International Journal of Computational and Electronic Aspects in Engineering
Volume 2, Issue 2, June 2021, pp 14 - 17
https://doi.org/10.26706/ijceae.2.2.20210407

Server Intrusion Protection System

Madhuri R. Charpe
madhurcharpe@gmail.com

Nikita S. Nandapure
nnandapure@gmail.com

Pratiksha M. Hatekar
Pratikshahatekar123@gmail.com

Akshay O. Sakhare
akshay.locked@gmail.com

Department of Information Technology, Smt. Radhikatai Pandav College of Engineering, Nagpur, India

***Abstract*— The dramatic growth of usage of HTTP, FTP, SSH, SFTP, email, online data banks, online data storage, online gaming then on leads us to higher usage of network terminal IPV4 and IPV6 which needs certain protocols of configuration without which the system won't run and obtain hacked. Those protocols or measures are named as Server security system or in non-technical manner Anti Hacking Tricks. These protocols are basic requirement of every and each system or server where data is stored or getting accessed by public through there user details. because the network protocols are becoming advanced by new cyber security flaws, security system is getting advanced by an equivalent amount. during this paper we are getting to see the methodologies used for securing the server from unauthorized access by third party and destroying our data.**

Keywords*— *Server, Server Security System, Anti Hacking Tricks, Security protocols, Htaccess.

I. Introduction

Servers are powerful computers that provide one or more services (such as email, web, or file servers) to users on a specific network. Cybercriminals frequently target servers due to the character of sensitive data they often hold. what's server security: Server security focuses on the protection of knowledge and resources persisted the servers. It comprises tools and techniques that help prevent intrusions, hacking, and other malicious actions. Server security measures vary and are typically implemented in layers. They cover:

a. The bottom operating system-focusing on the safety of critical components and services.
b. Hosted applications-controlling the content and services hosted on the server.
c. Network security-protecting against online exploits, viruses, and attacks.
d. In-secure servers are significant business risk and may cause many networks security issues.

Securing large, complex servers can require specialist skills. However, any business employing a server should remember of the risks and - at the very least - use basic cyber security measures. Good management practice can assist to improve business's server and network security.

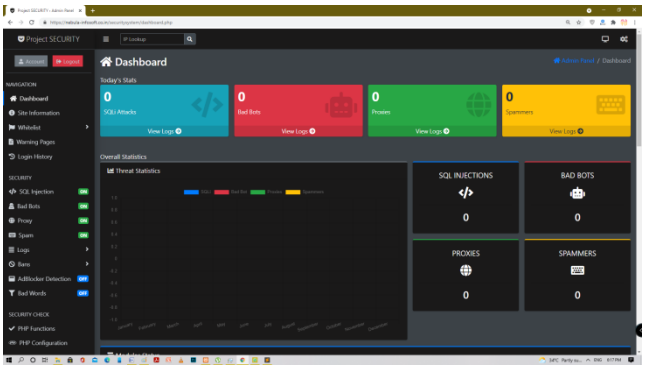

Figure 1: Security system dashboard

II. Server Protection

An example of one server is considered that contains a corporation website and another example of a server that contains a hosting application. Now single server that contains our company website are often secured in multiple factors like IP blocker, non-authorized backend access, spam protection, server monitoring. But a hosting

Research Article
First Online on – 8 June 2021

Cite this article – Madhuri R. Charpe, Nikita S. Nandapure, Pratiksha M. Hatekar, Akshay O. Sakhare, "Server Intrusion Protection System", *International Journal of Computational and Electronic Aspects in Engineering*, RAME Publishers, vol. 2, issue 2, pp. 14-17, 2021.
https://doi.org/10.26706/ijceae.2.2.20210407

application would require a particular number of technological methodologies which can be wont to secure network protocol ipv4 and IPv6 and ssh access for unauthorized access. Now as per the need of the system, the different sorts of security protocols are used which can help to reinforce the firewall system which can be safeguarding the information stored in our server.

There are multiple factors and multiple technological improvements which may be used for safeguarding.

1. SQL injection method
2. IP address header insertion method
3. Bad bots blocking system
4. TCP/UDP networking system
5. Proxy connection checking system
6. Spam blocking system
7. Brute force blocking system then on.

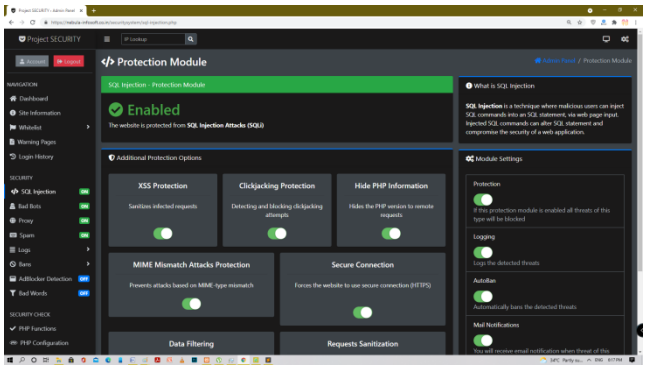

Figure 2: SQL Injection board

A. *SQL injection method*

SQL injection may be a web security vulnerability that permits a hacker or attacker to interfere with the queries that an application makes to its database. It normally allows the hacker to try to crud operations on to the server without the knowledge of the network administration team. because the attacker gains access off the server they will terminate, change, modify, and delete the info belonging to other users and also as the other data which is employed by the appliance to run flawlessly. In some situations, an attacker or hacker escalates an SQL injection attack to compromise the underlying server's other backend infrastructure or perform a network D-DOS attack [1].

B. *IP address header insertion method*

Now as all you recognize everyone who is connected to the web features a certain address by which he or she will get connected to the WWW network. But some people can mask the header to realize access to our network security and do a spread of service stoppage works for the clients which you've got [2].

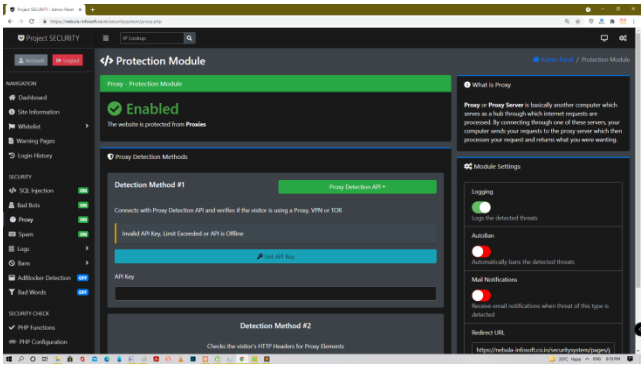

Figure 3: Bad Bots Board

C. *Bad bots blocking system*

Bad bots are bots that perform malicious acts, steal data, or damage sites or networks through such things as distributed denial of service (DDoS) attacks, which suggests simply flooding the location with much more data requests than it can handle. Bad bots are mostly organized in botnets [3,4].

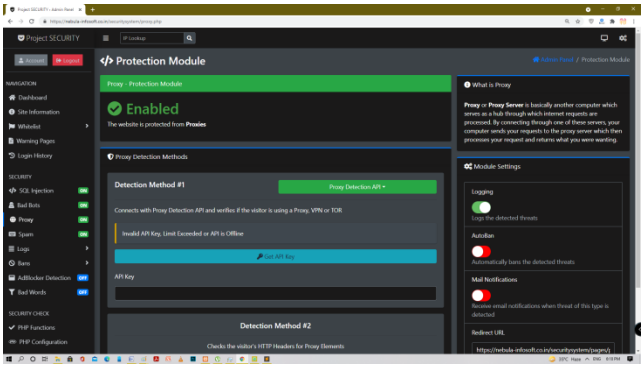

Figure 4: TCP/UDP Flooding System

D. *TCP/UDP Network Flooding System*

"UDP flood" may be a sort of Denial of Service (DoS) attack during which the attacker overwhelms random ports on the targeted host with IP packets containing UDP datagrams.

The receiving host checks for applications related to these datagrams and finding none sends back a "Destination

Unreachable" packet. As more and more UDP packets are received and answered, the system becomes overwhelmed and unresponsive to other clients [5].

In the framework of a UDP flood attack, the attacker can also spoof the IP address of the packets, both to form sure that the return ICMP packets don't reach their host and to anonymize the attack. Several commercially available software packages are often wont to perform a UDP flood attack (e.g., UDP Unicorn).

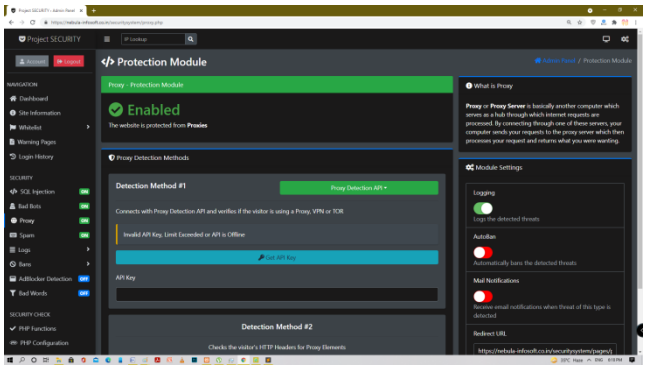

Figure 5: Proxy Connection Checking System

E. Proxy Connection Checking System

Proxy hacking, also referred to as proxy hijacking, is an attack technique designed to supplant an authentic website during a search engine's index and search results pages. An attacker may use proxy hacking to realize a plus over a competitor or, ultimately, to redirect users requesting the targeted page to a malicious or fraudulent website.

The attacker creates a replica of the targeted website on a proxy server and uses methods like keyword stuffing and linking to the copied page from external sites to artificially raise its program ranking. The authentic page will rank lower and should be seen as duplicated content, during which case an enquiry engine may remove it from its index [8].

F. Spam Blocking System

An E-mail has spawned one among the foremost significant sorts of cybercrime spam, or unsolicited advertisements for products and services, which experts estimate to comprise roughly 50 percent of the e-mail circulating on the web. Spam may be a crime against all users of the web since it wastes both the storage and network capacities of ISPs, also as often simply being offensive. Yet, despite various attempts to legislate it out of existence, it remains unclear how spam is often eliminated without violating the liberty of speech during a liberal democratic polity. Unlike spam, which features a postage cost related to it, spam is almost free for perpetrators—it typically costs an equivalent to send 10 messages because it does to send 10 million [6].

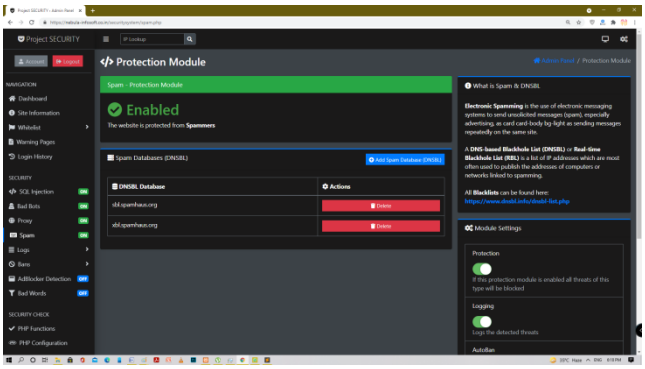

Figure 6: Spam Blocking Board

G. Brute Force Blocking System

A brute force attack uses trial-and-error to guess login info, encryption keys, or find a hidden website. Hackers run through all possible combinations hoping to guess correctly. These attacks are done by 'brute force' meaning they use excessive forceful attempts to undertake and 'force' their way into your private account(s). this is often an old attack method, but it's still effective and fashionable hackers. Because counting on the length and complexity of the password, cracking it can take anywhere from a couple of seconds to several years [7].

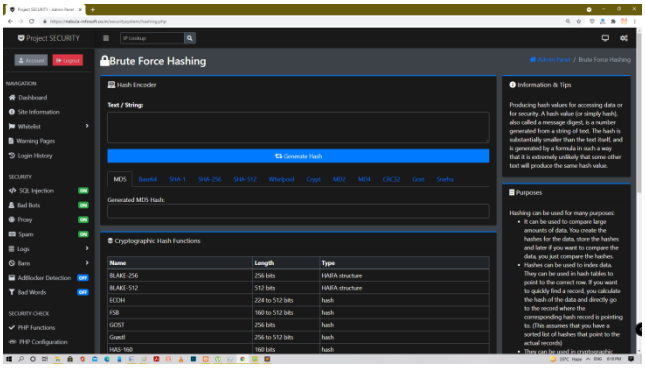

Figure 7: Brute Force Board

III. CONCLUSION

It is observed that the necessity for cybersecurity is getting increase day by day because the attackers are

becoming advanced in algorithms breaking protocol. And same the usage of the safety system should be enhanced likewise. At the Enterprise level, we will sterilize the output with Machine Learning and AI and gain high-level security which can used this technology for the protection of multiple servers and data-related hard drives.

REFERENCES

[1] Limei Ma; Dongmei Zhao; Yijun Gao; Chen Zhao, "Research on SQL Injection Attack and Prevention Technology Based on Web", International Conference on Computer Network, Electronic and Automation (ICCNEA), IEEE Xplore, 27-29 Sept. 2019. DOI: 10.1109/ICCNEA.2019.00042

[2] Hussein Lema; Fatuma Simba; Abdulla Ally, "Preventing Utilization of Shared Network Resources by Detecting IP Spoofing Attacks through Validation of source IP Address", IST-Africa Week Conference (IST-Africa), IEEE Xplore, 9-11 May 2018. https://ieeexplore.ieee.org/document/8417335

[3] Mohamed Torky; Ali Meligy; Hani Ibrahim, "Securing Online Social Networks against bad Bots based on a Necklace CAPTCHA approach", 12th International Computer Engineering Conference (ICENCO), IEEE Xplore, 28-29 Dec. 2016. DOI: 10.1109/ICENCO.2016.7856462

[4] T. Indhumathi; R. Harshini; S. Janani; S. Navaneetha, "An efficient scheme for identifying spam bots and terminate mailing", Second International Conference on Science Technology Engineering and Management (ICONSTEM), IEEE Xplore, 30-31 March 2016. DOI: 10.1109/ICONSTEM.2016.7560918

[5] Abdullah Aydeger; Mohammad Hossein Manshaei; Mohammad Ashiqur Rahman; Kemal Akkaya, "Strategic Defense against Stealthy Link Flooding Attacks: A Signaling Game Approach", IEEE Transactions on Network Science and Engineering, Volume: 8, Issue: 1, Jan.-March 1 2021, PP 751 – 764. DOI: 10.1109/TNSE.2021.3052090

[6] Sujatha Sivabalan; P J Radcliffe, "A novel framework to detect and block DDoS attack at the application layer", IEEE 2013 Tencon – Spring, IEEE Xplore, 17-19 April 2013. DOI: 10.1109/TENCONSpring.2013.6584511

[7] Ajit Patil; Aishwarya Laturkar; S. V. Athawale; Rutuja Takale; Priya Tathawade, "A multilevel system to mitigate DDOS, brute force and SQL injection attack for cloud security", International Conference on Information, Communication, Instrumentation and Control (ICICIC), IEEE Xplore, 17-19 Aug. 2017. DOI: 10.1109/ICOMICON.2017.8279028

[8] P. Pandiaraja; J. Manikandan, "Web proxy-based detection and protection mechanisms against client-based HTTP attacks", International Conference on Circuits, Power and Computing Technologies [ICCPCT-2015], IEEE Xplore, 19-20 March 2015. DOI: 10.1109/ICCPCT.2015.7159344