Low interaction honeypot as the defense mechanism against Slowloris attack on the web server

N R Fitri¹, A H S Budi¹,*, I Kustiawan¹ and S E Suwono²

¹Department of Electrical Engineering Education, Universitas Pendidikan Indonesia, 40154, Bandung, West Java, Indonesia
²Group of Faculty Member, Telkom Corporate University Center, 40152, Bandung, West Java, Indonesia

*agusheri@aol.com

Abstract. Threats and attacks on internet services are in line with developments in internet technology. One of the main risks is Distributed Denial of Service (DDoS). In this paper, we focus on the Slowloris attack which is an open-source DDoS attacker that generally attacks the Apache webserver. Apache is one of the most popular web servers in the world and is still used by many companies. This research presents another way to reduce attacks to the firewalls and load a counterweight by using a low interaction honeypot, HoneyPy. In normal conditions, attack schemes and defense mechanisms are evaluated by conducting experiments. Slowloris attacks cause high traffic because it prevents the socket from closing, so the webserver cannot handle other connections from legitimate users. When defense mechanisms are applied to the network, Slowloris attacks that enter the webserver are minimized because most packets are discarded and directed to the honeypot without the attacker's knowledge. It seems like the attacker has managed to attack the web server even when the attack becomes slower.

1. Introduction
The development of internet technology goes hand in hand with threats and attacks on internet services. One of the main risks is the Denial of Service (DoS). Denial of Service (DoS) is an attack program to prevent legitimate users from gaining access services from servers. This type of attack causes the system resources to become saturated [1]. If a DoS attack is implemented in a distributed manner and carried out by more than one machine, the attack is called Distributed Denial of Service (DDoS). The DDoS attack is launched by installing a backdoor into many computers as botnets to flood a server causes a denial of service for legitimate users. The botnets are controlled by the Command and Control (C&C) server. The attacker sends commands to the Command and Control server (C&C) then it is forwarded to the machines or computers that have been infected with malware or a backdoor to denial of service attack on the server for an undetermined time [2]. As a result, users cannot access services from the server. The most famous DDoS attack method now is to involve application-level flooding, especially on web servers. These methods can include HTTP GET Flood, HTTP Post Flood, Slowloris, DNS, etc. [3]. Slowloris is a DoS attack but can function as a DDoS because only one execution by one machine can "flood" the webserver with HTTP Flooding. Slowloris cannot be detected by Intrusion Detection System (IDS) or Intrusion Prevention System (IPS) because Slowloris does not send malformed HTTP packets so that it is detected by IDS or IPS like legitimate users [4]. Slowloris sends partial HTTP
connections so that the connection remains open for a particular time so that the packets can pass IPS [5]. Apache-based web servers are vulnerable to Slowloris attacks, because in the process of handling requests with a queuing system with M/M/N so the probability of transitioning to "excessive" or saturation conditions is higher [6]. If Slowloris attacks a web server, users cannot access HTTP services or web pages as if the user does not have an internet network to access the web page. Nowadays, there are several ways used to mitigate Slowloris attacks, namely limiting the number of connections from specific hosts, determining the different timeouts for each link as a function of the number of links and delayed binding carried out by load balancers [7]. Besides, it can use Firewall and operating system security mechanisms such as Dynamic IP Restriction, mod_evasive, mod_qos, IPTables, and Fail2Ban [1].

In this paper, besides using Firewall on routers and Honeypot as a web server security system. Low to Medium Interaction Honeypot will be used as a trap server for attackers where some HTTP requests from Slowloris will be directed towards the honeypot with Port Forwarding. Honeypot is implemented on the Raspberry Pi 3. With the honeypot, it is expected to minimize the Slowloris attack on the webserver.

2. Related works
Shorey et al. explain that Slowloris uses HTTP and DNS because HTTP uses DNS as address resolution. Slowloris attacks have a high traffic rate [4]. Papadie et. al suggested the defense mechanism against Slowloris is using Firewall, Cisco and operating system load-specific tools such as Dynamic IP Restriction, mod_evasive, IPTables, and Fail2Ban [1]. There is also another proposed mitigation mechanism suggested by Arafat et al. which is a reverse web proxy to protect servers from a sudden surge of attack flows [8]. Tambunan et al. suggested a mitigation system using Glastopf Web Honeypot. But Glastopf doesn't give any reaction towards the Slowloris attack [9]. Avinash et al. proposed several ways to mitigate Slowloris attacks including increasing the number of connections that webservers allow so the legitimate users can still access the service [10]. IP-tables firewall rules can be used to limit connections from specific hosts. Then, configuring a fixed time-out connection between the web server and the client is set for how long it can stay connected and reduced the period of its connection. So that it can limit Slowloris attacks.

3. Design and testing
The network topology for this study is designed based on references in three conditions, normal conditions are shown in Figure 1, when the webserver is attacked without a security system shown in Figure 2 and with a network security system shown in Figure 3.

![Network Topology](image_url)
Under normal conditions, the network topology consists only of routers, web servers, and one laptop as a client. Activities on the network only browse with the browser on one laptop. There is no attack on the webserver.

![Diagram](image1.png)

**Figure 2.** The attacking condition network topology.

In the attacking condition, the network topology consists of routers, web servers and one computer as an attacker without a security system. The attack was carried out for five minutes with one Ubuntu-based computer.

![Diagram](image2.png)

**Figure 3.** The attacking condition with the defense mechanism network topology.

In the attacking condition with the defense mechanism, the network topology consists of a MikroTik RouterBoard (RB 951 2n), a webserver, a computer, and a honeypot. The defense mechanism is a combination of a firewall on the router and honeypot. The attack was carried out for five minutes with one Ubuntu-based computer. This network topology is a local network consisting of a computer as the attacker, a laptop as a monitor and setting up the firewall on the router, honeypot implemented on the RaspberryPi 3 Model B+, and RaspberryPi 2 Model B as a web server. Figure 4. shows the ports on the router.
The router has an IP Address 192.168.100.1/24 with port 2 to port 4 as a bridge. Port 5 is removed from the bridge as a simulation of the attacker attacking through the internet with 192.168.25.1/24 as the IP Address. Port 2 is connected to a webserver, port 3 is connected to a honeypot, port 4 is connected to a laptop, while port 5 is connected to a computer as the attacker. The IP address of the webserver 192.168.100.250, the honeypot is 192.168.100.248, and the attacker is 192.168.25.252.

4. Proposed mitigation system
The security system to minimize Slowloris attacks is a combination of a firewall and a honeypot. The firewall is set up in a MikroTik router and honeypot as the fake server. We used HoneyPy as low interaction honeypot. The honeypot runs a full service, for port 80 it opens on port 10080. Figure 5 is a web server security system algorithm.

![Diagram of the proposed mitigation system](image_url)

**Figure 5.** Defense mechanism algorithm of the webserver.

Every connection that passes through the router will be detected, and then the traffic is processed in the firewall chain. The traffic is entered and managed first in the forward chain, then the chain changes to the detect-ddos chain. If the packet data traffic detected for the source address (src-address) and destination address (dst-address) as the connection rate exceeds 32/s and the burst exceeds 32, then the sender's IP Address will be appeared on the address list as "ddoser" as well as IP The address that is the destination of the attack is appeared on the address list as "ddosed". The detected address list has a
timeout of ten minutes. Then, some packet data traffic from the sender is processed to be dropped and forwarded to the honeypot without the attacker's consent.

5. Results and Discussion
The results of recording traffic data packets are recorded on the webserver using tcpdump, then the results of the data are analysed in the Wireshark. The graph displayed is an I/O Graph in TCP Connection, HTTP Connection and TCP Errors. The Y-axis indicates packet/second and the X-axis shows time. The Flow Graph displayed shows packets are sent and received by the webserver and honeypot.

5.1. Normal traffic
Figure 6 shows a TCP Connection graph and Figure 7 shows a diagram of an HTTP connection in normal condition. The webserver with the IP address 192.168.100.250 sent 200 good HTTP requests to the laptop that send HTTP GET requests seen in the Flow Graph in Figure 8.

Figure 6. The graph of TCP connection in normal traffic.

Figure 7. The graph of HTTP connection in normal traffic.
5.2. Data package traffic when an attack occurs
The attack occurred for five minutes without a defense mechanism. In Figure 9, the traffic is high. In Figure 10, it shows high traffic because the Slowloris attacks are slow but numerous in a certain amount of time. The Slowloris attack takes up webserver resources, so the webserver experiences saturation as in Figure 11. Figure 12 shows the TCP errors traffic due to Slowloris attack also causes a reset connection.

![Figure 8. Flow graph HTTP connection.](image1)

![Figure 9. The graph of TCP connection for five minutes.](image2)

![Figure 10. The graph of HTTP connection for five minutes.](image3)
Figure 11. Flow graph HTTP request timeout.

Figure 12. Graph TCP connection errors for five minutes.

5.3. The attacking condition with the defense mechanism
Slowloris is going slower when the defense mechanism is implemented the network as shown in Figure 13. The data packets are sent less than 500 packets. Figure 14 shows lower TCP traffic and high traffic only appears when the 105th second and the connection rate is reduced to 144 packets/second. HTTP traffic also becomes lower to 11 packets/second when the second is 125 as shown in Figure 15.
Figure 14. The graph of TCP connections for five minutes when an attack is mitigated with a defense mechanism.

Figure 15. The graph of HTTP connections for five minutes when the attack is mitigated with a defense mechanism.

5.4. Data package traffic to the honeypot
Some Slowloris attacks are directed into the honeypot based on the firewall rule. Figure 16 shows the data traffic sent into the honeypot for 5 minutes. The traffic is high for 1000 connections every 5 seconds and the highest when the 35th second is 230 packets/s. Figure 17 shows an HTTP GET request from the attacker directed into a honeypot.
6. Conclusion
The defense mechanism consisting of a firewall and a honeypot is proven to mitigate the Slowloris attack. Most of the packets are dropped and directed into the honeypot without the attacker's knowledge. It looked like the attacker had succeeded attacked the webserver even though when the attack became slower.

References
[1] Papadie R and Apostol I 2017 Analyzing websites protection mechanisms against DDoS attacks In 2017 9th International Conference on Electronics, Computers and Artificial Intelligence (ECAI) (pp. 1-6) IEEE
[2] Bhosale K S, Nenova M and Iliev G 2017 The distributed denial of service attacks (DDoS) prevention mechanisms on application layer 2017 13th International Conference on Advanced Technologies, Systems and Services in Telecommunications (TELSIKS) (pp. 136-139) IEEE
[3] Choi J, Park J G, Heo S, Park N and Kim H 2016 Slowloris DoS Countermeasure over WebSocket International Workshop on Information Security Applications (pp. 42-53) Springer Cham.
[4] Shorey T, Subbiah D, Goyal A, Saxxena A and Mishra A K 2018 Performance comparison and analysis of slowloris, goldeneye and xerxes ddos attack tools 2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI) (pp. 318-322) IEEE
[5] Duravkin I, Loktionova A and Carlsson A 2014 Method of slow-attack detection. In 2014 First
International Scientific-Practical Conference Problems of Infocommunications Science and Technology (pp. 171-172) IEEE

[6] Rahmatullah D K, Nasution S M and Azmi F 2016 Implementation of low interaction web server honeypot using cubieboard 2016 International Conference on Control, Electronics, Renewable Energy and Communications (ICCEREC) (pp. 127-131) IEEE

[7] Beard C and Stallings W 2015 Wireless communication networks and systems (Boston: Pearson)

[8] Arafat M Y, Alam M M and Alam M F 2015 A Practical Approach and Mitigation Techniques on Application Layer DDoS Attack in Web Server International Journal of Computer Applications 131(1) 13-20

[9] Tambunan B, Raharjo W S and Purwadi J 2013 Desain dan Implementasi Honeypot dengan Fwsnort dan PSAD sebagai Intrusion Prevention System Ultima Computing: Jurnal Sistem Komputer 5(1) 1-7

[10] V Avinash and K Sornalakshmi 2015 HTTP Reverse Proxy Authentication International Journal of Advance Engineering and Research Development 2(03)