National Conference on
"Role of Engineers in Nation Building" organized by VIVA Institute of Technology, Mumbai
(6th and 7th March 2020)
International Journal of Engineering Research & Science (IJOER)
ISBN:[978-93-5391-287-1] ISSN: [2395-6992] [Vol-6, Issue-3, March- 2020]

Securing Web Server Against DDoS Attack

Shivam Ladumor[1],Paresh Patil[2],Omkar Vanjare[3],Vinit Raut[4]

[1]Department of Computer Engineering , VIVA Institute of Technology,Virar(east),401305
16301055shivam@viva-technology.org
[2] Department of Computer Engineering , VIVA Institute of Technology,Virar(east),401305
163301053paresh@viva-technology.org
[3] Department of Computer Engineering , VIVA Institute of Technology,Virar(east),401305
17301087omkar@viva-technology.org
[4] Department of Computer Engineering , VIVA Institute of Technology,Virar(east),401305
vinitraut@viva-technology.org

Abstract*—A DDoS attack is a malicious attempt to disrupt normal traffic by exhausting web server resources. The DDoS attack is used to block normal traffic flow, crack login credentials, scraping data, bring down websites, reduce domain ranking etc. Securing the web server from DDoS attacks is one of the major problems in network technologies. There are various algorithms to mitigate DDoS attacks but these algorithms have many flaws that are to be overcome. The proposed system can detect and prevent DDoS attack on any live server.*

The main goal of this system is to filter incoming traffic based on various parameters and to secure the channel from different types of DDoS attacks. The system is capable of recognizing the behaviour of abnormal traffic by tracking session. This approach can be useful for securing servers from random query injection, botnets, port scanning, directory traversing, brute force, and flooding attacks. The system can help to identify the criticality of the attack. As per criticality, system can stop DDoS attacks with various methods like reducing request per second, captcha, checking browser access, cookie checking. The implementation of this approach can easily be applied to any web server.

Keyword—DDoS attacks, Security, Web Security, DDoS Prevention, Proactive Approach.

I. INTRODUCTION

Preventing network attacks is one of the most difficult tasks in the field of information systems protection. Most modern systems have a distributed structure, their architecture is based on the use of network technologies. And ensuring the operability of such systems depends on the ability to resist malicious acts that are aimed at disrupting the work of both the network itself and the information system functioning within its framework. One of the most dangerous types of criminal activities on the Internet are the so-called DDoS-attacks [8][9].The International Telegraph and Telephone Consultative Committee (CCITT) describes denial of service as "The prevention of authorized access to resources or the delaying of time-critical operations".

To achieve a bigger attack traffic size, many attack sources can be used. A Denial of Service technique that uses numerous hosts to perform the attack is called Distributed Denial of Service (DDoS). Attacker does not need to own big number of computers and can use an army of corrupted hosts (botnet) [12] to execute DDoS attack. Such attacks attempts to create congestion by consuming all available bandwidth between the target and the larger Internet.

There are currently a lot of efforts being made to come up with mechanisms to detect and mitigate such attacks. Attackers constantly modify their tools to bypass these security systems, and researchers in turn modify their approaches to handle new attacks. There are different types of methods which are used to handle DDoS attacks like the rate limit solution [10][11], defense by offense, active filtering, IP trace back, blocking etc.

DDoS attacks can create significant business risks with lasting effects. Therefore, it is important for any website owner to protect

International Journal of Engineering Research & Science (IJOER)
ISBN:[978-93-5391-287-1] ISSN: [2395-6992] [Vol-6, Issue-3, March- 2020]

his/her web server against this attack, it is important to understand the threats, vulnerabilities and risks associated with DDoS attacks. The system introduced can detect and prevent various types of DDoS attacks like flash crowd, botnets, port scanning, directory traversing, brute force, and flooding attacks on any web server [13].

II. LITERATURE REIVIEW

Ilya V. Chugunkov, et. al. [1] describes Pulse Wave attack which can last very long and can have multiple targets at once. The model is created which simply uses classifier and rule sets with respect to IP table. The results of attack simulation done using python bots the system can reduce DDoS attack significantly. The result of the solution's work was a decrease in the number of time-consuming waits for user model queries from 98% to 5-10% for the duration of the attack. This system is good for all over request flow but not for individual request.

Simona Ramanauskaitơ, et. al. [2] proposed different models for detection of DDoS attack by considering resources usages. The system requires to calculate memory and CPU work exhaustion probability the bandwidth exhaustion probability to determine the level of DDoS attack. Model is implemented on network layer for checking real-time data statics. Mitigation of flooding attack can be easily done. However the two-tier architecture does not influence the performance of the model if queuing based models are used for the modeling.

Vaishali Kansal, et. al. [3] proposed an effective system which is able to detect DDoS attack on server and reduce the impact of DDoS attack on main server. Detection is based on IP rule sets and Data exhaustion information. For isolation they are diverting DDoS attack to proxy servers which acts as the original target keeping main server protected. Using the proactive approach proposed in this paper DDoS attack is mitigated at the proxy level efficiently. EDIP deploys two types of proxies one is head proxy which is randomly assigned to clients and another is attack proxy which is instantiated during attack time. This technique helps server running normally without user letting know about attack.

V. Priyadharshini, et. al. [4] developed a New cracking algorithm is implemented on the application layer of web server. It uses pattern checking on incoming traffic and store IP address of the client when they arrived to the website. Mitigation of DDoS is based on blocking if abnormal IP is found. When the new user enters into the site continuously, the new cracking algorithm to determine whether the user is DDoS attacker. Such systems are effective for all scenarios, should have more parameters of detection and various methods for nullifying DDoS attack. But the system is unable to find what kind of DDoS attack occurred and on what part of web page it happened.

S. Renuka Devi, et. al. [5] introduced an metrics algorithm based on information theory for Detecting DDoS attacks on application layer. It consists of two main parts, monitoring and detection system. The system calculates entropy request per session and degree of data usage. The scheme proposed, provides double check point to differentiate the malicious request flow from the normal request flow. It validates legitimacy of user based on the previously recorded history. Based on the information metric of the current session and the user's browsing history, it detects the suspicious session. According to that system has a mechanism for rate limit and scheduling. System also session data to use when client sends request again as per the checking IP is assigned a score.

A DDoS attack is a type of DoS attack in which many computers are used to cripple a web page, website or web-based service. This analysis study on flood attacks and flash crowd increases their improvement. Attacks are either classified into high rate flood or low rate flood. For detection system uses α-Stable Model and the EM Algorithm.[6]

Dr. Punidha R, Pavithra K, Swathika R and Dr. Sivaram M,[7] introduced the algorithm which is node blocking algorithm implemented on network layer. It uses multiple nodes from which the packets are to be sent from the sender to the receiver. It checks from various parameters if it satisfies the condition the user is considered as normal or marked as attacker. If user is genuine then the system provide the right path form multiple nodes. If user is attacker the it is unable to reach original server through routers. System maintain the packet address history and store the pack-address of client when it on network.

International Journal of Engineering Research & Science (IJOER)
ISBN:[978-93-5391-287-1] ISSN: [2395-6992] [Vol-6, Issue-3, March- 2020]

III. PROPOSED SYSTEM

The system acts as a starting point when user sends a request to the website before session is granted. It consists of two main modules, one for checking behavior of individual request and other for monitoring overall request flow of website. Once the request is granted to a user the session log is created which is used to monitor user behavior. The session log includes data like request protocol, header information, access port and directories, time, and request query. Pattern checking is done on each request to determine the purpose of each request, if abnormal behavior is detected then user IP & headers are black-listed. This data is valid for one month since IP are dynamic.

Pattern checking algorithm for single request requires different parameter on bases of which it predicts genuineness of the user. It requires header information, user IP, agent, protocol, request page, upload/download size, url query and domain origin. Algorithm have real-time database of blocked IP's and query injection pattern are always constant. Every request is recorded in the session log. Figure 1 shows the work flow of individual request checking module.

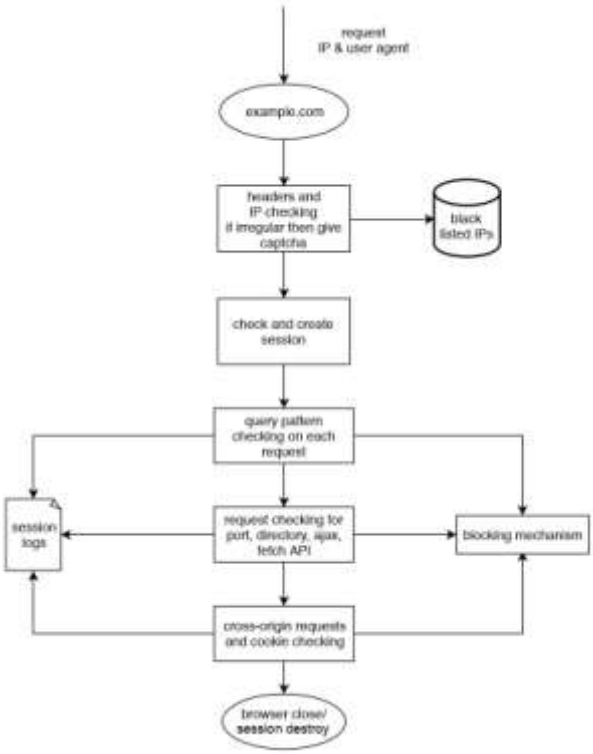

FIGURE 1: Working of individual request checking module

Another module in system is for regulating overall requests to the web-server. This module monitors overall requests to the website which is helpful for detecting flash crowd and flooding attacks on website. After every certain number of requests this module calculates the time elapsed between current request and previous 1000^{th} request. This interval between requests is dynamically set in order to meet website normal traffic rate, otherwise if we preset this it will delay every 1000^{th} request even if that is normal traffic for that website. After detecting any abnormalities in request flow module will take action such as rate limiting to delay request's access to the website. Figure 2 shows work flow of this module.

International Journal of Engineering Research & Science (IJOER)
ISBN:[978-93-5391-287-1] ISSN: [2395-6992] [Vol-6, Issue-3, March- 2020]

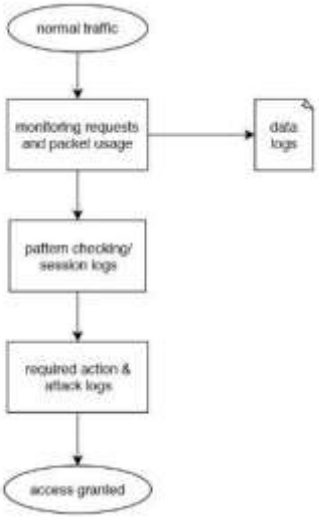

FIGURE 2: Working of overall request monitoring module

IV. RESULTS

We have implemented above mentioned system as wordpress plugin. We simulated different attacks like brute force, spamming, flash and flood, etc. These attacks then successfully mitigated by proposed system. We have used captcha, rate limiters as a solution for mitigating these attacks. Following figure shows simulation of flash crowd attack on website.

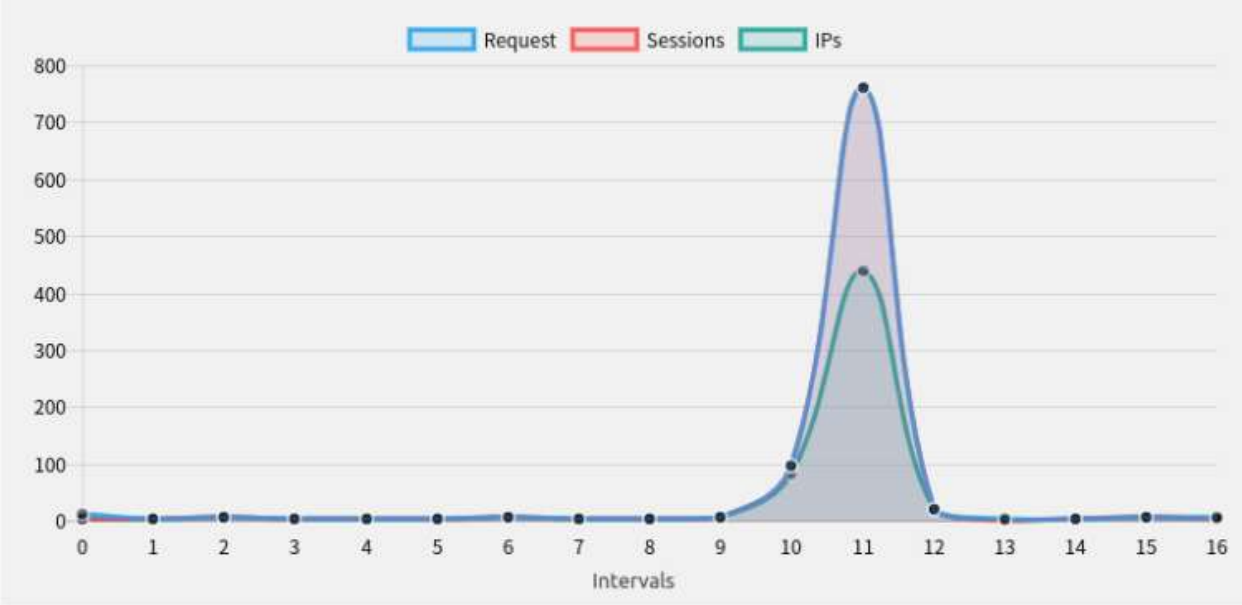

FIGURE 3: Simulation of flash crowd attack and mitigation of the same.

In above figure it is shown that there are multiple requests incoming to the website. And these requests are also coming from multiple IP's. After detecting large number of requests in very small amount of time, algorithm applies rate limiting for each new session.

International Journal of Engineering Research & Science (IJOER)
ISBN:[978-93-5391-287-1] ISSN: [2395-6992] [Vol-6, Issue-3, March- 2020]

IV. CONCLUSION

The proposed system is able to detect and prevent DDoS attack of type single IP multi-request. System is able to use robots checking verification method for blocked black listed IP's and request which are coming from dark web source. System is also protected malicious user agents and provides extra security headers. System also provides detailed information about DDoS attack with attack type and region of attack. Further implementation can stop various DDoS attacks like multi-IP attack, brute force, random query injection, flash crowd, flood attack and also a combination of the above attacks.

V. REFERENCES

[1] Ilya V. Chugunkov, Leonid O. Fedorov, Bela Sh. Achmiz and Zarina R. Sayfullina, "Development of the Algorithm for Protection against DDoS-Attacks of Type Pulse Wave" IEEE, 2018, pp. 292-294.

[2] Simona Ramanauskaitơ, Antanas ýenys, Nikolaj Goranin and Justinas Janulevičius, "Modeling of Two-tier DDoS by Combining Different Type of DDoS Models" IEEE, 2017, pp. 978-981.

[3] Vaishali Kansal and Mayank Dave, "Proactive DDoS Attack Detection and Isolation" IEEE, 2017, pp. 334-338.

[4] V. Priyadharshini and Dr.K.Kuppusamy, "Prevention of DDOS Attacks using New Cracking Algorithm" IJERA, 2012, pp. 2263-2267.

[5] S. Renuka Devi and P. Yogesh, "Detection of Application Layer DDoS Attacks Using Information Theory Based Metrics" CS & IT-CSCP, 2012, pp. 217-223.

[6] Anup Bhange, Amber Syad and Satyendra Singh Thakur, "DDoS Attacks Impact on Network Traffic and its Detection Approach", International Journal of Computer Applications, 2018, pp. 36-40.

[7] Dr. Punidha R, Pavithra K, Swathika R and Dr. Sivaram M, "Preserving DDoS Attacks Using Node Blocking Algorithm", International Journal of Pure and Applied Mathematics, 2018, pp. 633-639.

[8] https://www.us-cert.gov/ncas/tips/ST04-015,last accessed on: 04/01/2020.

[9]https://www.imperva.com/learn/application-security/denial-of-service, last accessed on 28/12/2019.

[10] https://www.keycdn.com/support/rate-limiting, last accessed on: 06/01/2020.

[11]https://www.ibm.com/blogs/security-identity-access/web-reverse-proxy-rate-limiting, last accessed on: 03/01/2020.

[12]https://en.wikipedia.org/wiki/Botnet, last accessed on: 12/01/2020.

[13]https://www.imperva.com/learn/application-security/ddos-attacks/laset accessed on: 18/01/2020.