Ethical Hacking

Presented By : CYBER SHIELD

From Zero To Hero

Contents Of This Course

Here's what you'll find in this course:

Part 1 : Preliminaries

1. Introduction
2. Ethical Hacking
3. Who Are The Hackers
4. Why do Hackers Hack
5. Types of Hackers
6. What should do after hack
7. Why do We Need Ethical Hacking
8. Required Skills For An Ethical Hacker
9. What do hackers do after Hacking?
10. Most Frequently Asked Questions

Part 2 :

- Main Course Materials

01

Preleminaries

Why Do Hackers Hack ?

- Just for fun.
- Show off.
- Hack other systems secretly.
- Notify many people their thought.
- Steal important information.
- Destroy enemy's computer network during the war.

Types of Hackers

- Black Hat Hacker
- White Hat Hacker
- Grey Hat Hacker

What Should I Do After I Have Being Hacked?

- ✓ Shutdown or turn off the system
- ✓ Separate the system from network
- ✓ Restore the system with the backup or reinstall all programs
- ✓ Connect the system to the network
- ✓ It can be good to call the police

Hacking Process

01

Foot Printing

02

Scanning

03

Gaining Access

04

Maintaining Access

Foot Printing

- Whois lookup
- NS lookup
- IP lookup

Scanning

- Port Scanning
- Network Scanning
- Finger Printing
- Fire Walking

Gaining Access

- Password Attacks
- Social Engineering
- Viruses

Required Skills of an Ethical Hacker

Here's what you need to becime an ethical hacker:

1. Microsoft: skills in operation, configuration and management.
2. Linux: knowledge of Linux/Unix; security setting, configuration, and services.
3. Firewalls: configurations, and operation of intrusion detection systems.
4. Routers: knowledge of routers, routing protocols, and access control lists
5. Network Protocols: TCP/IP; how they function and can be manipulated.
6. Project Management: leading, planning, organizing, and controlling a penetration testing team.

What do hackers do after hacking ?

1. Patch Security hole
2. Clear logs and hide themselves
3. Install rootkit (backdoor)
4. The hacker who hacked the system can use the system later
5. Install irc related program
6. Install scanner program
    - mscan
    - sscan
    - nmap
7. Install exploit program
8. Install denial of service program
9. Use all of installed programs silently

02

Course Materials

Introduction to Cyber Security

1. Introduction to Cyber Security

- - Basic Networking Skills,TCP and IP Routers
- - Linux Command Line
- - Windows Command Line
- - Introduction to Programming

2. Bash Scripting

3. Python Basics
- - Python request

4. Kali Linux Basics

Introduction to Cyber Security

5. Working with Essential Tools
- - Netcat
- - Wireshark
- - TCPdump

6. Passive Information Gathering
- - Whois
- - Theharverster
- - Dork
- - Recon

7. Active Information Gathering
- - Host
- - DNSENUM

Introduction to Cyber Security

8. Enumeration
- - Port Scanning
- - IP Scanning
- - Shodan
- - ASN Scanning
- - IP Info and Iraq ASN Summary
- - All Device Scanning (Routers, Cameras, Microtek Systems, Network)

9. Scanning Vulnerability
- - Website Scanning
- - Subdomain Scanning

10. System Hacking
- - Computer and Mobile Hacking
- - Metasploit
- - Armitage

Introduction to Cyber Security

11. Password Cracking
- - Cracking Hash
- - Hash Bounty
- - Cracking Accounts

12. Exploiting Vulnerabilities
- - Scanning for Exploits
- - exploit-db
- - searchsploit

13. Privilege Escalation
- - IDOR

14. SQL Injection
- - SQL Injection Basics
- - Manual SQL Injection
- - Blind SQL injection
- - New Method for Finding SQL injection

15. XSS
- - XSS Reflector
- - XSS dom Based
- - XSS Stored

Introduction to Cyber Security

16. D/DoS Attacks
    - Cloudflare
    - Real IP Address

17. Social Engineering
    - hacking with link
    - Fake Pages
    - Beef

18. Web Application Testing
19. Web Pentesting Methodology
20. CSRF
21. File Uploads
22. OS Command Injection
23. File Includes
24. Directory Traversal
25. Buffer Overflow
26. Windows Buffer Overflow
27. Linux Buffer Overflow
28. Malware Attacks
29. Port Forwarding & Tunneling

Thanks!

Do you have any questions? Email us on
cybershield@gmail.com
+91 620 421 838