Analysis of denial of service attack on web security systems

Iswandi Walad S., Prof. Dr. Muhammad Zarlis and Dr. Syahril Efendi, M.IT

Department of Information and Technology, Faculty of Computer Science and Information Technology, University of Sumatera Utara, Medan, Indonesia.

Abstract. In this study, an analysis of the Web security system from a Denial-of-Service Attack (DoS) with SYN Attack, Ping of Death, Land Attack, Smurf Attack and UDP Flood types. The server computer that will be tested for DoS attacks is a local web server including humpuss.com IP: 54.169.71.56, horasindo.com IP: 104.152.168.14, kinarsih.com IP: 156.67.210.132, padanglws.co.id IP: 202.162.207.101 and arianaas.com with IP Address 213.136.83.52 port 80. The attack on the local web server computer was carried out through attacking cloned computers as many as 5 zombie computers and then observing data traffic on each Web server computer. The test results use ping to the local web server computer, where the target web server sends a replay request time out and the check results in the Google Chrome browser are slow to inaccessible conditions. Ping access time the greater the packet, the greater the average time when accessing a local web server with 5,000 packets is 242.68 seconds, 10,000 packets is 310.28 seconds, 20,000 packets are 337.4 seconds, 30,000 packets are 377.2 seconds, 40,000 packets are 398.4 seconds, 50,000 packets are 545.4 seconds and 100,000 packets are above 600 seconds with the condition that the web server will recover after 600 seconds where the system recovery process depends on each local web server.

1. Introduction
Denial of service attacks have been known to the network community since the early 1980s. The final impact of this activity resulted in obstruction of the victim's computer activity as a user of data communication services. Target DoS attacks can be aimed at various parts of the network. Can go to routing devices, the web, electronic mail, or the Domain Name System server. This attack aims to make the server shutdown, reboot, crash, or "not responding". The server is a computer system that provides certain types of services in a computer network (Harshita & Nayyar, R. 2017).

This attack produces damage that is persistent meaning the DoS condition will still occur even though the attacker has stopped attacking, and the new server will return to normal after restarting / rebooting. Basically DoS is an attack that is difficult to overcome, this is caused by the risk of public services where the admin will be in a confusing condition between service and convenience to security. As we know, comfort is inversely proportional to security. Therefore, risks that may arise always follow this law. Based on the network security issues above, this study aims to find out more about the system or method used in attacking DoS, the effects of DoS and the security that needs to be done to prevent DoS Attack. In addition to knowing whether a denial of service attack on a network system causes system losses on a web server (Sutarti, 2016).In this study the Web security system that
was attacked was a local web server with a Denial-of-Service Attack (DoS) with SYN Attack, Ping of Death, Land Attack, Smurf Attack and UDP Flood types.

2. Study of literature

2.1 Web Server
Understanding Website is a document in the form of a collection of web pages that are interconnected and their contents consist of various information in the form of text, sound, images, video, etc., where all the data is stored on the hosting server. To open a website the user must have a device (computer, smartphone) connected to the internet or intranet. Website or web pages are generally in the form of documents in Hyper Text Markup Language (HTML) format, which can be accessed via HTTP or HTTPS, a protocol that conveys various information from the website server to be displayed to users or users through a web browser. A website has a unique and specific URL address called a domain. For example the domain Maxmanroe.com, Google.com, Facebook.com and so on. The website can be accessed using a browser and internet connection. However, there are several websites that can be accessed using a local network (LAN).

2.2 Denial Of Service Attack (DoS Attack)
Denial-of-Service attack is an attack carried out by a hacker to disable a web network system by flooding the server with a high amount of data traffic, or making data requests to a server so that the server can no longer provide services and crash (Kolahi et al., 2016). The types of DoS Attack, namely:

a. Ping of Death
Ping of Death is a classic attack that was often used. This attack is carried out by using the ping utility on an operating system. Ping is usually used to check the presence of a host or IP address of a website. Data sent by default is 32 bytes, but in reality this program can send up to 65 kilobytes of data. Now attacks like this are not very effective anymore, because many systems have updated the patch and closed the holes. Plus the more sophisticated technology and the wider bandwidth available, so this attack no longer has a significant impact on a system. Figure 1. shows the process of pinging Death.

![Figure 1. Ping of Death](image)

b. SYN Flood Attack
SYN Flood Attack is an attack carried out by utilizing the weaknesses of the protocol when the handshake process (unification). When two computers decide to start communicating, the sending computer (the attacker) will send a SYN, the recipient (target) will respond by sending the SYN ACK to the sending computer. After receiving the SYN ACK reply from the recipient, the sender must send
the ACK to the recipient to process the handshake. But in reality, the sender sent many SYN packages
to the recipient which resulted in the recipient having to continue to answer requests from the sender.
The attacker's IP address has usually been hidden or spoofed so that the address recorded by the target
is the wrong address. The recipient will be confused to answer the new TCP connection request
because it is still waiting for the number of ACK replies from the unknown sender. Besides that the
connection will also be flooded by SYN requests sent by the sender continuously. Attacks like this
inhibit the recipient (server) providing services to other users. For more details the process of Syn
Flood Attack can be seen as in Figure 2.

![Figure 2. Syn Flood Attack Process (Pengfule, 2016).](image)

c. Remote Controled Attack
Remote Controled Attack is basically controlling several other networks to attack targets. Attacks with
this type will usually have a big impact, because usually the servers to attack have a large bandwidth.
Attackers can also freely control their dolls and hide themselves behind these servers. Many tools can
be used to carry out attacks with this type. Generally these tools have the type of Master and client or
agent. The master is the master computer that has been controlled by the attacker and will be used to
give orders to the agents to launch the attack. While the client is a zombie computer that has been
mastered by an attacker, the attacker then implements a client application that is ready to wait for the
command to attack the target. Attackers use two master servers that are used to spread commands to
zombies to attack targets.

d. UDP (User Datagram Protocol) Flood
UDP Flood is an attack that utilizes the UDP protocol in a connectionless way (reducing connections)
to attack targets. Because of its nature, UDP flood is quite easy to do. A large number of data packets
were sent to the victim. Victims who are shocked and not ready to accept this attack will certainly be
confused and the server computer will hang because of the large data packet received. Attackers can
use spoofed techniques to hide their identities. Figure 3 shows the UDP Attack process.

![Figure 3. UDP Attack Process (Pengfule, 2016).](image)
e. Smurf Attack

Smurf Attack is an attack using ICMP (Internet Control Message Protocol) echo requests that are often used when broadcast (broadcast) identity to broadcast addresses on a network. When broadcasting a broadcast address, all computers connected to the network will respond to the request. This of course will slow down traffic on the network because computers that are not asked contribute to the request. This will certainly have a greater impact if the sender's request address is disguised and not only sends ICMP requests to a network but to several networks. Of course the reply received will be even greater, not only there. The sender disguises his identity by using another person's IP address.

f. Smurf attack

During a Smurf attack, hackers flood the router with an Internet Control Message Protocol (ICMP) echo request packet known as a ping application. Because the destination IP address on the packet sent is the broadcast address of the network, the router will send this ICMP echo request to all machines on the network. If there are many hosts on the network, ICMP traffic responses and requests in very large numbers will occur. In Figure 3.5 the hacker chose to spoof the IPMP source address of the ICMP request. By using IP spoofing, the response from the ping was addressed to the computer whose IP was spoofed. As a result, the computer will receive many packages. Because ICMP traffic occurs that will not only jam the intermediary computer network, but the network whose IP address is spoofed. Figure 4. shows the Smurf Attack process.

![Smurf Attack Process](image)

**Figure 4.** Smurf Attack Process (Pengfule, 2016).

3. Findings and Discussions

For further research to test the attack on the actual web server and try the attack through zombie computers that are cloned even more with the type of IP address that is spoofed to disguise the original IP Address.

4. Conclusion

Testing DDoS attacks against the TCP protocol on a target webserver is known to be effective for crippling a website, the amount of bandwidth from DDoS sources has an effect in speeding a target website down. The amount of bandwidth also supports accelerating normal data into data flooding on a website. Indicating the website is really down when we do connection testing, in this case the researchers use testing via the ping command on the Windows CLI and in the browser application. The test results use ping, after DDoS is done on the target website, where the target webserver sends a replay request time out and is checked in the Google Chrome browser, the website cannot be accessed anymore. The average time to access a local web server with 5000 packets is 242.68 seconds, 10000 packets is 310.28 seconds, 20000 packets is 337.4 seconds, 30000 packets are 377.2 seconds, 40000 packets are 398.4 seconds, 50000 packets are 545.4 seconds and 100000 packets are above 600 seconds.
seconds with the condition of the web server will recover after 600 seconds the system recovery process depends on each local web server.

References

[1] Donny K. Sutantyo, Darmawan Utomo. 2016. Implementasi Embedded Web Server Via Modem Berbasisan Mikrokontroler. Jurnal Teknik Elektro Vol. 6, No. 1, Maret 2016. Jurusan Teknik Elektro, Fakultas Teknologi Industri – Universitas Kristen PetraImplementasi Embedded Web Server Via Modem Berbasisan MikrokontrolerFakultas Teknik jurusan Teknik Elektro, Universitas Kristen Satya Wacana, Salatiga.

[2] Geetha, M. K. 2017. Syn Flooding Attack – Identification And Analysis. Department of Computer Science Periyar Arts College Cuddalore, India.

[3] Ikhsanto, M. N. & Nugroho, H. W. 2015. Analisis performa dan desain jaringan komputer menggunakan top-down network desain studi kasus pada CV. Merah putih. Jurnal TIM Darmajaya Vol. 01 No. 01 Mei 2015. Magister Teknik Informatika Institut Bisnis dan Informatika Darmajaya.

[4] Jamaluddin, M, Touqir Anwar, M, K. Saira, M.Y. Wani. 2016. DDoS SYN Flooding; Mitigation and Prevention. International Journal of Scientific & Engineering Research, Volume 5, Issue 12, December-2016.

[5] Kolahi S. S., Alghalbi, A. A, Abdulmohsen F. Alotaibi, Saarim S. Ahmed & Divyesh. 2016. Performance Comparison of Defense Mechanisms Against TCP SYN Flood DDoS Attack. 6th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT). Lad Unitec Institute of Technology, Auckland, New Zealand, 2014 IEEE.

[6] Nakashima, T. & Sueyoshi, T. 2017. Performance Estimation of TCP under SYN Flood Attacks. Department of Information Science, Kyushu Tokai University 9-1-1 Toroku, Kumamoto, Japan Proceedings of the First International Conference on Complex, Intelligent and Softwage Intensive Systems (CISIS07).

[7] Nurahman, D. A. 2017. Penggunaan Kriptografi Dalam Firewall To Firewall System. Jurnal Ilmiah Genesa Bandung.

[8] Nurwenda, S.,Irwan, B. & Irzaman. 2017. Analisis Kelakuan Denial-of-Service attack (DoS attack) pada Jaringan Komputer dengan Pendekatan pada Level Sekuritas. Jurnal IPTEK Ilmiah 2017. Jurusan Teknik informatika, FT, Jl. Dipati Ukur Bandung.

[9] Pengfule, D., Zhihong, T., Hongli, Z., Yong, W. & Liang, Z. 2016. Detection and Defense of SYN Flood Attacks Based on Dual Stack Network Firewall. IEEE First International Conference on Data Science in Cyberspace Sanchuan Harbin Institute of Technology, Harbin.

[10] Prasetyo, H. 2016. Analisa KeamananWeb Server MenggunakanWeb Application Firewall Modsecurity. Jurnal Ilmiah Wacana No,363 2016.

[11] Praveen, N. & Kumar, K. 2016. Software-Defined Networking: Reconfigurable Network Systems in LAN Topology. 2016 3rd International Conference on Advanced Computing and Communication Systems (ICACCS -2016), Jan. 22 – 23, 2016, Coimbatore, INDIA. India.

[12] Ramadhan, H., Saputra, E. & Fronita, M. 2016. Analisis Kualitas Layanan Jaringan InternetMenggunakan Metode RMA (Reliability, MaintainabilityAnd Availability) Dan Qos (Quality Of Service)(Studi Kasus : SMK Negeri 1 Bangkinang). Jurnal Rekayasa Dan Manajemen Sistem Informasi , Vol.2, No 2, Agustus 2016.

[13] S.H.C. Haris, R.B. Ahmad, M.A.H.A. Ghani. 2017. Detecting TCP SYN Flood Attack based onAnomaly Detection. 2017 Second International Conference on Network Applications, Protocols and ServicesSchool of Computer and Communication Engineering,Universiti Malaysia Perlis.