2010 qualquer um poderá ser dono de uma emissora de televisão, transmitindo de dentro do seu quarto de dormir. Tudo isso estará nas mãos dos programadores.

Mas afinal, como se programa os computadores?

Antes de prosseguir e responder esta pergunta, peço que leia a frase abaixo, a minha descrição do que é um computador:

Computadores são máquinas-ferramenta, que tem por finalidade aumentar o potencial de quem os utiliza.

Isto quer dizer o seguinte: o limite do computador é o dono. Já falei sobre lamer que se esconde atrás da pergunta _*"Qual o melhor computador para usar numa invasão?"* Qualquer computador em funcionamento atualmente possui condições para ser usado em um ataque ou invasão. Rodando um serviço tipo o Terminal server do Windows eu posso trazer o Office XP para dentro de um PC 486. Você conseguirá extrair do computador (qualquer um) o que você conseguir extrair dele.
Menos de dois anos atrás quando eu ainda não tinha notebook, decidi viajar para escrever um livro. Em Nilópolis(RJ), cidade dormitório densamente povoada, eu não estava encontrando a tranquilidade (ausência de ruídos) tão necessária a minha inspiração. Comprei um PC 386 com monitor monocromático, 16 MB de RAM e HD de 500 MB. Instalei o Windows 95, Pagemaker 5 e Photoshop 3. Com este equipamento escrevi a maior parte do livro ***Java 2 e Banco de Dados*** (*www.editoraerica.com.br*). Tentei doá-lo a biblioteca da cidade, mas ninguém quis por ser um micro ultrapassado e com monitor preto e branco (riram na minha cara). Deixei-o no quarto do hotel onde me hospedei. Com aquele micro seria possível muitos ataques e invasões, embora na época, não tenha sido este o objetivo. Crianças abastadas ganham de presente possantes *Pentiuns 4*, dos quais não usam nem 1% do processamento total que têm a disposição.

Antes de finalmente responder a pergunta título deste parágrafo, quero fazer uma pergunta: _"Como é que se usa um computador?" A resposta mais comum que recebo é _"Usando os programas." Está correto, mas como se usa os programas? Não vale as respostas que mais ouço _"Usando, pois!?" e _"Com o mouse." O computador para ser operado precisa dos programas. Os programas funcionam através de comandos. Comando para imprimir, para salvar, para resgatar um documento salvo, para enviar E-Mail, para invadir um servidor...

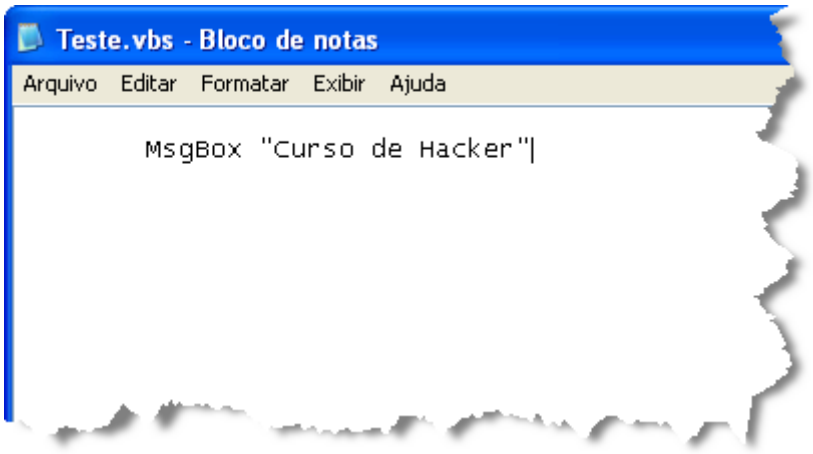
O que um programador faz em um programa, é organizar os comandos possíveis de serem executados pelo computador. Além de cuidar da organização lógica destes programas, ele também se ocupa do desenho e funcionalidade da iterface gráfica com o usuário. Cada linguagem de programação possui um conjunto de instruções que permite ao computador executar determinadas tarefas. Nem todas as possíveis ações de um computador estão disponíveis em todas as linguagens de programação. Linguagens de programação são como idiomas. Computadores são poliglotas. Entendem diversos idiomas. Você pode conversar com um computador em Basic, Assembler, C, Pascal, Delphi, Visual Basic e diversas outras linguagens, cada uma com uma funcionalidade diferente.

Um hacker com pretensões a crackear softwares vai optar por C e Assembler. Um hacker que pretenda criar seu prórpio trojan talvez queira fazê-lo em Visual Basic ou Delphi. Um hacker em busca da fama mundial, obtida através de um vírus que leva o seu nome, poderá se dedicar ao estudo de Visual basic, VBA ou VBScript. Um hacker que pretenda capturar o maior número possível de cartões de crédito e contas bancárias poderá deenvolver suas peças de phishing scam em HTML, ASP e JavaScript. Ou quem sabe queira se aventurar no mundo dos vírus para celulares e programar em Java? O Flash da Macromedia evoluiu ao ponto de poder ser usado para criar trojans e peças de phishing scam bastante sofisticadas e com design impecável. O Java também pode ajudar o scammer na construção dos tecladinhos virtuais. Conhecimentos de HTML, ASP, JavaScript, Perl, PHP e SQL serão úteis ao hacker especializado em defacement. Como podemos perceber, cada linguagem possui uma facilidade para obter determinado resultado.

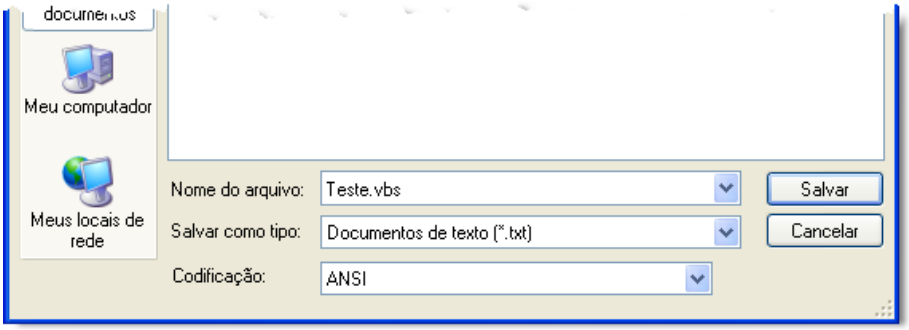
Linguagens podem ser COMPILADAS ou INTERPRETADAS. Linguagens compiladas são aquelas que criam programas executáveis dependentes, apenas da plataforma. Linguagens interpretadas são aquelas que dão instruções ao processador de comandos, sendo executadas em tempo real. O Internet Explorer possui um interpretador embutido que interpreta HTML, VBScript e JavaScript. Antes que as críticas invadam minh'alma quero dizer que HTML não é uma linguagem de programação. É uma linguagem de formatação. Mas dá quase na mesma, ainda mais se usarmos folhas de estilo.

Ambiente de Programação

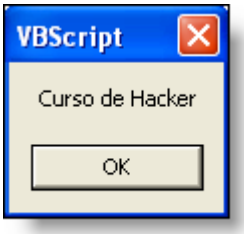
Para cada linguagem vamos precisar preparar o computador para ser usado como máquina de programação. Há caso em que apenas o bloco de notas será suficiente. Sim. Apenas com o bloco de notas podemos criar programas com HTML, JavaScript e VBscript. Vamos praticar um pouco. Abra o bloco de notas e digite **`MsgBox "Curso de Hacker"`**. Se estiver com medo (de errar) ou preguiça (de digitar) procure pelo código pronto no CD-Rom que acompanha este livro:



Agora salve com o nome **Teste.vbs**:

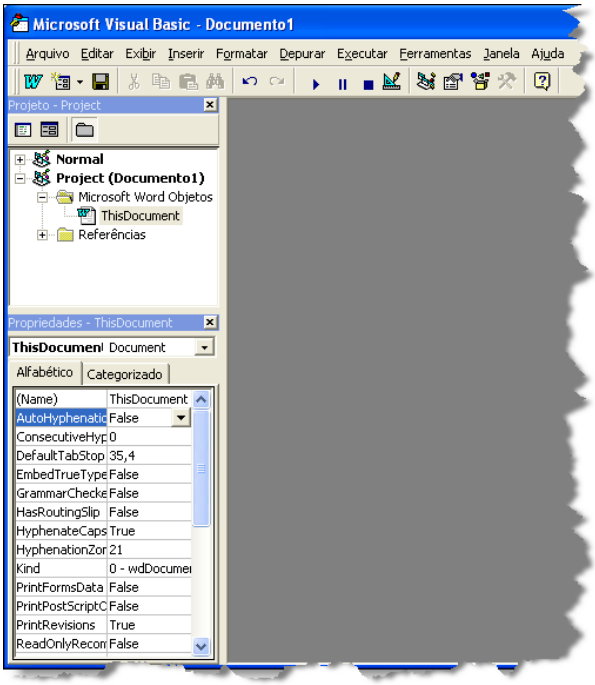


Dê dois clique sobre o arquivo salvo para executá-lo. O resultado esperado é a exibição de uma caixa de mensagens com o texto *Curso de Hacker* e um botão *OK*.

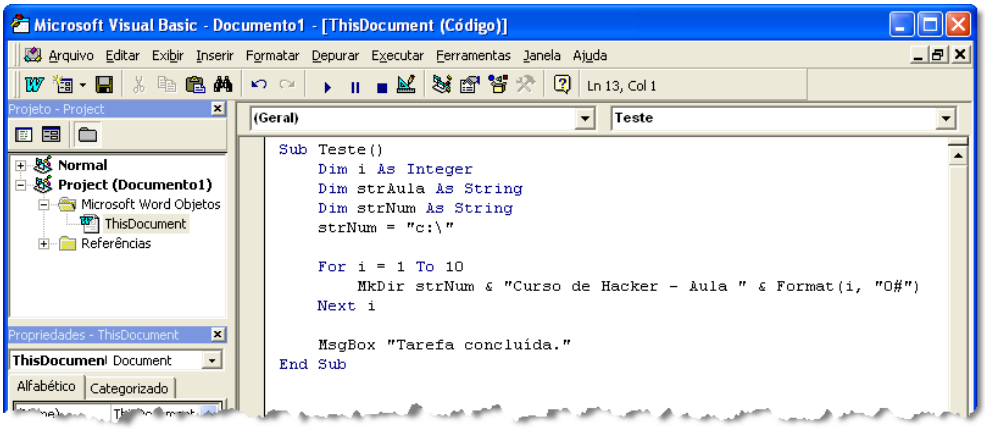


Com apenas uma linha de código você criou uma caixa de mensagens. Se isto não foi suficiente para provar o poder que um programador tem, vamos a mais uma demostração prática, a sua espera na próxima página.

Abra o programa Microsoft Word e pressione ALT+F11 simultâneamete. A seguinte janela deverá ser exibida:



Agora pressione a tecla **F7** e digite as seguintes linhas de código, conforme a figura abaixo:



Ao terminar a digitação, pressione a tecla F5 para executar as linhas de código. O resultado será a criação de dez pastas vazias no seu disco rígido. Pode executar o código acima sem medo. O único trabalho que vai ter é o de apagar as pastas depois.

Isto foi só um exemplo. Este mesmo código poderia ser modificado para apagar pastas e arquivos no disco rígido, no lugar de de criá-los. E poderá ser distribuído em forma de um documento do Word, Excel, Powerpoint ou arquivo executável. Você acaba de saber como são criados os vírus de macro, mas para aprofundar o assunto será preciso um livro inteiro. E este livro está a sua espera, com 350 páginas, no CD-Rom. Incluindo vários projetos prontos para uso e estudo, usando a linguagem VBA que vem embutida nas aplicações Microsoft.

Criando Vírus Sem Saber Programar

É possível a criação de programas sem saber progamar? É possível, mas não é a situação ideal. E é óbvio que o programa gerado será limitado ao conjunto de opções que o programa gerador de código oferece. Desta forma, podemos criar vírus sem saber programar, bastando usar um programa gerador de vírus. Incluimos um gerador de vírus no CD-Rom para você experimentar. Atenção redobrada para o feitiço não virar contra o feiticeiro. Faça este tipo de teste em uma máquina virtual. Em tempos idos cheguei a conhecer e experimentar um sistema de criação de vírus on-line. Você escolhia as diversas opções de configuração, batizava o vírus com seu nome e em poucos segundos era gerado o código do para distribuição. Não precisa dizer que este site saiu do ar. Mas se você acha que não existem ferramentas de criação de vírus em quantidade suficiente para causar preocupação, é que ainda não viu as dezenas de opções registradas em:

http://www.pestpatrol.com/pestinfo/virus_creation_tool.asp

Continua...

A pergunta que o programador sempre deve fazer é: _*"O que quero que este programa faça?"* A descrição passo-a-passo do que se espera do programa será a base de criação do algoritmo. Algoritmo é o conjunto de regras a serem utilizadas na construção do código.

Querer que o programa simule a geração de créditos para celular, se esconda em uma pasta do sistema e dez dias depois de instalado, apague todos os programas existentes no disco rígido, é um exemplo informações que podem ser usadas para a construção de vírus. Vírus deste tipo são fáceis de fazer e a eficácia só vai depender da sua capacidade em convencer as pessoas a executar o arquivo. Mas não é com este tipo de vírus que você vai conquistar o respeito do mundo hacker. Lembre-se de que, qualquer que seja o programa que pretenda criar, você precisará saber executar as tarefas que espera que o programe execute. Senão, como espera criar um programa de cálculo de massa corporea, por exemplo, se não souber a fórmula? Paramos por aqui, mas este capitulo sobre programação continua com a imensa quantidade de material que disponibilizamos no CD-Rom.

Capítulo 5:

Invasão Linux

Capítulo 5:

Linux

Objetivos Deste Capítulo:
Após concluir a leitura deste capítulo você deverá ser capaz de instalar e configurar corretamente o Linux. Também deverá ser capaz de descrever as particularidades das distribuições mais conhecidas, usar o Linux a partir de um CD-Rom, sem precisar instalar, conhecer algumas das ferramentas hacker para Linux e saber como são feitas as invasões do sistema Linux, vencendo as primeiras etapas do DESAFIO HACKER. No CD-Rom você encontra material adicional em português, com mais de duas mil páginas de informações sobre Linux, nos níveis básico, intermediário e avançado.

Breve História do Linux

Para entender direito o Linux, primeiro é preciso entender o que é SOFTWARE LIVRE. O conceito ás vezes é entendido como SOFTWARE GRÁTIS. Não são a mesma coisa. 'Software livre' se refere à liberdade dos usuários executarem, copiarem, distribuírem, estudarem, modificarem e aperfeiçoarem o software. Os requisitos para um software ser reconhecido pela comunidade como SOFTWARE LIVRE, são :

1) A liberdade de executar o programa, para qualquer propósito;

2) A liberdade de estudar como o programa funciona e adaptá-lo as suas necessidades. Aceso ao código-fonte é um pré-requisito para esta liberdade.

3) A liberdade de redistribuir cópias de modo que você possa ajudar ao seu próximo.

4) A liberdade de aperfeiçoar o programa e liberar os seus aperfeiçoamentos, de modo que toda a comunida-

de se beneficie. Acesso ao código-fonte é um pré-requisito para esta liberdade.

Isto quer dizer que o programa classificado como 'software livre' tanto pode ser encontrado de graça, como pode ser encontrado a venda. Mas o que ganha a empresa que 'vende' um programa que pode ser encontrado de graça? Qual é o atrativo para o usuário final em um programa que ele pode baixar de graça ou receber de brinde em uma revista?

Um grande número de usuários, o suficiente para dar lucro e manter a empresa funcionando, vai preferir comprar o programa, no lugar de baixá-lo da Internet ou como brinde de revista. Isto ocorre por que as empresas que comercializam softwares livres, além de tornar seus produtos mais atraentes (embalagem), fornecem todos os manuais necessários a instalação, configuração e uso do programa, além de suporte técnico por fax, E-Mail, telefone e chat. Estes atrativos fazem com que empresas optem por adquirir uma cópia do software, no lugar de baixá-lo de algum site.

Um exemplo nacional é a empresa Conectiva (*www.conectiva.com.br*) que possui uma distribuição Linux om o mesmo nome. Você pode baixar do site da empresa e de outros espalhados pela Internet, qualquer uma das últimas versões do Linux Conectiva, incluindo seus manuais em formato PDF. Mas devido a comodidade (nem todos possuem conexão banda larga), facilidade de leitura de um manual impresso (nem todos vão se meter a imprimir 600 páginas em suas jato de tinta) e suporte técnico em caso de dúvidas, muita gente prefere pagar pelo programa. Esta é a filosofia do software livre. Vende quem quer. Compra quem quer. distribuir quem quiser. Modifica quem souber. Todo software livre permite que o código fonte também seja baixado.

Softwares proprietários como os da Microsoft, são chamados de 'caixa preta', pois ninguém sabe se o programa faz só o que se espera dele. Há indícios de que o Windows XP envie para a Microsoft as palavras que você usa quando faz uma pesquisa (***Iniciar -> Pesquisar***). Mesmo que seja local. Esta comunicação com a Microsoft ocorre independente da sua vontade, sem o seu conhecimento e muito menos consentimento.

Voltando a explicação sobre o que é o Linux, precisamos saber que antes do Linux, existia (e existe até hoje) o projeto GNU. O projeto GNU, sob a liderança do polêmico Richard Stallman, queria (e ainda quer) criar um sistema operacional compatível com o UNIX mas

totalmente livre. Só que eles começaram a escrever primeiro os aplicativos e bibliotecas e deixaram o kernel por último. Além do GNU, haviam muitos outros softwares livres, feitos por outros autores e organizações, como o X, TeX, aplicativos BSD, Sendmail, Apache, Ghostscript e muitos outros. Todos esses programas eram bons, confiáveis e muito usados, mas que estavam espalhados, sem um núcleo (literalmente) que pudesse reuni-los e formar um sistema operacional completo. Foi aí que nos idos de 1991, o estudante Linus Torvalds da cidade de Helsinki (Finlândia), estava insatisfeito com o DOS/Windows mas não tinha dinheiro para comprar uma estação Unix. Assim, ele simplesmente resolveu escrever um sistema operacional decente para o 386 dele, e começou a escrever um kernel (cerne, em português) , que é a parte fundamental de um sistema operacional.

No início, esse kernel se baseava no Minix (versão simples para fins educacionais do UNIX), e precisava do Minix para ser rodado. Mas ajudados por alguns poucos no começo, e por um verdadeiro exército de voluntários atualmente, ele conseguiu criar um kernel próprio, sem ser baseado nos demais Unix (no sentido de que não existe nenhuma linha em comum no código fonte), que é estável, rápido e poderoso.

Atualmente, Linus Torvalds continua trabalhando no Linux e conta com o auxílio de programadores e hackers do mundo todo.

Distribuições

Por ser um software livre, o Linux foi personalizado conforme o gosto e interesse de empresas e pessoas. A estas personalizações damos o nome de 'distro' ou distribuição. As principais são as seguintes:

Caldera - *www.caldera.com*
Conectiva - *www.conectiva.com.br*
Debian - *www.debian.org*
Fedora (da Red Hat) **-** *http://fedora.redhat.com/*
FreeBSD - *www.freebsd.org*
Kurumin - *www.guiadohardware.info/linux/kurumin*
Mandrake - *www.linux-mandrake.com*
RedHat - *www.redhat.com*
Slackware - *www.slackware.com*
Suse - *www.suse.com*
TechLinux - *www.techlinux.com.br*
TurboLinux - *www.turbolinux.com*

Recentemente começaram a surgir as distribuições Linux rodando em memória RAM, o que torna desnecessária (embora desejável) a presença de disco rígido na máquina. Consideramos estas distribuições ótimas para hacking, pois podem ser levadas no bolso (algumas distros cabem em um mini CD). Imagine a visita de um hacker a um cybercafé pouco protegido (a maioria). Basta dar um novo boot na máquina para ter um Linux pronto para ser usado em ataques ou invasões. Isto se não quiser instalar uma máquina virtual com Linux. Segue os links com maiores informações e download das principais distribuições que rodam a partir de CD:

Adios (baseado na Red Hat) - *http://dc.qut.edu.au/adios/*
Fire - *biatchux.dmzs.com*
FreeBSD LiveCD - *livecd.souceforge.net/pt_br*
Knoppix - *www.knopper.net/knoppix*
Kurumin - *www.guiadohardware.info/linux/kurumin*
Slackware-Live - *www.slackware-live.org*

O site Superdownloads (*www.superdownloads.com.br*) possui uma área dedicada ao Linux. Lá você poderá baixar, além de qualquer uma das principais distribuições existentes, qualquer tipo de programa, de jogos a aplicativos.

Vale a pena Trocar o Windows pelo Linux?

Não. Apesar do Linux ser mais estável e seguro, nada que um Windows 2000, 2003 ou XP bem configurado não consiga reproduzir, a oferta de softwares ainda é pouca se comparada a oferta de programas para o Windows. E se você precisa compartilhar arquivos gerados pelo Office, Corel, Page Maker ou Photoshop, terá problemas de compatibilidade. Não não acredite na propaganda que garante a compatibilidade destes arquivos em suas versões Linux. Erros são comuns ao fazer a importação ou exportação de arquivos entre plataformas.

O maior impedimento para a escolha entre o Linux e o Windows seria o preço de uma licença Windows + Office, superior a mil reais. Mas nós sabemos da facilidade em se adquirir estes programas por menos de 15 reais. Poucos são os que podem ou querem adquir uma cópia legalizada do Windows e do Office.

Até mesmo micros comprados em lojas costumam ver com licenças pirateadas. Recentemente aqui em Salvador(BA), um vizinho comprou um PC Desktop da Toshiba na rede de supermercados Bom Preço. O micro apresentou problemas e foi levado para a assistência técnica autorizada. Como não havia o Office instalado de fábrica, a assistência técnica autorizada ofereceu esta instalação por apenas 20 reais. E ele se orgulha de ter um computador marca, sem programas 'piratas'. Com a facilidade para aquisição de cópias 'alternativas' e com a fartura de programas para o Windows, não é uma boa opção ter o Linux no computador de casa. Esta situação pode mudar com a decisão do Governo Federal em implantar, nos próximos cinco anos, o Linux e softwares livres nos computadores governamen-

tais. Com a carência de profissionais na área, haverá boas chances de trabalho para técnicos, instrutoes, programadores e profissionais de segurança. Paralelamente os hackers poderão fazer a festa, devido a quantidade de sistemas vulneraveis que estarão disponíveis.

FreeBSD não é Linux

O Unix foi inicialmente desenvolvido nos Laboratórios Bell da AT&T em 1969. Mas neste período a AT&T estava sendo investigada pelo Comitê Antitruste do Governo americano e não quis comercializar o software. O Unix foi então distribuído para diversas instituições educacionais através de um acordo de licenciamento. Na Universidade de Berkley (*www.berkeley.edu*), na Califórnia, a disciplina de Sistemas Operacionais apresentava o código fonte do Unix e projetos de estudantes implementavam melhoramentos e novas características ao código base.

Ao longo dos anos foram implementadas características tais como: memória virtual, identificação de sockets, protocolos de comunicação TCP/IP etc. E as licenças Unix puderam obter estes melhoramentos da Universidade de Berkley. Esses melhoramentos ficaram conhecidos como "Berkeley Software Distribution" (BSD).

O BSD desenvolvido em Berkley foi escolhido pela DARPA (Defence Advanced Research Projects Agency) para receber a primeira implementação, em um sistema operacional, da especificação do protocolo TCP/IP. A escolha aconteceu devido à performance e à estabilidade apresentada. Além disso, o BSD de Berkley foi escolhido para ser o "sistema computacional universal" da ARPANET (Advanced Research Projects Agency Network), a sucessora da DARPA.

Em resumo, o BSD foi a peça vital da infra-estrutura que deu origem à Internet. Duane Adams, o responsável na DARPA pela contratação de Berkley, garantiu que uma das razões que mais pesaram na escolha do Unix foi a disponibilidade do seu código fonte.

Independente da sua decisão de optar pelo Linux para uso doméstico ou no escritório, ele passa a ser a melhor opção quando se trata de servidores de rede. Mas de nada adianta usar um sistema técnicamente mais seguro sem o conhecimento necessário para implementar um alto nível de segurança. Um Windows bem configurado é tão seguro quanto o Linux. E é mais fácil aprender a lidar com o Windows do que com o Linux. Computadores antigos como o 486, Pentium 100 e K6-2 tem sido ressuscitados para usar versões do Linux otimizadas para compartilhamento de conexões com a Internet, principalmente em banda larga.

Quando se trata de ações hacker, o uso do Linux é imprescindível. As melhores ferramentas de segurança, as que são usadas pelo hacker para ataques e invasão, primeiro são disponibilizadas para o Linux, só depois, quando o são, é que surgem versões para o Windows. E mesmo quando existe versão para o Windows, a versão para Linux é mais atualizada ou possui mais recursos.

O aprendizado do Linux é lento, demorado, mas sem ele você não será um hacker de verdade. Além de saber programar, um hacker tem que saber Linux.

O Pinguim e o Diabo

A mascote do Linux é o *Tux* e a mascote do FreeBSD é o *Daemon*.

Instalando o Linux

No CD que acompanha este livro você encontra um tutorial passo-a-passo ensinando a instalar e configurar o Linux. Também vai encontrar uma distribuição do Linux em formato ISO, para possa gerar o CD de boot e instalação ou usar em uma máquina virtual. Já foi o tempo em que instalar o Linux era algo complicado. Se usar um Live-Cd, é só dar o boot, selecionar a resolução de tela e aguardar aparecer o ambiente gráfico exibir a área de trabalho.

Ambiente Gráfico: XWindow, Gnome e KDE

Em volta do núcleo do sistema operacional (kernel) gravitam todos os outros aplicativos. O Linux original era totalmente baseado em linha de comandos. Muitos ainda preferem esta forma para trabalhar com o Linux. É mais versátil, mais rápido (depois que se acostuma) e podem ser gerados arquivos com lotes de comandos para o sistema operacional executar.

Para tornar o Linux mais fácil de usar, as distribuições vem com um ou mais ambientes gráficos, sendo os mais populares o XWindow, o KDE e o Gnome. Estes ambientes gráficos sao instalados com diversos programas e jogos, às vezes incompatíveis entre um ambiente gráfico e outro.

Servidor Web Apache

Junto com o Linux é instalado o servidor Apache, um servidor Web concorrente direto do IIS da Microsoft e presente em mais de 60% dos servidores espalhados pelo mundo. O IIS da Microsoft ocupa o segundo lugar, sendo usado por pouco mais de 20% dos servidores. Um servidor Web é o que permite a hospedagem de páginas e sites no servidor de rede. Existem versões do Apache tanto para Windows como para Linux, sendo pouco comum o uso profissional do Apache em servidores Microsoft.

Da mesma forma que encontramos vulnerabilidades nos servidores Microsoft, também vamos encontrar vulnerabilidades nos servidores Apache. A grande vantagem é que estas vulnerabilidades são detectadas, divulgadas e corrigidas muito mais rápido que as do IIS. No caso do Apache temos a comunidade mundial trabalhando em sinergia. No caso da Microsoft, temos que contar com uma única empresa e seus recursos humanos para lidar com o problema.

PHP

PHP quer dizer PHP: *Hypertext Preprocessor* e é uma linguagem *server-side* (processada no servidor) e *open-source* (código aberto) para criação de páginas Web dinâmicas e outros aplicativos da Web. Uma página Web dinâmica é aquela que interage com o usuário de forma que cada usuário ao visitar a página verá informações personalizadas, como data, hora, dia da semana e até o seu nome, caso tenha feito algum cadastro prévio. Páginas dinâmicas permitem a validação dos dados de um formulário, consultas e conexões a banco de dados, entre outras coisas.

O PHP oferece uma solução simples e universal para páginas Web dinâmicas e de fácil programação. A interface intuitiva permite que os programadores incluam comandos PHP diretamente na página HTML. A sintaxe do PHP é similar ao do C e Perl, tornando-o de simples domínio mesmo para aqueles com conhecimento básico de programação.

O PHP oferece excelente possibilidade de conexão para todas os bancos de dados populares incluindo a Oracle, a Sybase, a MySQL, a ODBC e muitas outras. O MySQL é um banco de dados distribuido livremente e tem sido usado na construção de sites, em substituição ao MS Access e MS SQL Server da Microsoft.

MySQL e PHPNuke

O PHPNuke (*www.phpnuke.org.br*) é um CMS (*Content Management Script* ou Sistema de Gerenciamento de Conteúdo) cujo o objectivo é criar com rapidez e facilidade, websites com notícias e fóruns. O uso do PHPNuke tem crescido bastante nos ultimos meses.

Falhas em qualquer um destes sistemas: servidor Apache, código PHP, PHPNuke ou MySQL, podem ser usadas para um ataque ou invasão.

Invasão Linux - HackersLab

A melhor maneira de aprender invasão é praticando. Para o ambiente Linux, podemos praticar sem a preocupação de cometer algum delito, se utilizarmos os servidores da HackersLab. O Desafio HackersLab é um servidor a disposição de quem queira praticar invasão e testar seus conhecimentos. Funciona como uma espécie de jogo, onde a cada nível de invasão você consegue a senha para o próximo nível, com grau de dificuldade crescente. O HackersLab não é o único a oferecer este tipo de serviço. A UFRJ (Universidade Federal do Rio de Janeiro) dispõe de um serviço parecido, disponível em *www.lockabit.coppe.ufrj.br/rlab/rlab_desafio.php*.

A compreensão dos níveis de invasão e o sucesso no jogo dependerão de seu conhecimento de Linux. Como sabemos que as páginas deste livro são insuficientes para expor todo o conhecimento que você necessita sobre Linux, necessários a uma invasão bem sucedida, incluimos no CD-Rom que acompanha este livro, farto material sobre Linux em português. Também incluimos no CD-Rom dois eBooks bastante úteis. Um com o passo-a-passo para você vencer os próximos níveis do Hackers Lab, um outro com os comandos do Unix, alem de material sobre linguagem C.

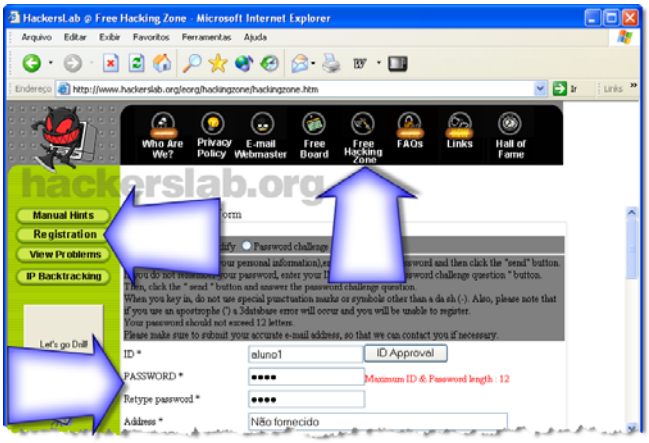
Tudo o que você fizer no HackersLab ou outros desafios hacker espalhados pelo mundo poderá ser reproduzido em um servidor real. É óbvio que o sucesso dependerá deste servidor apresentar ou não a vulnerabilidade explorada. Podemos considerar que para os níveis inciais do HackersLab, a maioria dos servidores do mundo real estará protegida. Conforme você sobe de nível, o número de servidores Linux com a vulnerabilidade semelhante no mundo real aumenta.

DESAFIO HACKERSLAB - Nível 0

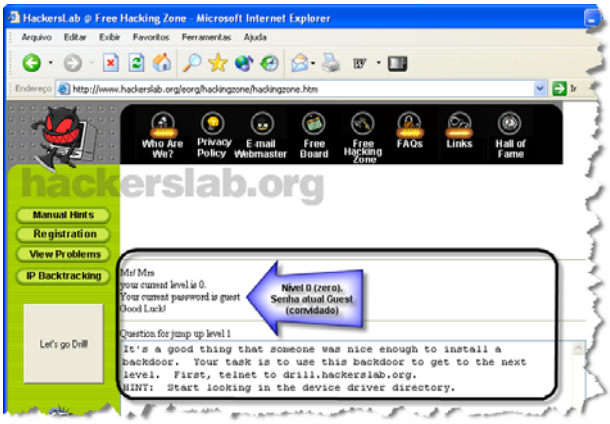
1. Acesse:

http://www.hackerslab.org/eorg/hackingzone/hackingzone.htm

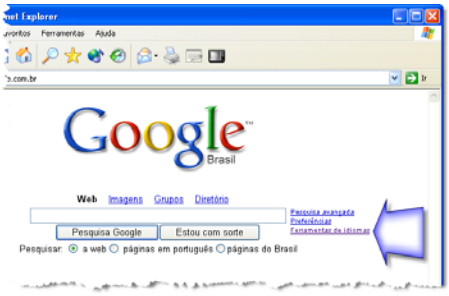
2. Clique na opção ***Registration*** e preencha o registro com seus dados ou preferencialmente os de um avatar. Após o cadastro, clique em **View Problems**. Abrirá uma tela de login. Entre com o **nome de usário** e **senha** que você especificou no cadastro.



3. Será apresentado o primeiro desafio. Para cada nível há uma explicação de um problema e uma dica para ajudá-lo a vencer o desafio e passar para o próximo nível.



4. Se o seu inglês for *In* (insuficiente ou insatisfatório), sugiro que use a ferramenta de idiomas do Google (*www.google.com*) para auxiliar na tradução. Copie no HackersLab o texto em inglês e cole no Google.



Tradução *by Teacher*:

Sr/Srª
*Seu nível atual é 0 (zero) (**level0**).*
*Sua senha atual é **guest**.*
Boa sorte!

Desafio para passar para o próximo nível (nível 1):

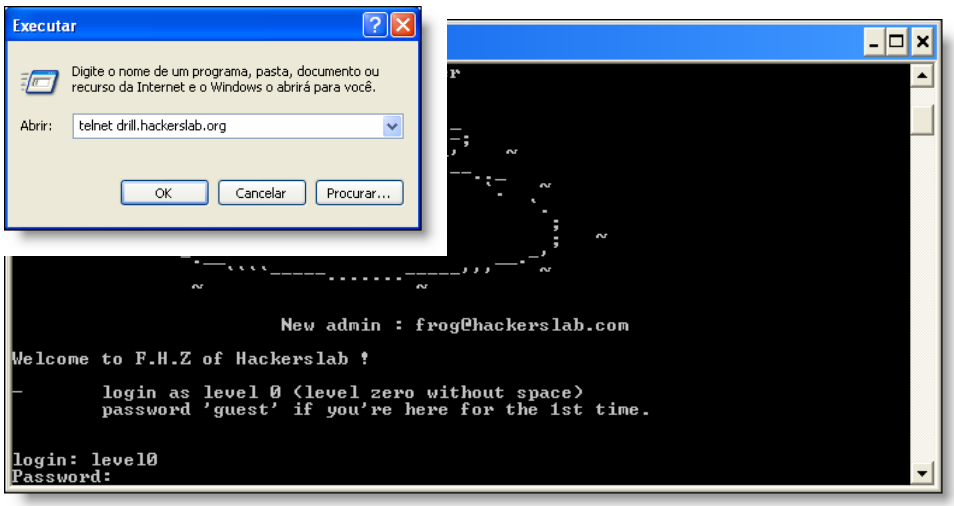
*Foi bom alguém ter instalado um **trojan**. Sua tarefa é usar o trojan para alcançar o próximo nível. Primeiro dê **telnet** em **drill.hackerslab.org***
***DICA:** Olhe no diretório de drivers de dispositivo.*

5. O problema é _*"Como passar para o nível seguinte? Como ter acesso a um nível não autorizado usando o trojan?"* É só analisar o desafio. Alguém instalou um trojan no servidor. Vamos acessar o servidor via Telnet e seguindo a dica, procurar o trojan no diretório ***dev*** (devices ou driver de dispositivo). Se você não entendeu direito, o melhor é por as mãos na massa (Ôpa!) para ir entendendo no caminho.

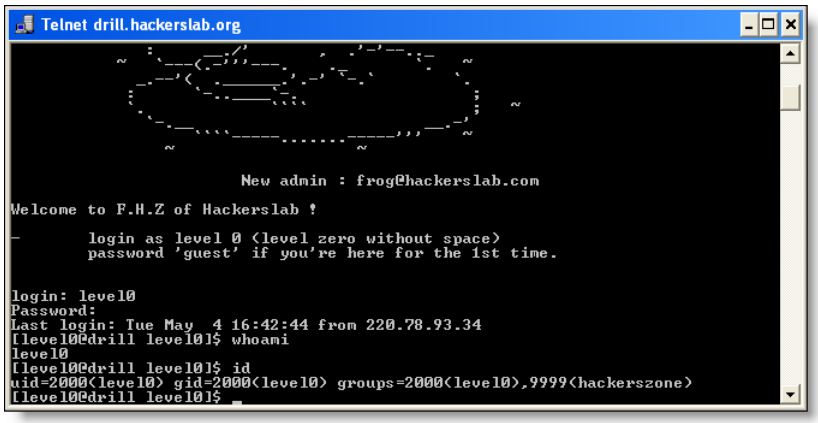
6. Dê Telnet em drill.hackerslab.org Como? Basta ir em **Iniciar -> Executar** e digitar:

telnet drill.hackerslab.org

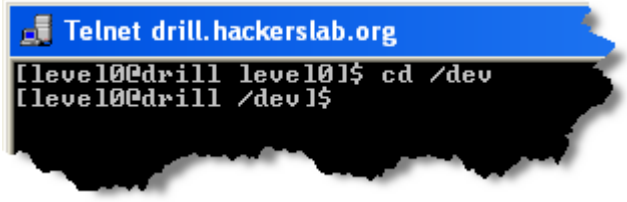
Usuário: ***level0*** (sem espaço entre level e zero e tudo em minúscula)
Senha: ***guest***



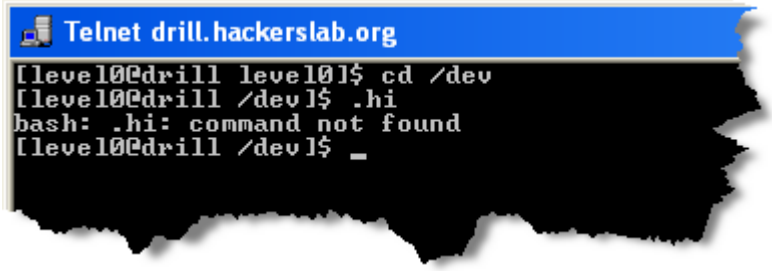
7. Entramos no sistema. Digite o comando ***whoami*** para ver o nome do usuário e em seguida ***id*** para ver os números de identificação.



8. Digite o comando: ***find / -user level1 -group level0 2>/dev/null***
O que estamos dizendo com este comando é: *procure arquivos criados por algum usuário do nível 1 e tendo nível 0 como grupo*. O sistema encontrou alguns arquivos que correspondem a nossa pesquisa, entre eles o ***/dev/.hi***. *Dev* você já sabe que é o diretório de drivers de dispositivo (device) e *.hi* é um programa. Devido a dica que foi fornecida para este nível, vou começar por ele. Digite ***cd /dev*** para entrar no diretório. Quando quiser limpar a tela, digite ***clear***.



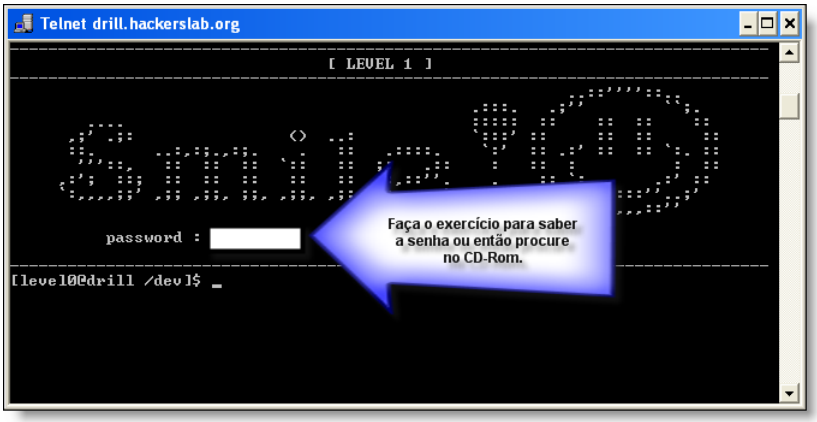
Repare que o arquivo ***.hi***,que está dentro do diretótio ***dev***, este que acabamos de entrar, tem permissão de execução para usuários ***nivel 0***. Vamos executá-lo para ver que acontece.



O sistema retornou erro dizendo que o comando não foi encontrado. Isso significa que o comando não está no *path*. Para resolver, coloque um ***./*** (ponto barra) na frente do comando e volte a executá-lo.

Aparentemente nada aconteceu. Use o comando ***id*** para checar. Apareceu um novo ID de nome EUID que não existia antes, foi nos dado pelo programa. Usaremos o comando ***whoami*** só para tirar as dúvidas. O sistema nos informa que agora temos privilégios de nivel 1.

O que aconteceu é que o programa ***.hi*** era um trojan e a função do trojan é permitir acesso não autorizado. No momento em que ***.hi*** foi executado, ele criou um outro ***shell*** dentro do nosso, mas com suas permissões (de nível 1). Usando o comando ***pass*** saberemos a senha do nível atual (nível 1):
Os demais exercícios se encontram no CD-Rom que acompanha este livro. O



que você não entender você deve procurar a resposta. Não admita não saber, mesmo que pareça difícil ou complicado. Estes conhecimentos distribuidos em diversas áreas: rede, programação, hackerismo, UNIX, Linux. A melhor maneira de não se estressar durante o aprendizado é compreender bem cada nível, repeti-lo pelo menos três vezes, antes de passar para o próximo. Seguindo estas dicas, verá que seu conhecimento vai aumentar assustadoramente.

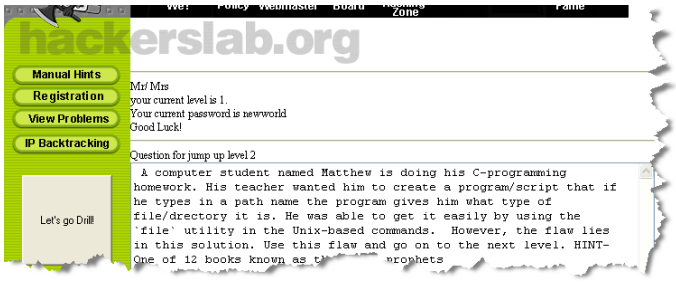
Para melhor organizar seus pensamentos, sugiro que ao final de cada nível e mesmo ao final de cada capítulo deste livro, você coloque em uma folha de papel quais foram as perguntas que ficaram sem resposta. A lista abaixo é uma sugestão de perguntas que ajudarão a entender este primeiro nível do HackersLab:

_O que é Telnet?
_Quais são os comandos aceitos pelo Telnet?
_Posso dar Telnet em qualquer computador?
_O que é um trojan?
_O que faz um trojan?
_Quem plantou o trojan no servidor?
_Como o trojan foi plantado no servidor?
_Como eu ficaria sabendo que o servidor está com o trojan?
_Como é o sistema de organização de grupos e usuários no Linux?
_Como é o sistema de organização de arquivos e diretórios o Linux?
_Como é o processo de login em servidores Linux no modo shell (texto)?
_Para que serve o comando find?
_Para que serve o comando id?
_Para que serve o comando whoami?
_Para que serve o comando cd?
_Existem variações nestes comandos? Quais?
_O que farei se a tradução do Google for tosca e não permitir que eu entenda o problema corretamente?

As respostas podem ser encontradas no próprio capítulo, no material adicional incluso no CD-Rom do livro, em pesquisas na Internet ou comigo, por chat, E-Mail ou telefone. Procure no CD pastas sobre redes, Linux, Unix, programação e outros assuntos que precise pesquisar. Não há como incluir tantos detalhes em um único livro.

Passando Para o Próximo Nível

Assim que você conclui um nível e se achar pronto para o próximo desafio, , volte a página *www.hackerslab.org/eorg/hackingzone/hackingzone.htm*, clique na opção ***View Problems***, entre com o nome de usuário e senha informados no cadastro e, no fim da página, digite a senha para exibir o problema do próximo nível.



Capítulo 6:

Servidores Windows

Capítulo 6:
Servidores Windows

Objetivos Deste Capítulo:
Após concluir a leitura deste capítulo você deverá ser capaz de entender e executar todas as principais tarefas que permitam a invasão de um servidor rodando uma das seguintes versões do Windows: NT, 2000, 2003, XP ou Longhorn. Embora o foco deste capítulo seja a plataforma Windows, os mesmos procedimentos poderão ser usados para invasão de servidores Unix/Linux, além das situações já vistas no capítulo sobre Linux, o que inclui o material extra no CD-Rom. Neste capítulo você também aprenderá a usar exploits, o Nmap e fazer defacement.

Invasão de Servidores

Quando se fala em invasão de servidores, independente da plataforma, devemos ter em mente que isto pode ocorrer em vários níveis. Fazendo analogia com a invasão de uma residência, temos desde o braço que entrou por uma janela e pegou um documento importante que estava nas proximidades, até a quadrilha que se instalou dentro da casa e expulsou seus moradores ou convive em segredo com a família. Partindo desta afirmação, vamos descrever nas próximas páginas, técnicas e procedimentos que permitirão a invasão em diversos níveis.

Ataque

É qualquer ação cuja intenção seja paralisar ou dificultar a operação de um servidor, ou obter acesso não autorizado a alguns ou todos os seus recursos. Se eu uso um scanner de portas COM A INTENÇÃO de descobrir portas vulneráveis que permitam uma invasão, isto é um ataque. Se eu uso um scanner de portas, a pedido da própria empresa, para ajudá-los a detectar e corrigir vulnerabilidades na rede, isto NÃO É um ataque. Chama-se teste de intrusão ou *penetration test (Ôpa!)*.
É claro que, mesmo não tendo a intenção de invadir um servidor, mas mesmo

assim uso um scanner de portas 'só prá ver se tem alguma vulnerabilidade', é um ataque como outro qualquer.

Invasão

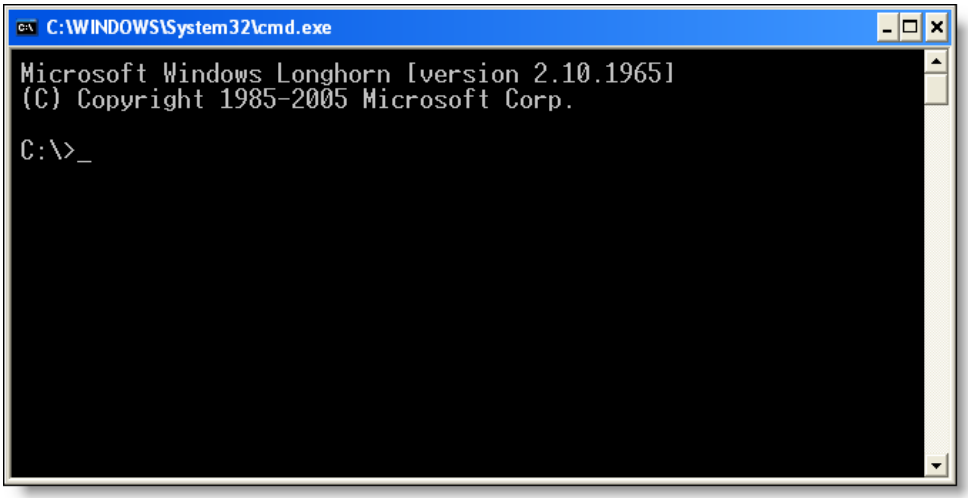
Um ataque bem sucedido transforma-se em uma invasão. A invasão que todos buscam é a mais difícil: obter o *prompt* do servidor. Como eu já disse antes, existem vários níveis de invasão. Obter acesso não autorizado a uma única conta de E-Mail é um tipo de invasão, e dos mais cobiçados.

Em minhas turmas do curso presencial é comum perceber um pouco de decepção nos alunos quando, já no final do curso, fazemos a invasão de um servidor passo-a-passo e eles se deparam com o prompt de comandos.

Muitos imaginavam que iria aparecer para eles o desktop do servidor, pronto para clicar, arrastar e soltar. (Ou será que se imaginavam teletransportados para a poltrona do administrador da rede?)

Outro motivo de frustração que percebo é, após estarem cara a cara com o prompt de comandos do servidor, não terem a menor idéia do que irão fazer a partir daí. Talvez se realmente se deparassem com o desktop do servidor, a primeira coisa que iriam fazer é jogar Paciência, Copas ou FreeCel. E talvez seja por isso que a maioria dos livros sobre hackers a venda no mercado, sejam inofensivos.

Atribuo esta falsa percepção do que é uma invasão aos filmes de Hollywood. Com raras exceções, quando o filme retrata um hacker em ação, exibe uma tela de computador salpicada de efeitos visuais, login e mensagens do sistema em modo gráfico, tudo inexistente no mundo real. Por isso a frustração do aluno, quando ele vem inspirado por esta propaganda enganosa e se depara com a tela abaixo, é decepção na certa.

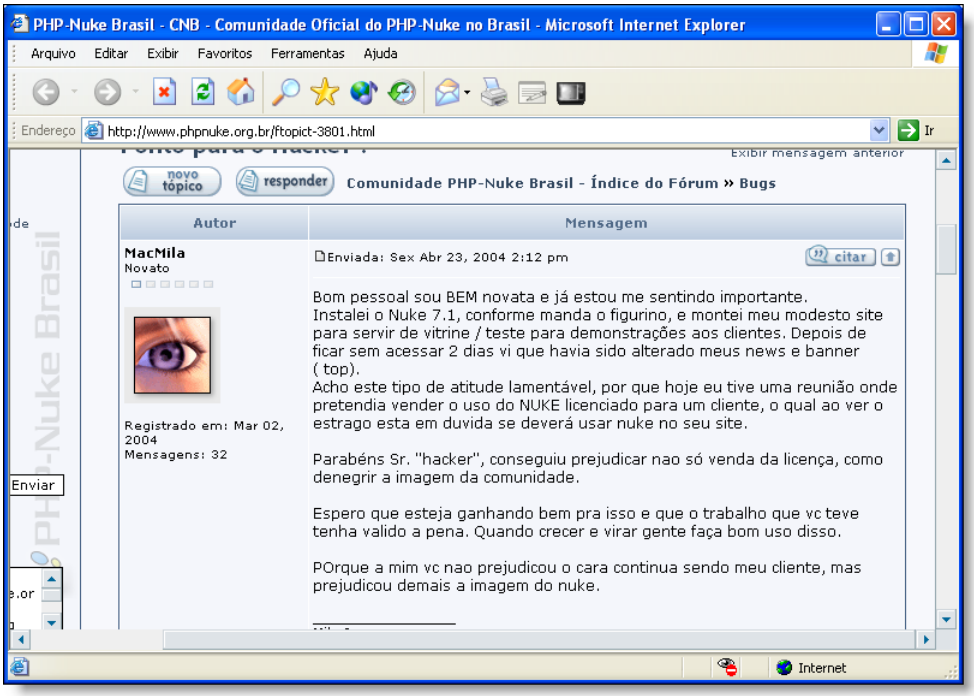


Alvo

O alvo é o objeto da invasão. Pode ser um alvo fixo ou móvel. Servidores são alvos fixo. Máquinas de usuários são alvos móveis. Querer invadir o micro de um usuário em particular, poderá ser uma tarefa impossível. A não ser que você possua informações suficientes sobre esta pessoa. No caso dos servidores, estes possuem IP fixo e costumam permanecer ligados 24 horas por dia, 7 dias por semana. Dá tempo de ir estudando o alvo, coletar informações e eleborar um plano de ataque sofisticado. Eu já passei por situação de ter que espreitar um servidor por mais de dois meses. Cerca de duas ou três vezes por semana eu me dedicava a estudar o servidor e testar partes da minha estratégia de ataque. Um belo dia foi divulgada uma nova vulnerabilidade que se aplicava aquela versão do servidor. Era tudo o que eu precisava.

Vítima

Chamamos de vítima o alvo que sofreu um ataque bem sucedido. Em se tratando de invasão hacker, o usuário comum é incapaz de saber se foi invadido. Embora desconheça estatíticas, acredito ser inexistente o número de usuários que tomam algum tipo de atitude contra o invasor. Na tela abaixo lemos o relato de uma vítima, que eu prefiro chamar de 'profissional incompetente', se lamentando por que o hacker mostrou a falha em um sistema que estava prestes a ser vendido.



Pesquisas revelam que apenas 1% das empresas tomam alguma atitude contra o invasor. Já disse e repito, as ações hacker que certamente lhe causaram problemas são as que envolverem fraudes no sistema financeiro (bancos, financeiras, operadoras de cartão de crédito, grandes sites de e-commerce, lavagem de dinheiro), pedofilia (hospedagem, divulgação ou distribuição de menores despidos, simulando ou mantendo realçoes sexuais), discriminação ou se tiver a falta de sorte de incomodar alguém influente. Nosso Brasil ainda funciona como no tempo dos coronéis.

Objetivo da Invasão

No Curso de Hacker que ministro on-line (*www.cursodehacker.com.br*) os alunos podem marcar sessões de chat para tirar suas dúvidas. É comum pedirem que os acompanhe em uma invasão. Em vez de sair transloucado com o aluno para fazer a tal invasão, começo a fazer algumas perguntas simples para verificar se o plano de ataque está bem feito. A primeira pergunta que faço é *_"Qual o alvo da sua invasão?"* Já vimos que o alvo é o objeto da invasão e geralmente a resposta que recebo é *_"Qualquer um."* ou *_"Fala o Sr."*. Respostas como estas servem para identificar um aluno que quer queimar etapas de um PROCESSO. Várias são as pistas que permitem diferenciar um hacker de um script kiddie. Esta é apenas uma delas. Não dá prá queimar etapas e esperar um ataque bem sucedido. Mas não são todos que chegam sem alvo definido. Alguns são humildes e querem invadir, nada mais nada menos que o site da Globo.Com. Não é que esta invasão seja impossível, já foi feito, no braço Kit.Net e demonstramos isto no Curso de Hacker on-line. Mas estas empresas de grande porte são as mais atacadas e obrigatoriamente as mais bem protegidas. Se não, não duram uma hora no ar. Não é alvo para quem está iniciando.

Depois que o aluno escolhe um alvo a altura da sua inexperiência, faço a segunda pergunta, geralmente fatal: *_"Qual é o seu objetivo para esta invasão?"* Por incrível que pareça, a maioria não tem a menor idéia do que pretende com a invasão. Ou então pede coisas absurdas como 'o gabarito do vestibular da faculdade tal'. Como saber se este gabarito está armazenado no servidor? Não é uma tarefa que possa ser feita em meia hora de aula. Nem existe a garantia de que o gabarito esteja acessível na rede. Não são poucos os casos de alunos meus que conseguem gabaritos de provas nas redes de seus colégios e faculdades. Mas neste caso eles operam na mesma rede em que funcionários e professores. Fica mais fácil e as chances de encontrar o que procuram aumenta.

Então eu pergunto a você, Qual é o seu alvo? Qual é o objetivo da invasão? Se você não tiver estas respostas, para que você quer aprender a ser hacker então? Acho melhor pensar primeiro nisso pra depois começar a invadir.

Inside e Outside

Quando o hacker tem acesso físico a rede interna da empresa, é um *hacker inside*. Se não tem acesso físico a rede da empresa, é um *hacker outside*. Isto faz diferença? Sim. Faz muita diferença. Primeiro por que existe algum nível de confiança entre os computadores da rede interna. Até certo ponto, todos os computadores de uma rede interna confiam uns nos outros. Depois por que o tráfego da rede interna não sai para a Internet. Então um inside vai ter acesso a pacotes que só circulam na parte interna da rede. E em terceiro e último, por que um inside pode se valer da inegenuidade e pouca experiência da maioria das pessoas com a informática, e obter senhas e contas de usuários dos mais diversos tipos.

Um caso...

Em uma faculdade onde trabalhei o diretor, que também era o dono, apesar de abastado, é um completo ignorante nos assuntos de informática. Na Intranet da empresa havia vários níveis de acesso e a cada nível um leque maior de opções e possibilidades era exibido. O maior nível era o meu, o 9. Uma vez este cidadão, que deve ter algum complexo de inferioridade, mas deixo isto para os psicólogos de plantão, me questionou por que o nível dele era o 8 e o meu era o 9? Ele não foi muito explícito, mas o que ele quiz dizer é _*"Por que você que é funcionário tem mais poder dentro da intranet do que eu que sou o dono? Não deveria ser pelo menos o mesmo nível que eu ou um nível abaixo?"* E de nada adiantou dizer que as opções do nível 9 eram pertinentes a operações técnicas e administrativas da Intranet, que não interessariam a ele. Sutilmente ele pediu para ser elevado a nível 9 ou que eu criasse um nível 10. Manda quem pode, obedece quem tem juízo ou conta pra pagar no fim do mês. Fiz o que me foi mandado. Não passou nem uma semana e constatei uma invasão com privilhégios do nível 9. Um aluno usando o laboratório da faculdade acessou a Intranet e conseguiu descobrir a senha do diretor. Era a repetição do nome dele.

Para não me indispor com aquele que pagava meu café da manhã com presunto alemão e *brownies*, criei para ele um nível 10, com menos poderes até que o nível 3. Só dava para fazer consultas e mais nada. Patrão satisfeito e gerente tranquilo. Este foi um exemplo de hacker inside. Estando na rede interna você tem como interceptar o tráfego. E pior ainda, pode sabotar a rede, fazendo com que o tráfego seja redirecionado para qualquer lugar, incluindo um computador externo.

Inclui no CD-Rom alguns programas do tipo *snnifer*. Basta executá-los na rede local da empresa, colégio ou faculdade para começar a interceptar todo o tráfego da rede. De uma tacada só você vai descobrir senhas e conteúdo dos E-Mails, contas de usuário e tudo o mais que circular pela rede local. Aproveite e procure pelos arquivos PWL que guardam as contas de usuário das estações Windows 9.x. Os programas para quebrar a senha dos arquivos PWL estão no CD.

Plano de Ataque

O plano de ataque pode ser a diferença entre transformar ou não um ATAQUE em INVASÃO. Já o sucesso da invasão está intimamente ligado ao OBJETIVO DO ATAQUE. Se o objetivo for obter privilégios de administrador, só podemos considerar a invasão bem sucedida, se realmente obtermos uma conta com privilégios de administrador ou explorar uma vulnerabilidade que permita este nível de acesso em qualquer conta. Vimos isto no capítulo sobre invasão Linux.
Um plano de ataque inclui:

1. Definir Alvo
2. Definir Objetivo
3. Traçar Perfil (*Footprint*)
4. Varredura
5. Definir Estratégia
6. Ataque
7. Invasão
8. Apagar Rastros

Veremos agora na teoria e na prática, cada um dos pontos de um plano de ataque para uma invasão bem sucedida:

1. Definir Alvo

Eu não posso definir o alvo por você. O máximo que posso fazer é sugerir que nesta fase incial do aprendizado você tenha como alvo faixas de IPs. Conforme você for entendendo, aprendendo e ganhando confiança nas invasões bem sucedidas, passe para os alvos de seu interesse.

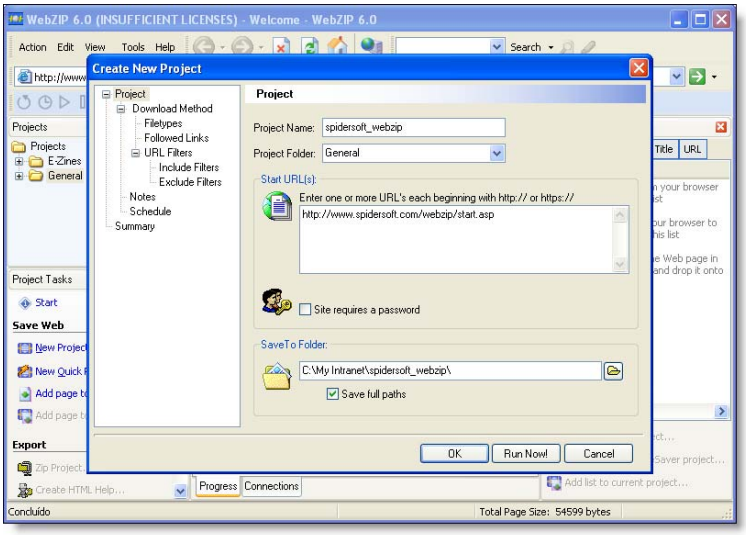
2. Definir Objetivo

Também não me peça para defnir um objetivo para você. Seria um anti-serviço ao seu aprendizado. Como sugestões de alvos temos obter acesso como root (Linux) ou Administrador (Windows), obter acesso a conta de E-Mail do usuário, obter acesso ao servidor Web para alterar a página inicial do site (defacement), obter acesso ao FTP da empresa para hospedar arquivos pessoais, fazer espionagem industrial via Internet, etc... São vários os objetivos que podem estar por trás de uma invasão. Não custa lembrar que só estamos descrevendo os objetivos. Você poderá ter problemas com a justiça caso decida colocar este conhecimento em prática.

3. Traçar Perfil (*Footprint*)

Se já temos o ALVO e o OBJETIVO, precisamos nesta etapa do PLANO DE

ATAQUE, coletar o máximo de informações possíveis sobre o alvo. Este processo é conhecido no meio como footprint. Um perfil pode e deve incluir diagramas representativos da rede e estrutura interna da empresa.
Formas de traçar o perfil:
- consultando todas as informações existente no site da empresa.
- entendendo como a empresa funciona, quais são os níveis gerenciais, departamentos, se tem matriz, empresas com as quais se relaciona, se tem webmail, se tem intranet.
- baixe o site inteiro da empresa e verifique se tem alguma informação iportante inserida nos comentários das páginas em HTML. Um dos programas que fazem isto é o Webzip (*www.spidersoft.com*).



O sistema de busca Google permite a busca por senhas, documentos, bancos de dados e outros recursos que normalmente ficam ocultos do usuário comum. Só com o Google já é possível hackear. Como? Você pode baixar o banco de dados com as senhas dos usuários e depois acessar a Intranet ou o FTP. Ás vezes, pelo FTP, temos acesso ao site da empresa. Está aí a porta aberta para um defacement. Abaixo vão alguns exemplos de como usar o Google para hackear. No CD-Rom você encontra a listagem completa dos comandos:

Para saber que páginas na Internet apontam para o site:

link:*www.empresa.com.br*

Para saber se a palavra *senha* existe em um site:

senha **site:***www.empresa.com.br*

ou senha **inurl:***www.empresa.com.br*

Para pesquisar em e por páginas específicas:
related:*sistema.html* ou **link:***hacker.html*

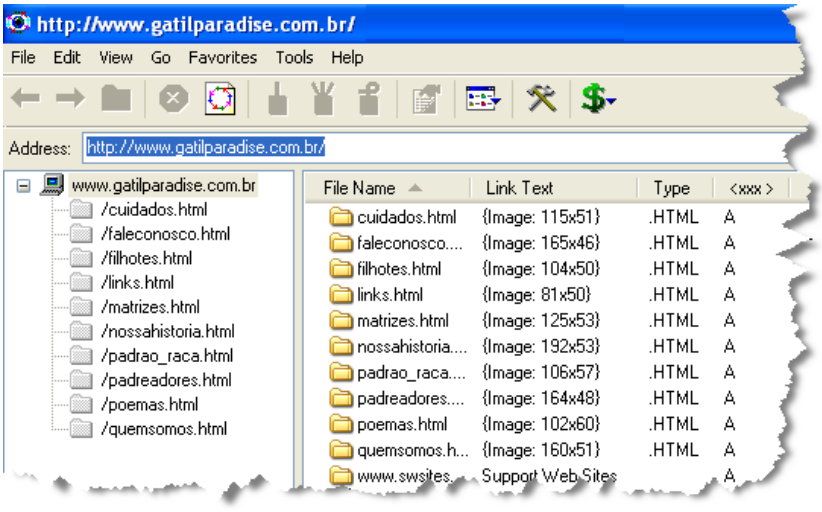
Para procurar por um nome ou um tipo de arquivo:
senha **filetype:***mdb*

Buscando por recursos não indexados:
"*index of*" **inurl:** */root* ou "*index of*" **inurl:** */home* ou qualquer coisa que vier na sua cabeça como por exemplo "*index of*" **inurl:** */.htpasswd*

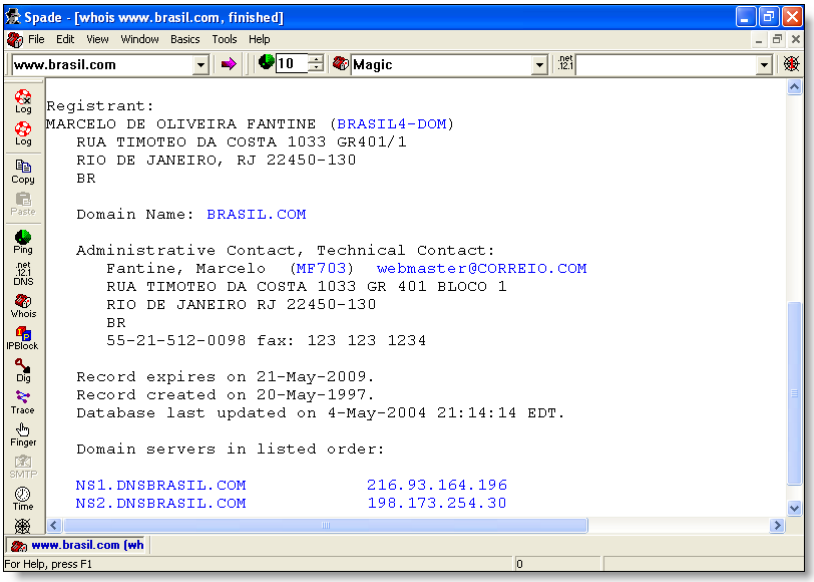
Outras fontes de informação durante a fase do footprint são os sites que possuem algum tipo de banco de dados, como os da Receita Federal (*www.receita.fazenda.gov.br*), Detran, INSS e demais órgãos governamentais. A principal fonte de contulta do hacker é o site Registro.Br, pois através dele teremos como descobrir o IP dos servidores, além de outras informações úteis. Caso o alvo esteja em outro país, a busca pelo IP será feita em um dos links abaixo:

IPs no Brasil - *http://registro.br*
IPs no Estados Unidos - *www.networksoultions.com*
IPs na Europa - *www.ripe.com*
IPs na Ásia e Pacífico - *www.apnic.com*

Programas aparentemente inofensivos podem se revelar grandes aliados do hacker, como é o caso do Get Right (*www.getright.com*), um programa de gerenciamento de



downloads que possui um módulo de mapeamento e exibição da estrutura do site. Acesse **Tools -> GetRight Browser**:
Além dos comandos de rede como por exemplo o ping e o tracert/traceroute, podemos usar softwares que, entre outras coisas, podem coletar informações sobre um ou mais alvos específicos. Como exemplo destes programas temos o Sam Spade, que tem uma versão on-line em *www.samspade.org*. Na figura abaixo, buscamos informações sobre o domínio *www.brasil.com*:



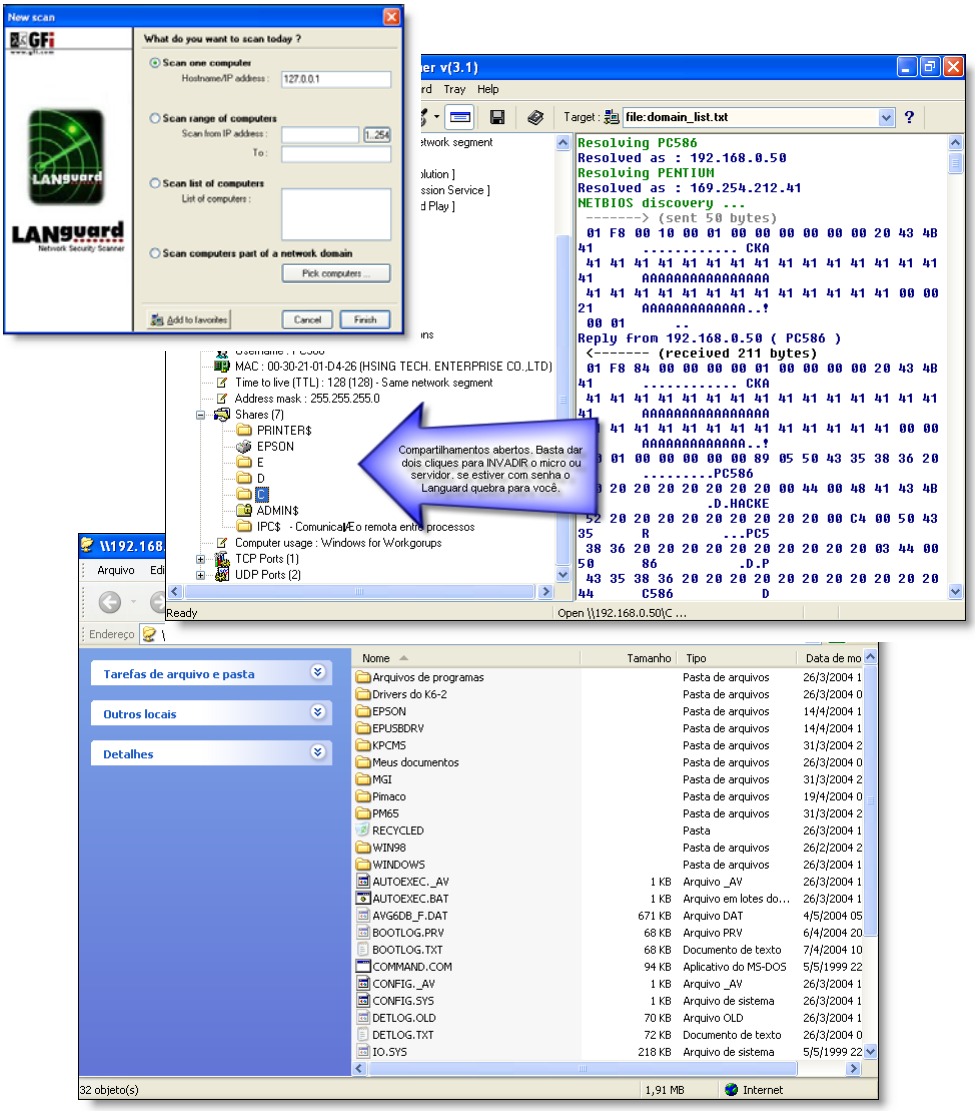
Perceba que são várias as formas de se obter informações sobre um alvo. Em alguns de meus planos de ataque, alguma informação que faltava foi obtida por E-Mail ou telefone. Este processo tornou-se conhecido como engenharia social e foi o que deu fama ao hacker Kevin Mitnick.

4. Varredura

De posse do perfil, vamos dar início a varredura do alvo. O objetivo da varredura é enumerar os recursos, suas características e, principalmente, suas vulnerabilidades. São vários os programas que fazem a varredura do alvo. O que varia de um programa destes para outro, além do preço, que vai de inteiramente grátis (freeware) a alguns milhares de reais, é a profundidade da varredura. Programas diferentes obtem resultados diferentes. O mesmo programa também pode obter resultados diferentes, conforme a configuração. Também podemos obter resultados diferentes em redes diferentes e em sistemas operacionais diferentes. Havendo versão Windows e Linux do programa, é quase certo a versão para Linux ser a mais atual ou ter mais recursos.

Os relatórios de busca incluem informações técnicas. Para o melhor aproveitamento do resultados destes relatórios, você vai precisar ampliar seus conhecimentos de redes, protocolos e sistemas operacionais de redes. A melhor fonte de aprendizado é a documentação do Linux. Pois trata-se de um sistema operacional que desde o início foi pensado para trabalhar em rede.

Para o iniciante, nossa sugestão é o uso da ferramenta Languard (*www.gfi.com*). Eficaz em suas buscas e é sem sombra de dúvidas a mais fácil de usar. Clique em ***File -> New Scan*** e escolha entre varrer um servidor isolado, uma faixa de IPs ou a partir de uma lista.



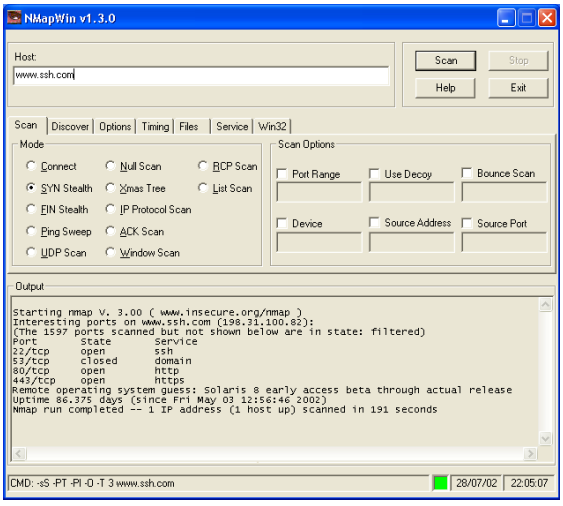
Este programa tanto pode ser usado na Internet como em uma rede local. Experimente diferentes configurações, principalmente as que dizem respeito ao tempo de espera por uma resposta do servidor e formas de autenticação.
Existem dezenas de outras ferramentas do tipo scanner. Sugiro que experimente várias, não só para comparar o resultado entre elas, como para decidir por si próprio qual é a sua preferida. Experimente as seguintes ferramentas (todas incluidas no CD-Rom que acompanha este livro): Nessus, Tara, Sara, Nikto, Typhon, SuperScan e Nmap. Inclui no CD-Rom alguns tutoriais que poderão auxiliá-lo no uso destas ferramentas, mas se mesmo assim encontrar alguma dificuldade, entre em contato comigo no E-Mail *atendimento@cursodehacker.com.br* ou adquira o **Livro Vermelho do Hacker Brasileiro**, também de nossa autoria, com as 100 ferramentas de segurança comentadas passo-a-passo e acompanhadas das respectivas vídeoaulas.

NMap

O Nmap é um dos melhores programas para scanner de servidores. Sua fama e confiabilidade são tão altas que foi usado no filme Matrix, em cena já comentada aqui nas páginas deste livro. Disponível em versões Linux e Windows, pode ser baixado do site ou em nosso CD-Rom. Para os usuários do Linux, segue abaixo a forma de instalar o NMap:

```
bzip2 -cd nmap-VERSION.tar.bz2 | tar xvf -
cd nmap-VERSION
./configure
make
su root
make install
```

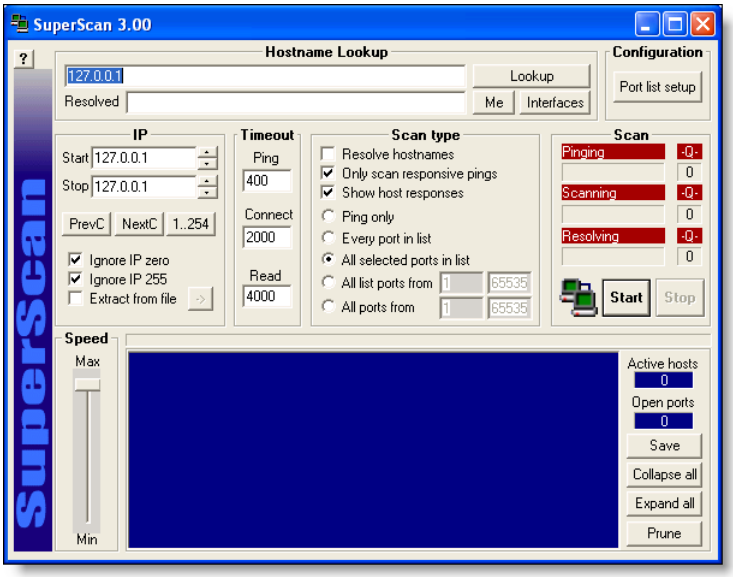
A instalação no Windows dispensa comentários. Por falar no Windows, esta é a tela da interface gráfica para uso do NMap no Windows.



O NMap é um programa complexo e que exige profundos conhecimentos de rede e TCP/IP. Repare que ao selecionar uma opção na interface gráfica, a linha de comando que seria digitada é exibida na barra de status do NMap.

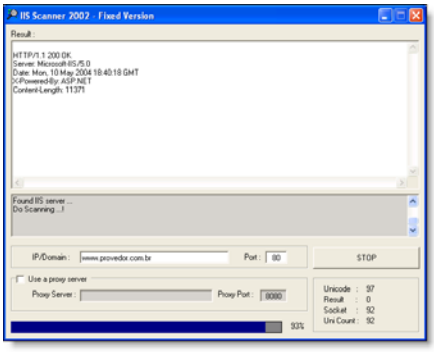
SuperScan

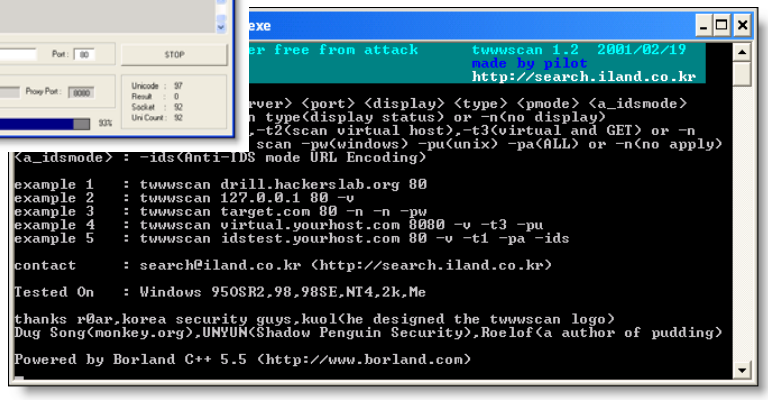
Para os usuários do Windows, sugerimos também o SuperScan, que pode ser baixado do site *www.foundstone.com*. É mais um programa que vai exigir algum conhecimento de redes e protocolos.



Scanners para o Servidor IIS

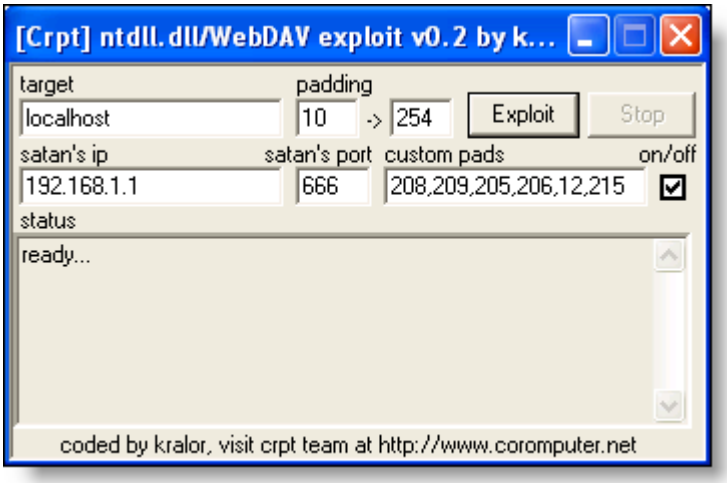
Alguns scanners são específicos para um serviço ou plataforma, como é o caso do IIS Scanner e Twwwscan, ambos no CD-Rom que acompanha este livro:





Scanner para WebDav

O servidor Web IIS da Microsoft inclui suporte para WebDAV, que permite a usuários manipular arquivos salvos em um servidor web. Uma falha de estouro de buffer existe no arquivo ntdll.dll. Um atacante pode executar código arbitrário, dando ao invasor praticamente o controle total do sistema. Esta vulnerabilidade tem mais de um ano e pode ser econtrada esporadicamente em alguns servidores. Na figura um scanner para WebDAV.



5. Definir Estratégia

A estratégia vai depender do seu objetivo em relação ao alvo. Se a sua intenção for acesso a conta de E-Mail do alvo, então deverá usar o Brutus para ataques de força bruta com e sem dicionário. Mas caso seja um hacker inside, poderá plantar trojans em pontos estratégicos da rede e receber de mão beijada a senha do E-Mail.

A definição da estratégia vai ser decidida entre as variáveis objetivo e seu nível de conhecimento técnico. Um mesmo plano de ataque elaborado por pessoas diferentes, vai gerar estratégias diferentes. Talvez eu prefira explorar um bug e compilar um exploit em C. Talvez você não conheça C o suficiente para fazer os ajustes necessários no código de alguns exploits. Então esta estratégia não servirá pra você. A não ser que deixe a invasão de lado por um tempo e depois que aprender o suficiente de linguagem C para alterar exploits, volte mais preparado e em condições de definir uma nova estratégia para o alvo.

A definição da estratégia vai possibilitar responder a seguinte pergunta _*"Já tenho um alvo, um objetivo e sei informações sobre o servidor. Como estas informações e o meu conhecimento técnico poderão ser usados para chegar ao meu objetivo?"*. Talvez a resposta ainda não exista. Provavelmente por você ainda não ter conhecimentos suficientes ou por não ter informação suficiente que permita a definição da estratégia de ataque.

6. Ataque
O ataque é a ação definida na estratégia. Ás vezes será algo simples como dar dois cliques em uma pasta compartilhada que aparece no relatório do Languard. Ás vezes será digitar meia dúzia de comandos em uma página dinâmica vulnerável. E ás vezes será algo tão complexo como infectar milhares de máquinas para promover um ataque em massa a determinado site.

7. Invasão
Um ataque bem sucedido tem como resultado a invasão. Uma invasão bem sucedida significa que o objetivo foi alcançado. Nem sempre é o que você esperava alcançar. Entre os casos de decepção temos contas de E-Mail invadidas que não continham nenhuma mensagem ou nada de relevante, um defacement de um site com um número de visitantes tão insignificantes que quase ninguém ficou sabendo da façanha, uma conta bancária invadida, com tão pouco dinheiro no saldo, que deu vontade de fazer algum depósito para a vítima.
Estas decepções vão ocorrer com muita frequência no início das suas incurções no mundo hacker. Até que suas expectativas se ajustem a realidade. Eu digo que nem sempre você vai encontrar o que esperava encontrar, porque o que você esperava encontrar só existia na sua imaginação. Salvo casos em que temos certeza da existência do que estamos procurando. Então alguém que espera encontrar o gabarito da prova do concurso no site da faculdade, está se iludindo. Não há nenhum tipo de garantia deste gabarito estar onde ele acha que está.

8. Apagar Rastros
Você talvez leia ou ouça por ai, que será rastreado, mas apenas se ficar mais de cinco minutos conectado a um servidor. Não é assim que as coisas funcionam. Os servidores realmente mantem um registro de todas as atividades, principalmente as relacionadas com a segurança. Este registro pode ser de 5 em 5 minutos ou em períodos maiores ou menores. Quem programa isto é o administrador da rede. Mas supondo que seja 5 minutos e o próximo *log* está previsto para ser gravado às 00:05h, quem entrar no servidor às 00:04h terá sua atividade registrada no minuto seguinte.
Além do sistema de log dos servidores, você também vai se deparar com outras ferramentas de segurança, cada vez mais utilizadas em redes corporativas. Estas ferramentas, além de manter um registro mais detalhado, possuem sistema de alerta contra invasões (IDS - *Intrusion Detection System*) que pode entrar em contato com o administrador via E-Mail ou SMS (*Short Message Service*). O administrador poderá acessar o servidor da empresa de qualquer ponto de acesso a Internet e averiguar o grau de risco do ataque. Para um hacker iniciante isto chega mesmo

a representar um perigo, pois o atacado poderá ser você.
Outra forma de defesa que as empresas tem adotado é o *honeypot*. Honeypot ou pote de mel, é um conceito que na prática pode ser um programa, uma máquina virtual configurada de forma a permitir alguns tipos de ataques ou sofisticados e caros sistemas de detecção de intruso, interligados com o sistema de telefonia, que permite, através do BINA, identificar o número de telefone que originou o ataque.
O apagamento de rastros no sistema dependerá do seu conhecimento sobre cada sistema operacional, principalmente o da vítima. A pergunta que você deve responder é *_"Onde estará armazenado o arquivo de log deste sistema operacional? como faço para apagá-lo?"* - A melhor maneira de saber isto é instalando o mesmo sistema operacional do alvo e, após simular um ataque (use a máquina virtual), verificar a localização e o tipo de informação que foi armazenada nos arquivos de log. E mais um detalhe, se você apagar completamente o log vai causar suspeitas. O que se faz é remover ou mascarar as entradas.
Como medida de proteção, alguns administradores de rede decidem por armazenar os arquivos de log em local diferente do usual. O mesmo ocorre com os sites hospedados nos servidores da empresa. Se o servidor for Windows, o local padrão para armazenamento dos sites é *c:\inetpub\wwwroot*. Mas nada impede do administrador mudar a localização padrão, inclusive podendo ser em outra máquina, dentro ou fora da rede, funcionando o servidor apenas como um apontador para o verdadeiro local de hospedagem.

Rootkit
Rootkit é o nome dado a um conjunto de ferramentas que reúne tudo o que é necessário para uma invasão bem sucedida. Isto inclui um processo automático de busca e apagamento das entradas no log. Rootkits automatizam o processo de invasão e são mais comuns no ambiente Unix/Linux.

Deface
O Brasil é conhecido mundialmente como o número Um em porcentagem de hackers ativos. É claro que neste saco entrou de tudo, de lamer a scammer. O Brasil também é campeão no número de páginas alteradas. Nunca o número de páginas alteradas por hackers brasileiros foi tão grande quanto hoje - são milhares de grupos de 'um homem só' que sentem prazer em perder algumas horas de sono a procura de sites vulneráveis ao deface.
Defacer é o nome dado ao hacker que altera páginas de um site. Profissionais de segurança torcem o nariz quando ouvem a associação hacker/defacer. Muitos não consideram o defacer um hacker. Só que a opinião pública e a imprensa mundial pensam diferente.

O motivo do defacer ser marginalizado até entre os próprios hackers é que a maioria possui pouco conhecimento técnico, mas tem tempo de sobra. Passam horas na Internet, procurando sites que estejam vulnerável ao seu exploit (exploit este que não foi desenvolvido por ele) para alterar a página principal do servidor bugado.
Vejo um pouco de hipocrisia nestas afirmações, pois quase todos os melhores nomes da segurança já fizeram um deface, nem que tenha sido 'prá ver como é'.
Todo site tem uma página principal, do tipo, "Seja bem-vindo ao meu site", PRINCIPAL, HOME, Welcome, etc. O defacer altera a página principal, incluindo uma desenvolvida por ele, na maioria das vezes com palavrões e ofensas dirigidas a empresa ou ao administrador. O deface é isto. A substituição da primeira página de um site por outra. O deface pode ser prova de invasão, pois se o defacer alterou a página principal do site, muito provavelmente obteve sucesso na invasão do servidor.
Nos Estados Unidos, berço do hackerismo, a legislação impõe pesadas multas e penalidades para ações hacker. O pessoal de lá, embora tenha acesso ao que exista de mais recente na área de segurança, pode ir parar na cadeia só por usar o Languard para varrer um IP qualquer.
Existem os falsos defacers, pessoas que registram um domínio supostamente da empresa invadida e hospedam uma página normalmente, tentando passar a impressão de que foi uma invasão. Tem um caso deste com repercussão internacional que pode ser visto em:

www.infoguerra.com.br/infonews/talk/1044611173,85608,.shtml

Defacements são divulgados em sites conhecidos como mirrors ou espelhos. Veja alguns destes espelhos nos links abaixo:

defaced.alldas.org
www.zone-h.org
www.attrition.org/mirror

E não esqueça de inscrever seu feito em um destes mirros, depois de criar o seu clã (de um homem só) e fazer seu primeiro deface.
Para fazer o defacement você vai precisar saber o mínimo de HTML . Ou então criar a página substituta no Word e *Salvar Como* html. Também vai precisar saber linguagem C e Perl, sendo que a maioria dos exploits são codados em C. Um defacement pode ser feito de uma das seguintes formas:
- a partir da invasão, seguindo o mesmo roteiro do PLANO DE ATAQUE e tendo como objetivo a INVASÃO DO SERVIDOR WEB.
- a partir da descoberta de alguma vulnerabilidade no servidor Web (IIS ou Apache,

os mais usados) que permita, através de um exploit, alterar a página principal do site. Neste caso a invasão do servidor foi parcial. E como estas invasões são todas em linha de comando, a página substituta talvez tenha que ser criada em uma janela semelhante a do antigo MS-Dos (shell). Não é a tôa que a maioria das páginas de defacement são toscas, só texto em fundo colorido.
- a partir da descoberta de alguma vulnerabilidade em um serviço, como por exemplo o PHPNuke, um sistema de construção automático de portais de notícias e fóruns, cuja vulnerabilidade das últimas versões, permite o acesso do hacker como se fosse o administrador. Esta vulnerabilidade é recente e posso garantir que a maioria dos sites usando PHPNuke ainda estão vulneráveis.
- alterando os dados do DNS nos servidores da Fapesp

Hackeando o Registro.Br (1)

O sistema de registros brasileiros mantido pela Fapesp pode ser facilmente burlado. Os pontos fracos são estes:
- todas as informações sobre o detentor do registro ficam expostas para quem quiser ver
- o registro de domínios pode ser feito com um gerador de CNPJ e um avatar com personalidade jurídica
- mesmo para os registros .org é possível enviar documentos forjados, basta conhecer o modelo de Ata e estatuto usados pelas OCISPs
- de posse dos dados do registro é possível um ataque de engenharia social
- a página é muito fácil de ser clonada
- enviando documentos forjados da empresa detentora do nome (que podem ser obtidos cópias na Internet, a partir do CNPJ), podemos conseguir uma transferência de domínio

Passo-a-Passo para Hackear o Registro.Br

1. Conseguir a senha do responsável pelo domínio:
    - engenharia social
    - phishing scam
    - força bruta
2. Obter dois servidores DNS gratuitos (*www.zoneedit.com*)
3. Obter uma conta de hospedagem gratuita e sem propaganda (*www.ukonline.net*)
3. Configurar os servidores DNS gratuitos para redirecionar o acesso para a página falsa

Nota: se você não tem experiência com o registro de sites, vale a pena registrar algum (usando avatar) para entender como funciona o processo.

Usando Exploit

Um exploit é um programa que explora falhas em outros softwares. Por exemplo um exploit do IIS explora alguma falha neste servidor, um exploit do Apache explora falha no servidor Apache e assim sucessivamente.

O uso de exploit é bastante fácil e vamos ensinar daqui a pouco. O que talvez você ache dificil é fazer o exploit funcionar. Isto por que, para evitar o uso indevido do exploit por lamers, os criadores costumam inserir um caractere estratégicamente posicionado no código, que faz com que o exploit não funcione. Ou pior, o que você pensa ser um exploit é um trojan. Tanto para fazer o exploit funcionar, como para ter certeza de que o exploit não é nocivo a você mesmo, não tem jeito. Só conhecendo C e Perl. Mas a maioria dos exploits são em C. Está é a parte dificil e a mais importante, pois você poderá passar o dia compilando e rodando exploits sem sucesso algum e muito risco. Então não perca tempo, procure um curso de linguagem C on-line ou se matricule em nosso Curso de Hacker (*www.cursodehacker.com.br*) e aguarde chegar ao módulo quatro.

Basicamente um exploit é uma coisa simples: nada mais é que um programa que "exploita" ou seja, explora um bug em um software ou sistema operacional específico. Todos os exploits são diferentes, eles fazem coisas diferentes, exploram bugs diferentes que por sua vez irão também explorar programas diferentes. Por isso não dá para ensinar mais que isto: como obter e usar o exploit. O detalhe que vai ficar faltando está em suas mãos: entender a linguagem na qual o exploit foi codificado.

Na maioria das vezes o objetivo do exploit é fazer com que você adquira o status de root em vários tipos de sistemas operacionais, principalmente em sistemas Unix/Linux: 'root' é o usuário que tem poder total sobre o sistema, ou seja, ele pode criar contas, excluir usuários, criar diretórios, acessar todas as pastas do disco rígido, etc. Precisa mais? Eles alcançam este privilégio pela exploração de uma falha em um software. De forma simplificada, o exploit 'crackeia' o software (servidor) enquanto este esteja ativo, para dar a você um belo prompt de root.

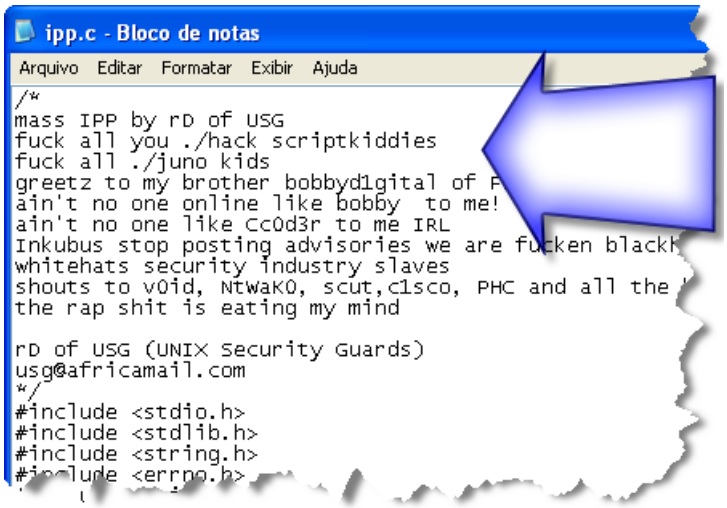
Exploits funcionam em linha de comando. Existe uma minoria de exploits com interface gráfica.

Como Usar Exploits

A maioria dos exploits estão codificados em C, pois esta é a liguagem padrão dos sistemas Unix. Para rodar o exploit você precisará ter uma conta Unix em algum lugar ou, de preferência seu próprio Unix instalado em seu PC. Na prática usamos instalar uma máquina virtual com Linux. O exploit, na maioria das vezes, precisará estar rodando no mesmo ambiente para o qual foi projetado.

Na figura abaixo temo um exploit codado em C e aberto no bloco de notas do

Windows. Repare nas ofensas que o programador dirige aos script kiddies:



Agora você precisará pegar o código fonte do seu exploit ou o binário e colocar em um diretório qualquer (*/usr/usuario*, por exemplo). Agora que você tem o exploit copiado para um diretório, entre no diretório e compile-o:

gcc nome_do_exploit.c

Uma vez compilado é só usar. As instruções de uso de cada exploit se encontram nas linhas iniciais do próprio exploit, que pode ser aberto (código fonte) no bloco de notas. A forma mais comum é ***nome_do_exploit IP***, como por exemplo: ***torpedao 127.0.0.1***.

De qualquer maneira, esteja consciente de que a maioria dos programadores insere pequenos bugs em seu próprio exploit (geralmente é um caractere qualquer inserido no meio do código, facilmente identificável) para evitar que pessoas que não conheçam a linguagem façam besteiras em seu próprio sistema. Quando os programadores não inserem o bug de proteção no exploit, eles se tornam perigosos. Estes programas são feitos por e para pessoas com conhecimentos de programação, portanto se você não conhece a liguagem C, não brinque com ela, tente aprendê-la e depois pense em usar os exploits. Ou o feitiço poderá virar contra o feiticeiro.

Você pode compilar o exploit no Windows, instalando a biblioteca CygWin que pode ser encontrda no CD-Rom do livro ou baixada do site:

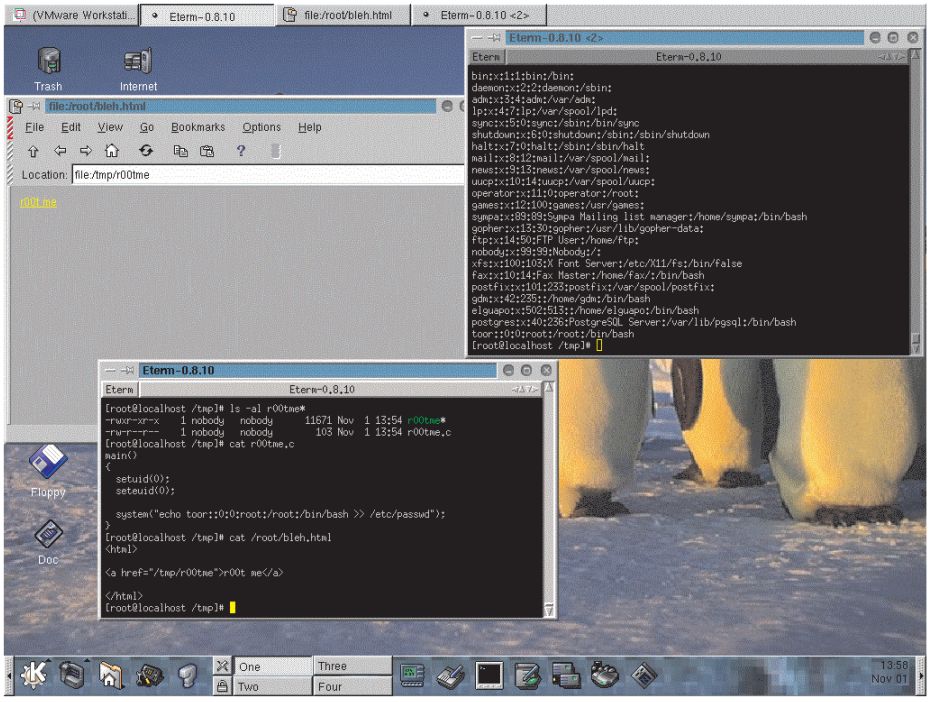
http://sources.redhat.com/cygwin/

Alguns podem perguntar assim: não tem um jeito mais fácil? Mais fácil que isto só se eu for aí digitar pra você. O problema aqui não é a facilidade, é conhecer o sistema operacional invadido e programação em C. Aí já não é comigo, pelo menos não neste livro.

Como informação final, saiba que o deface não dura para sempre. Ás vezes só fica alguns minutos no ar. O motivo? Um site como o da Globo.Com por exemplo, se feito um deface, vai receber imediatamente milhares de telefonemas e mensagens de E-Mail, alertando o pessoal da administração da rede que vai corrigir o problema. Tudo muito rápido. Mas existem casos em que o deface fica por horas, dias ou semanas. Os melhores dias para um deface são os fins de semana e véspera de feriado prolongado. Lista de onde baixar exploits:

http://packetstormsecurity.nl/
http://neworder.box.sk/codebox.links.php?key=exxx
http://www.ussrback.com/archives/
http://www.insecure.org/sploits_microshit.html
http://lsd-pl.net/vulnerabilities.html

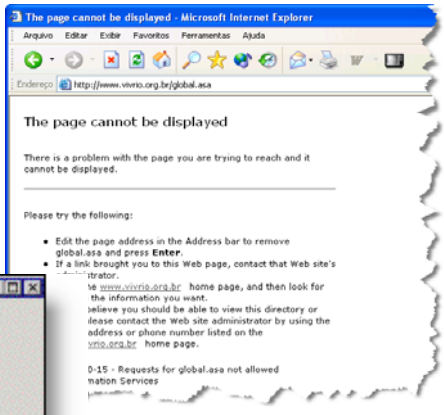
Procure no CD-Rom que acompanha este livro um arquivo texto com dezenas de links de onde tem mais exploits.

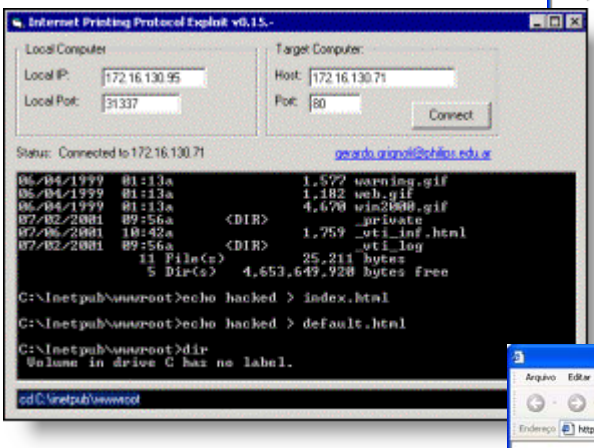


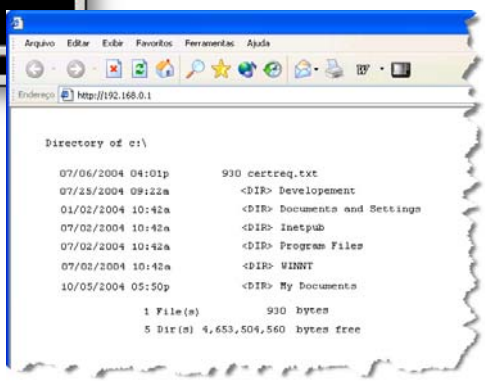
Exploits para o IIS Listar Diretório e Exibir o Conteúdo dos arquivos .asp no servidor

A finalidade de alguns exploits dedicados ao servidor IIS da Microsoft é exibir a listagem do diretório ou o conteúdo dos arquivos dinâmicos com extensão **.asp**. Através da listagem do diretório, podemos verificar se existe algum arquivo útil ou algum outro diretório que possa ser útil ao nosso plano de ataque.

Listando o diretório, podemos visualizar arquivos que não aparecem como link nas páginas do site e nem são indexados pelo Google ou outro serviço de buscas. Quanto a exibição do código fonte das páginas **.asp**, vai permitir a análise de como os dados estão sendo acessados no servidor. Será possível encontrar senhas de acesso a áreas restritas do site, caminhos para o banco de dados, localização de arquivos estratégicos, como o **global.asa**. Esta vulnerabilidade quando descoberta é logo corrigida, pois é gravíssima. Em tempos idos bastava colocar um ponto (.) após o nome do arquivo para visualizar o código fonte. Mais recentemente bastava inserir **::$DATA** após o nome do arquivo para visualizar o código fonte. Para você se beneficiar das próximas descobertas que permitam a visualização do código fonte ou listagem de diretório dos servidores Web, procure manter-se informado. Esta é um tipo de vulnerabilidade que, uma vez descoberta, é corrigida no menor tempo possível.







A exibição do conteúdo dos arquivos .asp atualmente só é possível via exploits e desde que o alvo possua a vulnerabilidade anunciada.

Capítulo 7:

XP

Capítulo 7:

XP

Objetivos Deste Capítulo:
Após concluir a leitura deste capítulo você deverá ser capaz de entender qual tem sido a estratégia da Microsoft para aumentar a segurança dos novos sistemas operacionais, como Windows XP, 2003 e Longhorn. Você aprenderá a técnica homem no meio e a usar trojans corretamente. Também deverá ser capaz de tornar um sistema rodando Windows XP mais seguro. Entre outros assuntos será ensinada a quebra de senha dos sistemas Windows 2000, XP, 2003 e Linux.

O Windows XP

Apesar de todos os ataques que sofre da opinião pública mundial, não há como negar que os produtos Microsoft são mais compatíveis com dispositivos de hardware e mais fáceis de usar que os dos seus concorrentes. Também não há como negar a genialidade do Bill Gates ao criar um império a partir do nada. Mas é justamente esta facilidade de uso que os produtos Microsoft oferecem que permitiu, durante os anos de 2000 a 2002, os maiores ataques de que a Internet tem notícia.

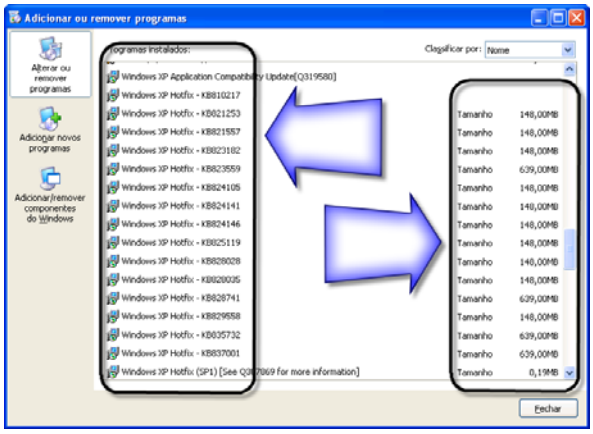
Visando facilitar o processo de instalação e configuração dos seus produtos, já que o Windows NT oferecia pouca compatibilidade de hardware e é de instalação problemática, criou-se o Windows 2000. As principais características deste sistema operacional são, entre outras, a compatibilidade com vários dispositivos de hardware e a facilidade de instalação. Esta facilidade de instalação, planejada para que o produto competisse com o Linux, foi obtida graças ao sacrifício quase que total da segurança. Um servidor Windows 2000, ao ser instalado, configura automaticamente um monte de serviços, às vezes desnecessários naquela instalação em particular. Exemplos? Um escritório de contabilidade que não hospeda o próprio site, pra que precisaria de um servidor Web e FTP rodando? E é isto o

que ocorre quando o Windows 2000 é instalado. Ele deixa rodando um servidor Web e FTP, o IIS, entre outros serviços igualmente desnecessários na maioria das instalações.

O resultado veio logo em seguida com a enxurrada de invasões que ocorreram nos dois anos seguintes ao lançamento do Windows 2000. Ou seja, o tempo que os hackers precisaram para entender o sistema e preparar seus planos de ataque. Muitos de você não devem recordar, mas a Internet se não parou, chegou próximo a isto, com os ataques de negação de serviço, possíveis graças a falhas no Windows 2000.

Você não precisa acreditar em mim. Basta tirar o Windows 2000 da caixa, instalar em um PC, conectar-se a Internet e em menos de 30 minutos seu Windows já terá saído do ar, seja por invasão, seja pela ação de vírus oportunistas que espreitam na rede.

O Service Pack 4 para o Windows 2000 é do tamanho do Windows 2000. Ou seja, você não está baixando um simples remendo, está baixando o sistema operacional todo - Service Pack ou SP é um pacote de correções para o sistema operacional. Verifique em ***Painel de Controle -> Adicionar Remover programas*** a quantidade de correções que o sistema operacional teve que receber para se manter de pé. Na figura vemos a 'pequena' lista de correções para o Windows XP.



Um Caso...

Minha primeira ou segunda impressora colorida, num tempo em que a impressora colorida mais barata custava quase mil reais, foi comprada em uma sexta-feira no Edifício Avenida Central, point de informática no centro do Rio de Janeiro. Passei o fim de semana inteiro tentando fazê-la funcionar. Na segunda-feira, quando a levei para trocar, já havia outra me esperando e a atendente já sabia que eu levaria a impressora para troca. Como, se eu não avisei? Sabe o que eu acho? Eles estavam com uma única impressora com defeito e talvez só recebessem uma boa

na segunda-feira ou até no sábado. Se não me dessem aquela, eu provavelmente teria comprado em outra loja. A impressão que eu tenho é que a Microsoft faz a mesma coisa. Lança o produto inacabado e vai corrigindo conforme o tempo ou conforme os hackers vão explorando o problema. Enquanto isso todos se f.....

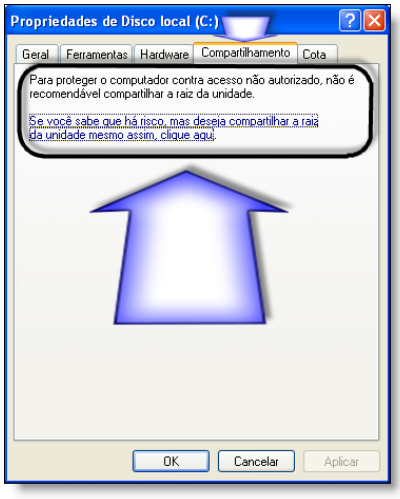
Voltando ao Windows XP, depois da Microsoft passar poucas e boas nas mãos dos hackers, devido ao excesso de serviços padrão no Windows 2000, resolveu investir em design (para competir com os ambientes gráficos do Linux e iMac) e segurança (para competir com o Linux e melhorar a imagem da empresa).

O que surgiu da experiência negativa da Microsoft são os sistemas Windows XP e Windows 2003, além do Longhorn. Este último deve mudar de nome quando for lançado em 2005.

O Windows 2003, ao contrário do Windows 2000, vem com quase todos os serviços desabilitados, cabendo ao administrador de redes instalar e configurar cada um separadamente. A facilidade de uso continua, mas agora se faz necessário um pouco mais de conhecimento sobre redes e sistema operacional de rede. Para maiores informações sobre o Windows 2003 eu recomendo o livro de minha autoria ***Windows Server 2003 - Administração de Redes*** (*www.editoraerica.com.br*).

Já o Windows XP, além das melhorias no seu sistema visual e multimídia, também sofreu melhorias na parte de segurança, incluindo a comunicação com o usuário e um firewall interno. Estar parte da comunicação com o usuário é muito importante, pois serve para alertar e educar as pessoas que até pouco tempo, não se davam conta dos problemas de segurança em informática.

Na tela abaixo temos a opção de compartilhamento de discos e arquivos em rede. Ao contrário das versões anteiores, agora recebemos um aviso sobre os riscos oferecidos pelo compartilhamento de discos, pastas e impressoras:



Muito da segurança do Windows XP trabalha nos bastidores do sistema operacional e o usuário não vai se dar conta. O que posso afirmar é que alguém com o Windows 98 ou Millenium está mais vulnerável a um ataque, se compradao ao usuário do Windows XP. São correções e implementações de segurança cujas principais implicações práticas para o hacker são o menor número de máquinas de usuários vulneráveis e o mal funcionamento ou não funcionamento de algumas ferramentas hacker, quando instaladas no Windows XP. de certa forma a Microsoft se preocupa em proteger você e os outros (de você).

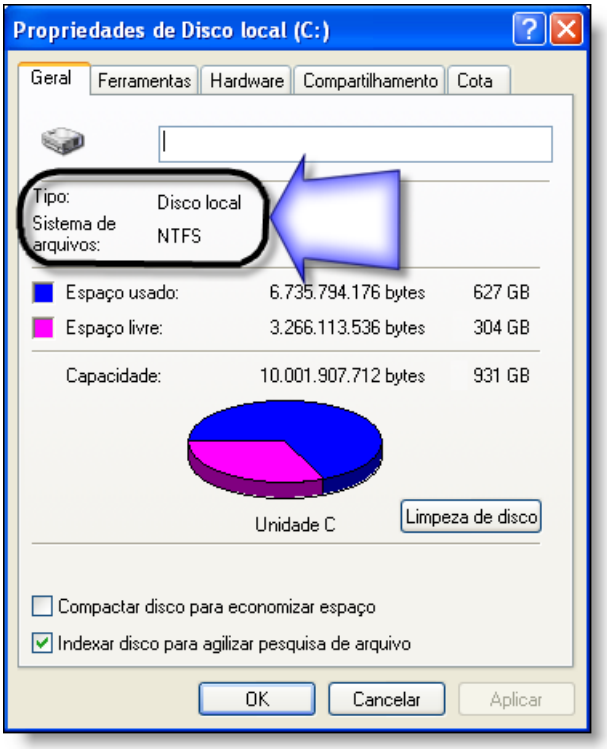
Firewall

Além da melhora na parte de segurança que comprometia o próprio sistema operacional, além da remoção ou limitação das ferramentas de rede, que foi de grande auxílio aos hackers em início de carreira, o Windows XP vem com um firewall. Não é grande coisa, mas é melhor que nada:

Sistema de Arquivos

O Windows XP e também o Windows 2000 e o 2003, permitem que você trabalhe com sistemas de arquivos mais seguros, como o NTFS. O sistema de arquivos mais comum entre os usuários do Windows é o FAT. Acontece que este

sistema de arquivos oferece pouca segurança. Vimos com o Languard, que pastas compartilhadas com senha no Windows 9.x são facilmente quebradas. O mesmo não ocorre com o sistema de arquivos NTFS.
Entre outras coisas, o sistema NTFS permite controlar a quantidade de dados armazenadas em um HD. Ótimo para quem usa banda larga e tem um disco rígido de 80GB a disposição do hacker. O sistema NTFS também permite a criptografia dos dados de uma pasta. Característica extremamente útil e independente de softwares de terceiros. O sistema NTFS permite controlar as permissões de acesso por pasta ou volume de disco. Todas estas caractéristicas, antes disponíveis apenas ao usuário corporativo e administrador de redes, agora está ao alcance do usuário comum. Para usá-las, basta acessar as propriedades do disco rígido ou da pasta a ser protegida.



Convertendo para NTFS

Como saber se o disco do seu computador usa o sistena de arquivos FAT ou NTFS? Clicando em cima da letra correspondente a sua unidade de disco rígido e acessando Propriedades. Para converter um disco sistema FAT para NTFS faça assim:

1. Clique em ***Iniciar -> Executar*** e digite ***cmd*** para abrir o *prompt* de comandos
2. Digite o comando convert ***C:/FS:/NTFS*** (a letra C: corresponde ao drive)
3. Quando surgir a pergunta se você deseja *desmontar o drive*, escolha ***não*** para a pergunta se d*eseja desmontar na sessão atual* e ***sim*** para *desmontar na inicialização*.
4. Feito isto processo é dó dar o boot, aguardar a conversão (uma tela azul parecida com a do scandisk em modo MS-Dos) e conferir o novo formato de arquivos em Propriedades da nova unidade NTFS. Um detalhe: o Windows 95, 98 e Me não lêem partições NTFS. Por falar em formatação, esta opção também apareça na instalação do Windows 2000, XP e 2003. Existem programas que fazem esta conversão em modo gráfico, como o Partition Magic (*www.powerquest.com*).

Trojan

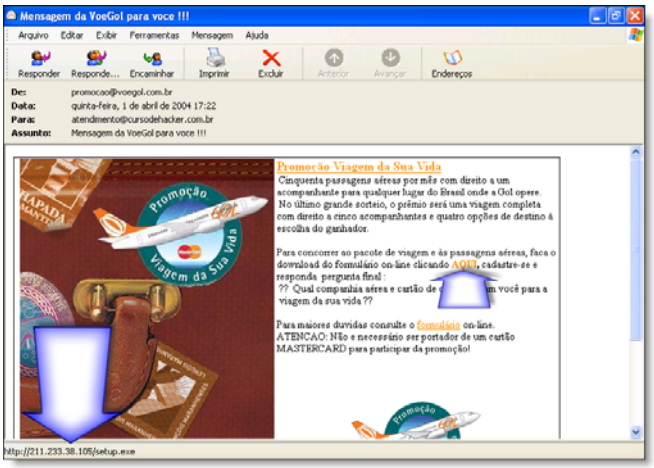
A pergunta é: _"*Se os sistemas domésticos estão se tornando mais seguros, como fazer para burlar esta segurança?*" Por questões práticas e operacionais, a segurança de qualquer sistema pressupõe que, internamente, os usários são pessoas confiáveis. Explicando de outra maneira, isto significa que os fabricantes partem do princípio que alguém que acesse o seu computador de dentro da sua casa ou empresa, é mais confiável que alguém tantando o acesso do lado de fora.
Esse pensamento também se aplica ao uso do firewall, cujo nível de segurança é maior para as conexões de entrada, do que para as conexões de saída. Partindo desta informação, podemos concluir que, se não dá para entrar, por que não forçar a comunicação de dentro pra fora?
É como um porteiro de festa que só olha pra fora. Se alguém de dentro falar com alguém de fora tudo bem. Mas quem está de fora ou não consegue, ou tem dificuldade para falar com quem está dentro.
É aí que entram programas do tipo *trojan horse*, também conhecidos como *backdoor* ou *cavalo de tróia*. São programas aparentemente inofensivos, na maioria das vezes instalado com a colaboração do usuário, e que permitem a comunicação de dentro para fora.
O nome trojan horse (cavalo de tróia) tem a ver com a Guerra de Tróia. Os gregos estavam perdendo a guerra e tiveram a idéia de fingir uma rendição e dar de presente um imenso cavalo de madeira. Só que dentro deste cavalo estavam alguns soldados que, ao cair da noite, abriram os portões da impenetravel Tróia para que os gregos invadissem e ganhassem a guerra.

E tudo isto no meio de uma briga entre deuses e por causa de uma mulher que foi raptada. Do episódio, além do termo *Cavalo de Tróia*, surgiu também o *Presente de Grego*. Para saber mais, leia (ou assista em vídeo) a *Odisséia* e a *Ilíada* de Homero.
A completa semelhança com a função do backdoor usado pelo hacker, fez com que o nome cavalo de tróia, trojan horse ou apenas trojan, se popularizasse.
O trojan mais famoso e que já teve seus dias de glória, foi criado pelo grupo *Culto a Vaca Morta* (*www.cultdeadcow.com*). O *BO* ou *Back Orifice* (uma sacanagem com o nome da suíte *Back Office* da Microsoft e também uma tiração de sarro, pois pode ser traduzido como buraco de trás ou coisa pior).
Programas do tipo trojan são formados por duas partes: o ***cliente***, que será instalado no computador do hacker e o ***servidor***, que será instalado no computador do usuário. Este servidor é um arquivo de pequeno tamanho, gerado pelo trojan.
Os erros mais comuns cometidos pelos iniciantes são os seguintes:
- instalam o cliente e o servidor na própria máquina
- não tem ou não sabem configurar um serviço smtp válido (para que o trojan avise quando o alvo estiver on-line)
- enviam o trojan em formato **.EXE**. Este formato é barrado por quase todos os principais serviços de E-Mails. O formato que ainda é aceito é o **.ZIP**.
- falta de criatividade no envio do trojan
- uso de trojans bugados (um hacker mais experiente modifica o código do trojan para que apenas ele receba a notificação de usuário on-line. O hacker inciante faz tudo direitinho e fica dias esperando por uma notificação do trojan)
- falta de senha para a conexão com o trojan. Não havendo senha, um scanner poderá identificar o trojan (ou a porta aberta pelo trojan) e outro hacker fazer uso dele.

Passo-a-Passo Para Criar o Trojan

1. Consiga um trojan sem bug e que ainda não seja reconhecido por antivírus. Eu recomendo o *Beast* ou o *SubSeven* que se tiverem o *patch* tratado, tornam-se indetectáveis.
2. Crie o servidor do trojan e instale em uma máquina virtual. Aguarde a notificação. Se a notificação não ocorrer em poucas horas, suspeite do próprio trojan ou reveja as configurações, principalmente do smtp (que é o protocolo de envio de mensagens). Existem ferramentas de rede que verificam a comunicação de cada programa com a rede externa. São úteis para verificar se o servidor do trojan está pelo menos tentando a comunicação, ou se está tentando a comunicação com o criador. Mas é preciso saber usar estas ferramentas. No CD-Rom que acompanha este livro você encontra ferramentas de escuta de portas, muito úteis para testar trojans.

3. Se tudo estiver funcionando, use a criatividade para enviar o servidor do trojan para o alvo. Aqui é que mora o problema. As pessoas não estão mais tão bobinhas como antigamente. Embora ainda tenha gente que clique em qualquer coisa que venha com o E-Mail, muitos já abandonaram este hábito. Veja abaixo uma peça de scam com trojan. Ela está bem feita e muita gente deve ter caido neste golpe.



Achar o 'ponto' certo de um trojan pode levar algum tempo. Entenda o trabalho com trojans como o de um laboratório. Não sabendo criar o próprio trojan, teremos que experimentar vários até achar um que corresponda a nossas expectativas e que funcione corretamente. A persistência é a principal característica dos vencedores. Não aceite a derrota, pois corre o risco de se acostumar com ela.

Formas de DistrIbuir o Servidor do Trojan

1. Enviar por E-Mail

O problema do envio por E-Mail, com eu já disse, é que as pessoas estão cada dias mais espertas, aprendendo com os próprios erros e não aceitam com facilidade arquivos anexos em mensagens de desconhecidos.

As soluções possíveis são:

- durante o footprint, identificar pessoas e empresas ligados ao alvo e que sejam da sua confiança. Envie o E-Mail com o remetente falsificado (veremos como fazer isto no capítulo sobre phishing scam) e tendo no assunto URGENTE. Seja criativo aqui também. Algumas sugestões de assunto incluem: *Veja isto...*, *Re:*, *Seu currículo*, *Urgente*, *Proposta*, etc...

- entre em grupos de discussão no Yahoo! Prefira os que tem muitos membros e muitas mensagens. Passe um tempo lendo as mensagens para se familiarizar e, quando ganhar confiança dos outros membros, mande o trojan anexado ou

em forma de link para baixar de um site. Você pode armazená-lo em um servidor de hospedagem grátis, mesmo que não tenha a intenção de hospedar um site inteiro. Exemplo de mensagem para um grupo sobre cães:

Oi pessoal.
Consegui um programa que simula aqueles apitos de chamar cachorro. Quando você executa o programa você não houve nada, mas se tiver algum cachorro a até dez metros de distância, ele começa a latir. Eu usei de madrugada aqui em casa e foi uma latição danada. Acordou a vizinhança. (rs) O programa pode ser baixado do site:

http://...

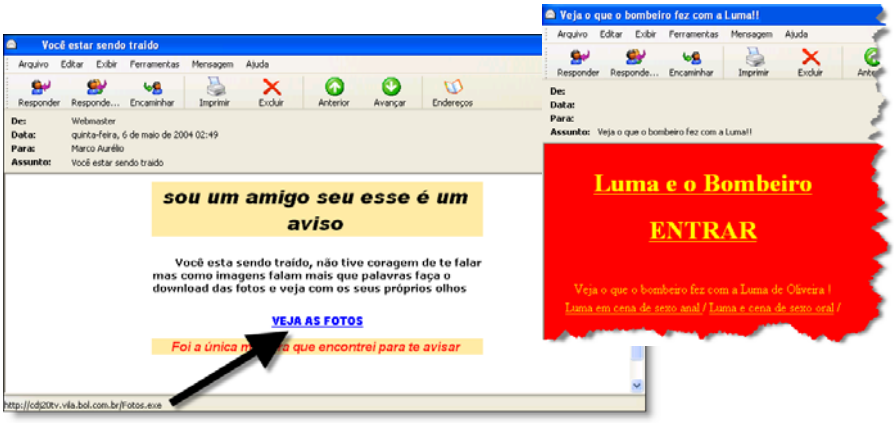
O texto está dentro do contexto do grupo. Mexe com a curiosidade natural das pessoas e tem grandes chances de ser aberto. Acho que até você abriria este arquivo se recebesse este E-Mail. Mesmo você que sabe dos riscos que corre. Sabe por que? Usei técnicas de neurolinguística e tornei a mensagem irresistível. Quem abrir o arquivo e ver que nada aconteceu, provavelmente não vai suspeitar de ter instalado um trojan. E se quisermos tornar a peça (o nome de um trojan, ao fazer parte de uma estratégia, inclusive de phishing scam, se chama peça) mais atrativa, podemos criar uma interface bonitinha usando Delphi ou Visual Basic, criar vários arquivos MP3 com o Cool Edit, cada um usando frequência acima de 15kHz. Cada botão pressionado vai gerar um som de alta frequência que só é ouvido pelos cães. Desta forma o trojan vai realmente fazer o que alvo espera dele (e o hacker também). Todos ficaram felizes. Poderá ser distribuido até no Superdownloads ou por mala direta eletrônica em forma de freeware. Vai ser um sucesso. Quem não vai querer um programa que chama cachorro sem que ninguém perceba? Só para perturbar os vizinhos por exemplo. Em vez de Visual Basic ou Delphi, podemos usar o Flash que tem vários templates prontos.

AVISO: Este programa não existe. Eu não o fiz e nem o vou fazer. Foi apenas um exemplo de como a criatividade e uma mente hacker pode criar programas de fácil aceitação e usá-los como cavalos de tróia. Se por acaso você algum dia o encontrar na Internet, provavelmente será obra de algum leitor deste livro que resolver colocar a idéia em prática.

2. Também podemos enviar o trojan pelo correio disquete, CD-Rom ou impresso de boa qualidade.
3. E que tal um disquete ou CD-Rom esquecido dentro do elevador da empresa com o nome *Backup da Folha de Pagamento*? Você pode até colocar uns arquivos do

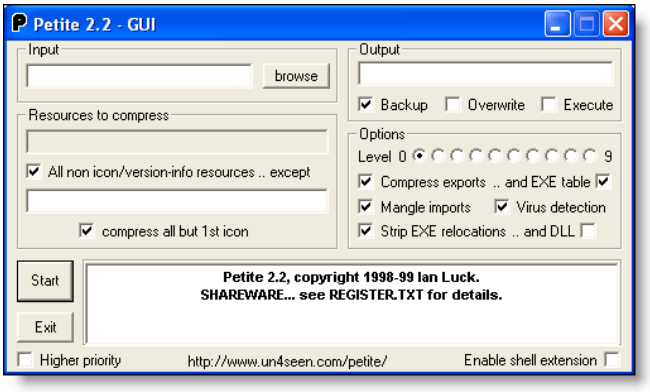
Excel com senha para dar mais veracidade. Na curiosidade o alvo vai tentar abrir todos os arquivos. Em tempos idos eu já andei 'esquecendo' disquete com vírus no balcão de um concorrente desleal. Pena que não deu prá ver o resultado da brincadeira.

Não importa a forma que você use para enviar sua peça. O que importa é você convencer o alvo de que pode confiar e abrir o E-Mail, visitar o site ou executar o programa gravado no Cd-Rom ou disquete. Temas como traição são ótimos, pois geram reação de cólera imediata. Experimente enviar E-Mails do tipo "*estou saindo com a sua mulher, veja as fotos...*" ou se aproveitando de alguma situação, como aquela história da Luma e o bombeiro. E não será nenhuma novidade, eu já recebi E-Mail com este conteúdo.



Tornando Trojans Indetectáveis

São duas as formas de tornar um trojan indetectável: compressão e vinculação. Na compressão o código do trojan é compactado, tornando sua assinatura ilegível para o antivírus. Na vinculação o trojan é unido a um segundo programa. Quando este segundo programa for executado, o trojan também o será. Há casos em que o trojan não é percebido, até ser executado junto com o programa vinculado. Isto ocorrendo, você de comprimir e vincular. Os programas usados para realizar esta tarefa são o Petite e o PExplorer.



Criando o Próprio Trojan

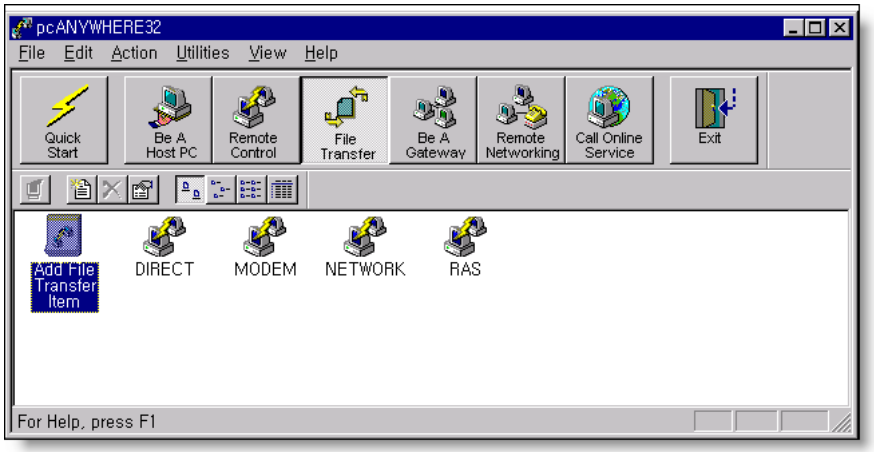
Em capítulos passados já falamos sobre os programas geradores de trojans. Estes programas possuem eficácia duvidosa e você corre o risco de gerar e distribuir servidores de trojans para o criador do programa. Ou seja, o servidor vai funcionar, mas em vez de entrar em contato contigo, vai entrar em contato com o criador do gerador de trojans e provavelmente, também vai abrir algumas portas do seu micro.

Estou formatando um CD avulso sobre a criação de trojans em várias linguagens. Neste CD avulso eu ensino o necessário sobre programação de sockets e no final da lição você terá criado um trojan, podendo depois adaptá-lo às suas necessidades. A grande vantagem do trojan criado por você é que ele vai funcionar como um programa comum feito para o Windows, e nunca será detectado por antivírus ou firewall.

O grande segredo e sucesso dos trojans da nova geração é serem distribuídos camuflados em forma de programas de grande interesse, como o gerador de créditos para celular, o chama cachorro, o calculador de dias férteis e por aí vai.

Trojans Comerciais

Programas como VPN, PC Anywhere, Carbon Copy e até mesmo o serviço de terminal do Windows, podem ser usados como trojans sem a menor preocupação quanto a ação do antivírus. Como são de empresas confiáveis, nem o antivírus nem o firewall se preocupam com suas atividades. Cybercafés rodando Windows não sabem o risco que correm. Um logon com terminal server por exemplo, é completamente invisível.

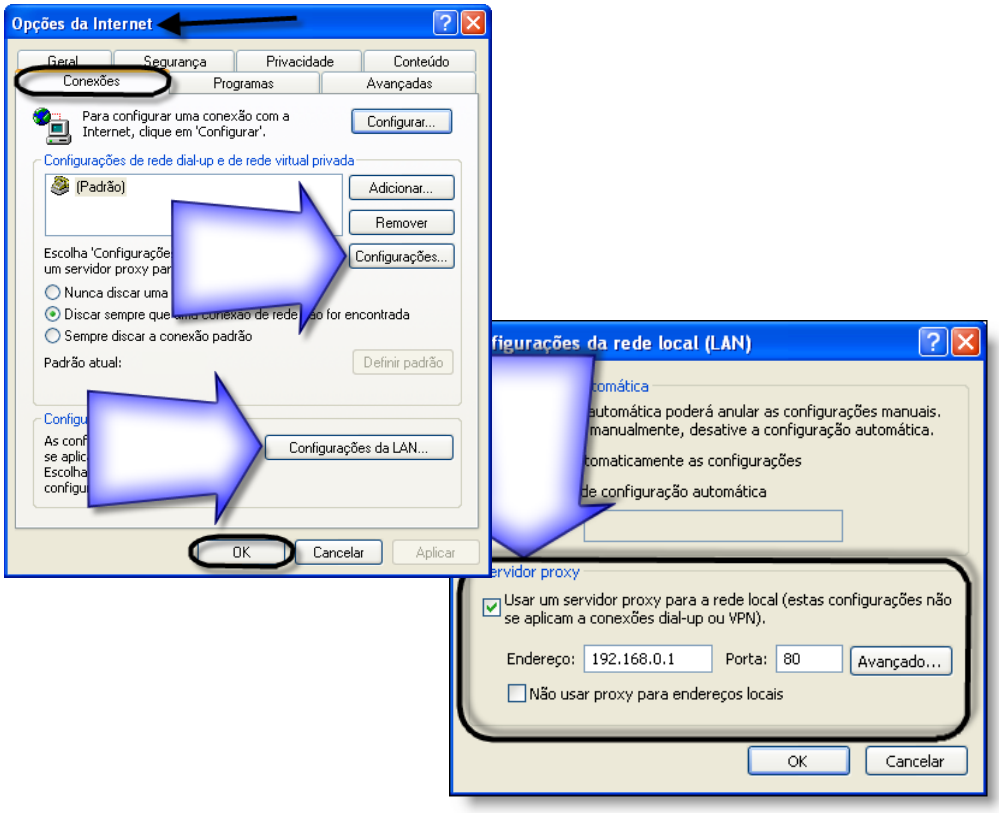


Homem no Meio (WEB Attack Proxy)

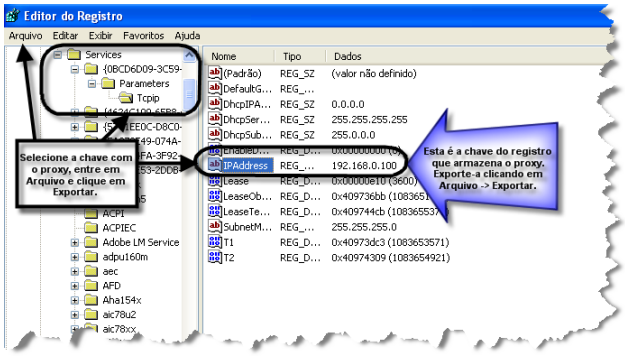
Uma técnica que foi muito falada em 2003 é a *Man in the Middle* ou Homem no Meio. Esta técnica pode ser usada tanto em rede local como via Internet. Para ser usada, precisa da colaboração do alvo, mesmo que involuntária. Este técnica permite a captura dos dados trocados entre o micro do usuário e outro micro, como o servidor do banco, por exemplo. Com prática o hacker pode, inclusive, interferir nas mensagens que aparecem durante a navegação do usuário. Para isto precisará ser ágil e conhecer bem HTML, JavaScript e CSS.

Técnica Homem no Meio Passo-a-Passo

1. Primeiro você precisa preparar o computador do alvo, forçando a navegação via proxy. Para isto você deve abrir o Internet Explorer, acessar na barra de menus as opções ***Ferramentas -> Opções da Internet***. Na aba ***Conexões*** você deve acessar ***Configurações*** (se a conexão for discada) ou ***Configurações da Lan*** (se a conexão for banda larga ou via rede) e inserir um servidor proxy para navegação Web. Este servidor proxy pode ser um servidor proxy público ou pode ser o do seu micro, caso tenha um IP fixo (dificilmente) ou semi-fixo (banda larga).



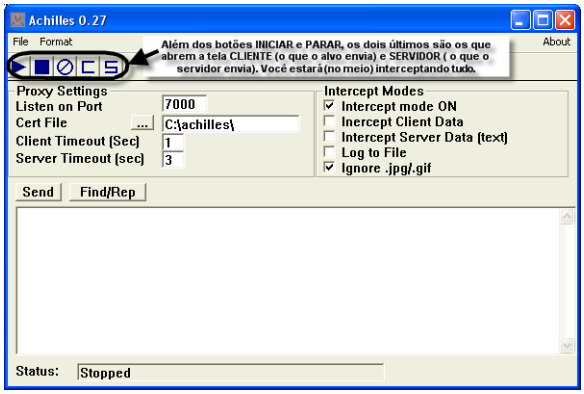
A pergunta é _*"Como posso usar a técnica homem no meio se não tiver acesso so computador do alvo?"* É possível, mas neste caso haverá necessidade de conseguir a colaboração do alvo, mesmo que involutaria. Se você for bom em edição de registro, não terá dificuldades em fazer um arquivo (extensão .reg) que ao ser clicado, insira no registro do alvo o proxy necessário a técnica. Uma forma mais simples e ao alcance de qualquer pessoa, é fazer a configuração na sua máquina ou em uma máquina de testes (pode ser máquina virtual) e exportar a chave do registro. Este procedimento pode ser feito via editor de registros: ***Iniciar -> Executar - >RegEdit***



Só que você ainda vai precisar contar com a ajuda do alvo, para executar o arquivo que vai alterar a chave do registro. Você pode fazer algumas experiências de engenharia social, como por exemplo, se passar pelo provedor e convencer o alvo que precisa reconfigurar o Internet Explorer para uma navegação mais segura.

2. Feito o primeiro passo, que é a configuração do proxy na máquina alvo e TAMBÉM NA SUA MÁQUINA, você vai precisar do programa Achilles para fazer a interceptação do tráfego. Para esta técnica não há proteção. Ela captura mesmo conexões criptografadas, trapaceia o certificado de segurança e captura tudo o que for trocado entre as duas máquinas, mesmo se utilizarem o tecladinho virtual. Parece complicado? Impressão. Experimente e verá. Segue um resuminho:

1. Configurar o proxy na sua máquina e na máquina alvo;
2. Executar o Achilles e abrir as janelas CLIENTE e SERVIDOR;
3. Observar o tráfego e ver o que interessa ou não (vai precisar de conhecimentos de HMTL, CSS e JavascrIpt).



Capítulo 8:

Scammer

Capítulo 8:

Scam

Objetivos Deste Capítulo:
Após concluir a leitura deste capítulo você deverá ser capaz de planejar e criar uma peça de phishing scam completa. Entenda que as informações aqui apresentadas são meramente informativas. Em nenhum momento as informações deste capítulo foram colocadas em prática (a não ser em ambientes simulados) e caso você as coloque em prática, certamente terá problemas com a justiça. Não sei se a proibição da publicação deste livro foi só devido a este polêmico capítulo, mas que foi o que mais contribui para esta censura, isto foi. Aprenda para saber, aprenda para se proteger, aprenda para entender como funciona o processo de phishing scam e ajudar na criação de técnicas de segurança, mas não coloque em prática, é crime.

Phishing Scam

O Phishing Scam ou pescaria de senhas, é uma das técnicas mais usadas atualmente, devido a sua facilidade de implementação e altos índices de retorno. Não é uma técnica recente, há casos que datam de antes do ano 2000. Mas a técnica continua causando grande impacto.

Em rápidas palavras, o phishing scam é o ato de obter informações do alvo a partir da fraude. As informações mais cobiçadas são números de cartão de crédito e senhas de contas bancárias e as fraudes mais usadas são sites clonados de bancos e empresas conhecidas. Esta técnica fez surgir, inclusive, uma nova classificação de hackers, os 'scammers'. É um tipo de ataque que se vale do descuido e da ignorância do usuário final, ainda desacostumado a lidar com a tecnologia da informática. Eu e você, que acredito também passar horas na frente do micro, sabemos o quanto este

equipamento gosta de complicar as coisas simples do dia-a-dia. Quem nunca passou pelo dissabor de ter um arquivo desaparecido do diso rígido, sem que tenha qualquer indício de vírus, ataque, invasão ou ação hacker (inside ou outside)? E quando é um cliente, falar o que? Que ele apagou o arquivo sem perceber? Que no Windows alguns arquivos somem sem explicação? Então é disto que eu estou falando, de um equipamento que pode tornar-se imprevisível.
Cursos de informática não preparam o suficiente. Não dá para capacitar alguém em informática com apenas 3 a 4 horas de aula por semana. Com todo o conhecimento de informática que tenho, acumulado em mais de vinte anos de labuta na área, se não me dedicar algumas horas por dia ao aprendizado de novas técnicas e aperfeiçoamento do que já conheço, fico para trás. E ás vezes ainda tenho que relembrar como tratar as linhas órfãs no Word, personalizar um dicionário ou vincular uma tabela no Access. Que dirá uma pessoa que faz um curso entre o básico e o intermediário e não possui computador para praticar. São estas pessoas, a maior parte da população, o alvo dos scammers.

Criando Uma Peça de Phishing Scam

Usando como referência o nosso PLANO DE ATAQUE, as primeiras providencias do scammer é definir ALVO e OBJETIVO. Vamos supor, e só supor, que o ALVO seja o usuário eventual de computador ou aquele que usa o computador diariamente, mas nunca além dos conhecimentos básicos elementares. E vamos supor, só supor, que o objetivo seja capturar a maior quantidade possível de números de cartões de crédito válidos.
Analisando o objetivo, a obtenção de números de cartão de crédito não precisa ser exatamente através do phishing scam. Outras opções seriam:
- invasão de sites de pequeno porte. Um alvo excelente para captura de números de cartão de crédito são os pet shops virtuais. O dono de um cachorro de raça costuma gastar mais com o animal do que custaria educar uns três a quatro meninos de rua. Compram qualquer besteira para o cachorro. Os sites de pet shops costumam vender alguma coisa on-line e como formam uma comunidade de abastados, muito provavelmente ali estarão vários números de cartão de crédito.
- um outro tipo de golpe é o site de e-commerce falso. O hacker cria um avatar, um site falso e oferece alguma oferta irresistível. Oferece a opção de pagamento por cartão e é desta forma que irá pegar os números do cartão de crédito. Cada desavisado que entrar no site e fizer uma compra (que nunca vai ser entregue), deixa o número do cartão para o hacker.
- IRC/mIRC - nos canais do IRC você pode obter uma penca de números de cartão de crédito válidos. É só ganhar a confiança dos kiddies e vai receber milhares de números de cartão. O motivo? Quanto mais gente usar, mais difícil será

pegar quem roubou os números dos cartões. Se você quiser entrar para o mundo do crime, é só dar uma olhadinha no CD-Rom que acompanha este livro e procurar por programas geradores de números de cartão de crédito.


```
* 5863264630514054 *  MASTERCARD
* 4461306454200754 *  VISA
* 4160457421407636 *  VISA
* 5052616713018017 *  MASTERCARD
* 5171318881271686 *  MASTERCARD
* 3766584435266466 *  AMERICAN EXPRESS
* 4666381247208300 *  VISA
* 3475468161283683 *  AMERICAN EXPRESS
* 5610106463227807 *  MASTERCARD
* 4363508835345138 *  VISA
* 5302477801878224 *  MASTERCARD
```

Só um aviso. As empresas de cartão de crédito costumam ter honeypots com números de cartão isca. Se um destes cartões tentar comprar alguma coisa, já se sabe que foi fruto de um ataque bem sucedido, pois nunca foram emitidos. Não confie em números de cartão de crédito baixados da Internet ou pegos no IRC. Não é só do lado de cá que tem gente esperta.

- usar KeyLogger para pegar números de cartão de crédito. Em Salvador, Bahia, no Centro Histórico, mas precisamente no Pelourinho, tem cerca de 10 cybercafés. Ficam repletos de turistas de diversas partes do mundo. Muitos destes turistas compram suas passagens pela Internet. Sai mais barata, pode ser parcelada e tem prazo para começar a pagar. Também evita o desgaste de ter que tratar com algum funcionário mau humorado em alguma agência de viagem.

Quando viajo entre Rio de Janeiro, São Paulo e Salvador, compro as passagens pela Internet a 280 reais (ida e volta, preços de abril de 2004 na Gol!). De ônibus, além das 28 horas de viagem, as passagens de ida e volta custam 340 reais. É por isso que cada vez mais pessoas estão optando por comprar passagens pela Internet (usando o cartão de crédito). Basta o hacker ir de cybercafé em cybercafé, instalar keyloggers e aguardar em casa a chegada dos números de cartões de crédito e contas internacionais em seu E-Mail. As contas bancárias também serão descobertas, por ser muito comum conferir o saldo várias vezes quando estamos a passeio ou trabalho em outra cidade ou país. Você faria o mesmo se estivesse no exterior. E não precisa nem ser o keylogger que envia notificação por E-Mail. Pode ser aquele mais simples, que faz a gravação local. É só ir buscar o arquivo no final do dia ou no dia seguinte. Ou então instalar um trojan na máquina e

acessar o computador do cybercafé a partir de casa. Como você vai ter acesso ao mesmo computador do alvo, poderá instalar um trojan comercial e até um pequeno servidor de FTP, que independe da versão do Windows. O cybercafé também é o lugar ideal para a técnica *homem no meio*.
A opção por cybercafés frequentados por turistas é que estas pessoas só vão dar conta do problema quando estiverem bem longe daqui. Tudo será mais dificil para elas. Desconfiar que foi em um cybercafé. Descobrir que foi você.
Na agência de Correios de Nilópolis(RJ) o computador que dá acesso a Internet roda o Windows 95 (abril 2004). Configuramos o *homem no meio* para testar o funcionamento. O grosso da comunicação era recadastramento de CPF, troca de E-Mails com futilidades e pesquisas do resultado da colocação em concursos. Quando experimentamos a mesma técnica em um cybercafé localizado em Ondina, bairro nobre de Salvador(BA), o tráfego capturado passou a ser consulta de saldos, E-Mails em vários idiomas, reservas de passagem co cartão de crédito. A escolha do ponto de coleta de dados também influencia o tipo de tráfego que você vai interceptar.

E onde entram os E-Mails e sites falsos?
Primeiro eu quis mostrar que para obter números de cartão de crédito não é necessário uma peça de phishing scam . Temos o IRC e os cybercafés em pontos turísiticos, que dão conta disso. São planos que podem usar como estratégia técnicas simples como keylogger e 'homem no meio' (se tornará fácil por que você tem o acesso a máquina alvo).
O phishing scam tem sido usado para coletar dados de contas bancárias, incluindo senhas. O keylogger e o 'homem no meio' também podem ser usados para esta finalidade. A vantagem estratégica do phishing scam é a possibilidade de receber de uma só vez um grande número de contas bancárias. E quanto maior o número de contas recebidas, maiores as chances de encontrar contas bancárias com dinheiro. Ninguém vai querer entrar em uma conta com duzentos contos de saldo.

Uma pausa...
Um engenheiro morador de Copacabana, bairro nobre do Rio de Janeiro, adquiriu recentemente meu livro e DVD **Proteção e Segurança na Internet** (*www.editoraerica.com.br*). Um hacker invadiu sua conta bancária e se aproveitou do empréstimo automático que o banco disponibiliza, para tirar mais mil reais, além do que já havia desviado. E não foi o primeiro aluno que relatou ter passado por experiência semelhante.

Uma Peça de Phishing Scam

O processo completo do phishing scam é este:

1. Defina objetivo (senhas e dados de contas bancárias)

2. Defina alvo (escolha um banco por peça, o alvo são os clientes)

3. Abra uma conta no banco alvo para receber o dinheiro. Esta conta terá obrigatóriamente de ser aberta usando um avatar ou laranja. Isto é crime e você sabe disso. Não faça.

3. Estudar o funcionamento do sistema *Internet Bank* do banco alvo, ou seja, o passo-a-passo da operação desde o login até aparecer a tela com o saldo e extrato. Você poderá ver isto na conta fantasma que você abriu.

3. Fazer uma cópia do site do banco alvo para o seu HD

4. Pesquisar se não existe uma campanha em andamento. Você poderá usar as mesmas informações da campanha oficial. Isto vai causar confusão, por que se o cliente for conferir no teleatendimento, a atendente vai confirmar que a campanha existe.

5. Clonar o site do banco.

6. Para a hospedagem você tem duas opções: gratuita ou paga. A vantagem da hospedagem paga é você poder usar o SSL (*Secure Sockets Layer*) e exibir o cadeadinho na barra de status e o *https://* na barra de endereços.

7. Criar a peça da campanha. A peça é o E-Mail que vai atrair o alvo para o site clonado. Uma peça também pode servir para distribuir trojans com keyloggers.

8. Obter a lista de E-Mails.

9. Obter a lista de contas bancárias para dissimulação.

10. Montar o servidor de E-Mails.

11. Rodar a peça (enviar os E-Mails em massa).

12. Quando começar a chegar os dados das contas, fazer transferências para umas cinquenta contas diferentes, incluindo aquela aberta com o avatar ou laranja. Você também poderá fazer compras a serem entregues em caixas postais, posta restantes e hóteis onde se hospede por no máximo dois dias. Algumas empresas entregam no mesmo dia (o Submarino por exemplo).

13. Finalize a operação.

Phishing Scam Passo-a-Passo

1. Definir objetivo

Este já está definido pela natureza da ação: obter o maior número possível de dados de contas bancárias, incluindo senhas.

2. Definir alvo
O alvo será o banco, de preferência aquele com muitos correntistas na Internet e que permita abrir conta fantasma com pouco risco.

3.Abra uma conta corrente ou poupança no banco alvo
O Bradesco reúne todas as características que nos interessa: facilidade para abrir a conta, muitos clientes na Internet e faz campanhas por E-Mail. Além disso, em parceria com o Correios, criou o Banco Postal. É uma conta corrente do Bradesco aberta diretamente na agência dos Correios, sem a necessidade de comprovar renda. Basta a identidade, o CPF e um comprovante de residência. O depósito incial é de apenas dez reais. Trata-se de uma excelente opção, pois o pessoal do Correios é menos preparado que o pessoal do banco no que diz respeito a assuntos bancários.
A Caixa Econômica também oferece facilidades para abertura de contas sem comprovação de renda, bastando a identidade, o CPF e um comprovante de residência. As contas podem ser abertas em casas lotéricas.
O HSBC, um dos piores bancos que eu conheço, mas quando está precisando encher o cofre, faz uma campanha de abertura de contas populares sem comprovação de renda. Mas costuma pedir um apresentante (fiador).
A conta para receber as transferências pode ser do tipo conta poupança que é até mais fácil de abrir. Nas grandes capitais você pode abrir conta bancária sem a agência bancária. Procure nos classificados dos jornais, por anúncios do tipo *'limpo seu nome no SPC e Serasa, abro conta com cheque especial'*. Como sugestão final, experimente botar um anúncio no jornal oferecendo-se para comprar contas bancárias zeradas.

4. Estudar o funcionamento do sistema Internet Bank
O processo mais comum que os bancos utilizam é:

PÁGINA INCIAL + PÁGINA DE SENHA + PÁGINA DE EXTRATO

Vamos falsificar a PÁGINA INICIAL + PÁGINA DE SENHA e o que seria a exibição da PÁGINA DE EXTRATO, será um redirecionado para a PÁGINA DE SENHA (verdadeira). Desta forma o usuário vai pensar que digitou a senha errada e na segunda tentativa vai conseguir acessar sua conta normalmente.

A PÁGINA DE SENHA possui um formulário que envia os dados digitados para o hacker. O tecladinho virtual? Ele também será clonado e pode ser feito em java, flash ou javascript. O cadeadinho? Basta hospedar o site em um provedor

que ofereça o serviço SSL. Tanto o cadeadinho como o prefixo ***https://*** poderão ser usados. vai aparecer. mas quer saber de uma coisa? Você acha mesmo que as pessoas sabem o que significa o cadeadinho? Quantas vezes você já clicou em um cadeadinho para ver a procedência?

5. Fazer uma cópia do site do banco alvo para o seu HD

No CD-Rom que acompanha este livro você encontra vários programas que permitem fazer a cópia de um site para o seu HD. Pode ocorrer de as animações em flash não serem baixadas. Também incluimos um programa que salva no HD as anaimações em flash, caso as animações em flash não venham junto com as páginas do site. Estude o código de cada uma destas páginas. O ideal é que você mescle a sua peça (E-Mail e site) com links do site verdadeiro.

6. Pesquisar se existe alguma campanha em andamento

Um phishing scam não é algo que se faz de uma hora pra outra. Para que se obtenha sucesso é preciso planejamento. Você pode montar a peça e aguardar o banco começar uma campanha. Aí você lança a peça simultâneamente. Quem desconfiar e se informar com o banco, vai ser avisado de que a campanha existe.

7. Clonar o site do banco

Você já tem todas as páginas em html, imagens e animações guardados no seu HD. Abra cada página no Dreamweaver e arrume todos os links, inclusive o carregamento das imagens, para apontar para o site do banco verdadeiro. O úncio link que deve ser apontado para o site falso é o que abre a página de senha.

Se você não souber HTML, Flash com Action Script, ASP, Java e JavaScript, vai encontrar dificuldade para recriar o site do banco, principalmente o teclaidnho virutal. A forma mais prática para criar um tecladinho virtual é montar um mapa de imagens em cima da figura do teclado e usar a opção *onClick* do javascript para preencher os campos da caixa de texto. Ou então separar cada tecla em 

forma de imagem isolada em vez de usar mapa de imagem. Também temos a opção de criar o tecladinho no Flash ou em Java. Procure no CD-Rom o código de um tecladinho pronto pra uso.

8. Hospedar o site clonado

A primeira opção de hospedagem é o servidor gratuito. Não use nada no Brasil. A polícia precisa ter o maior número de obstáculos possível para chegar até você. Um site hospedado em ilhas ou na Àsia já começa por impor a barreira do idio-

ma. Os policiais daqui vão ter que contar com a cooperação do pessoal de lá. E vão ter que se comunicar pelo menos em inglês. Para encontrar servidores gratuitos é só usar o Google. Experimente as opções de busca só pela extensão, como por exemplo: **.jp** (japão).

O servidor pago tem a vantagem de poder exibir o cadeadinho. Este cadeadinho é um certificado de segurança. Você também pode obter um cadeadinho criando um certificado de segurança no site *www.thawte.com*. Eles te dão um prazo de vinte e um dias gratuito. Você pode se cadastrar com um nome parecido com o do banco ou até o nome banco, caso o cadastro não dê erro.

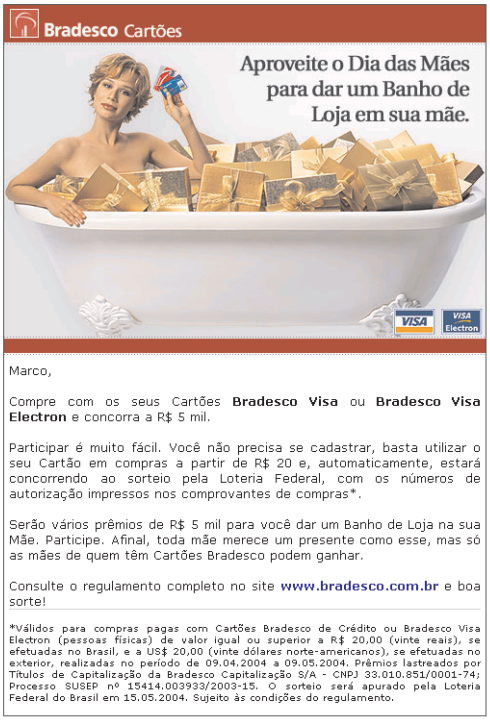
O fato do provedor ser pago não implica em pagamento ao provedor. Você pode invadir a conta de um usuário e hospedar o site clonado no meio das páginas dele. Você pode invadir um provedor do interior e hospedar tudo lá, sem que eles saibam. O problema é que pelo tráfego gerado, o site será descoberto muito rápido e retirado do ar. Ou usar provedores que oferecem um mês de hospedagem gratuita, como o Neosite (*www.neosite.com.br*). Experimente usar dois ou três apontadores: um site aponta para outro, que aponta para outro, que aponta para outro.

9. Criar a peça da campanha

A peça da campanha é o E-Mail com a isca para visitar o site clonado. Por força da minha profissão, eu coleciono peças de phishing scam. Alguns alunos gentilmente me enviam outras. Algumas peças são idênticas as da campanha oficial. Outras são tão absurdamente cheias de erro que é impossível achar que alguém vai cair no golpe.

Se você é ruim em redação publicitária, o melhor é copiar na integra uma campanha existente, passada ou futura. Aquela do bonequinho do Bradesco por exemplo, é uma campanha que dá resultado.

Algumas peças, no lugar de levar para o site clonado, instalam trojans para permitir o acesso ao computador remotamente ou para capturar todas as digitações feitas dai em diante.



10. Obter a lista de E-Mails

. . . . . .

Quanto mais gente receber o E-Mail com a peça do scam, maiores são as chances de nos depararmos com correntistas do banco e, principalmente, correntistas que de *alvo* passem a *vítima*.
A lista de E-mails pode ser obtida de diversas formas, sendo a mais comum a lista comprada de sites especializados neste tipo de produto. Quem mora em São Paulo poderá comprar CDs com mihões de E-Mails nas imediações da Rua Santa Efigência (tradiconal mercado de equipamento de informática). Mas não é dificill encontrar a oferta destes CDs nos jornais das capitais ou mesmo procurando na Internet. Outra forma de obter E-Mails é usando programas do tipo spiders (incluidos no CD) para capturar E-Mails de determinado provedor.

12. Obter a lista de contas bancárias para dissimulação
O maior problema de quem comete este tipo de golpe é responder a pergunta, _*"Para onde levar o dinheiro?"* Sim, por que o dinheiro vai ser transferido eletrônicamente e terá como ser rastreado. Agora imagine que o banco, ao rastrear a transferência, descobrir que cinquenta pessoas receberam dinheiro da conta hackeada. Qual destas é o hacker? E se estes números forem parar no IRC? E é por isso que vão parar lá. Muito mais gente vai ter acesso as contas hackeadas, isto vai dificultar muito as investigações. Repare que nas notícias de crimes de informática via Internet Bank, a polícia passa anos em busca de provas. No caso das compras com cartão de crédito, as grandes lojas de e-commerce e as operadoras de cartão de crédito, identificam o uso de vários números de cartão partindo de um único IP. É possível prender o estelionatário em flagrante.
A lista de contas para dissimulação, pode ser criada com as informações de contas que forem chegando ao seu E-Mail. Não é a melhor opção, por que a polícia vai atrás de todo mundo. O ideal é que sejam contas sem nada a ver com o golpe , como o exemplo que eu dei das contas compradas através do anúncio *'compro contas zeradas'*. Este anúncio deve ser colocado em cidade diferente da sua e semanas ou meses antes do scam ser usado. Isto vai fazer com que o laranja não ligue uma coisa a outra, pelo menos não imediatamente.

13. Montar o servidor de E-Mail
Este servidor para enviar o spam não pode ser nunca na sua casa. Grampeie a linha de um hotel, um telefone público, uma caixa de distribuição de prédio, mas nunca da sua casa. A máquina usada para enviar os E-Mails tem que ser limpa. Não pode ter nada que comprometa você. Não navegue nesta máquina, não acesse chat com esta máquina, não visite o site clonado com esta máquina. Só a utilize para enviar os E-Mails. Depois do envio suma com o HD ou use programas de apagamento definitivo, já vistos no capítulo dois.

Para enviar os E-Mails em massa você vai precisar de programas de envio de E-mail em massa com substituição do IP. Tem vários no CD-Rom que acompanha este livro. Você pode enviar os E-Mails a partir de um site, rodando um script em ASP ou PHP e lendo a partir de um banco de dados. Mas para isso vai precisar conhecer programação em ASP ou PHP e Access ou MySQL. Neste caso também vai precisar contratar os serviços de um provedor pago e verificar se não existe restrição de tempo para execução de scripts no servidor (sempre há).

14. Rodar a peça
Neste ponto começamos o envio dos E-Mails em massa. O ideal é que comecem na madrugada da sexta-feira, quando os expediente bancário e policial estão reduzidos, como também o *staff* do provedor.

14. Fazer a transferência
Assim que começar a chegar os dados das contas você deve agir rápido e fazer a transferência para as contas de dissimulaçaõ e quando chegar a 30% ou 70% de trasnferências em contas dissimuladas, transfira para a do seu laranja (pessoa inocente que cedeu a conta) ou avatar (identidade falsa).
Outras opções de lavagem de dinheiro consiste em fazer compras que sejam entregues rapidamente, como o serviço Atômico do Submarino (compras feitas até 15 horas são entregues no mesmo dia nos principais bairros de São Paulo) e de coisas que possam ser convertidas em dinheiro com facilidade. Uma quadrilha no Rio de Janeiro comprava ingressos on-line para shows e eventos e trocava por dinheiro em poucas horas.

15. Encerrar a campanha
O prazo máximo que uma peça deve circular é de 24 a 72 horas. Quando mais tempo, maior o risco de você ser rastreado. Encerrado este prazo, apague tudo. Não deixe nada, mas nada mesmo. Nem com alguém de confiança. Se não houver provas contra você, pouco poderão fazer. Existe um tipo de prisão, chamada de prisão preventiva, usada quando se quer investigar alguém e esta pessoa pode fugir ou interferir nas investigações. Se você não deixar qualquer tipo de rastro (vão revirar tudo), não haverá como mantê-lo detido por muito tempo. Principalmente se contar com um advogado. E esta é a dica final: tenha um de confiança pronto para te socorrer. É claro que são só suposições, pois você não fará mal uso destas informações.

Demos todo o passo-a-passo para um phishing scam altamente técnico. Como não havia espaço aqui no livro para detalhamento de códigos, optei por inseri-los

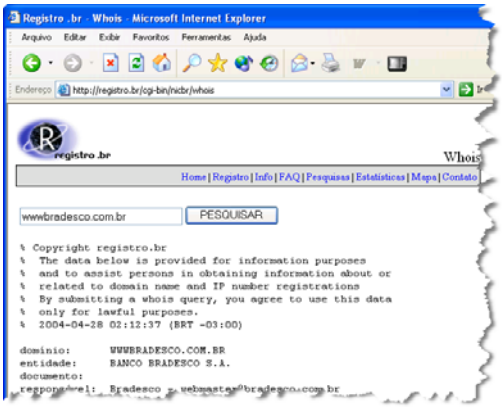
no CD-Rom que acompanha este livro. Mas também de nada adiantaria detalhar códigos para quem não conhece linguagem de programação. Este é um dos principais erros dos livros hacker que vendem por aí. Enchem o livro de códigos de programa sem saber se o leitor tem facilidade para interpretar aqueles códigos. Optei por deixar no CD-Rom os códigos citados no livro (inclusive um de tecladinho virtual em javascript).

Capturando senhas bancárias por erro de digitação

Existe uma outra maneira de capturar senhas, se proveitando dos erros de digitação. Ás vezes, durante a digitação, o usuário erra uma ou outra letra. E existem letras que são mais comuns. Então para o banco Bradesco, podemos esperar que as pessoas cometam erros do tipo:

badesco - brdesco - bradsco - bradescio - bardesco

A falta do ponto entre o *www* e o nome do domínio, como em *wwwbradesco.com.br*, também pode ser aproveitado, pois é considerado um novo domínio. Este erro é tão comum, que só no mês de maio, 1.051 pessoas digitaram errado. É claro que o banco Bradesco registrou para si esta forma de digitação errada, para que seus clientes não caiam em armadilhas. Mas ainda tem muita empresa que não se ligou neste risco.



E um monte de outros erros. Mas como saber se estes erros estão mesmo sendo cometidos, saber que outras palavras estão sendo digitadas por acidente e criar um site clonado para se aproveitar disso? É fácil. Existe um site (*www.terespondo.com.br*) onde basta você fazer um cadastro e terá acesso a uma ferramenta que informa o número de vezes que uma palavra foi digitada. Veja no exemplo abaixo que a grafia *wwwbradesco.com.br* foi digitada 1.051 vezes em um mês. Isto quer dizer que se exis-

tisse um site clonado neste endereço, teriamos recebido mil e cinquenta e um visitantes, totalmente inocentes quanto a veracidade do site. Pensando nisto, os principais bancos trataram de registrar também estas palavras, mas não são todos que fizeram isto.

Hackeando o Registro.Br (2)

Supondo que alguém vá criar um site armadilha, se aproveitando do erro na digitação do domínio, como deverá fazer? Segue o passo-a-passo:

1. Crie dois avatares, um de pessoa jurídica (com CNPJ) e um de pessoa física (com CPF)
2. Entre no site *http://Registro.Br* e faça dois cadastros. Um de RESPONSÁVEL TÉCNICO e um outro de ENTIDADE.
3. Agora cadastre os domínios com a grafia semelhante. Como o Registro.Br vai levar quase um mês para emitir a cobrança, isto quer dizer que você terá um site no ar durante um mês, sem pagar nada.
4. Agora você vai precisar informar dois números de DNS válidos para o site. Estes números de DNS são fornecidos pelo provedor de acesso. Procure por um provedor pago que dê ´'amostra grátis', como o Neosite (*www.neosite.com.br*)que oferece um mês de hospedagem inteiramente gratuita. Se preferir pagar os 30 reais anuais da Fapesp e manter o site no ar por mais tempo, consiga números de DNS, também gratuitos, no site *www.zoneedit.com*. Faça o redirecionamento para uma hospedagem gratuita.
5. Hospede o site.
6. Aguarde os visitantes, que chegarão automaticamente conforme forem digitando o nome de domínio errado.
7. A partir daqui é com você (e com a polícia).

Spoofing

Spoofing é quando você se faz passar por um computador que não é o que a pessoa realmente queria acessar. O Spoofing pode ser no DNS, no E-Mail no IP e até na URL. Este é um dos tipos de golpes que podem atingir usuários de Internet Banking. Também é chamado seqüestro ou envenenamento de DNS (DNS Hijacking, DNS Poisoning, ou ainda, DNS Spoofing). O ataque é dirigido ao servidor de nomes (DNS) do provedor de acesso ao qual o cliente está conectado. Este servidor possui a tarefa especial de transformar a requisição de um endereço compreensível para o ser humano (por exemplo, *www.bradesco.com.br*) em um endereço numérico (IP) que possa ser interpretado pelas máquinas que compõem uma rede. Já vimos isto no capítulo um deste livro.

Se o software instalado no servidor DNS para fazer esta transformação estiver com brechas de segurança, ele pode ser remotamente instruído por um hacker para desviar uma solicitação legítima de página para um endereço IP forjado. Num caso assim, se o cliente digitasse em seu navegador o endereço *www.bradesco.com.br*, por exemplo, em vez de ser levado para o site do banco, poderia ser direcionado a uma página clonada. Este tipo de golpe foi largamente utilizado contra instituições bancárias nacionais pela quadrilha de Guilherme Amorim Alves, primeira pessoa condenada no Brasil, no final de 2003, por crimes financeiros cometidos através da Internet.

Uma maneira mais simples de se obter este efeito (um nome na barra de endereços, outro site na janela do navegador) é criando um frame horizontal, tendo o primeiro apenas um pixel ou 1 % de largura e contendo o site verdadeiro. O segundo frame, com 99% de largura, contem o site falso.

Hackeando o Mercado Livre e Outros Leilões Virtuais

Sites de leilão tentam ser locais seguros para transações eletrônicas. O Mercado Livre é um dos maiores sites de leilão do mundo. Como política de segurança, tanto vendedor como o comprador precisam fazer um cadastro prévio, que inclui a digitação do número de CPF e de um número de telefone fixo. E para fazer com que os compradores conheçam o vendedor antes de decidir por fechar o negócio, existe um sistema de reputação, onde cada comprador ou vendedor, qualifica a parte na transação.

Tudo isto pode ser burlado da seguinte maneira:

- O nome deverá ser o que consta no CPF. O sistema faz esta checagem. A primeira opção é gerar diversos números de CPF (programa no CD) e verificar no site da Receita Federal se existe algum nome vinculado a um dos CPFs gerados. A segunda opção é até mais fácil. Usar o Google para buscar nomes com CPFs, comuns em páginas com resultado de concursos.
- Burlado o CPF, vamos burlar o telefone fixo. Em várias cidades do Brasil existe um serviço gratuito chamado de caixa postal de voz. Consiste em um número de telefone fixo com uma secretária eletrônica personalizável. É só informar este número, que é fixo, e quando o Mercado Livre ligar para conferir, vai ouvir sua voz dizendo: "No momento eu não estou em casa. Após o sinal deixe o seu recado e um número de contato.". No Rio de Janeiro a empresa que presta este serviço gratuitamente é a Televox.
- Para burlar o sistema de qualificação, encontre um produto barato, de menos de um real e que possa ser enviado por E-Mail (Ex.: *GRÁTIS: 100 links hacker comentados*). Em pouco tempo você estará bem qualificado e aí é só ofertar o produto que não vai ser entregue e receber o dinheiro na conta bancária. Mas não faça isto.

Capítulo 9:

Phreaker

Capítulo 9:

Phreaker

Objetivos Deste Capítulo:
Após concluir a leitura deste capítulo você deverá ser capaz de entender que o hacking de telefonia é um dos mais exigentes no que se refere a conhecimento técnico. Que o hacking começou com a telefonia, passou para os computadores, e está voltando para a telefonia. Que mexer com o sistema de telecomunicações poderá lhe trazer problemas graves, por se tratar de assunto de segurança nacional. Que para usufruir do que há de melhor em phreaking você vai precisar de dinheiro. Mas para você não ficar com água na boca, vamos ensinar como desbloquear telefones celulares.

Phreaking

O Phreaking ou hacker do sistema telefônico, é o mais exigente da categoria. Não é a tôa que os phreakers são raros entre os hackers. Talvez só comparados aos criadores de vírus. As necessidades incluem, além de tudo o que já vimos para a formação do hacker, profundos conhecimentos do funcionamento do sistema telefônico, seus softwares e hardwares. É preciso conhecimentos de eletrônica analógica e digital, telecomunicações, microprocessadores, PIC, SMD, tecnologia dos *smart cards*, linguagem de programação C e assembler. São temas pesados, que não são aprendidos de um dia para o outro e nem todas as pessoas se interessam por estes assuntos ou consegue assimilá-los. Sem estes conhecimentos, o máximo que você vai poder fazer é alterar algumas das características do seu telefone celular ou, se tiver coragem, grampear uma linha de telefone fixo. Para todo o resto você vai precisar de dinheiro e conhecimento, muito dos dois. Para começar, vamos dividir o sistema de telefonia em quatro: fixa, celular, móvel e voz sobre IP. Só vamos falar dos dois primeiros: a telefonia fixa e a telefonia celular. A telefonia móvel (Wireless) não está presente na maioria das cidades brasileiras e a voz sobre IP ainda está na fase embrionária.

Telefonia Fixa

O sistema de telefonia fixa é um dos mais antigos sistemas de rede do mundo e que provavelmente você tem em casa. Seu funcionamento depende de uma central telefônica. Imagine esta central como uma caixa de sapatos e todos os fios de telefone entram lá dentro. Quando você faz uma ligação, um anão dentro da caixa de sapatos pega o seu par de fios e liga no par de fios do telefone com o qual você deseja falar. Existem outras caixas, cada caixa suportando de 10 mil a 100 mil pares de fios. Quando o telefone que você quer chamar está ligado em uma caixa diferente da sua, o anão faz a ligação entre uma caixa e a outra, um pouco mais distante. Existem caixas maiores só para interligar as caixas menores. Existem caixas só para interligar caixas entre as cidades, estados e países. Neste caminho entre o seu telefone e o telefone de destino, o sinal pode passar por cabo metálico, fibra ótica, ondas de rádio, cabos submarinos e até satélites. Depende da distância e do percurso.

O anão não existe e o nome da caixa é Central Telefônica. No lugar do anão temos computadores que comandam pequenos relês eletrônicos, responsáveis por interligar um par de fios ao outro, ao outro, ao outro, até o destino final.

A parte que nos interessa é a que sai da central telefônica do bairro até a sua casa. A central não é mais um prédio centralizador, como era antigamente. Estes ainda existem. Mas as centrais modernas tem formato de um armário de metal e ficam na calçada. Geralmente são de cor cinza ou chumbo. Ali dentro está o computador que faz o papel de anão e conecta eletrônicamente o seu par de fios ao par de fios subsequente, até o destino final da ligação.

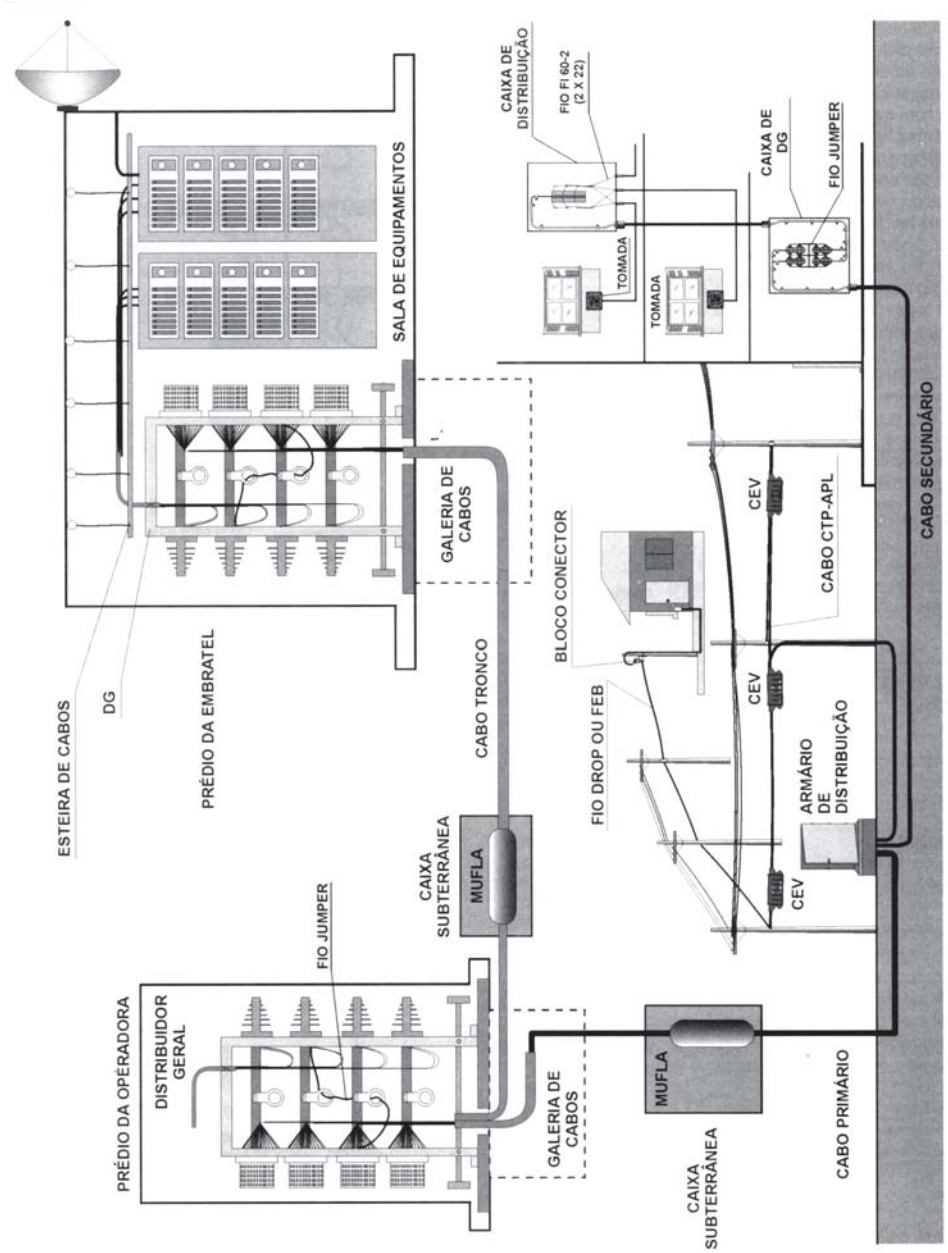
Não confundir o armário da Central Telefônica com Armário de Distribuição. A Central Telefônica pode ser em um prédio ou estar na mesma cabine que a do armário de distribuição.

Saindo da central temos os cabos com dezenas ou centenas de pares de fio colorido. É pela cor dos fios que o instalador faz a contagem dos pares. Este cabo pode seguir por baixo da terra (subterrâneo) ou por cima (aéreo). A quantidade de pares de fios e a facilidade para vir por cima ou por baixo é quem determina isto.

Este cabo vai se dividindo no caminho até chegar a sua casa. Esta divisão pode ser feita em armários de poste, subterrâneos ou em caixas de emenda ventiladas (CEV). Se você mora em prédio, haverá um armário de prédio para dividir os pares de fios entre os andares. E em cada andar haverá uma caixa para distribuir os pares de fios entre os apartamentos.

Em qualquer ponto destes: central, armário, duto subterrâneo, armário aéreo, armário de prédio, caixa de emenda ventilada (aquela caixa comprida presa diretamente no cabo telefônico), caixa de distribuição (aquela caixinha presa nos postes de rua), basta seccionar dois fios para ter acesso a linha telefônica de alguém.

Isto é proibido por Lei. Além de ser possível o uso da linha para navegar na Internet ou fazer ligações, será possível ouvir tudo o que estiverem falando (grampo).
Uma outra forma de burlar o serviço de telefonia fixa é acessando o par de fios que chega até o telefone público. A linha que chega ao telefone público é uma linha comum, programada para não gerar contas. Isto quer dizer que é uma linha onde você pode ligar para qualquer lugar do mundo sem necessitar de cartão.



Uma rede telefônica urbana típica.

Basta interceptar o par de fios que chega até o telefone público para ter acesso a uma linha direta. Conecte os fios com os de qualquer aparelho. Não é preciso dizer que se trata de furto (de serviço público) com direito a repressão policial.
Outra forma de burlar o serviço de telefonia fixa é através da programação. Consulte a operadora local e pergunte como programar o telefone para fazer o desvio das ligações para um outro número. Usando técnicas de engenharia social você liga para a casa da vítima (selecionada do catálogo telefônico) e pede para fazerr alguns restes. O falso teste consiste em orientar o usuário (se for criança ou empregado doméstico, melhor ainda) a digitar os números que correspondam a programação do aparelho para desviar todas as ligações para o seu celular por exemplo. O que você ganha com isso? É um número que pode receber ligações a cobra por exemplo.
Alguns tipos de fraude só se tornarão possíveis com o CPF e as informações do dono da linha. De posse do CPF, as demais informações podem ser catadas na Internet (sites governamentais) ou com o próprio usuário, através da engenharia social. Alguns exemplos do que é possível fazer com o CPF do usuário: alterações no cadastro junto a operadora de telefonia, solicitações de serviços, consertos e até linha adicional para outro endereço. Imagine o cenário. O hacker chega na cidade, aluga uma vaga e diz que vai precisar pedir uma linha telefônica (isto se não puxar da linha do locador) e pede uma linha em nome de terceiros. Não precisa dizer que o hacker se apresentou com um nome forjado. E se houver necessidade de se identificar para o instalador, o que dificilmente ocorrerá, basta uma identidade trabalhada no Photoshop. Estas são apenas algumas das possibilidades. Cobranças da sua conta na conta de terceiros, unificação de contas, etc...
Moradores de prédio com conhecimentos de phreaking são um perigo, pois podem acessar despreocupadamente o armário (que geralmente fica no térreo ou na garagem, local escuro e pouco frequentado). Dali poderão fazer uma ponte para a caixa de distribuição do seu andar e depois fazer a ligação para o seu apartamento.

Números de Serviço

As empresas de telefonia fixa não utilizam todos os números da central. Alguns números ficam como reserva técnica e também para uso em serviço, sem geração de conta. Só funcionários antigos e de confiança conhecem estes números. Uma invasão de um computador de uma central telefônica e alteração do cadastro da sua linha para linha sem geração de conta é um feito digno de um phreaker.

Escuta Telefônica em Linhas de Telefone Fixo

Para fazer a escuta em linhas de telefone fixo, as possibilidades são estas:
- conseguir o programa de grampo usado pela Polícia Federal. Este programa

permite a escuta telefônica a partir de qualquer computador ligado a Internet. E não se trata de um programa recente. O Kevin Mitnick foi preso, entre outras coisas, por roubar este programa. Você não percebeu a quantidade de grampos que começou a aparecer na TV de uns tempos prá cá? Repare que foi após a privatização e troca do sistema analógico pelo digital. Quando alguém tem um telefone grampeado, não é mais por um furgão preto parado em frente a casa. É de qualquer lugar, via Internet. Ou então a empresa de telefonia faz uma extenção interna, lá na central telefônica, com a sala destinada a escuta e gravação do grampo (que pode estar em qualquer lugar).

- fazer a ligação direta. Neste caso você vai ter que interceptar o par de fios em qualquer dos pontos. Existem formas de saber qual o número do telefone ligado aquele par de fios, mas o espaço neste livro é insuficiente para este nível de detalhamento.
- escuta por indução. O campo magnético em torno de um fio telefônico é suficiente para ser captado por uma bobina feita com carretel de linha e fio de cobre esmaltado. Um pequeno amplificador ou um walkman adaptado e você tem um aparelho de grampo que não precisa ser ligado diretamente ao fio. Basta estar próximo ou ter uma ponta enrolada em torno do fio telefônico.
- escuta com transmisssor. Um circuito que também usa a indução e pode ser ocultado por fita isolante, é de um pequeno transmissor na frequência de VHF/FM. Basta um walck-man com sintonizador de FM para ouvir as conversas. Este dispositivo não usa pilhas. A própria indução eletromagnética é suficiente para fazê-lo funcionar.
- escuta com gravação. Existe a venda em lojas de eletrônica e de equipamento para telemarketing, pequenos gravadores que se acoplados a linha telefônica, gravam horas de coversação em fitas k-7 miniatura, do tipo das usadas em secretária eletrônica.

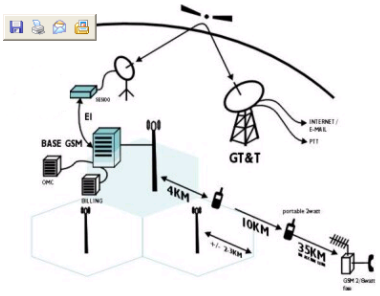
Um Caso...

Há muito tempo, trabalhei em uma empresa em que o chefe não era nada confiável. Você entrava para um periodo de experiência sem carteira assinada, enviado de uma falsa coperativa (que era mantida por ele), sem direito trabalhista algum. Depois de três a seis meses eles alegavam contenção de despesas e te mandavam embora sem direito a nada (por que você era da cooperativa, e não funcionário). Logo depois contratavam outro infeliz e assim se passavam os anos. Quando soube destes boatos tratei logo de me proteger. E a melhor proteção é a informação. Como era chamado para resolver pepinos na rede da empresa (minha função não era esta, mas pra tudo eu era chamado), aproveitei para instalar um microfone de eletreto tirado de um telefone quebrado, na ponta do cabo de rede que

ficava na sala do chefe. A outra ponta ficou ligada na entrada se áudio da minha placa de som. A rede local não usa todos os pares do fio para comunicação entre PC x HUB. Era divertido ouvir o pilantra em ameaçando as funcionárias caso não fossem pra cama com ele. Também era hilário ele cantado as estagiárias, sendo cobrado por estar devendo a banco e outras coisas do tipo. Até que chegou uma semana que o serviço não era passado pra mim. Fiquei de antena ligada e já me preparando para partir a qualquer momento. Um belo dia ele chegou todo sorridente no setor, cumprimentando todo mundo. Ele sempre cumprimentava, mas não com o sorriso amarelo daquele dia. Fiquei atento e assim que ele chamou o encarregado do departamento pessoal na sala dele, botei o fone de ouvido na cabeça e fiquei a espreita. Não deu outra: _*"Sr. Oliveira. Prepare a rescisão do Thompson e dos dois estagiários."* _*"Eles não estrão trabalhando direito? Nunca ouvi ninguém reclamar!?"* - _*"Eles ão boa gente. Mas muito espertos. Vá que resolvam correr atrás dos seus direitos trabalhistas e vão me complicar."* Passei o dia catando minhas coisas e me despedindo do pessoal. A tarde, assim que ele saiu (sem falar com ninguém), veio o Sr. Oliveira trazer a 'novidade'. Eu já estava pronto para ir embora. Só perguntei _*"Onde é que eu assino?"*.

Sistema de Telefonia Celular

O sistema de telefonia celular funciona da mesma forma. Só que no lugar dos fios, temos as ondas de rádiofrequência, que entram e saem do aparelho celular. Telefones celulares são aparelhos de rádio capazes de enviar e receber sinais. Da mesma forma que no sistema com fio, existem centrais que se comunicam, tanto com outras centrais sem fio como com as centrais com fio.



Disposição em forma de células das centrais telefônicas para rede celular
(ERB - ESTAÇÃO RÁDIOBASE)

Para que o sinal chegue a todos os lugares previstos pela empresa de telefonia, são necessárias várias centrais (chamadas de estação rádio base). Estas centrais fecham uma malha de sinal, como se fosse as células formando a pele e cobrindo o corpo. Daí o nome telefonia celular, sendo as células, as centrais sem fio (estações rádio base) que formam a área de cobertura (como as células do corpo lado a lado).

GSM

Os telefones celulares atuais estão migrando para uma tecnologia chamada GSM (*Global System Mobile*). Esta tecnlogia permite a counicação entre aparelhos com mais segurança além de disponibilizar outros recursos como navegação na Internet e download de programas que podem ser baixados para o aparelho.

Os aparelhos celulares atuais são computadores com conexão celular. Ou seja, tudo o que um computador pode fazer, um celular GSM também pode (desde que o modelo possua o software e o hardware adequado).
Para fazer a escuta de telefones celulares você vai precisar de um scanner. Um scanner de frequência é vendido em Miami ou no Paraguai por cerca de 10 mil dólares. Este aparelho já foi mostrado no Fantástico e grandes empresários e políticos costumam usar os serviços de 'detetives particulares' e possivelmente policiais corruptos também, para rastrear a conversa de seus desafetos e concorrentes.
Na Internet prolifera manuais de boxes, receitas de água sanitária no cartão telefônico e papel aluminio colocando a bateria do celular em curto. Nada disso funciona. Nem o diodo que tantos benefícios me trouxe na época do quartel é útil hoje em dia. Brincar com phreaking atualmente é coisa de gente grande.
Os telefones GSM possuem um chip. Este chip é um CARTÃO DE MEMÓRIA MICROPROCESSADO, ou seja, ele armazena informações sobre você, sua agenda, seu aparelho e sua relação com a empresa de telefonia. No 2000, quando estes telefones ainda não estavam a venda, eu disse nas páginas do livro *Proteção e Segurança na Internet* que os telefones GSM poderiam ser burlados com a troca do chip. Não deu outra, atualmente é possível adquirir o chip por 25 reais e ativar qualquer aparelho, mesmo os roubados. Também é possível desbloquear o aparelho e usá-lo com o cartão de qualquer operadora. O desbloqueio funciona até para aqueles aparelhos desligados por falta de cartão ou pagamento de conta.
E aquela história do hacker pegar o aparelho, digitar alguns códigos e o aparelho falar de graça pra qualquer lugar do mundo? Para programar um aparelho telefônico celular você precisa conhecer os códigos e a linguagem de programação aceita por estes aparelhos. Muita coisa pode ser feita por quem tem o conhecimento de como se programa um aparelho celular. Mas tornar um telefone *free* para o resto da vida é exagero.
E dá pra clonar um celular só digitando códigos de programação? Sim. É possível habilitar um celular em uma linha existente, só usando códigos de programação. Mas quando a central receber os sinais de dois aparelhos com o mesmo número e ao mesmo tempo, vai bloquear os dois e aguardar um dos dois reclamar. eu aposto no dono. O que tem sido feito nestes casos é a troca do número do assinante e o bloqueio do número antigo. Um transtorno.
O momento ideal para a clonagem é quando o aparelho é ligado. Nesta fase, por um breve momento, o aparelho estará operando no modo analógico e estará vulnerável. Como é proibido o uso de aparelhos celulares em aeronaves, várias pessoas estarão ligando seus aparelhos ao chegarem ao aeroporto. Desta forma, aumentam as chances de conseguir um sinal vulnerável para ser clonado.
O assunto é extenso e exige conhecimentos profundos sobre o funcionamento, con-

figuração e programação do sistema celular GSM. Um livro só sobre este assunto não daria conta da tarefa. No módulo cinco do Curso de Hacker nos aprofundamos um pouco mais no tema e estamos traduzindo e adaptando um material recém chegado da Itália, com informações phreaking acerca da tecnologia GSM e *smart cards*. Os smart cards ainda não são tão populares no Brasil quanto o são na Europa. As ligações via telefone público são feitas com smart cards. E é possível recarregá-lo. Mas vocês não imaginam o trabalho que dá.

É mais fácil lidar com um celular do que com o computador. Um aparelho celular tem preço subsidiado, mais pessoas tem e terão celulares. A tendência é o computador, como o conhecemos, perder cada vez mais espaço. Aparelhos celulares já estão sendo usados para baixar programas e jogos da Internet. Conhecimentos de linguagem C, assembler e Java são úteis aos que desejarem criar vírus e trojans para telefones celulares. Uma das possibilidades é fazer com que todos os telefones infectados liguem para um determinado número. Já aconteceu na Ásia, onde os telefones ligaram sem a interferência dos donos para a delegacia local. Um vírus deste tipo, programado para uma final do Big Brother Brasil, é algo realmente espetacular.

Clonagem de Telefones Celulares

A primeira forma usada para clonar os celulares é habilitar uma linha já existente em outro aparelho. Por algum tempo as duas linhas vão funcionar, até que os próprios computadores da central identificarão a anomalia e bloquearão as duas linhas. Alguém vai reclamar e eu continuo apostando no verdadeiro dono.

Uma outra maneira de clonar a linha de um celular é através de leitores de memória. Estes aparelhos fazem a laitura da memória interna, única por aparelho, e as transfere para a memória interna de outro aparelho, criando dois celulares realmente idênticos (e não dois aparelhos diferentes com a mesma linha).

Como podem perceber, alguns tipos de clonagem só funciona por algum tempo. É uma operação de pouco risco. Sigilo por parte das empresas de telefonia, pouca experiência da polícia (e falta de recursos) para fazer triangularização e identificar o phreaker. Vendedores ambulentes nas grandes capitais e anúncios de jornal oferecem aparelhos celulares das mais diversas procedências, por menos de 60 reais. Se a questão é ter um telefone sem registro, dá menos trabalho comprar um destes. Sabemos que alguns destes aparelhos foram roubados, mas há também aquelas pessoas que querem trocar seus dinossauros por modelitos mais novos e afrescalhados. Nem se dão conta de que o cadastro do aparelho continuará em nome do antigo dono. Com o baixo preço do aparelho novo e o preço irrisório de um aparelho usado, a clonagem de celular tende a desaparecer. A moda agora é desbloqueio e escuta.

Desbloqueio

Algumas coisas interessantes que podem ser feitas com celulares GSM é a personalização e o desbloqueio. Com a chegada das várias operadoras, passamos a encontrar o mesmo fabricante do aparelho oferecendo o mesmo modelo em operadoras diferentes. Encontramos também modelos exclusivos da operadora. Para evitar que um aparelho seja habilitado em operadora diferente, todos saem de fábrica com um código de proteção que não permite o funcionamento em operadora diferente para a qual foi programado. O motivo é simples. Os aparelhos são baratos por que as empresas de telefonia bancam parte do custo do aparelho. Elas esperam lucrar com as contas (por isso os aparelhos de conta são mais baratos) e com a venda dos créditos (por isso o prazo de validade da recarga caiu dos seis meses que era no início, para apenas um mês atualmente).

Se a operadora A banca um parelho que vai ser usado na operadora B, ela estará perdendo dinheiro, pois a compra de créditos será revertida para a operadora B. Pior ainda, as duas correm o risco de ficar sem receber pelo uso do serviço.

Para fazer o desbloqueio do aparelho celular e também para ter acesso a outras funções avançadas, será preciso algum tipo de comunicação com o celular. As possibilidades desta comunicação incluem:

- cabo de dados: um cabo feito sob medida, que conecta o celular ao computador pela porta serial (do mouse), paralela (da impressora) ou USB.

- IrDA: a comunicação também pode ser feita por infravermelho. Celulares com sensor infravermelho podem inclusive ser usados como controle remoto substituto e comandar outros aparelhos eletrônicos. Imagine você no consultório médio trocando o canal da TV com o celular. Inclui um programa destes no CD-Rom.

- via teclado: algumas funções podem ser acessadas via teclado.

- via E-Mail (POP3): é possível enviar um E-Mail com instruções para o celular executar.

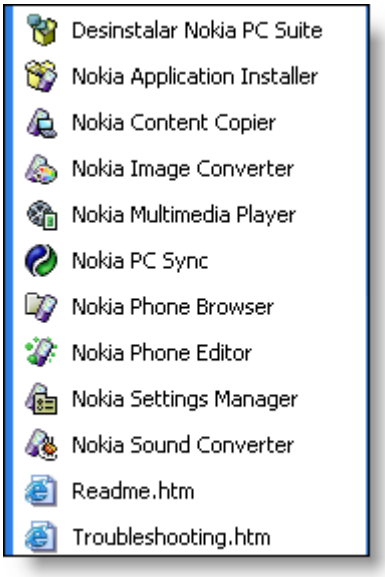
- via Wap: é possível, via Internet, fazer alterações no aparelho celular, principalmente as que tratam da personalização do aparelho.

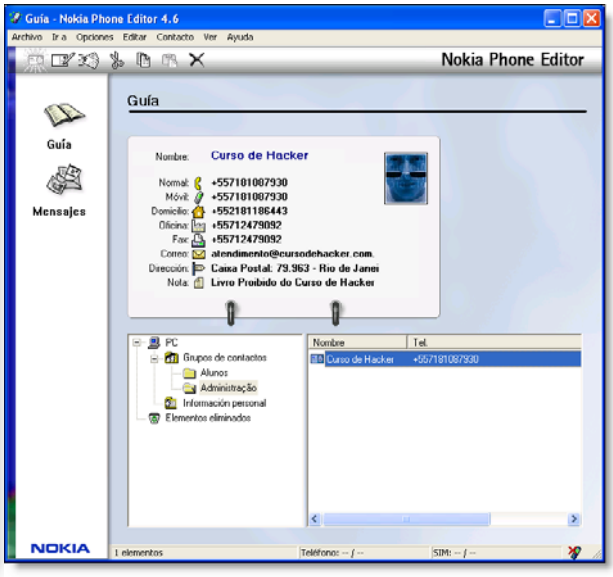
- via clip: o clip consiste em um

cabo de conexão do celular, ligado a um circuito dentro de uma caixinha. O circuito presente dentro da caixinha funciona com uma bateria 9 volts e é o responsável pelo desbloqueio. O clip não é comum no Brasil e é preciso um clip para cada modelo ou fabricante.

Cada aparelho permitirá um ou mais dos meios de acesso acima descritos. Nem todos os meios de acesso descritos acima, permitem o acesso a todos os recursos do aparelho celular. A conexão por cabo é a que oferece o maior número de recursos. Além do cabo é preciso o programa que vai permitir o acesso aos recursos do aparelho, incluindo o desbloqueio.

O cabo pode ser feito por você a partir de esquemas encontrados na Internet. Mas se você não tem habilidade mecânica, o melhor é adquirir um cabo pronto. Isto pode ser encomendado em lojas que fazem a manutenção de aparelhos celular. Por falar nisso, fazer um curso de manutenção de celulares é uma boa maneira de conhecer melhor este assunto. E quem sabe ganhar algum dinheiro prestando este serviço. No Mercado Livre prolifera a oferta de pessoas se oferecendo para desbloquear os aparelhos. Isto você também poderá fazer.





Personalizando o Telefone Celular

Sabemos que as operadoras de telefonia costumam cobram para você baixar novos toques para o celular. Após descobrir qual a melhor maneira de se comunicar com o seu aparelho, poderá baixar ou criar novos toques sem pagar a mais por isso.

O visor do aparelho também pode ser personalizado, o que inclui a troca do logo

da operadora. Programas convertem uma foto em pixels e esta foto pixelada pode ser colocada no lugar do logotipo original. Você pode personalizar tudo no seu aparelho. Só não esqueça de que aparelhos mais antigos possuem poucos recursos a serem personalizados. Cada aparelho possui uma quantidade de recursos diferentes.

Segredos dos Aparelhos Celulares

Como os aparelhos são programáveis, existem alguns códigos secretos que não fazem parte do manual. Cada aparelho possui seus códigos secretos. No link abaixo você pode procurar os códigos secretos do seu aparelho. Procure também no CD-Rom que acompanha o livro:

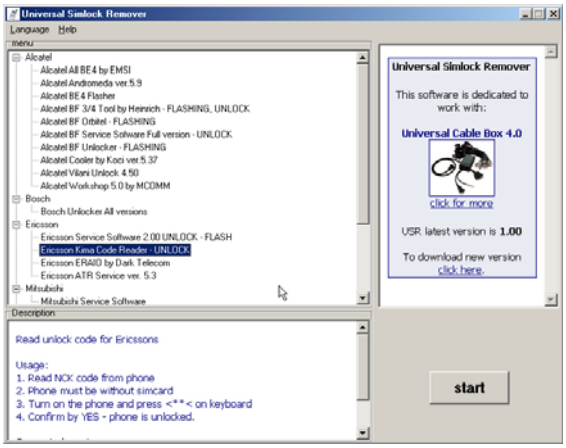
Desbloqueio de Aparelho Celular Passo-a-Passo

Dependendo da operadora e do modelo, as instruções abaixo podem ser diferentes. Nada que uma consulta ao link acima não resolva. O desbloqueio permitirá que o aparelho mudo volte a falar e use cartão de recarga de qualquer operadora. Com um pouco de sorte o seu aparelho pode ficar direto (sem a preocupação de recarregar para não perder a linha), mas apenas para receber ligações.

1. Digite o seguinte código em seu aparelho *#06#
2. O número que aparece é o número de série
3. Entre no site *www.gsmhelp.info/unlock.htm* e preencha o formulário
4. Após clicar no botão *Generate Unlock Code*, você receberá o número de desbloqueio

É simples assim. O nível de desbloqueio (celular desligado pela operadora por conta atrasada) pode necessitar de conexão via cabo.

Agora o melhor. No link abaixo cocê vai encontrar centenas de sites sobre telefonia celular e GSM. Procure informações sobre o seu aparelho como códigos secretos, manuais de serviço, programas de personalização, esquemas de cabos, código de desbloqueio e muito mais coisas que talvez você nem imaginasse existir ou poder ser feito com um simples aparelho. Não quer se arriscar com seu caríssimo *olho azul*? Compre um aparelho de segunda mão só para praticar. Vai valer a pena.



Capítulo 10:

Wi-Fi

Capítulo 10:

Wi-Fi

Objetivos Deste Capítulo:
Após concluir a leitura deste capítulo você deverá ser capaz de montar uma antena para rastrear redes sem fio. Você vai precisar de um mínimo de habilidade com trabalhos manuais. Uma rede sem fio (wireless) funciona da mesma forma que uma rede com fio. O que mostraremos neste capítulo é como ter acesso a esta rede usando um notebook, uma antena e alguns programas.

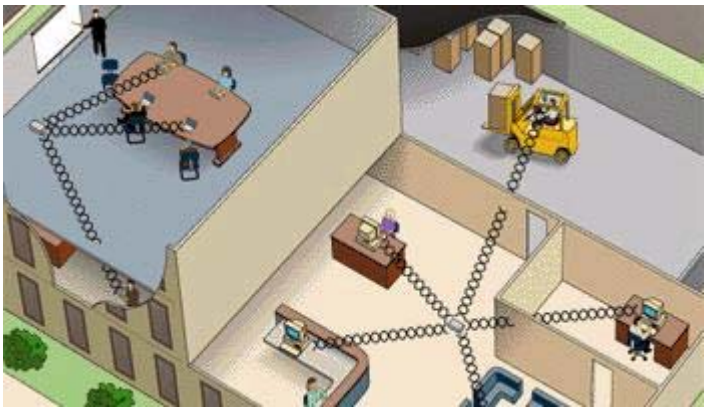
O que é Wi-Fi ?

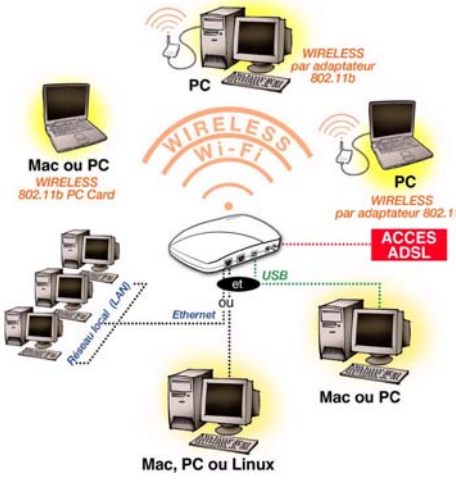
Wi-Fi é a abreviatura de '*Wireless Fidelity*' (fidelidade sem fios). Este termo é usado para se referir a um conjunto de normas criados pelo IEEE (Instituto de Engenharia Elétrica e Eletrônica) para a comunicação sem fio. O padrão mais conhecido e utilizado no mundo é o 802.11b. Este padrão utiliza a banda de 2,4 Ghz (mesma frequência usada por um microondas e telefones sem fio) e pode transferir dados a uma velocidade de 11 megabits por segundo (mbps). Já existem padrões com parâmetros mais elevados.

A tecnologia das atuais redes wireless (wireless quer dizer sem fios) permite o acesso em banda larga (até 11Mbps) via rádio, de curto alcance. A infra-estrutura de acesso pode ser instalada em locais públicos (Hotspots), como por exemplo, Aeroportos, Hotéis, Centros de Conferências, Centros Empresariais ou Estádios de Futebol. No Rio de Janeiro o estádio Maracanã oferece acesso Wi-Fi aos jornalistas e torcedores. Basta estar na área de cobertura e ligar o dispositivo de acesso sem fio, como computadores com placa de rede Wireless, notebooks com cartão PCMCIA Wireless ou PDAs com acesso Wirelles.

É claro que o Wi-Fi no Maracanã não foi pensado para os torcedores, que dificilmente levariam para um estádio de

futebol seus notebooks ou PDAs (se é que possuem). Muito provavelmente destina-se aos jornalistas que necessitam enviar o material coletado durante o jogo o mais rápido possível para as redações. Não é de se admirar que minutos após um gol, a foto já se encontre nos sites e portais sobre futebol.





Wi-fi é isso. Uma rede sem fios onde basta estar na área de cobertura para se conectar. Wi-fi não é sinônimo de Internet sem fio. Embora atualmente seja difícil imaginar uma rede local sem Internet, é perfeitamente possível existir uma rede Wi-fi sem conexão com a Internet, da mesma forma que existem redes com fio sem conexão a Internet.

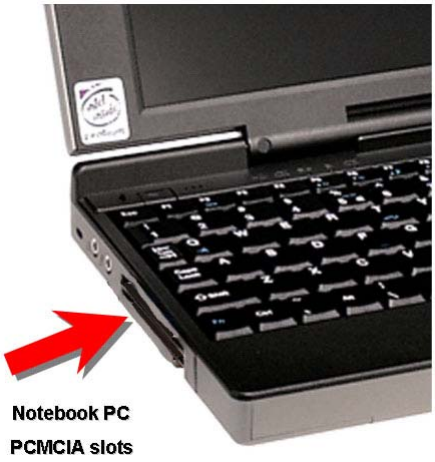
No Brasil ainda é timido o uso do Wi-fi fora das capitais e grandes centros. Mas já encontramos Hotspots (pontos de acesso) nos principais aeroportos e hotéis internacionais.

Com o tempo, empresas instalaram pontos de acesso nos bairros e ofereceram o serviço de acesso a Internet por banda larga sem fio aos moradores do local. Um dos principais motivos para o crescimento do Wi-fi é a praticidade. Enquanto que em uma rede tradicional é necessário distribuir cabos interligando todos os computadores ao concentrador, na instalação Wireless basta ligar os computadores (clientes e servidor) e eles se comunicarão entre si.

A pergunta é *_"Se uma rede Wi-fi tem acesso pelo ar, num raio de aproximadamente 100 metros em volta do HUB, o que acontece se um computador for ligado dentro da área de cobertura?"* Acontece isto que você pensou: o computador entra na rede. O sistema foi projetado para ser o mais prático possível. Qualquer dispositivo ligado dentro da área de cobertura recebe um IP do servidor e passa a fazer parte da rede. *_"E não tem nenhuma proteção?"* Existe a possibilidade de criptografar todo o tráfego, mas da mesma forma que nas redes com fio, este recurso quase não é usado. Quando a instalação é feita por uma empresa séria, todos os procedimentos de segurança são implementados, inclusive com a adoção de padrões mais seguros. Só que, por questão de custos, muitas empresas deixam esta tarefa para técnicos autonômos ou pequenas empresas com pouca infraestrutura e sem *know-how*. Montar uma rede Wi-fi é simples: compre o servidor, o hub sem fio, as placas de rede sem fio e ligue tudo. Depois de configuradas as opções de praxe em ***Ambiente de Redes***, as máquinas se comunicarão entre si como num passe de mágica.

_"E por que se fala tanto na antena de batatas?" É que o sinal da rede sem fios vai perdendo a força a medida em que se afasta do transmissor (o hub wireless). Uma lata de batatas Pringles funciona concentrando os sinais. Ao captar uma grande quantidade de sinais fracos, os torna suficientes para uma conexão. Então o que o hacker faz é criar condições para captar este sinal, mesmo que não esteja dentro da área de cobertura e sua limitação de 100 metros.

_"E não poderia usar um computador de mesa no lugar de um notebook?" Sim. É possível acessar usando qualquer dispositivo que permita este tipo de comunicação: computador de mesa (desktop), notebook, PDA e alguns dispositivos que já estão saindo de fábrica com este recurso, como telefones celulares, geladeiras, fornos de microondas, automóveis, relógios, filmadoras e máquinas fotográficas. Já deve ter dado pra você perceber que o futuro é Wi-Fi. Mas voltando ao uso do



computador de mesa, o problema é a mobilidade. Nada garante que por instalar uma placa wireless no seu micro você esteja em uma zona de cobertura wireless. Por outro lado, o uso do notebook permite que você vá em busca dessa rede. Como fariamos para carregar um computador de mesa? Onde o ligariamos? Se torna inviável, mas não impossível. Uma hipótese seria você estar (morando ou trabalhando) em um prédio comercial, onde sabidamente vários escritórios possuem redes Wi-fi. Poderá acessar a rede dos seus vizinhos.

_*"E quando esta rede estiver criptografada?"* Existem softwares que quebram a criptografia, além de 'fuçar' o tráfego da rede sem fios.

_*"Uma placa de rede wirelless é ligada a alguma antena externa?"* Não. Na parte traseira da placa de rede Wireless tem uma antena parecida com a de um rádio FM ou embutida na placa (vide foto). Antenas não necessariamente tem de ser em forma de vareta vertical, se bem que este tipo é o mais indicado para recepção multidirecional. Um phreaker pode abrir a parte da antena da placa de rede Wireless e ligá-la a uma antena externa, aumentando consideravelmente o seu alcance.

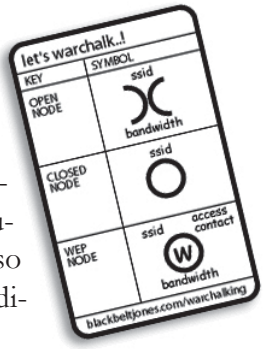
Quem não conhece as peculiaridades dos notebooks, é importante saber que este equipamento, por questões de espaço e economia, permite a inserção de cartões de expansão chamados de PCMCIA. Existem cartões com modem, com rede 10/100 e também com rede Wireless, entre outros. Um hacker que pretenda rastrear redes sem fio precisa ter, além do notebook, um cartão PCMCIA para rede wireless e uma antena, que pode ser comprada pronta ou construída por você, conforme a orientação que daremos ainda neste capítulo. Além dos programas *Net Stumbler*, *AirSnort* e *WEPCrack*, necessários para rastrear e quebrar a segurança das redes sem fio (todos incluídos no CD que acompanha este livro).

Você também vai precisar de coragem, para sair as ruas do centro de São Paulo ou do Rio de Janeiro, portando um notebook em uma das mãos e uma antena, no mínimo estranha aos passantes, na outra.

Mas não é esta a única maneira e nem a mais

indicada. O ideal é ir de carro, de olho no monitor de sinais, e quando uma rede aberta for encontrada, estacionar o carro em local reservado e onde houver o maior nível de sinal, com o menor nível de ruído (em relação ao sinal de RF).
Mesmo em aeroportos, onde se supõe haver maior segurança, é bastante arriscado transitar com um notebook. Em tempo, a rede Wi-fi em um aeroporto, é aberta a todos, bastando ter o provedor de acesso. O provedor Terra possui presença nos principais aeroportos do país. Neste caso o alvo não é a rede, que é aberta a todos, e sim quem estiver acessando do mesmo local.

Warchalking (guerra de giz) **-** O hacker marca com giz os pontos de acesso vulneráveis. Estas marcas podem ser feitas no chão ou na parede.
Wardriving - o hacker sai de carro a caça de redes abertas.



Embora dificilmente você encontre estas figuras nas esquinas do Brasil, elas foram criadas para informar a comunidade hacker passante, a existência de pontos de acesso wirelles naquele local. São marcas feitas com giz que indicam rede aberta, rede fechada ou rede criptografa.

O que é WLan?

Siginifica Wireless Lan ou rede de área local sem fio.

O que é Wep?

WEP que dizer *Wired Equivalent Privacy* ou *Privacidade Equivalente à das Redes Com Fios*. É uma característica opcional do padrão IEEE 802.11, utilizada para proporcionar segurança de dados equivalente à de uma rede com fios sem técnicas de criptografia avançada de privacidade. A WEP permite que os links de rede local sem fio sejam tão seguros quanto os links com fios. De acordo com o padrão 802.11, a criptografia de dados WEP é utilizada para impedir o acesso não autorizado e a captura do tráfego (sniffing).
As primeiras imlementações da WEP, ainda em uso, mostrou-se insuficiente para garantir a segurança de uma rede Wi-Fi. O software WepCrack é usado para quebrar com relatividade facilidade, a criprografia das redes Wi-Fi com Wep ativado. Por falar nisso, nem todos os instaladores ativam a criptografia Wep, ou por desconhecimento ou por problemas de incompatibilidae entre aplicativos.
O WEP já tem um sucessor: o WAP (*Wi-Fi Protected Access*).

O que é Bluetooth™?

Bluetooth é uma tecnologia sem fio de pequeno alcance que permite aos telefones enviarem e receberem dados de outros telefones e dispositivos próximos. Isso inclui PCs, fones de ouvido sem fio e uma grande variedade de outros acessórios.

Imagine-se sentado em um ônibus quando, de repente, aparece uma mensagem de texto no seu notebook, desafiando-o para o jogo "*Apuros de Penelope*". Você olha e sorri para o outro passageiro que está com um PDA, sem dar a mínima para o fato dele(a) ser um transexual. Basta teclar alguns botões para começar a partida. Esta viagem promete. Este é um exemplo da liberdade sem fio que a Bluetooth oferece.

Como Montar Sua Antena de 'Batatas'

A montagem de antenas de comunicação é uma arte. No Brasil nem tanto, mas nos EUA existem grupos que se reúnem periódicamente para compartilhar informações e decidir quem constrói a melhor antena artesanal. E estes amadores levam muito a sério os Encontros. A ponto de apresentar relatórios detalhados com informações sobre ganho, desempenho e influência das manchas solares nos testes paramétricos. Este hábito americano não se restringe a comparação e demonstração de antenas. Existem grupos que se dedicam a construção de foguetes, envenenamento de motores, cultivo da maior abóbora, e um sem número de outras atividades. Na área hacker temos vários eventos, sendo o mais famoso a DEFCON (*www.defcon.org*) que, inclusive, queremos reproduzir no Brasil.

Voltando ao assunto 'antena de batatas', quero dizer duas coisas: a antena usando tubo de batatas Pringles não é o único formato de antena existente para exploração de redes Wi-fi e o tubo de batatas Pringles (*www.pringles.com.br*) não é o único tubo possível de ser utilizado na construção deste modelo de antena.

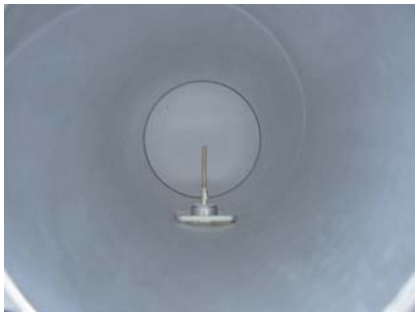
Curiosidade: a batata Pringles não é exatamente 'batata'. É feita a base de soja e batata transgênica. Você nunca estranhou o fato de todas as fatias serem idênticas?

Lista de Material para uma Antena de Cinco Elementos

- 5 arruelas de aproximadamente 1" cada
- 2 porcas auto travantes ou normais
- 1 vareta rosqueada de 1/8" (parece um parafuso sem cabeça, só o corpo rosqueado)
- 1 tubo de aluminio (pode ser elemento de antena de TV quebrado)
- 1 disco plastico (pode ser de tampa de Nescau, da Pringles ou outra qualquer)
- 1 tubo de Pringles (também servirá algumas embalagens de bebida)
- 1 pedaço com 5cm de fio de cobre (fio rígido usado em instalação elétrica)
- 1 conector tipo N fêmea (prefira o de sobrepor, mas também serviá o de rosquear)
- cola de silicone (aquela que parece uma prótese peniana e é usada usada em pistola de cola quente)

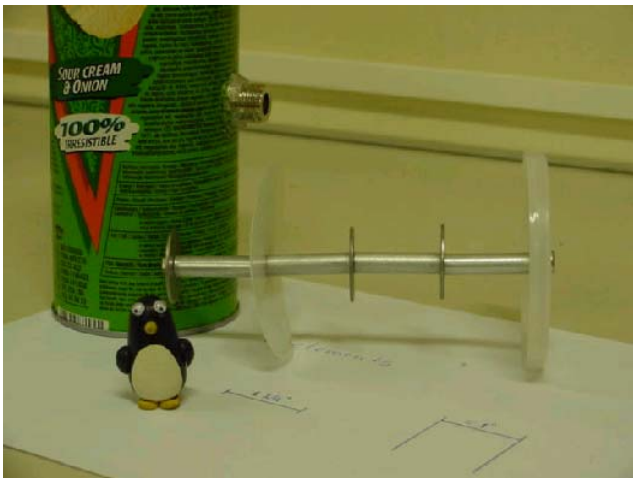
Onde comprar?
Todo material acima pode ser encontrado em lojas especializadas em parafusos, casas de material de construção, lojas de eletrônica, ferro-velho e até no lixo.

Como fazer?
1. Solde o pedaço de fio de cobre no conector N.
2. Prenda o conector N no tubo de Pringles. Use a cola de silicone. pela foto dá pra ter uma idéia da posição e localização correta.



Nota: para ligar o PDA ou Notebook a antena você vai precisar de um cabo de conexão. Sugiro que você consulte alguma loja especializada em manutenção de notebooks para que eles te orientem quanto o tipo de cabo e cartão PCMCIA apropriado para o seu notebook.

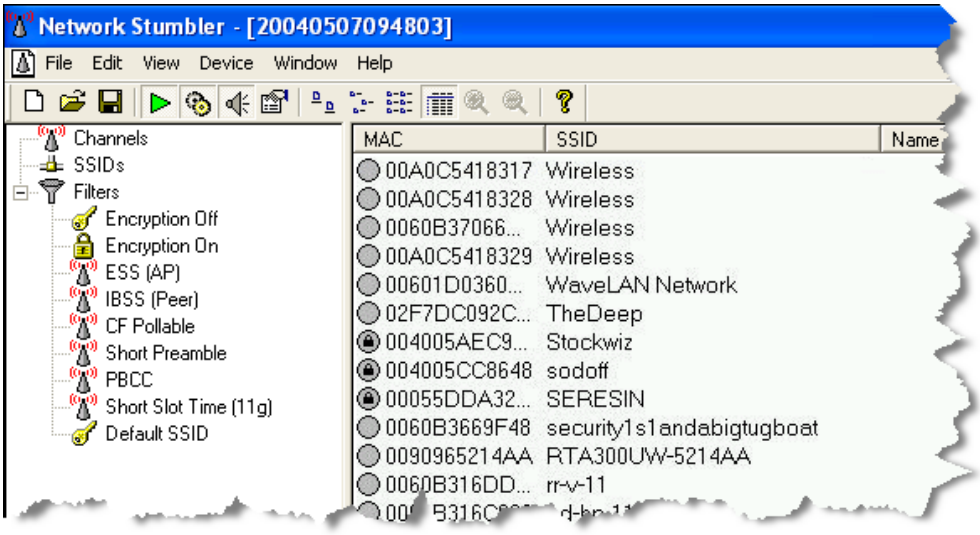
2. A segunda parte é uma antena de cinco elementos, feita com um sanduíche de tubinhos e tampas plásticas. Veja a foto que é autoexplicativa:



Como sair a caça das redes wireless?

Agora é só ir a pé (louco) ou de carro de olho na tela do notebook. Existem vários programas para rastrear e quebrar a criptografia WEP das redes Wireless. Incluimos alguns no CD que acompanha este livro. A placa de rede Wireless também vem com alguns programas, sendo que um deles se destina a verificar a intensidade e qualidade do sinal captado (relação sinal x ruído).

Na figura abaixo vemos a tela do programa após detectar a presença de várias redes wireless. repare que a maioria está sem a criptografia ativada. E mesmo as que estão podem ser quebradas.



Conclusão

Chegamos ao fim do Curso de Hacker em versão livro. Procurei reunir nesta obra, todos os assuntos que um hacker precisa desenvolver. São muitas áreas de ação e pode ser difícil o domínio de todas elas, até devido a inovação constante no setor. Mas você pode selecionar os temas que mais se identificou e se aprofundar neles. Em 300 páginas esta tarefa tornou-se um grande desafio, mas acho que conseguimos. Alguns assuntos poderiam ter sido mais aprofundados, porém deixariamos outros, igualmente importantes, de fora. Também devemos levar em conta que nosso público alvo é o usuário com pouca experiência em informática e nenhuma em atividades hacker.

Este livro/curso segue o mesmo programa do **Novo Curso de Hacker** a distância, agora em dez módulos. São vídeoaulas para assistir em qualquer computador PC. Todos os programas citados foram incluidos nos CDs que acompanha cada módulo do curso.

Eu fico por aqui. Obrigado por você ter vindo. Até a próxima!

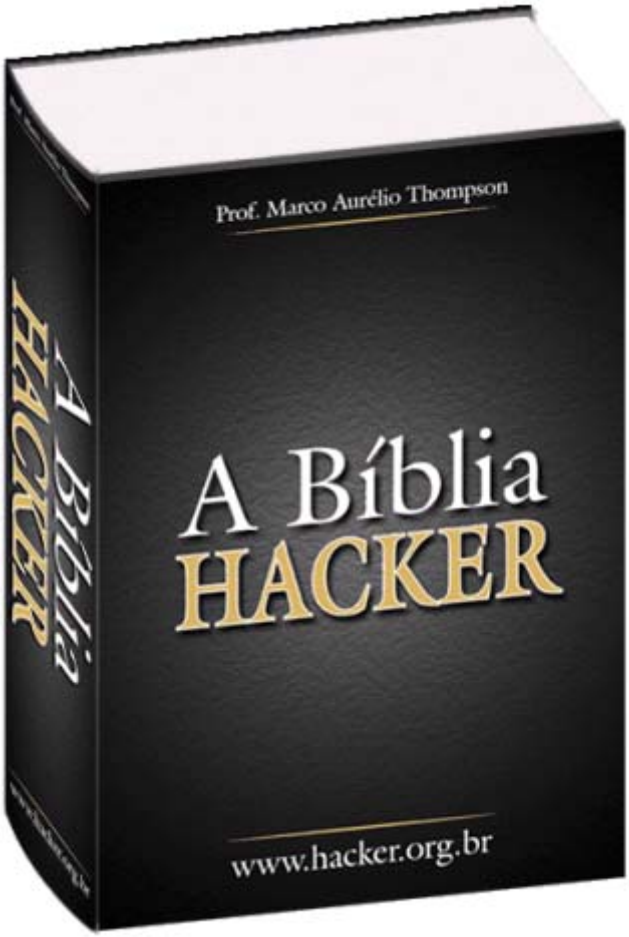
Prof. Marco Aurélio Thompson
atendimento@cursodehacker.com.br
Tel: +55 71 8108-7930

Conheça também o Novo Curso de Hacker em vídeoaulas para PC

http://www.cursodehacker.com.br

Quer Mais? Então toma:

A Bíblia Hacker

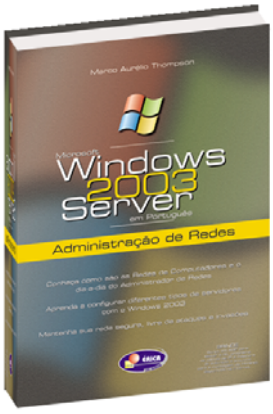


. 1200 páginas
. Capa dura
. Encadernação de Luxo
. Formato grande
. Lançamento: nov/2004

Obs.: Este livro não estará a venda em livrarias. Ele é parte integrante do Novo Curso de Hacker e será entregue gratuitamente, como presente de formatura, aos alunos que concluirem o Curso de Hacker - Edição De Luxe.

Título: Proteção e Segurança na Internet
Autor: Marco Aurélio Thompson
Editora: Érica, SP, 2002 **ISBN:** 9131
Páginas: 248 **Formato:** 17 x 24 cm
Categoria: Internet
Sinopse: Este livro é destinado a todos aqueles que queiram aumentar o nível de segurança de seus computadores pessoais. Quem não se proteger corre sério risco de perder arquivos, encontrar seus dados pessoais ou de seus clientes espalhados pela Internet, ter o saldo de sua conta bancária zerado ou o limite do cartão de crédito estourado em poucas horas.
O autor, Consultor de Informática e atual presidente da ABSI - Associação Brasileira de Segurança na Internet, ensina de forma prática e didática como fazer para configurar uma máquina segura à prova de ataques e invasões. Também explica como agir caso seu micro já tenha sido invadido.
Conheça casos reais de falhas de proteção. Entenda por que não há segurança real no mundo virtual. Domine todas as técnicas de segurança necessárias a uma navegação segura. Ou seja você a próxima vítima...

Título: Java 2 & Banco de Dados
Autor: Marco Aurélio Thompson
Editora: Érica, SP, 2002 **ISBN:** 847x
Páginas: 200 **Formato:** 17 x 24 cm
Categoria: Linguagem de Programação
Sinopse: Este livro tem como objetivo mostrar os conceitos necessários ao aprendizado e uso do Java como linguagem de programação para acesso a banco de dados relacional.
Com capítulos fáceis de ser assimilados, repletos de exemplos e exercícios, explica como preparar seu PC para programar em Java 2, como criar Bancos de Dados Relacionais com facilidade por meio das instruções passo a passo, como criar rapidamente conexões ODBC/JDBC, como usar uma IDE gratuita para a prática das instruções SQL e como melhorar a aparência das suas classes criando Interfaces Gráficas com o Usuário (GUI).



Título: Windows 2003 Server - Administração de Redes
Autor: Marco Aurélio Thompson
Editora: Érica, SP, 2003 **ISBN:** 9808
Páginas: 376 **Formato:** 17 x 24 cm
Categoria: Sistema Operacional
Sinopse: Este livro tem o objetivo de ensinar a gerenciar o Windows 2003 Server em rede e mostrar como realmente é o dia-a-dia do administrador. Está organizado de forma didática, abordando conceitos básicos sobre redes, arquiteturas, protocolos e instalação da versão Server, os tipos de servidor em que o Windows 2003 pode se transformar (Controlador de Domínio, Servidor de Arquivos, de Impressão, DNS, WINS, DHCP, Servidor Web (WWW e FTP), etc.), criação de uma Intranet, adotando uma política de segurança, além de dicas e macetes do Windows 2003 e orientações para certificação Microsoft. É indicado aos profissionais e alunos da área de informática que desejam ingressar no lucrativo mercado de administração de redes.

Fale Conosco

O Prof. Marco Aurélio Thompson se coloca a disposição de seus alunos, leitores, imprensa e autoridades competentes, para quaisquer esclarecimentos que se façam necessários, sobre esta obra e os assuntos relacionados:

ABSI - Associação Brasileira de Segurança na Internet
http://www.absi.org.br
atendimento@absi.org.br

Curso de Hacker do Prof. Marco Aurélio Thompson
http://www.cursodehacker.com.br
atendimento@cursodehacker.com.br

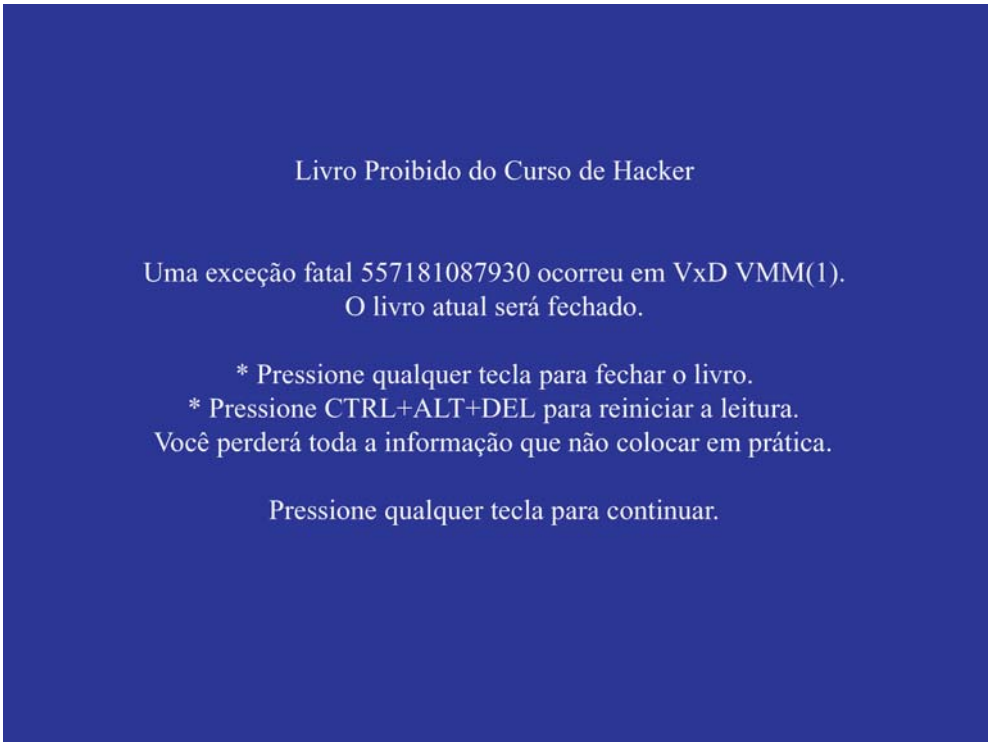
Prof. Marco Aurélio Thompson
http://MarcoAurelio.Net
atendimento@marcoaurelio.net

Tel: (71) 8108-7930

Erratas e Atualizações

Eventuais erratas e atualizações estarão disponíveis no seguinte link:

http://www.cursodehacker.com.br/Errata.htm


Livro Proibido do Curso de Hacker
Uma exceção fatal 557181087930 ocorreu em VxD VMM(1).
O livro atual será fechado.
* Pressione qualquer tecla para fechar o livro.
* Pressione CTRL+ALT+DEL para reiniciar a leitura.
Você perderá toda a informação que não colocar em prática.
Pressione qualquer tecla para continuar.

Biblioteca Digital 2006/2007

A **ABSI** disponibiliza aos seus associados uma exclusiva **Biblioteca Digital**, com títulos que complementam o **Curso de Segurança da Informação 2006/2007** (formação do Hacker Ético). São eBooks para ler na tela do computador PC. Alguns destes títulos em breve estarão disponíveis também na versão impressa, podendo ser adquiridos com desconto na **Loja da ABSI**.

A Biblioteca Digital da ABSI é GRATUITA para os alunos ativos do **Curso de Segurança da Informação 2006/2007** (formação do Hacker Ético). Enviaremos o link por e-Mail para download de um eBook por mês, a todos os compradores que quitarem a compra deste produto até dezembro de 2007. Os associados da ABSI têm acesso a este e outros eBooks na área de membros.

A idéia da Biblioteca Hacker não é nova. Já em 2004, quando o Curso de Hacker era comercializado pelo Prof. Marco Aurélio Thompson (atualmente as vendas são feitas pela ABSI), houve uma tentativa de criar uma biblioteca de apoio ao curso, que esbarrou nos problemas legais da distribuição de livros com direitos autorais. Na versão 2006 da biblioteca, nos baseamos nas dificuldades e necessidades que os alunos manifestaram no decorrer do antigo Curso de Hacker (atual Curso de Segurança da Informação). Como ocorre em qualquer programa de treinamento, além do tema da aula, surgem dúvidas que não fazem parte do programa de estudo, mas são igualmente importantes. Então o que fizemos foi criar dezenas de livros como forma de complementar o programa de estudos do Curso de Segurança da Informação 2006/2007 (formação do Hacker Ético).

Abaixo você confere a lista de títulos da Biblioteca Digital 2006/2007. Os clientes que adquirem o Curso de Segurança da Informação 2006/2007 (formação do Hacker Ético), recebem um eBook por mês, gratuitamente, enquanto permanecerem ativos.

Obs.: Os eBooks são em formato que permita assistir na tela do computador PC. A ordem de apresentação abaixo não representa a ordem de envio do link para download. Estes eBooks não são vendidos. Favor não insistir.

Capa	Título, autor e descrição:
	**A Casa do Hacker - *Prof. Marco Aurélio Thompson*** Imagine o que aconteceria se os hackers já fizessem parte do nosso cotidiano? Baseado nesta premissa, o autor nos brinda com vários *causos* bastante plausíveis.Em **Um Dia de Hacker** você fica sabendo como é o dia no escritório de um hacker profissional. Os clientes pedem cada coisa. Só lendo para saber. Em **Procurado**, ficamos sabendo das dificulades de uma delegacia de polícia para registrar uma ocorrência envolvendo hackers. **O Estagiário** fala de como uma diretora autoritária pode ser mansa como uma... Em **Um Pouco de**

Sexo, o hacker é contratado por um homem para descobrir se a mulher é fiel. Em **O Melhor Aluno**, ficamos sabendo como um estudante medíocre se tornou o melhor aluno da escola depois que leu um certo *livro proibido*. **Vidaboas** é o relato de um hacker brasileiro que mora no Caribe. Você vai descobrir o que os *black hats* fazem com o dinheiro que desviam das contas bancárias. O livro tem outras histórias, igualmente engraçadas e curiosas: **Hacker Por Acidente** e **A Senha** são outros dois *causos* que você lê neste eBook. Se você achava que os hackers ainda não estavam entre nós, vai mudar de opinião após a leitura deste eBook.

* Algumas destas histórias podem ser lidas na revista digital **Hacker.BR**.

BAIXAR

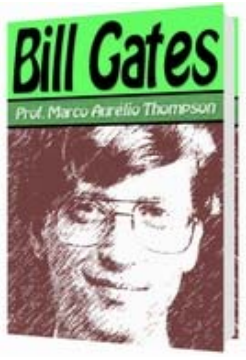
Tudo o Que Você Sempre Quis Saber Sobre Hackers e Não Tinha a Quem Perguntar - Vol. 1 - *Prof. Marco Aurélio Thompson*

Este livro surgiu a partir de uma idéia do autor e foi proposta na maior lista de discussão sobre hacking do Brasil. O autor convidou os participantes da lista a fazerem as perguntas que quisessem e se prontificou a respondê-las na forma de um eBook. Foram mais de seiscentas perguntas. Depois de removidas as repetidas, as fora do contexto e as bobagens, resultou neste primeiro volume com duzentas perguntas.

BAIXAR

Tudo o Que Você Sempre Quis Saber Sobre Hackers e Não Tinha a Quem Perguntar - Vol. 2 - *Prof. Marco Aurélio Thompson*

Este é o segundo volume e atualmente está em fase de captação das perguntas. Em breve disponibilizaremos o link para que você possa contribuir com perguntas e participar do segundo volume desta coleção.



Biografias Não Autorizadas: Bill Gates - *Prof. Marco Aurélio Thompson*

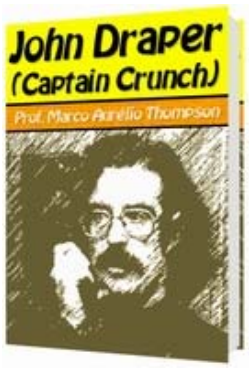
Neste eBook vamos conhecer um pouco mais sobre a vida de Sir William Henry Gates III. Mas não espere nada de comportado nesta narração. Este não é o estilo do autor. Saiba como um produto com defeito de fabricação é vendido até hoje e porque Bill Gates é atualmente o homem mais poderoso do planeta. Pesquisa, dedução, suposição, fatos, documentários. Tudo foi usado para trazer até você uma biografia diferente de tudo o que você já leu por aí.

BAIXAR

Biografias Não Autorizadas: Kevin Mitnick - *Prof. Marco Aurélio Thompson*

Neste eBook vamos conhecer um pouco mais sobre a vida de Kevin Mitnick. Mas não espere nada de comportado nesta narração. Este não é o estilo do autor. Saiba como um rapaz comum, especialista em contos do vigário, se tornou o maior hacker do mundo, graças a imprensa da época. Pesquisa, dedução, suposição, fatos, documentários. Tudo foi usado para trazer até você uma biografia diferente de tudo o que você já leu por aí.

BAIXAR



Biografias Não Autorizadas: John Draper - *Prof. Marco Aurélio Thompson*

Neste eBook vamos conhecer um pouco mais sobre a vida de John Draper, o inventor do phreaking. Mas não espere nada de comportado nesta narração. Este não é o estilo do autor. Saiba como um mero entusiasta da eletrônica interferiu no sistema da maior empresa de telefonia do mundo. Pesquisa, dedução, suposição, fatos, documentários. Tudo foi usado para trazer até você uma biografia diferente de tudo o que você já leu por aí.

BAIXAR

Afiando o Machado: Como Desenvolver a Mente Hacker - *Prof. Marco Aurélio Thompson*

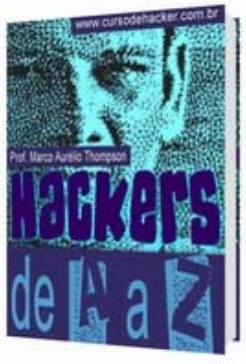
A teoria das inteligências multiplas foi desenvolvida a partir dos anos 80 por uma equipe de pesquisadores da universidade de Harvard, liderada pelo psicólogo Howard Gardner, que identificou sete tipos de inteligência. Esta teoria teve grande impacto na educação no início dos anos 90. Neste eBook o autor fornece subsídios práticos para o desenvolvimento da inteligência através da ludicidade. Estes são alguns dos temas tratados: Logic Puzzle Games, Memory Games, Role-Playing Games, Estratégia em Tempo Real, Simuladores, Block Puzzle Games, Pattern Puzzle Games (Tangram, K-Dron), Soroban, Origami, Criptograma, Desafios de Lógica, Caça-palavras, Jigsaw, Jogo da Vida, Anagrama, Kakuro/Sudoku, Notação musical, Código Morse, Astronomia, Microscopia, Tradicionais (Xadrez, Damas, Gamão), Geografia, Desconstrução de grandes estruturas, Química e Física, Quebra Cabeças Tridimensionais, Lego, Dramatização, Simulador de tráfego, Simulador de veículos, Simulador de processos, Simulador de vida, Simulador de circuitos, Color Book, Estereograma, Gerador de histórias, Yoga, Nunchaku, Malabares.

BAIXAR

Aprenda a Jogar Hacker Games - *Prof. Marco Aurélio Thompson*

O lançamento do CD-Rom com jogos hacker em versão shareware foi um sucesso. Mais de cem unidades vendidas em apenas dois meses. Infelizmente nem todos conseguiram compreender os objetivos dos jogos ou ir além das telas iniciais. Pensando nisto, o autor criou um eBook onde comenta sobre diversos jogos hacker disponíveis atualmente na Internet e ensina como jogar um deles. A partir daí você poderá explorar qualquer outro game de estratégia hacker em tempo real.

BAIXAR



Hackers de A a Z - *Prof. Marco Aurélio Thompson*

Em **Hackers de A a Z** o autor explica de forma fácil e descomplicada, o significado de termos, frases, siglas e abreviaturas encontadas na literatura técnica especializada. Se ao ler livros sobre redes de computadores e segurança da informação você tem dificuldade em entender algumas palavras e siglas, como **gateway**, **daemon**, **proxy**, **RPC**, **icmp**, **smtp** e tantas outras, vale a pena a leitura do **Hackers de A a Z**. O autor usou um método inusitado para a elaboração deste eBook. Reuniu algumas dezenas de livros de tecnologia da informação e redes no formato digital, usou um gerador de palavras e selecionou aquelas que certamente são de difícil compreensão para um leigo. Este método garante que o leitor deste eBook vai aumentar consideravelmente o seu grau de interpretação da literatura técnica de informática.

BAIXAR

A História Ilustrada do Hacking - *Prof. Marco Aurélio Thompson*

Neste eBook o autor usa a linha do tempo para descrever todos os acontecimentos relevantes da história do hacking. Vamos saber um pouco mais sobre a origem da palavra hacker e acompanhar a evolução das ações hacker, desde os tempos do MIT até as quadrilhas internacionais que agem no Século XXI. Um capítulo especial trata da história do hacking no Brasil.

BAIXAR

A História Ilustrada do Phreaking - *Prof. Marco Aurélio Thompson*

Outro eBook que também usa a linha do tempo para descrever a história do phreaking no Brasil e no mundo. Vamos descobrir que John Draper pode não ser o verdadeiro pai do phreaking como pensávamos. Também vamos saber um pouco sobre a polêmica envolvendo Alexander Graham Bell e o registro da patente do telefone. Um capítulo especial aborda a história das telecomunicações no Brasil, desde a época de D. Pedro II, passando pelos Brasilsat, até os nossos dias.

BAIXAR

Guia da Certificação de Segurança - *Prof. Marco Aurélio Thompson*

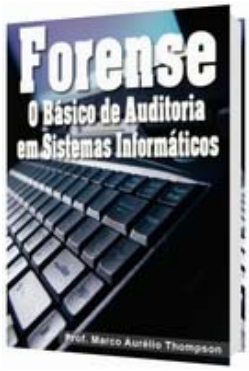
Um dos pontos polêmicos da obra do autor é a questão das certificações, especialmente as certificações de segurança. Até que ponto uma certificação faz diferença na vida profissional de quem escolhe este caminho? Fruto de uma pesquisa séria, envolvendo fabricantes, empresas de certificação, profissionais certificados e independentes, o autor procura dar uma visão geral de como é o mercado de certificações, na prática. Você vai conhecer um pouco mais sobre o que está por trás da sopa de letrinhas que povoa o mercado das certificações: CISSP, A+, SANS, CISM, Security+, MCSO, CISA, PMP, CEH, CCSA, CCSE, MCP, MCSA, MCSE, ITIL e ABSI+. Você vai descobrir SE e QUANDO vale a pena a certificação. Esperamos com isto poder ajudá-lo na decisão de se tornar ou não um profissional certificado.

BAIXAR

ABSI+ - Guia de Estudos para a Certificação de Segurança da ABSI - *Prof. Marco Aurélio Thompson*

Em fase de regulamentação, a certificação ABSI+ é a resposta da ABSI para atender o mercado das micros e pequenas empresas. O autor é consultor pelo Sebrae e não está medindo esforços para que a certificação ABSI+ esteja entre a melhor opção para o profissional que atende o pequeno e médio empresário. Todas as principais certificações de segurança atuais, tratam de uma realidade que está longe de ser o cotidiano das PMEs brasileiras. Na primeira parte deste eBook o autor esclarece a proposta da certificação ABSI+. Na segunda parte comenta o programa de estudos, como preparatório para o exame da certificação. A terceira parte encerra com um simulado para quem pretende se preparar para a certificação da ABSI.

BAIXAR

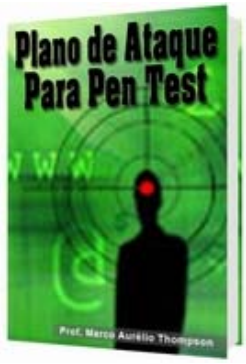


Forense - O Básico de Auditoria em Sistemas Informáticos - *Prof. Marco Aurélio Thompson*

Neste eBook você vai aprender como a Perícia Forense trabalha na obtenção de evidências nos crimes de informática. Este eBook atende a uma necessidade de complementar do Curso de Segurança da Informação 2006/2007. O autor demonstra na prática como as evidências são armazenadas no sistema, como auditá-las e como é possível aos hackers adulterá-las ou removê-las, dificultando ou impedindo a ligação do invasor com o crime. Estes são alguns capítulos deste eBook: 1) O que é Perícia Forense?; 2) Funcionamento do judiciário: Como eles prendem os hackers; 3) O sistema operacional na visão do perito; 4) Montando um Live CD com ferramentas Forense; 5) Cópia exata do sistema comprometido; 6) Recuperação de dados; 6) Recuperação de informações; 7) Perícia em máquinas de usuários: quem fez, o que, quando e como? 8)

Perícia em servidores: o que fizeram, quem, quando e como? 9) Periciando e-Mails; 10) Rastreando IPs; 11) Check-list do auditor independente; 12) Deixando o perito na mão: Como os hackers eliminam evidências.

BAIXAR



Plano de Ataque Para Pen Test - *Prof. Marco Aurélio Thompson*

Neste eBook você vai reforçar o seu conhecimento de plano de ataque (*pen test*) aprendido no Curso de Segurança da Informação 2006/2007. O autor analisa cada fase do plano de ataque, com exemplos reais em cada etapa da execução. Você vai saber também quais são as diferenças entre os *pen tests* regulamentados pelas normas ISO e o *simple pen test* proposto em nosso treinamento. Dicas de uso do MS Project e dos mapas mentais com MindManager para aumentar a eficácia do planejamento.

BÔNUS ADICIONAL: Junto com este eBook você receberá um software desenvolvido pelo autor para a geração de planos de ataque personalizados (*simple pen test*). Responda a algumas perguntas feitas pelo programa. Se não souber a resposta clique em ajuda e receba orientação adicional. Ao terminar de responder às perguntas do programa, você terá um plano de ataque personalizado e pronto para uso. Também receberá modelos de planos de ataque em .XLS, .MPP e .MMP.

BAIXAR

AVISO IMPORTANTE: A Biblioteca Digital da ABSI é formada por eBooks mensais gratuitos, exclusivo dos associados da ABSI e clientes que adquirem o Curso de Segurança da Informação 2006/2007. Os eBooks são registrados na Biblioteca Nacional e no cadastro ISBN e não damos autorização a ninguém para redistribui-los. Estes eBooks são personalizados com a identificação de cada cliente. Quem não aceitar esta personalização da versão digital não os poderá recebê-los. Alguns dos títulos acima em breve estarão disponíveis na versão impressa e poderão ser adquiridos em nossa **loja virtual**. Cadastre seu e-Mail na loja para ser avisado das novidades e lançamentos.