International Journal of Sustainable Applied Sciences (IJSAS)
Vol.1, No.1, 2023: 35-46

The Impact of Smurf Attack on Web Server in Communication Network and its Preventions

Sri Hartanto
Universitas Krisnadwipayana
Corresponding Author: Sri Hartanto; srihartanto@unkris.ac.id

A R T I C L E I N F O

Keywords: DDoS, Smurf Attack, PING, Web Server

Received : 04, May
Revised : 14, June
Accepted: 24, July

©2023 Hartanto: This is an open-access article distributed under the terms of the Creative Commons Atribusi 4.0 Internasional.

A B S T R A C T

The Smurf Attack is a type of Distributed Denial of Service (DDoS). Generally, DDoS attacks that paralyze the Web server computer as the target of the attack so that it cannot provide services. Smurf Attacks send a Gropher Communication Packet request (PING Request) to all addresses in a communication network by broadcast. All computers within the broadcast address will answer the PING request. If a network system has many computers (devices) and PING is broadcast continuously, the network system can be met by responses from PING requests, which results in the bandwidth of the communication network being reduced or even exhausted, so that the communication network becomes slow and paralysed. In order to identify how a Smurf Attack occurs on a Web Server computer, in this research, a simulation of a Smurf Attack is carried out on a Web Server computer in a Local Area Network (LAN) and observes the number of packets received by a Web Server computer to determine the performance of the Web Server computer after receiving a Smurf Attack.

INTRODUCTION

Denial of Service (DoS) attack and Distributed Denial of Service (DDoS) attack have become a major threat to present computer networks (Juwita Siregar). A DoS is an attack which is launched to make networks' and systems' resources unavailable for the legitimate users so that no one else can access it. Hackers can create a situation in which the organizations come to a grinding halt. The main targets of these attacks are web servers, default gateways, personal computers, etc (Iswandi Walad). A DoS attack attempts to disable the network system that is the target of the attack, preventing it from performing its functions. A DoS attack is when an uncontrolled volume of worthless data packets are sent to a Web Server computer. DoS attacks can employ erroneous services on a communication service in order to obstruct other parties from accessing the services provided by a Web Server computer (Meenakshi, S, etc), (Huda Basim Said). A DoS attack is a malicious attempt by a single person or a group of people to disrupt an online service. DoS attacks can be launched against both services, e.g., a web server, and networks, e.g., the network connection to a server. The impact of DoS attacks can vary from minor inconvenience to users of a website, to serious financial losses for companies that rely on their on-line availability to do business (Sri Hartanto).

A DDoS attack is a largescale, coordinated attack on the availability of services of a victim system or network resource, launched indirectly through many compromised computers on the Internet. The services under attack are those of the "primary victim", while the compromised systems used to launch the attack are often called the "secondary victims." The use of secondary victims in performing a DDoS attack provides the attacker with the ability to wage a much larger and more disruptive attack, while making it more difficult to track down the original attacker connections with legitimate clients (Xiapu Luo, etc). DoS attacks are a major cause of incorrect operation in the Internet and are arguably the most serious threat that the Internet community faces today. A DDoS attack is a large-scale, coordinated attack on the availability of services at a victim system or network resource. The DDoS attack is launched by sending an extremely large volume of packets to a target machine through the simultaneous cooperation of a large number of hosts that are distributed throughout the Internet. The attack traffic consumes the bandwidth resources of the network or the computing resource at the target host, so that legitimate requests will be discarded. The impact of these attacks can vary from minor inconvenience to the users of a web site, to serious financial losses to companies that rely on their on-line availability to do business (H.R. Nagesh, etc).

One form of DDoS attack, namely Smurf Attack, can be carried out using IP Spoofing, which is changing the IP Address of the communication device or attacker's computer with the IP Address owned by the communication device or computer target of the attack (victim) so that it is as if the communication device or the attack target computer (victim) is the origin (source) of the PING request to the network system (Saravanan Kumarasamy, etc). Spoofing attacks are used by hackers and unauthorized users to hide their original identity. There are two basic types of spoofing attacks which are used by majority of the

hackers (S Behin Sam, etc). As a result, the communication device or computer of the attack target (victim) will receive many IP request and response data packets. It is conceivable if the spoofed computer has a low-speed connection and the PING is directed to a network system that has many hosts. This can cause paralysis of the communication device or computer of the target of the attack (the victim) as well as the network system that connects the communication device or computer of the target of the attack (the victim) with other computers that receive IP Requests. Ultimately, this can result in a denial of service (Saravanan Kumarasamy, etc).

The smurf attack is a type of ICMP flood, where attackers use ICMP echo request packets directed to IP broadcast addresses from remote locations to generate DoS attacks . There are three entities in these attacks: the attacker, the intermediary, and the victim. First, the attacker sends one ICMP echo request packet to the network broadcast address and the request is forwarded to all the hosts within the intermediary network. Second, all of the hosts within the intermediary network send the ICMP echo replies to flood the victim. Solutions to the smurf attack include disabling the IP-directed broadcast service at the intermediary network. Nowadays, smurf attacks are quite rare in the Internet since defending against such attacks are not difficult (Asma Basharat, etc).

During smurf attack, a huge amount of icmp packets are broadcasted by the attacker to all the subnet of hosts in SDN network. The ip address of particular host is spoofed to become a victim to attack. In our network, the compromised controller will spoof the particular host and flood the flow rules to particular switch in the network. This will affect the network traffic in terms of resource. A threshold value is set for every available switch in the network. The value is set based on icmp packets. If that value exceeds during the attack and it is detected as attack. The window size should be set to be very small or equal to the number of switches in order to provide accurate calculations. The total packet size is divided intoset of icmp packets. It is possible to see its value during detection when a large number of packets are attacking one host or a subnet of hosts (Bima Putra Firdaus, etc).

This research is focused on identifying how Smurf Attack occurs on a Web Server computer. In this research, a simulation of Smurf Attacks on a Web Server computer from three client computers in a network type Local Area Network (LAN) is carried out. The Web Server computer and the three client computers in the LAN network use the Linux OS. Furthermore, every hour, the number of packets received by the Web Server computer is observed to determine the performance of the Web Server computer after receiving a Smurf Attack.

LITERATURE REVIEW

DoS attacks are a form of threat in communication networks. DoS attack is an attempt to paralyze the network system that is the target of the attack so that the network system cannot provide its services, or the level of service quality can decrease drastically in a short time. (Xiapu Luo, etc) A traditional DoS attack is an attack that floods (DoS based) a server with uncontrollable

amounts of useless packets. Furthermore, several subsequent lower-speed DoS attacks were delivered. These new attacks can attack TCP streams more effectively than traditional attacks.(H.R. Nagesh, etc)

DoS Attack is an attack using an inappropriate service by a person or group of people on a service that is connected to active communication with the aim of disturbing other parties who enjoy the services provided by the server. Attacks in the form of DoS can be launched to all services, such as a Web Server that provides service pages in communications, and networks, such as a network connected to a server. The consequences of a DoS attack can vary, from the smallest thing, such as inconvenience received by a visitor (user) of a service page on the website, to serious matters, such as financial losses. a company entrusted with the availability of online financial data services on a website to carry out a business transaction. DoS attacks can be divided into several types, namely TCP SYN Flood Attack, UDP Flood Attack, Ping of Death Attack, Smurf Attack, Teardrop Attack, Bonk Attack, and Land And Latierra Attack. (Saravanan Kumarasamy, etc)

DDoS attacks is a DoS attack on a larger scale, where attacks are carried out in a coordinated manner using the availability of services found on the victim's network system. A DDoS attack is launched by sending a packet with an extremely large volume to the target machine through simultaneous cooperation of a number of hosts spread across a communication network. Such a large attack traffic will consume network bandwidth resources or computing resources on the attack target host, so that actual or legitimate connection requests cannot be serviced (discarded), as shown in Figure 1 below.

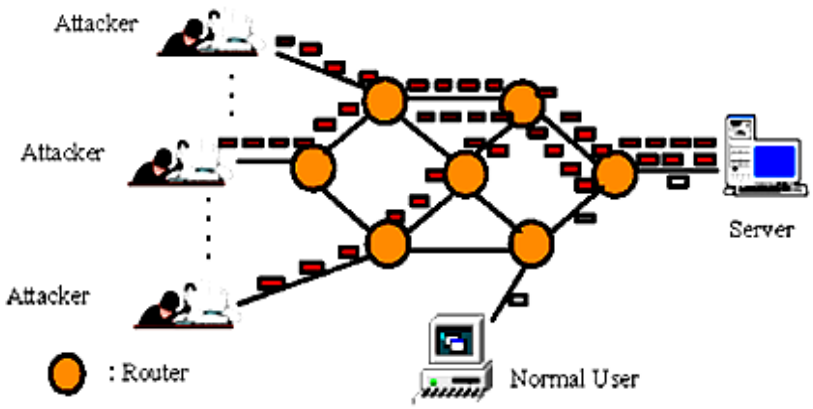


Figure 1. Distributed Denial of Service Attack (Meenakshi, S, etc)

The consequences of DDoS attacks can cause inconvenience to website visitors on a small scale, to a larger scale in the form of loss of financial data entrusted to online services through communication networks. DDoS attacks appear as a way that is commonly used to shut down an organization's activities on the internet and produce financial losses at the same time. In a DDoS attack, an enemy tries to disconnect one of the elements (devices) in a communication network by breaking the connection (link) or node of the communication network. (S Behin Sam, etc).

DDoS attacks as attacks sent from multiple source systems. If an attacker can manage a large number of users (users) to connect or connect to the same website at the same time, a Web Server is often configured to pass client computer connections up to the maximum number, resulting in the victim's Web Server computer rejecting connections from the next client computer. . of course, this will cause a denial of service. This method is a commonly used method by attackers.(H.R. Nagesh, etc)

So far, the attacker does not own the computers used to carry out the DDoS attack. The actual owners (actual owners) often don't care about the system they own, so it can be used as an intermediary in launching a DDoS attack. Attackers generally deploy Trojan Horses which consist of some malicious code that can allow an attacker to control the system they have. The malicious code can also be considered as a backdoor. Once the Trojan Horse is run, they will use the email to inform the attacker that the system can be controlled remotely (remotely controlled). The attacker will install the tools (tools) needed to perform an attack. Once an attacker can control the system properly, which is sometimes the system that has been controlled is called a zombie or slaves, then the attacker will easily launch an attack.(Asma Basharat, etc).

One form of DDoS attack, namely Smurf Attack. Smurf Attack is an attack that uses a Gropher Communication Packet request (PING Request) to all addresses on a communication network by broadcast. All computers (devices) within the broadcast address will respond to the PING request. If a network system has many computers (devices) and broadcast PINGs are carried out continuously, the network system can be met with responses from these PING requests. This will result in the bandwidth owned by the network being reduced, so that the network becomes slow or even paralyzed. (H.R. Nagesh, etc).

Smurf attacks are usually carried out using IP Spoofing, which is changing the IP address on the attacker's communication device or computer with the IP address that belongs to the attack target's communication device or computer (victim), so that it appears as if the communication device or attack target's computer (victim) is the origin. (source) PING requests to network systems. By using IP spoofing, the response from the PING is then addressed to the computer whose IP has been spoofed. As a result, the communication device or computer that is the target of the attack (victim) will receive many IP request response data packets. Look at Figure 2 below:

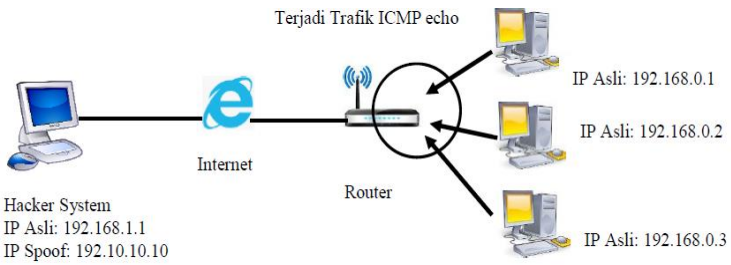


Figure 2. Example of a Smurf Attack (Iswandi Walad)

It can imagine if the spoofed computer has a low-speed connection and the PING is directed to a network system that has many hosts. This can cause paralysis of the communication device or computer that is the target of the attack (the victim) and the network system that connects the communication device or computer that is the target of the attack (the victim) with other computers that receive IP requests (IP Requests). In the end, this can result in a denial of service. (Harshita)

METHODOLOGY

In this research, an observation was made using the simulation method on a Local Area Network (LAN) where there is one Web Server computer and three client computers. The flowchart of this research can be seen in Figure 3.

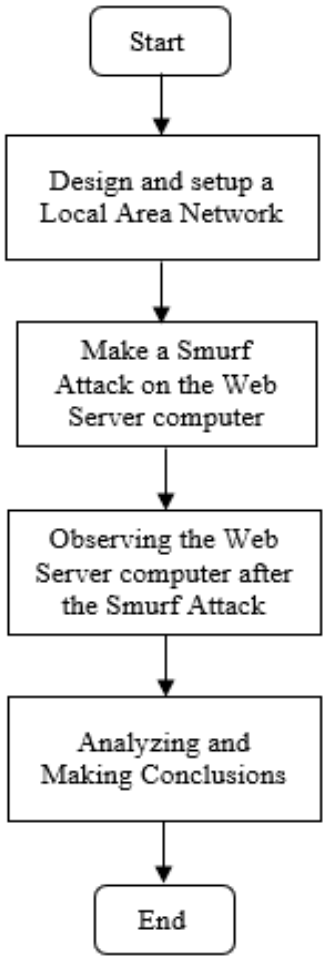


Figure 3. Flowchart of Research

This research begins with designing and setting up a network type Local Area Network (LAN), where there is one server computer and three client computers connected to a star topology via an IP switch using a UTP cable. All client computers use Kali Linux OS, and server computers use Ubuntu Server 18.04 OS. Each computer can be connected to each other and exchange data, as shown in Figure 4 below.

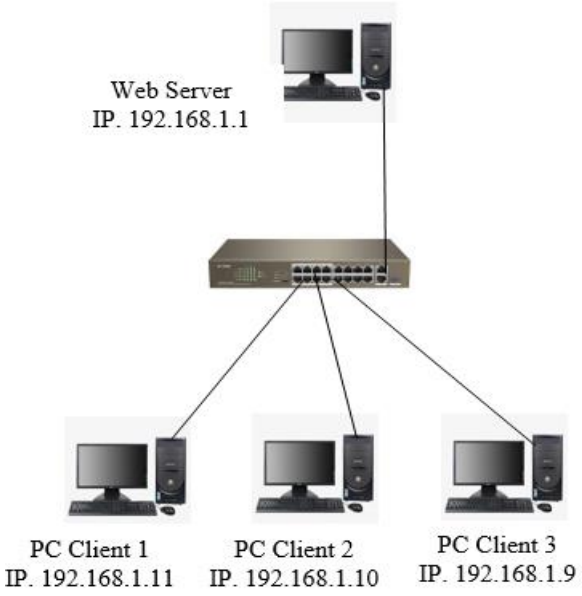


Figure 4. LAN Network Configuration

Next, the Web Server computer OS was installed using the Ubuntu Server 18.04 OS and the client computer with the Kali Linux OS. Installation of OS Ubuntu Server 18.04 and OS Kali Linux can be done by following the instructions that have been presented in the form of an easy-to-understand GUI. After the installation is complete, proceed with the steps to build a Web Server based on Ubuntu Server 18.04 OS on a Web Server computer, namely:

1. Run the following command to update the package: #sudo apt-get update
2. Install wget with the command: #sudo apt-get install wget -y
3. Run the following command to install GPGL: #sudo apt-get install gpg
4. Run the following command to install Apache: #apt-get install apache2 -y
5. Using the command to test Apache function: # status apache2 systemctl
6. Install PHP with the command:
   #sudo apt-get install phpPHP-cgi php-mysqli php-pear php-mbstring php-gettext libapache2-mod-php php-common php-phpseclib php-mysql-y
7. Verify the PHP installation with the command: # php –version
8. Run the following command to install and configure MariaDB:
   #sudo apt install mariadb-server mariadb-client mariadb-client-y
9. Run the following command to validate MariaDB installation:
   # mariadb systemctl statusConfigure MariaDB with the command: # sudo mysql_secure_installation
10. Install phpMyadmin with the command:
    https://www.phpmyadmin.net/downloads/phpMyAdmin-latest-all-languages.tar.gz
11. Checking the phpMyAdmin GPG key with the command:
    #wget-P http://files.phpmyadmin.net/phpmyadmin.keyring
12. Access the Downloads directory and import the keyring with the command:

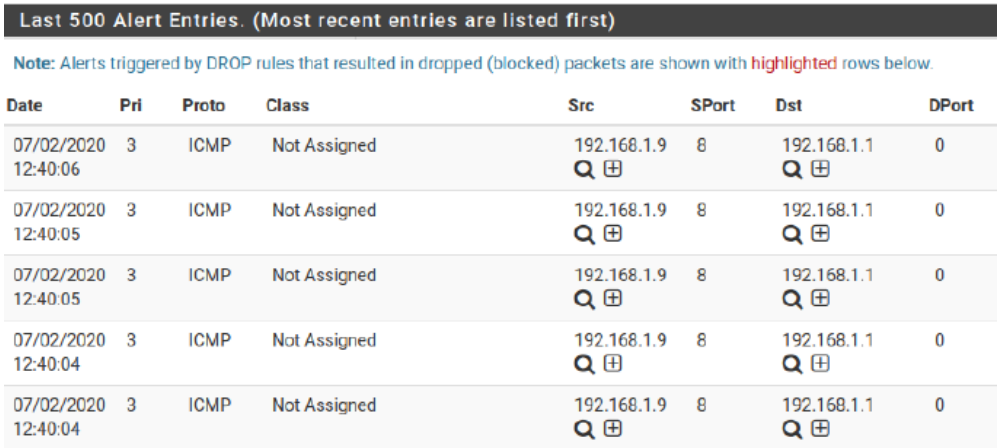
gpg--import phpmyadmin.keyring

13. Configure phpMyadmin with the command:
    mkdir /var/www/html/phpmyadmin sudo
14. Accessing phpMyAdmin from the browser with the command:
    # localhost/phpmyadmin

After building a Web Server based on Ubuntu Server 18.04 OS, each client computer simulates a DoS attack with hping3 on the Web Server computer, after first installing hping 3 on each client computer by typing the command: #apt-get install hping3 sudo. Next, client computer 1 (IP 192.168.1.11) sends data packets on behalf of client computer 3 (IP 192.168.1.9) to the Web Server computer (IP 192.168.1.1) by typing the command: hping3--icmp---flood –c 1000—spoof192.168.1.9 192.168.1.255.

RESULTS

In Figure 5, the results of the alert for the Smurf Attack are shown. The security feature that is activated at this stage is the detection mode. The detection mode only displays a warning when large data packets are received by the Web Server computer. The results of the detected attack alerts are on the ICMP protocol with the description of Smurf Attack DOS. This attack comes from the source of the attack (IP source) to the target of the attack (IP destination).



Last 500 Alert Entries. (Most recent entries are listed first)

Note: Alerts triggered by DROP rules that resulted in dropped (blocked) packets are shown with highlighted rows below.

Date	Pri	Proto	Class	Src	SPort	Dst	DPort
07/02/2020 12:40:06	3	ICMP	Not Assigned	192.168.1.9	8	192.168.1.1	0
07/02/2020 12:40:05	3	ICMP	Not Assigned	192.168.1.9	8	192.168.1.1	0
07/02/2020 12:40:05	3	ICMP	Not Assigned	192.168.1.9	8	192.168.1.1	0
07/02/2020 12:40:04	3	ICMP	Not Assigned	192.168.1.9	8	192.168.1.1	0
07/02/2020 12:40:04	3	ICMP	Not Assigned	192.168.1.9	8	192.168.1.1	0

Figure 5. Display ALERT Log View

By observing the ALERT Log View on the snort tool on the Web Server computer, the IP Address and the number of data packets sent from the client computer carrying out the Smurf Attack can be observed. The observed data is the data obtained by the IDS snort tool in the form of ICMP packets received by the Web Server computer. During the establishment of a TCP/IP connection between the Web Server computer and the client, more and more ICMP packets are sent, which can cause a "buildup of data packets" on the Web Server computer, resulting in the Web Server computer failing to execute ICMP packets received later and being unable to respond to requests on the Internet beyond the predetermined time limit.

Observations are made every hour for 24 hours to determine the number of ICMP data packets received by the Web Server, where packets containing large amounts of ICMP are displayed visually in the ALERT Log View. From the observations of data packets received by the Web Server computer displayed on the ALERT Log View in the snort tool, it is known that the range of data packets received on the Web Server computer is from a minimum of 856 data packets in the second hour to a maximum of 998 data packets in the sixteenth hour. The number of packets received by the Web Server computer from the three client computers is observed hourly for 24 hours and is shown in Table 1 below:

Table 1. Results of Observation of Data Packages Received by the Web Server Computer

Observation Hours	Number of Packages		
	PC Client 1	PC Client 2	PC Client 3
1	40	45	887
2	56	65	856
3	67	112	889
4	89	321	978
5	23	125	877
6	89	24	876
7	110	55	890
8	23	68	976
9	78	98	967
10	45	45	945
11	65	23	934
12	112	89	956
13	321	110	923
14	125	23	911
15	24	78	960
16	55	45	998
17	68	65	970
18	98	112	987
19	80	23	945
20	98	98	965
21	76	76	934
22	67	67	956
23	34	34	923
24	56	56	890

DISCUSSION

It is clearly seen from Table 1, that client computer 3 (PC3), which is used by client computer 1 (PC1) to launch a Smurf Attack in a DDoS attack scheme, sends a very large number of data packets. and not normal. Figure 6 clearly shows a graph of the number of data packets sent from each client computer every hour for 24 hours of observation.

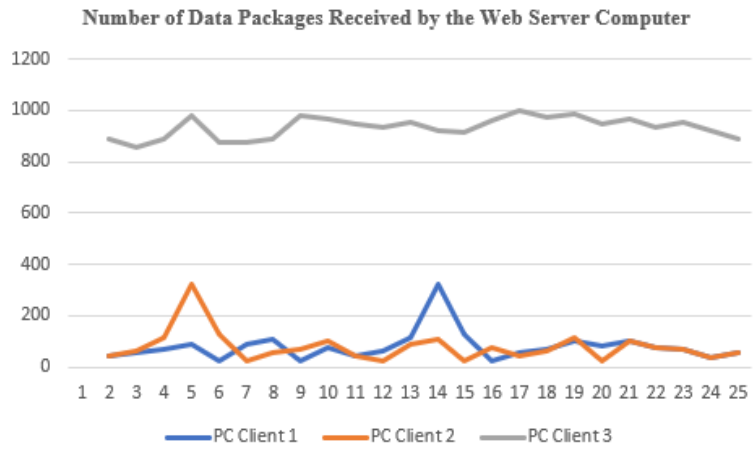


Figure 6. Number of Data Packages Received by the Web Server Computer

Overall, the number of ICMP data packets received by the Web Server computer for 24 hours from the three client computers in a simulated LAN network is 26149 data packets, and the total number of data packets received by the Web Server computer every hour from the three client computers is shown in Figure 7 below:

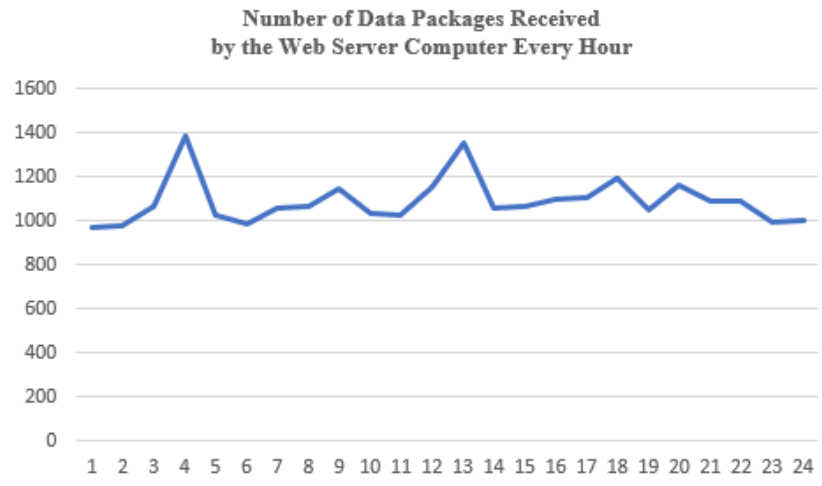


Figure 7. Number of Data Packages Received by the Web Server Computer Every Hour

To prevent Smurf Attacks, existing routers need to be configured to deny (deny) data traffic that broadcasts IP Addresses on managed communication

network systems, where attacks are likely to originate from outside networks. In almost all cases, the functionality of broadcast IP is not required. Then, the Web Server computer needs to be configured via kernel variables not to repeat (not reply) data packets to the sender of the packet that propagates the IP Address. Before installing snort, make sure the support package has been installed by entering a command that can run the snort support function automatically. The command is as follows: #apt-get install build-essential –y sudo.

By default, Snort works as an intrusion detection system. Therefore, several installation packages must be added in order to function as an intrusion detection and prevention system. To run Snort in intrusion prevention system mode, you need to add the following command:
#bison flex
#libpcap-dev libpcre3-dev libdumbnet-dev bison flex -yang
To set the snort installer to read the source code, type the command:
#./configure --enable-sourcefire
To configure snort, then type the command:
#sudo /etc/snort.conf and enter the ip to be protected
#Ipvar HOME_NET 192.168.1.1

After configuring the IP to be protected, the next step is to create rules as a form of detecting any ping attempts by executing commands on the Linux terminal.
#sudo gedit /etc/snort/sid--msg.map
#1 || 10000001 || 001 || icmp--event || 0 || There is a Ping trial || url,tools.ietf.org/html/rfc792

Next, create DDoS rules as a form of detecting any DDoS attacks that try to attack the server, it is found that they make rules with the command on the Linux terminal as follows:
#gedit /etc/snort/rules/local.rules
#alert icmp any any alert icmp any any --> $HOME_NET any (msg:"anyone tried > $HOME_NET any (msg:"anyone tried to DDoS"; GID:1; sid:10000001; rev:001; classtype :icmpdo DDoS"; GID:1; sid:10000001; rev:001; classtype:icmp--event;)event;)

CONCLUSIONS AND RECOMMENDATIONS

From this research, it can be concluded that:

1. The data packets received by the Web Server computer regardless of the source of the data packets are in the range of the lowest 972 data packets in the first hour and the highest 1388 data packets in the fourth hour.
2. Data packets sent from PC Client 3 as an intermediary for attacks whose source of attack originates from client computer 1 are monitored on the Web Server computer in the range of the lowest 856 data packets in the second hour to the highest 998 data packets in the sixteenth hour.
3. Prevention of Smurf Attacks can be done by creating DDoS rules as a form of detecting DDoS attacks.

REFERENCES

Junita Siregar, "Analisis Explotasi Keamanan Web Denial of Service Attack,". Journal ComTech, vol.4, no.2, pp. 1199-120, 2013.

Iswandi Walad, "Analisis Denial of Service Attack Pada Sistem Keamanan Web", Tesis Magister, Universitas Sumatera Utara, Indonesia, 2020.

Meenakshi, S & S.K Srivatsa, "A Distributed Framework with less False Positive Ratio Against Distributed Denial of Service Attack," Information Technolo gy Journal, vol.6, no.8, pp. 1139-1145, 2007.

Huda Basim Said, Ahmed Khaleel, "An Improved Strategy for Detection and Prevention IP Spoofing Attack," International Journal of Computer Applic ations, vol.182, no.9, pp.0975-8887, 2018.

Sri Hartanto, "Pencegahan dan Pendeteksian Serangan Penolakan Layanan (Denial of Service Attack) Dalam Jaringan Komunikasi," Jurnal Ilmiah Elektrokrisna, vol.1, no.3, pp. 133-144, 2013.

Xiapu Luo, Edmond W.W.Chan, and Rocky K.C. Chang, "Detecting Pulsing Denial of Service Attacks with Nondeterministic Attack Intervals," EURASIP Journal on Aadvances in Signal Processing, Article ID 256821, pp. 1-13, 2009.

H.R. Nagesh, and Chandra Sekaran, "Design and Development of Proactive Models for Mitigating Denial of Service and Distributed Denial of Service Attacks," International Journal of Computer Science and Network Security (IJCSNS), vol.7, no.7, pp. 167-175, 2007.

Saravanan Kumarasamy & Dr.R.Asokan, "Distributed Denial of Service (DDOS) Attacks Detection Mechanism," International Journal of Computer Science, Engineering and Information Technology (IJCSEIT), vol.1, no.5, pp. 39-48, 2011.

S Behin Sam, S Sujatha, A Kannan, and P Vivekanandan, "Network Topology Against Distributed Denial of Service Attacks," Information Technology Journal, vol.5, no.3, pp. 489-493, 2006.

Asma Basharat, Rabia Sirhindi, Ahmad Raza Cheema, and Imtiaz Khokhar, "A Novel Solution for IP Spoofing Attacks," Proceeding of 6th WSEAS International Conference on Information Security and Privacy", pp. 107-110, Tenerife, Spain, 2007.

Bima Putra Firdaus & I Made Suartana, "Implementasi Keamanan Jaringan Intrusion Detection/Prevention System Menggunakan PFSense," Jurnal Manajemen Informatika, vol.11, no.1, pp. 40-47, 2020.

Harshita, "Detection and Prevention of ICMP Flood DDOS Attack," International Journal of New Technology and Research (IJNTR), vol.3, no.3, pp. 63-69, 2017.