ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 5, Issue 3, pp: (90-98), Month: July - September 2017, Available at: www.researchpublish.com

Secure Website from Network Attack

[1]Mohammed Rajhi, [2]Hatim Madkali

[1,2]Teacher Assistance, Jazan University, Dept. of Computer Science and Information System, Jazan, Saudi Arabia

Abstract: **System security is substantial for computer clients, networks, and different organizations. With the advancement of the web Applications, security has turned into a significant attention for the web developers and a clear historical backdrop of security allows for a preferable understanding, development, and optimization of security websites. Multiple techniques are currently employed in the market to cater for the safety websites for network attacks. The proposed model helps a web server administrator to monitor the services. It terminates unnecessary ports and services and thus makes the system less vulnerable. There are six stages of the model: analysis stage, design stage, implementation stage, testing stage, running stage, optimization stage. However, it is imperative to keep updating the security system to fixing any newly found loopholes which may make the system vulnerable.**

Proposal: This paper analyses the condition of current security websites from network attacks and proposes a model that can help improve the security websites. The software tool for securing web servers is raised in this paper. The proposed apparatus helps a web server overseer to oversee running administrations and opening ports on the server. It puts off unnecessary occupations and ports, and it stops unused administrations, this implies it diminishes some vulnerabilities could be gotten to by programmers, and it diminishes chances of trading off Framework security, along these lines it gives guard top to the bottom or various layers of assurance against assailants.

Keywords: **Website, DOS, Hacking, Exploits, IP, Security, Access, Reconnaissance, Worms, viruses, Trojan horses.**

1. INTRODUCTION

System security turns out to be much more substantial to associations, PC clients, merchant organizations and the military. Besides the advancement of the web applications, security shifts within a noteworthy interest and the historical backdrop of security privileges for the better understanding of the rise of security innovation. The web structure itself takes toward consideration numerous security dangers that can occur. The main scheme of the web, while modified have the ability to decrease the possible network assaults that can be sent across the system. Awareness the attack strategies authorizes for the proper security to rise. Numerous companies defend themselves from the web by the technique for firewalls and encryption components. The companies make the "intranet" to keep associated with the web, nevertheless, secured from conceivable dangers. Numerous companies defend themselves from the web by the technique for firewalls and encryption components. The companies make the "intranet" to keep associated with the web, nevertheless, secured from conceivable dangers. The entire domain of system security is endless and in the transitional stage. With a particular end aim to understand the examination being conducted now, foundation learning of the web, its vulnerabilities, assault techniques throughout the web, and security innovation is imperative before presenting a model for protection [1-2].

1.1 Network Attacks:

- Denial of service
- Worms, viruses, and Trojan horses
- Reconnaissance
- Access

1.2 Denial of Service (DoS):

Denial of service proposes that the attacker cripples or adulterates systems, frameworks, or administrations with the goal to dismiss any assistance to Planned clients. The attacker crashes the system or sometimes slows it down to the extent that it is unusable. Be that as it may, DoS can likewise be as straightforward as erasing, on the other hand, undermining data. Much of the time, playing out the assault just includes running a hack or script. The assailant is not required access to the objective previously because an approach to get to it is all that is typically required. Consequently, DoS attacks are the most dreaded.

1.3 Worms, Viruses, and Trojan Horses:

Malicious software is injected into a host to harm a system; degenerate a framework; duplicate itself; or refuse any assistance or access to services, networks or systems. They can likewise permit delicate data to be replicated or resounded to different frameworks. Trojan horses can be utilized to request that the client enters sensitive data in a trusted screen. To illustrate this point, an attacker may sign into a Windows box and run a system that resembles the genuine Windows login screen, provoking a client to sort his username and secret key. The program would then send the data to the attacker and afterward give the Windows error for the wrong password. The client would then log out, and the right Windows login screen would show up; the client is unaware that his password has recently been stolen.

1.4 Reconnaissance:

Reconnaissance is the unapproved discovery and mapping of frameworks, administrations, or vulnerabilities. It is otherwise called information gathering and, and most of the time, it is followed by a denial of service (DoS) attack. Reconnaissance is to some degree closely resembling a thief mapping an area for homes to break into, for example, an abandoned house, simple-to-open door, or open window.

1.5 Access:

When an unauthorized intruder enters a system without having an authentic password or account, it is called system access. Entering systems without proper channel ordinarily include running a hack, script, or instrument that misuses a known vulnerability of the framework or application being assaulted.

1.6 Threats in Transit:

The network interface card (NIC) [10] of every host in a system is exceptionally related to a hardware address. The NIC will be modified to get just the packets addressed to (i) The unicast equipment address comparing to the host, (ii) The hardware multicast address relating to the multicast bunch where the host is an individual from and (iii) The hardware broadcast address. A competent intruder can reinvent the NIC with the equipment location of another host and acknowledge parcels tended to that host. To prohibit being caught, the thief can put a duplicate of the packet back to the system.

1.7 TCP Session Hijacking:

TCP session hijacking [23] alludes to the demonstration of assuming control over an effectively settled TCP session and infusing packets into the stream that are prepared by the recipient as though the bundles are originating from the credible proprietor of the session. A TCP session is recognized by the fourfold: customer IP address, port customer number, server IP location and server port number. Any packet that ranges either machine with the above identifiers is thought to be a piece of the current session. If assailants can parody these things, they can pass TCP parcels to the customer or server and have those packets prepared as originating from the other machine.

1.8 Man in the Middle Attack:

With a Man-In-The-Middle (MITM) assault [23], an attacker can read, change and embed messages among two parties, without either party realizing that the connection amidst them has been traded off. To effectively do this assault, one must have the capacity to watch and catch messages between the two parties.

1.9 Traffic Redirection:

A compromised router can convey route redesign messages to all its neighboring routers illuminating them that it lies on the shortest path to each system on the Internet [4]. The idea is to overwhelm the compromised router with data packets.

As a result of which the compromised router will begin dropping the data packets as the neighboring routers forward the greater part of their approaching data packets to this router. The data packets do not make it to the destination.

1.10 Smurf Control:

A culprit can dispatch the Smurf assault [25] by sending a spoofed Echo-Request message to a system's broadcast IP address. The source IP address which is the victim's IP address is used by the spoofed Echo-Request message. Henceforth, every host getting the broadcast Echo-Request message will send an Echo-Reply message to the victim. The victim will be overpowered with a surge of Echo-Reply messages. Consequently, the Smurf assault becomes a sort of Denial-of-Service (DoS) attack. Two arrangements have been as of now embraced on the Internet to keep a Smurf assault [23]: (i) Routers do not forward datagrams having the destination address as a broadcast IP location and (ii) Hosts are designed not to answer for Echo-Request messages that appeared as a broadcast message.

1.11 Syn Flood Attack:

Amid the TCP connection establishment process, the server kept up an SYN_RECV line to monitor the association demands for which it has distributed the resources and reacted back with an SYN/ACK message; however, the comparing ACK from the customer has not yet reached. The server in the end times out sitting tight for the ACK bundle and expels the inadequate association demand from its line. An assailant can dispatch a DDOS attack by sending a few SYN connection demand messages utilizing parodied non-existing IP addresses and never react back with the ACK messages [21]. The SYN_RECV line of the server gets overwhelmed with short connection request messages. Despite the fact that these deficient association solicitations are disposed of after the timeout, if an authentic customer endeavors to build up a TCP connection with the server Meanwhile, the server disposes of the SYN ask for from that client.

1.12 Network Security Control Methods:

Network and system control is a key innovation for a wide assortment of uses. Security is indispensable for systems and applications. Despite the fact that, system security is a fundamental necessity in raising systems, there is a critical absence of security strategies that can be effectively actualized. At the point when considering system security, it should be understood that the entire system is quite secure. System security is not just concerned the security in the PCs at each end of the correspondence chain. At the point when transmitting information, the communication route should be capable of defending against an attack. A programmer could focus on the communication path, acquire the information, unscramble it; and what's more, re-insert a false message. Securing the system is general as essential as securing the PCs and encoding the message. As in any quickly developing industry, changes are not out of the ordinary. The sorts of potential dangers to system security are continually advancing. On the off chance that the security of the system is compromised, there can be severe consequences, for example, loss of protection, burglary of data. This section analyses a few system security controls that have been embraced in modern computer systems to battle the dangers and avoid or decrease the odds of an attack.

1.13 Link Encryption and End to End Encryption:

Encryption applied among each pair of hosts connected by a link is termed as a link to link encryption [22]. Link encryption is preferable when each one of the hosts in the system is secure, yet the correspondence medium is shared among a few clients and is not secure. All the parts of a data frame (except the source and destination equipment addresses in the casing header) are encoded before the edge is embedded in the physical communication link. As the next host receives the framing (either a router or the end host), the edge is unscrambled at the base convention layer and sent to the higher layers for further processing and sending. Since encryption is at the base protocol layer, the message is uncovered in plain text at all alternate layers of the sender and recipient and the connection and Internet layers of the moderate hosts for hardware routing. Along these lines, link encryption secures the message in travel between two systems, yet the message is in plaintext bounded the end hosts and the middle hosts. One or a greater amount of the midst of the intermediary hosts may not be valid.

Encryption applied between two application programs running on the end hosts of communication is called end-to-end encryption [22]. Here, just the data of the packet encodes at the highest layer (i.e. the application layer), and the packet transmits the information in encoded form all through the Internet. Hence, end-to-end encryption ensures the information against exposure while in travel, however, the information could go through a channel of insecure intermediate hosts. Advancements in the scope of information security, individually in how to use encryption to preserve the confidentiality

of information, vastly enhance the safety for consumers and businesses. However, as products and services become more determined, it becomes difficult for law obligation and national security agencies to access some information that could help them prevent and investigate crimes and terrorism. This creates one of the most difficult policy dilemmas of the digital age, as encryption both promotes security for consumers and businesses and makes it difficult for governments to protect them from distinct threats.

1.14 Virtual Private Networks:

There are two sorts of IP locations: public and private. A public IP address [19] is globally unique, and public IP address is given to only one machine which is connected to the public internet. Private IP locations are one of the answers for lessening the exhaustion of IP address space [19]. A private IP address must be interesting just inside the arrangement of systems of a specific association. Bigger associations have destinations at various regions in the world. The hosts in the diverse locales of the organization might be related to a one of a kind private IP address. Be that as it may, the same arrangement of private IP locations can be utilized as a part of the systems of various associations. Henceforth, a bundle with a private IP address as the destination IP address cannot be appropriated to send packets from one website then onto the next web page of an organization through the public Internet. VPN gives a method for getting to a protected, private, inner system over uncertain open systems, for example, the Internet. Various VPN innovations have been sketched out, among which IPsec and SSL VPN are the most well-known. Despite the fact that a protected correspondence channel can be opened and burrowed through a shaky system using VPN, side customer security ought not to be neglected.

1.15 IP Security:

The IP Security Protocol suite (IPsec) [26] is executed at the IP layer, so it does not require any change to existing transport layer and application layer protocols. IPsec is necessarily intended to address the underlying deficiencies of the IP layer, for example, IP address spoofing, wiretapping and session hijacking. The following two protocols are utilized to give bundle level security to both IPv4 and IPv6:

- IP Authentication Header, AH (Next Header convention ID: 51) [24] gives trustworthiness, validation and non-denial
- IP Encapsulating Security Payload, ESP (Next Header convention ID: 50) [25] gives privacy, alongside verification and respectability insurance authorized obligation.

An overview of some of the conventional network security control methods is given in the literature review section.

2. LITERATURE REVIEW

The worldwide Internet has been changed from a scholarly play area to a medium for universal business and correspondence [3]. Sites serve as mission basic frameworks that ought to work productively to process a large number of activities different from basic day by day online exchanges to convey using informal organization. At the point when tending to Web server security issues, it is pertinent to remember the accompanying general data security standards: Uniformity, Safe-Fail, Flawless or Complete Mediation, Open Design, Separation of Privilege, Psychological Acceptability, Least Privilege, Least Common Mechanism, and Defense-in-Depth [4-5]. These are the security standards which must be kept in mind while analyzing or proposing a security model for network attacks.

As indicated by William Stallings [6], there are five fundamental security methods for a given framework, for example, e-communications environment of the web: Confidentiality, Integrity, Authentication, Non-revocation and Access Control. Notwithstanding these security methods, Bishop included the necessities, approach, and components when taking care of security framework [7]. Prerequisites depict the security goals that the given security approaches must consider. Arrangements are proclamations characterizing what is and is not permitted in the framework. Components frame either instruments or operational strategies to execute the arrangements. In the fact, security approaches are the establishment of the improvement and foundation of access control rules, create an operational methodology, and distinctive application, system, framework and physical controls [4].

The ISO/IEC 17799:2005 is one of the globally acknowledged principles for security data [8]. As indicated by this standard, security control is a countermeasure to deal with a given danger, including arrangements, methodology, rules, exercises or associations constructions [8]. While this standard incorporates an arrangement of security controls considered to arrive at a given security objective, it takes data as the objective resource, not tending to particular security

issues identified with resources as web servers. In light of this standard, the ISO security controls can be connected particularly to web servers to enhance the security components of web servers [8].

A security benchmark is proposed from Center for Internet Security (CIS) to determine the security setup settings and strategies for IIS and Apache [9]. This benchmark has numerous design levels, for example, confirmation instruments, patches upgrading, access control, demand impediment, cryptography, logging, and blocking working framework summons. Bhavya Daya in her article "Network Security: History, Importance, and Future" talks about various methods used for internet security [10]. She concludes that joined utilization of IPv6 and security devices, for example, firewalls, interruption location, furthermore, validation systems will demonstrate compelling in guarding protected innovation for the close future. The system security field may need to develop all the more quickly to manage the dangers further later on.

3. METHODOLOGY

The methodology that is adopted in this research is model methodology. The model methodology provides an abstract model on which a real system can be built. Modeling is the deliberate reflection of a genuine or an arranged system with the target of diminishing it to a constrained; however, illustrative, arrangement of segments and collaborations that permit the qualitative and quantitative portrayal of its properties. The model that is offered here is not as complicated as the system that is modeled on it. And along these lines, it will permit the analysts to comprehend the system better and to utilize the model to perform tests that couldn't be performed in the system itself as a result of expense or lack of proper resources. Experiments in light of a model are called simulations. Whenever a formal portrayal of the model is made to check the usefulness or rightness of a system, the assignment is called model checking. Prevalent security websites and models alongside their advantages and weaknesses were studied with an inductive approach to come up with a model that could help future developers and researchers to devise a security system against network attacks.

4. ANALYSIS AND DISCUSSION

4.1 The proposed security model:

Weigh against CIS standard; this proposed web server security model uses a considerable measure off more extensive arrangement of tests since it depends on the extensive variety of web server best practices. This proposed model comprises of six noteworthy stages: Analysis, Design, Implementation, Testing and Operation and Optimizing of a web server security framework. The beginning stage in the proposed model is the examination and classification stage. It depends on broad scanning for web server best practices; the yield from this stage goes to the configuration stage that distinguishes the security prerequisites.

The design stage gathers input for the analysis stage to submit or to ask for reevaluating necessities or different changes. When design stage completes, it passes its product to Implementation stage to execute the planned security best practices. The implementation stage gives feedback to the design stage to upgrade the outline of the security framework given any adjustment prerequisite found during the implementation stage. The capacity of the web server to give its administrations safely is checked in the proposed testing stage. After the introduced web server passes the testing stage, the web server is published, and the running stage begins. The product of this stage is the consequence of applying the best practices; the output goes to the analysis stage to be analyzed then the model cycle starts again to cater to any changes made. All stages were passing their yield to the optimization stage, and they get the input, the optimization stage speaks to the center (heart) of the model.

4.2 The web Serving Applications:

In the environment of web serving applications, Web servers assume an essential part and make an appealing focus for assailants for some reasons. Accordingly, it is imperative to check the accompanying web server's security angles: Level System Security, Application Level Security and Management and Documentation perspectives. System Level Security angles: Attacks to web servers contain system assaults, host assaults, working framework assaults notwithstanding physical security. Application Level Security features: they allude to vulnerabilities inborn in the code of web-application itself (regardless of the advances where it is executed or the security of the web server/back-end database on which it is worked). In the most recent couple of months, application-level vulnerabilities have been misused [11-12].

Management and Documentation features: they are identified with establishment administration, arrangement, Web substance and server-side applications. Assaults to the web servers in light of access rights misconfiguration are a genuine concern, as a result of assailants may misuse the setup document to find web server delicate data which might be an initial step to an unsafe assault. Web server's arrangements are a critical procedure of our proposed model. The information put away and served by the web server might be a wellspring of vulnerabilities; Furthermore, applications that are utilized by the web server may contain vulnerabilities that may influence the web server.

Documentations serve as rules for framework chairmen to design effectively the web server and to guarantee the congruity of exercises on account of the framework head all of a sudden stop from his association. Truth be told, the worry with the elaboration of an all-around characterized documentation is plainly communicated in the security suggestions made by NIST [13], US Government [14], and ISO [7]. Hence, this proposed model incorporates the confirmation of the accessibility of powerful documentation as a feature of the security evaluation method.

5. STAGES OF THE PROPOSED MODEL

The proposed web server security model comprises of six noteworthy stages which are discussed below. It depends on checking if a framework accomplishes the arrangement of security prerequisites set up sometime recently. To finish this objective, it is crucial to make check records, agent measurements, techniques and components to make a point to what level the related security prerequisites fulfills by the framework under evaluation. The check records and instruments ought to be authentic as much as important to be duplicated in taking after evaluations; furthermore, looking at security is gone for distinguishing which framework is the most secure, among two or more target frameworks, like this the security appraisal technique must be versatile over the diverse stage

5.1 Analysis Stage:

The objective of analysis stage is to discover where the issue of secure web servers is trying to alter this issue. This progression includes separating the web server framework into subsystems to examine the circumstance and objectives, and it includes separating the necessity errands to be made. The analysis stage comprises of two procedures: Data gathering and analysis.

5.2 Design Stage:

The initial inputs to the design stage are the security prerequisites recognized in the examination stage. In the design stage, the security best practices for the web server under establishment are planned. The security best practices are a security shield. They incorporate operational procedures, arrangements, rules or a choice for design alternatives went for either securing a framework contrary to assaults or leaving behind distinguished vulnerabilities. The security best practices can be executed in a variety of different techniques. These strategies incorporate redesigning the web server setup document or putting in new security instruments, for example, Intrusion Prevention Systems (IPS), antivirus and firewalls to give "safeguard inside and out."

The security controls (i.e., countermeasures) identified with every security measure must be recognized, given ISO/IEC 17799:2005. The idea is to recognize how non-exclusive web server security controls are [8]. The web server security best practices must be recognized in light of the fact that they are a key strive to actualize the security necessities of a web server. Then again, so far there is no asserting about the arrangement of security best practices that ought to be connected with general web servers. There is an enormous measure of different security suggestions as archives, aide's papers, reports, expert opinions, books and manuals on the subject of web server security.

However, there is no standard similarity on which best practices must be actualized. In the proposed plan stage, the security proposals gathered in the examination stage are utilized to recognize and to characterize the web security best practices given the security controls of ISO 17799 - ISO 17799. This grouping is useful to recognize a predetermined subset of security practices identified with a specific web environment, notwithstanding the fundamental aftereffects of the security evaluation undertakings. This characterization in light of ISO 17799-ISO 17799 incorporates six classes: security, arrangement, access control, correspondences, and operations administration, HR security, data frameworks obtaining, improvement and upkeep, physical and environment security. The web security best practices are assembled in light of these classes. Likewise, an information base for security best practices are made, this information base incorporates the security best practices taking into account the past order.

5.3 Implementation Stage:

In the proposed implementation stage the web server is introduced. The security arrangement of the web server is actualized in light of the security best practices recognized in the design stage, toward the end of the implementation stage a security appraisal report for the introduced web server is produced. To mechanize this stage, we created security programming instrument; this device controls the web server heads to design and send the web server security best practices appropriate for their web server's assignments. It gives a basic interface to an administrator to enter the administrations that the web server will give, then it creates an aide report, this report incorporates the prescribed choices for arrangement, sending and establishment procedures of the web server to give its administrations safely.

5.4 Testing Stage:

Before publishing the web server, the capacity of the web server to give its administrations safely is checked in the proposed testing stage. A filtering motor must be chosen to check superbly the security vulnerabilities against the security prerequisites characterized in the investigation stage. This checking apparatus is utilized as a benchmark for testing the site security. There are numerous sorts of these filtering programming relying upon the force of checking, a few devices play out the entire examining process naturally, and the others work physically and rely upon the involvement in the field of helplessness examining and the best practice tips.

There are numerous instruments like IBM's Rational AppScan, Nessus, Security Auditor's Research Assistant and Acunetix Web Vulnerability Scanner (WVS). In this proposal, WVS is proposed to be utilized for a few reasons. It bolsters testing of outsider destinations and trail variant with the full operation. Likewise, it is a mechanized web application security testing instrument that reviews web applications by checking for exploitable hacking vulnerabilities. Robotized outputs can be supplemented and cross-checked with the assortment of manual devices to take into consideration thorough site and web application infiltration testing. WVS has adequate capacities for testing, and it has adequate documentations for helping administration [15].

WVS can test an extensive number of various web application vulnerabilities; it can test the vulnerabilities of web server framework, web server stage, SSL encryption, HTTP strategy revelation, and HTTP convention. Likewise, it can test different vulnerabilities, for example, signature web assaults including IIS or Apache, CGI Security, PHP Security, ASP Security, Cross-Site Script Injection, SANS Top 20 and reinforcement security check. Furthermore, WVS is moderately simple to be utilized, and the security evaluation report can be exhibited on the PC screen, imprinted in a printed copy and saved money on the capacity media in various record groups.

5.5 Running Stage:

After the introduced web server passed the testing stage, the web server is published, and the running stage begins. The primary role of running stage is to bolster the head actually and practically amid the underlying Go-Live period for the new framework through utilizing check motor for vulnerabilities as a part of the web server framework.

5.6 Optimization Stage:

The optimization stage upgrades the input of every period of the proposed web server security model. In this way, every stage sends its input to the optimization stage. It, later on, sends its feedback after checking. This feedback may acknowledge the product of the output, or it might send restorative activities to upgrade this stage. The databases of the security prerequisites and the security best practices are often redesigned to be cutting-edge; these modifications can be executed in light of arrangements of online assets, fixes, and upgrades that might be useful for web server overseers to secure their web servers. The proposed enhancement stage cooperates with the others stages in the proposed model, in this manner it contains the accompanying streamlining process:

- Training, mindfulness, approach, and hierarchical abilities identified with web server security
- Requirements and beginning stage change Design issues change
- Implementation issues change
- Testing issues change
- Running issues change

Optimization stage concentrates entirely on procedure enhancements. It gives prescriptive, noteworthy direction on the most proficient method to improve the yield of every stage.

5.7 Loopholes and updates:

There exist numerous security dangers because of security vulnerabilities in administrations, applications, working frameworks and uses of gadgets. At the point when a new loophole in the system is discovered, the missing code is posted on Internet release sheets within the first few hours of the primary attack. Subsequently fixing and upgrading the server's product is the move toward securing the web server applications and database server. Lamentably at times defenselessness might be found, and no patch is accessible. in these cases, the overseer ought to know about the points of interest of the powerlessness to survey the danger of assault and take measures in like manner. In the improvement stage, the most recent administration packs and fixes of the product are introduced straightforwardly from its redesigning and fixing site.

In the optimization stage, it is required to give early warning of dynamic assaults, and empower the proposed model to organize IT assets with a specific end goal to ensure basic resources against a conceivable assault, consequently it is proposed to associate the web server to Symantec Threat Con framework and Homeland Security Advisory System (HSAS), these frameworks are utilized as a part of request to judge how a product (OS, web servers, …) or organizing adventure are perilous to the worldwide web and interchanges arrange in this way they are utilized as an estimation of the worldwide danger introduction [16]. Additionally, in the optimization stage, it is proposed to as often as possible update the databases of security prerequisites and best practices in light of the proposals of the security and web server sites assets [17-18].

6. CONCLUSION

Framework security is critical for PC customers, systems, and diverse associations. With the progression of the web, security has transformed into an imperative sympathy toward the web engineers and the authentic background of security takes into account a superior comprehension, advancement, and optimization of security sites. There are various systems that are right now utilized in the business sector to provide food for security sites for system assaults. The proposed model helps a web server executive to screen the administrations. It ends pointless ports and administrations and subsequently, makes the framework less powerless. There are six stages of the model: analysis stage, design stage, implementation stage, testing stage, running stage, optimization stage. In any case, it is essential to continue redesigning the security framework with a specific end goal to settle any recently discovered provisos which may make the framework helpless.

The web server models comprise of three classes: data (the substance of the sites), mode of communication (right now commanded by the Internet) and administrations (information/data preparing, content conveyance). In web framework, one feeble connection can prompt the entire framework down and causes result in the loss of finances, legality and even reputation which are not easy to be compensated. In this paper, a proposed web server security model in light of best practices is proposed. This model takes a lifecycle vision to create a security model from scratch and regularly updating it. The proposed web server security model can be connected with various web servers' apparatuses. It covers the security best practices identified with the components of the web server and arrangement of key components of the web server, web content, and working framework. Likewise, it covers the best practices for framework level issues and foundation issues.

REFERENCES

[1] By Ryan Russell (Author), Dan Kaminsky (Author), Rain Forest Puppy (Author), Joe Grand (Author), K2 (Author), David Ahmad (Author), Hal Flynn (Author), Ido Dubrawsky (Author), Steve W. Manzuik (Author), Ryan Permeh (Author) & 7 more. (2002, March). Hack Proofing Your Network (Second Edition) 2nd Edition. Retrieved September 4, 2016, from https://www.amazon.com/Hack-Proofing-Your-Network-Second/dp/1928994709

[2] Author Central Douglas E. Comer (Author). (2008, April). Computer Networks and Internets (5th Edition) 5th Edition. Retrieved September 8, 2016, from https://www.amazon.com/Computer-Networks-Internets-Douglas-Comer/dp/0136061273

[3] William C. Boni (Author), Gerald L. Kovacich (Author). (2010). Netspionage: The Global Threat to Information 1st Edition. Retrieved September 21, 2016, from https://www.amazon.com/Netspionage-Information-William-C-Boni/dp/0750672579

[4] Matt Curtin (Author), Peter G. Neumann (Author). December (2001). Developing Trust: Online Privacy and Security. Retrieved September 21, 2016, from https://www.amazon.com/exec/obidos/ASIN/1893115720/ref=pd_list_3/103-9171904-5739059

[5] M.D. Schroeder, B., & J.H. Saltzer. (2005, June 28). IEEE Xplore Document - The protection of information in computer systems. Retrieved October 9, 2016, from http://ieeexplore.ieee.org/document/1451869/

[6] J. Weise, & C. Martin. (2001, November). Developing a Security Policy. Retrieved October 1, 2016, from www.cacert.at/svn/sourcerer/CAcert/SecurityManual/secpolicy.pdf

[7] Mohamed M. Abd-Eldayem, & Dr. Sanaa A. Hanafy. (2012). A Proposed SecurityModel for Public Web Server. Retrieved October 3, 2016, from http://erepository.cu.edu.eg/index.php/cutheses/article/view/3100/3057

[8] Henrique Madeira, Naaliel Mendes, Afonso Araújo Neto, João Durães, & Marco Vieira. (2008). Assessing and Comparing Security of Web Servers. Retrieved September 25, 2016, from http://dl.acm.org/citation.cfm?id=1495156

[9] T. (2010, November 1). The CIS November 1st 2010 - Center for Internet Security. Retrieved November 15, 2016, from https://benchmarks.cisecurity.org/tools2/metrics/CIS_Security_Metrics_v1.1.0.pdf, https://www.cisecurity.org/

[10] Bhavya Daya (2016, August). Network Security History Importance and Future. Retrieved September 6, 2016, from https://ar.scribd.com/doc/208637789/Network-Security-History-Importance-and-Future

[11] Yao-Wen Huang†, & D. T. Lee‡. (2005). Web Application Security—Past, Present, and Future. Retrieved October 7, 2016, from http://www.iis.sinica.edu.tw/~dtlee/dtlee/KluwerBook_chapter_2005.pdf

[12] D, & R. (2003, July/August). Specifying and enforcing application-level web security. Retrieved November 15, 2016, from http://rich.recoil.org/publications/tkde.pdf

[13] M., W., K., & T. (2007, September). NIST SP 800-44 Guidelines on Securing Public Web Servers. Retrieved November 15, 2016, from http://csrc.nist.gov/publications/nistpubs/800-44-ver2/SP800-44v2.pdf

[14] D., & R. (2003, July/August). Specifying and enforcing application-level web security. Retrieved November 15, 2016, from http://rich.recoil.org/publications/tkde.pdf

[15] NIAP: Archived U.S. Government Approved Protection Profile - U.S. Government Protection Profile Web Server for Basic Robustness Env... (2011, September 1). Retrieved November 15, 2016, from https://www.niap-ccevs.org/Profile/Info.cfm?id=241

[16] National Homeland Security Knowledgebase. (n.d.). Retrieved November 15, 2016, from http://www.national homelandsecurityknowledgebase.com/

[17] Threatcon - Symantec Corp. (n.d.). Retrieved November 15, 2016, from https://www.symantec.com/security_response/threatconlearn.jsp

[18] CERIAS - Center for Education and Research in Information Assurance and Security. (n.d.). CERIAS - Center for Education and Research in Information Assurance and Security. Retrieved September 3, 2016, from http://www.cerias.purdue.edu/

[19] J. Postel, Internet Control Message Protocol, IETF RFC 792.

[20] D. Kaminsky, et. al., Hack Proofing Your Network, Syngress, 2nd Edition, Mar. 2002. ISBN: 1928994709.

[21] D. Senie, Changing the Default for Directed Broadcasts in Routers, IETF RFC 2644, Aug. 1999.

[22] D. Kaminsky, et. al., Hack Proofing Your Network, Syngress, 2nd Edition, Mar. 2002. ISBN: 1928994709.

[23] C. Pfleeger, Security in Computing, 4th Edition, Prentice Hall, Nov. 2006, ISBN: 0132390779

[24] Scott, D.J., & Sharp, R. (2002). Abstracting application-level web security. WWW. https://pdfs.semanticscholar.org/a6a9/3ff8672402d496055c6b5a642cc93be6d08b.pdf?_ga=2.220952408.1957577328.1494532788-293482664.1494524318

[25] S. Kent and R. Atkinson, IP Authentication Header, IETF RFC 2402, Nov. 1998.

[26] S. Kent and R. Atkinson, IP Encapsulating Security Payload (ESP), IETF RFC 2406, Nov. 1998.

[27] S. Kent and R. Atkinson, Security Architecture for the Internet Protocol, IETF RFC 2401, Nov. 1998.