Network Forensic on Web-based Applications using Network Forensic Development Life Cycle Method

Sukmawati Lasaharu
Department of Informatics
Universitas Ahmad Dahlan
Yogyakarta of Indonesia

Imam Riadi
Department of Information System
Universitas Ahmad Dahlan
Yogyakarta of Indonesia

ABSTRACT
It is important to note computer network security. At any point, a web server can be attacked. There are many types of attacks that can be carried out by attackers. One type of attack that is often carried out is a Distributed Denisal of Service (DDOS) attack. Distributed Denial of Service (DDOS) attacks are one type of attack that attackers frequently use to increase traffic to the point where the server cannot handle client requests and may even cause the server to fail. To limit the likelihood of an attack, a network security system able to detect attacks is required. Snort is a software program that is capable of detecting an attack in real time by executing a rule that produces a log file containing information about network activity. Additionally, it is used to conduct network forensic analysis using the Network Forensics Development Life Cycle (NFDLC) method, which is a branch of digital forensic science concerned with the steps necessary to discover evidence of attacks originating from log files. The analysis method is comprised of the following stages: Initiations, Acquisition, Implementation, Operations, and Disposition. According to the findings of the research, Snort's Intrusion Detection System (IDS) is capable of detecting DDOS attacks on web servers. Based on the analysis of the log files using wireshark, there are 3 IP addresses, who tried to commit crimes against the web server. From the results of the DDOS attack analysis, it can be used as digital evidence from the results of network forensic investigations.

Keywords
Network Forensics, DDOS attack, IDS, Snort, Web Server, NFDLC

1. INTRODUCTION
The development of information technology, particularly computer networks and the internet, is accelerating every year. The requirement for humans to communicate and exchange data rapidly and practically necessitates the use of computer networks. However, behind all of these technological developments, cybercrime on computer networks is increasing, making data or information management insecure. There are many attack types that attackers might use to gain access to the target computer system [1]. Typically, the attacker's target is a web server. A DDOS attack is a type of attack on a computer network that disrupts the server by repeatedly sending requests to the server, increasing traffic to the point where the server cannot manage client requests and may possibly damage the server [2].

Network forensics is a subset of digital forensics. Where this procedure records and analyzes many traffic activities that occur on the web server network. This aims to ascertain the attacker's IP address and the nature of the attack on a web server [3]. Intrusion Detection System (IDS) is a process that monitors network traffic for suspicious behavior. Snort is one of the IDS software that can be employed. Snort is free and open-source software that detects certain attacks against web servers and outputs data in the format required by the detection system. Snort is designed to scan all network traffic in order to sniff for and detect network intrusions [4].

In network forensic research, this web-based application is devoted to detecting attacks on web servers on the network where attackers send attacks to disrupt or stop a service. The attack that will be used in this research is a Distributed Denial of Service (DOS) or Denial of Service (DOS) attack [5].

2. STUDY LITERATURE
2.1 Computer Network
A computer network is a connection between two or more computers that is used to exchange or share data. Client-server architecture is used in computer networks, and the purpose of a computer network in this case is to be able to request and provide services to clients. The client is the party that requests or receives the service, whereas the server is the party that provides or sends the service.[6]

2.2 Computer Network Security
Network security is a process that protects a computer network system from unauthorized users. A secure system is one that is protected against all types of attacks that attempt to gain access to the system in a variety of methods with the intent of stealing or manipulating data [7]. Computer network security is to anticipate and resolve issues that could disrupt ongoing activities. Network security is composed of three concepts: danger level, threat, and system fragility. [8]

2.3 Network Forensics
Network forensics is defined as capturing, recording, and analyzing network events to determine the source of security attacks or other problematic incidents. Network forensics, in other terms, is the process of capturing, recording, and analyzing network traffic [9]. The network data is collected from existing network security equipment, such as firewalls or detection systems, and is analyzed for attack characterization and tracing back to the attacker. In many circumstances, crimes that do not break network security policies can nonetheless be prosecuted legally. Such crimes can only be prosecuted through network forensics**.** [10]

2.4 Web Server
The web server's work is to respond to client requests and can send or respond to client requests. When a browser (client) requests web page data from the server, the browser's request is packaged in TCP and then delivered to the next protocol address, which is either HTTP or HTTPS [11]. Additionally, the web server will search for the requested data on the server computer. If data is discovered, it is packaged by the web

server via TCP, and the web server responds by transmitting the discovered results to the browser [12].

2.5 IDS Snort

IDS Snort is a security alarm for a detection system that monitors network traffic system disruption caused by intruders. The IDS snort is used to identify suspicious behavior; when this occurs, the IDS notifies the system or network administration[13].

3. METHOD

3.1 Attack Simulation

Attack simulation is a system simulation stage for implementing network forensics. The purpose of this case simulation is to find out whether the Snort IDS that has been installed on the web server is able to detect an attack or not. In Figure 1, the following is a simulation of an attack case on a web server.

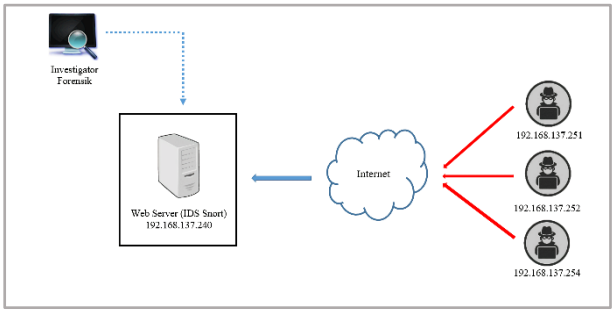

Figure 1.Attack Simulation on Web Server

An attacker tries to carry out a Distributed Denial of Service (DDoS) attack with Low Orbit Ion Cannon (LOIC) and Command Prompt (CMD) to the target web server via the internet and is captured or detected by IDS snort. Furthermore, all attack activity is recorded and stored in the form of a snort log file. The results of the log file containing the attack activity will be analyzed by investigators as evidence of crimes against the network on the web server.

3.2 Research Stages

The Network Forensics Development Life Cycle (NFDLC) method was utilized in this study to analyze the Distributed Denial of Service (DDOS) attack on the web server [14]. The method is illustrated in Figure 2.

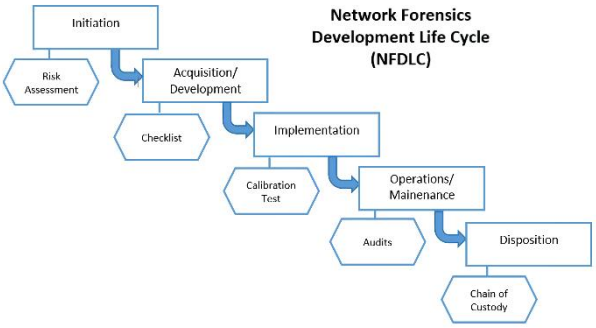

Figure 2. NFDLC Method

The Network Forensic Development Life Cycle (NFDLC) method is depicted in Figure 2 [15]. Each stage can be explained as follows:

1) *Initiation*
Initiation is aimed at determining network aspects of digital forensic protection that will be analyzed.
2) *Acquisition/Development* Acquisition/Development is the process of building or installing a system that contains evidence rules in the system, as well as verifying and calibrating the system.
3) *Implementation/Deployment*
Implementation is a basic test of the platform by verifying the network mechanism.
4) *Operations/Mainenance*
Operations/Maintenance is the process of checking, verifying and measuring the use of the network as digital evidence.
5) *Disposition*
Disposition is carrying out procedures to secure evidence in network forensics.

4. RESULT AND DISCUSSION

4.1 Initiation

The initiation stage is the first stage in the process of searching for and collecting the data required for this study, as well as documenting evidence. The device studied as evidence of network forensics is a web server with IDS Snort installed. The results of the IDS Snort detection will be reviewed, and then log data in the form of IP addresses will be collected [16].

4.1.1 System Requirements Analysis

In the analysis of system requirements, of course, tools and materials are needed to conduct research, as for the tools and materials needed for software used for forensic needs in this study, there are several components as shown in table 1 following Software Requirements.

Table 1. Software Requirements

No	Software	Description
1	OS Windows 10	Test Container
2	OS Windows 7	Attacker 1
3	OS Windows 7	Attacker 2
4	OS Windows 7	Attacker 3
5	Ubuntu Server 20.04	Object of research
6	Kali Linux	Client
7	Virtualbox	Virtualization Device
8	Wireshark	Analysis Tools
9	IDS Snort	Monitoring Tools
10	Low Orbit Ion Cannon (LOIC)	Attack Tool
11	Command Prompt (CMD)	Attack Tool

From Table 1 above, it can be explained that in this study 1 PC was available as a testing container. On the PC, virtualbox is installed, which is a virtualization device where in this virtualbox several software are installed, namely 3 windows 7 as attacker 1, 2 and 3, each of which has LOIC installed in it as attack software and 1 time linux as a client and Ubuntu server 20.04 as a web the server that became the object of the attack and on this server there is IDS snort as a monitoring tool and also wireshark as analysis software.

4.1.2 System planning

System design itself is the design of a system that contains the operating steps in the system installation process. The purpose of system design is to provide a clear picture and complete design. In Figure 4.2 the following is a flow diagram of system design to case simulation or system testing [17].

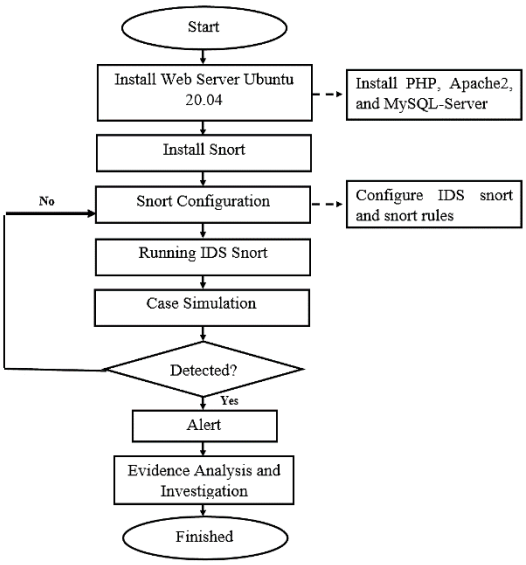

Figure 3. System Design Flowchart

1) Start, making preparations to conduct research
2) Installing the Ubuntu 20.04 web server as the object of research, then building a web server by installing several software namely PHP, Apache, and MySQL-Server.
3) Configuring the IP address is setting to determine the IP address on the web server
4) Install snort to detect Distributed Denial of Service (DDoS) attacks on web server networks
5) Snort configuration is to determine the IP address that will be monitored by snort and also configure the snort rule to detect any DDoS attacks according to the rules that have been made.
6) Running IDS Snort, to be ready to detect any attacks that occur on the web server
7) Perform system testing to find out whether IDS snort can work as expected, namely detecting DDoS attacks
8) Detected? This is a condition, where if snort can detect a DDoS attack according to the rules that have been made on the web server, then proceed to the next stage where there is an alert. If no attack is detected, it will repeat itself.
9) Alert, is a warning in case of a DDoS attack.
10) Perform analysis and investigation on log files to obtain evidence of an attack that occurred on the web server.

4.2 Acquisition

At this stage, the process of installing and configuring the research system will begin. The system's installation can be summarized as follows:

4.2.1 Install Ubuntu Server 20.04

In general, Ubuntu can be installed using a live CD, a USB drive, or a Virtual Machine. The researcher installs Ubuntu 20.04 on a Virtual Machine (VM) as a server machine. After installing Ubuntu, install the necessary web servers such as Php, Apache2, and MySQL-Server with the command #apt-get install php to install php, #apt-get install apache2 to install apache2, and #apt-get install mysql-server to install server [18].

4.2.2 Install Snort

Snort installation with the command #apt-get install snort or you can download the program directly on the official snort website, namely www.snort.org. This study used snort version 2.9.7.0 and the snort rule with the same version [19].

4.2.3 Snort Configuration

The snort configuration file is located in the /etc/snort/snort.conf directory and can be accessed through the nano /etc/snort/snort.conf command from the Ubuntu server terminal. The main setup required is for the network to be configured by inputting the IP Address. As illustrated in Figure 4, network settings on Snort [20].

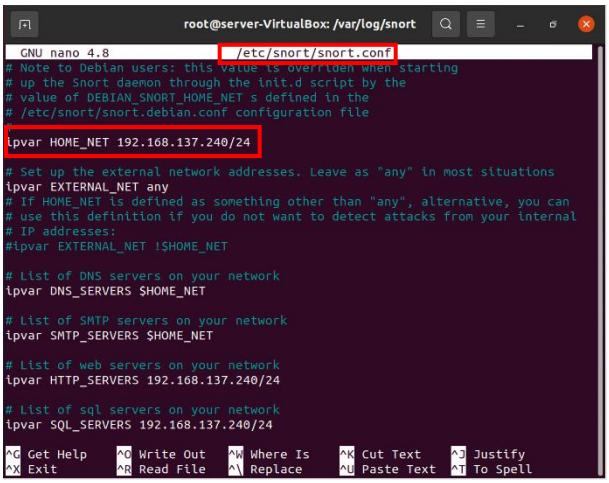

Figure 4. Snort Configuration

Figure 4 shows the #IpVar HOME_NET line 192.168.137.240/24 is the IP address that will be monitored by IDS snort.

4.2.4 Snort Rule Configuration

Configuring the rules in this study is to download the snort package. The rules files can be found in the /etc/snort/rules directory [21]. The settings needed in the research are configuring the snort rules by inputting the command nano /etc/snort/rules/local.rules on the ubuntu linux terminal. The configuration is shown as in Figure 5.

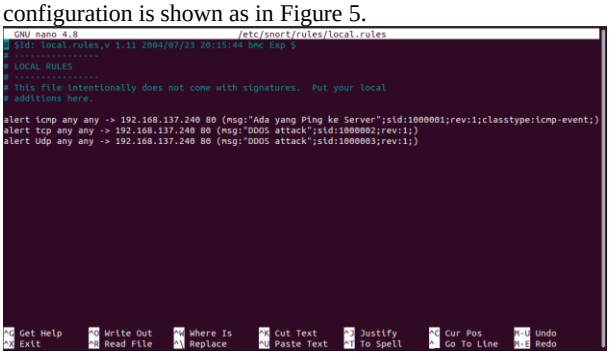

Figure 5.Snort Rule Configuration

From Figure 4 the configuration of the snort rules above is made 3 rules to be able to detect attacks that occur on the web server [22]. The explanation of the command is as follows:

- alert is a warning sign
- icmp is a type of transport protocol
- any any is the originating host that passes through any port
- -> is the flow from the originating host to the destination host
- 192.168.137.240 80 is the destination host passing through the destination port

- (msg: "Ping Attack"; is a message that is received when an event occurs
- Sid: 1000001; is the rule id snort
- Rev:1; is the 1st rule revision
- Classtype:icmp-event;) is to classify attacks

4.3 Implementation

Implementation is a system testing simulation process to determine whether the system has been installed and configured appropriately. This stage involves the testing of Distributed Denial of Service (DDOS) attacks. DDOS attack testing was conducted using two (2) software: LOIC (Low Orbit Ion Canon) and CMD (*Command Promt*).

4.3.1 DDOS Attack Simulation with LOIC

The attack testing process begins by entering the target IP address, 192.168.137.240, in the select your target section, then pressing the lock on button, then determining the target port, which is 80, selecting the target TCP/UDP protocol, specifying the number of threads to send, which is 10, and the rate at which packets are delivered, which is faster. Figure 6 depicts the attack process [23].

Figure 6. DDOS Attack Simulation with LOIC

After completing all configurations, initiate the attack by pressing the DDOS start button, which initiates the attack, and the DDOS stop button, which terminates the attack.

4.3.2 DDOS Attack Simulation with CMD

Testing the next DDOS attack is to use CMD. The attacker conducts this attack by sending ICMP attack packets. Internet Control Message Protocol (ICMP) records information about an attacker's attacks. When an attacker's IP sends an ICMP echo request to an IP server, the IP server responds with an ICMP echo reply. Figure 7 illustrates the ICMP attack using CMD.

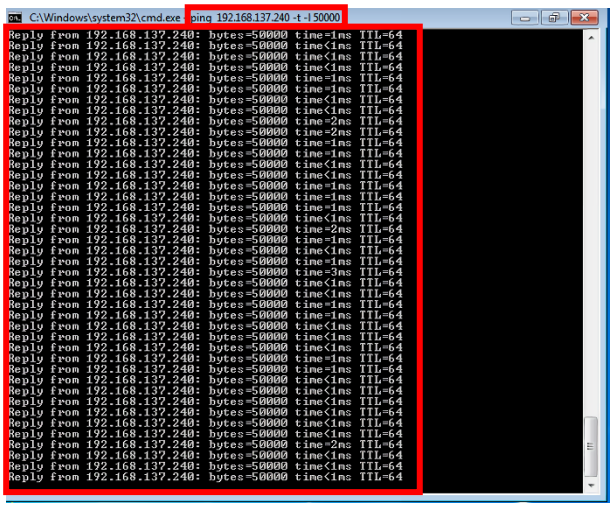

Figure 7. DDOS Attack Simulation with*Command Promt*

From Figure 7 above an attacker tries to carry out an attack by inputting the command ping 192.168.137.240 –t –l 50000. Where 192.168.137.240 is the IP address of the target or web server that will be attacked, -t is a command to perform recursive requests to the server, -l is the command to request the size request from the server and 50000 is the size sent [24].

4.3.3 Detect DDoS Attack

In this study, there are ways how IDS Snort works. In Figure 8 the following shows the simulation stages of detecting Distributed Denial of Service (DDoS) attacks on a web server.

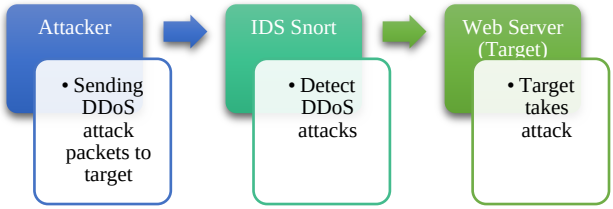

Figure 8. *Detect DDoS Attack*

4.3.4 Flowchart of Evidence Analysis

In this study, what will be analyzed is the snort log file using wireshark software. The log file contains the history of the attack, which will be investigated in detail to find the required information. The process can be made in the form of a flow chart as shown in Figure 9 Flowchart of Evidence Analysis.

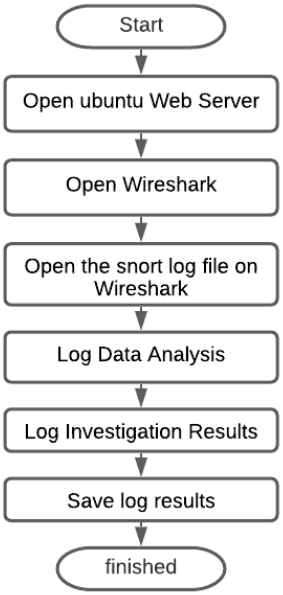

Figure 9. Flowchart Analysis and Investigation

4.4 Operations

Operations is the process of checking and analyzing network traffic on a web server in order to extract evidence from the snort log. The log file is checked using the results of the IDS snort recording inspection, which is collected using a packet sniffer contained on the IDS snort server [25].

Log file data that has been successfully checked will then be retrieved in the default form of p.cap (packet capture). After that all log file data will be analyzed using wireshark.

From the attack simulation that has been sent by the attacker to the web server, the IDS Snort traffic interface will be seen using the rules that have been created. The results of the detection of the attack simulation that occurred can be seen in Figure 10.

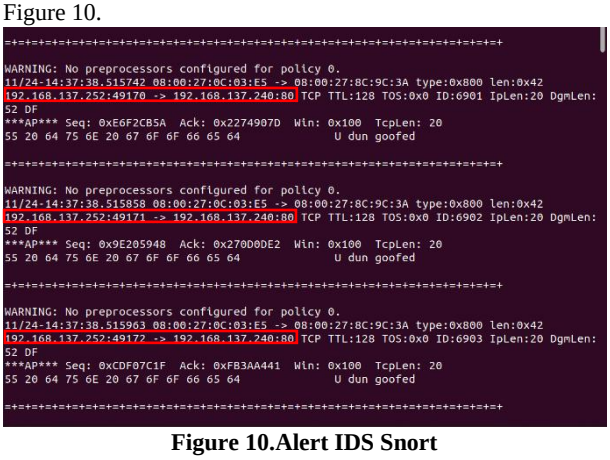

Figure 10.Alert IDS Snort

From Figure 10 above, it can be seen that IDS Snort is able to detect Distributed Denial of Service (DDOS) attacks that occur on the web server, and saves them into the Snort log file so that from these results the next step can be carried out the analysis process using an analytical tool, namely Wireshark.

System monitoring is also performed on the Ubuntu Web Server to ascertain the conditions prior to and following an assault on the web server. The monitoring system's state during regular operation or prior to an attack is demonstrated in Figure 11.

Figure 11. Monitoring System Before the Attack

According to Figure 11, the condition of the monitoring system before to the web server attack indicates that the CPU load is still below the average of 22.6%(percent), while memory usage is 1.6 GiB. (55.7%).

After the DDOS attack began, the CPU and memory usage of the attacker's PC increased. The condition of the monitoring system can be seen in Figure 12.

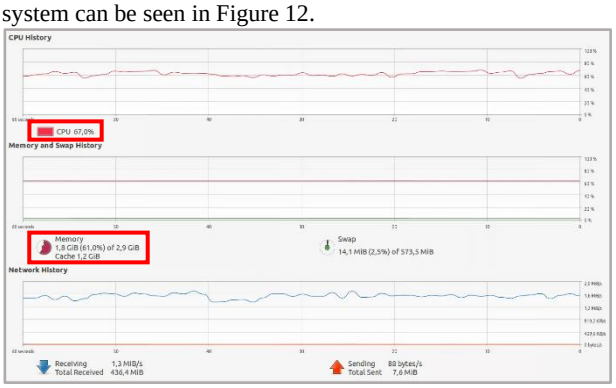

Figure 12. Monitoring System After an Attack

According to Figure 12, the monitoring system's condition following the attack was as follows: the CPU load, which was already above average, climbed substantially to 67.0%, while memory usage was 1.8 GiB. (61.0%).This indicates that the DDoS attack has managed to consume resources on the Ubuntu web server [26].

After seeing the monitoring system on the Ubuntu server, the log file is captured in real time for wireshark analysis. The traffic from the snort log file is presented via wireshark. After opening the snort log file using wireshark, the first step is to review the snort enpoint statistics to determine the total number of attack packets contained in the IDS snort log file during the attack simulation. Figure 13 illustrates the endpoint statistical results.

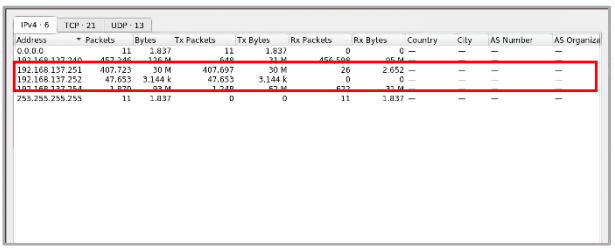

Figure 13. EndpointSnort Statistics

From Figure 13 Endpoint Snort statistics above, there are 3 IP addresses that performed DDOS attacks, each of which is 192.168.137.251, 192.168.137.252, and 192.168.137.254.

In the view of the snort traffic log file that has been opened with wireshark, then one line can be selected to analyze each part of the frame that represents a packet frame in a DDOS attack to obtain evidence in the form of when the attack occurred, the IP address of attacker, port and protocol type. The results of the analysis on the frame can be seen as shown in Figure 14.

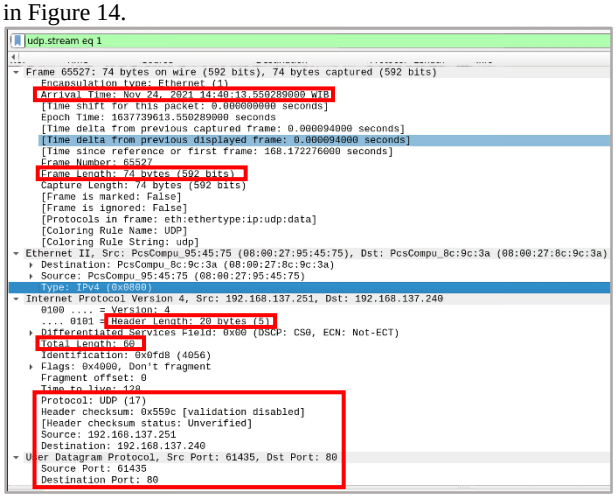

Figure 14. DDOS Attack Analysis Frame

According to Figure 14, in frame, which has a 74-byte frame length, the arrival time is Nov 24, 2021 14:40:13 WIB. The Internet Protocol Version 4 section reads 192.168.137,251 as the source IP and 192.168.137.240 as the destination IP, with a header length of 20 bytes and a total length of 60. The User Datagram Protocol (UDP) reads the source port 61435and the destination port 80.

4.5 Disposition

Disposition is the final result of the evidence's study and investigation. After IDS Snort detects an attack, the next step is to use Wireshark to collect evidence. At this point, the results can be produced and organized in tabular format for ease of reading. The table is shown in Table 2.

Table 2. Analysis and Investigation of Evidence Results

No	Timestamp	Source IP	Dest. IP	Source Port	Dest. Port	Protokol
1	24/11/2021 14:40:13	192.168.137.251	192.168.137.240	61435	80	UDP
2	24/11/2021 14:37:25	192.168.137.252	192.168.137.240	49166	80	TCP
3	24/11/2021 14:49:06	192.168.137.254	192.168.137.240	-	-	ICMP

According to Table 2, after analyzing the frame and examining the endpoint statistics in Wireshark, there are 3 (three) source IP addresses that attempt to attack the destination IP; the timestamp shows when the attack occurred; as can be seen from the table, the date of the attack is identical, with the exception of the minutes and seconds of attack time. Additionally, there is an attacker's source port and an attacked destination port. Then there is the protocol, which is the manner in which an attacker attacks.

5. CONCLUSION

The implementation of IDS Snort on the web server can help provide alerts so that it can minimize the presence of Distributed Denial of Service (DDoS) attacks by utilizing the rules that have been applied to IDS Snort. Based on the results of the study, the snort log file is a log file containing attack activity so that it can be used as evidence to be analyzed using wireshark and based on the results of the analysis found 3 IP addresses of attackers who carried out Distributed Denial of Service (DDoS) attacks with receiving frequency. data timestamp, source port, destination port, and attack protocol.

6. REFERENCES

[1] Adani, M. (2018). Web-Based Applications: Definition, Types, Examples, and Advantages. Sekawanmedia.

[2] Ahmad, M. S., Riadi, I., & Prayudi, Y. (2017). Live Forensics Investigation From User Side To Analyze Evil Twin-Based Man in the Middle Attack. ILKOM Scientific Journal, 9(1).

[3] University, S., Mada, G., & Mada, G. (2013). Network Forensic Analysis Case Study of SQL Injection Attack on Gadjah Mada University Server. IJCCS (Indonesian Journal of Computing and Cybernetics Systems), 6(2).

[4] Aji, S., Fadlil, A., & Riadi, I. (2017). Development of Computer Network Security System Based on Network Forensic Analysis. Scientific Journal of Computer Electrical Engineering and Informatics, 3(1), 11–19.

[5] Cahyanto, T. A., & Prayudi, Y. (2014). Forensic Investigation of Web Server Logs to Find Digital Evidence Related to Attacks Using Hidden Markov Models Method. Snati, 15–19.

[6] Nasution, A. M. (2021). Analysis and implementation of honeyd as a low interaction honeypot in improving network security systems.

[7] Dahlan M., Latubessy A., N. M. (2015). Web Server Security Analysis Against Possibility Sql Injection Attacks. SNATIF Proceedings, 0(0), 251–258.

[8] Triandini, R. (2016). Implementation of Intrusion Detection System Using Snort, Barnyard2 And Base On Linux Operating System. Essay.

[9] Putra, R. S., Mayasari, R., Bogi, N., Karna, A., Electrical, F. T., & Telkom, U. (2018). Hips Snort Virtual Network Security Implementation And Analysis On Web Server Services With Dos And Ddos Attacks Implementation and Analysis of Virtual Network Security With. 5(3), 4958–4965.

[10] Mualfah, D. (2016). Network Forensics To Detect Flooding Attacks On Web Servers.

[11] Usama, U. (2019). Performance Analysis of Network Intrusion Prevention System Using Snort Ids And Honeyd On Windows.

[12] Dewi, E. K., & Love, P. (2017). Snort log analysis using network forensics. 02, 72–79.

[13] Gaddafi, S., Pratiwi, Y. D., & Alfianto, E. (2021). Ids And Ips Based Ftp Server Security Using Ubuntu Linux Operating System. Network Engineering Research Operations, 6(1), 11.

[14] Hidayat, M. R., & Riadi, I. (2021). Investigation of Botnet Attacks using Network Forensic Development Life Cycle Method. *International Journal of Computer Applications*, *183*(25), 30–36.

[15] Tiara Dewi, Muhammad Amir Masruhim, R. S. (2016). Security System Implementation Using Snort IDPS (Intrusion Detection Prevention System) With SMS Gateway Notification. In the Research and Development Laboratory of Tropical Pharmaceuticals, Faculty of Pharmacy, Mualawarman University, Samarinda, East Kalimantan.

[16] Efrando, A., Herwin, & Haryono, D. (2019). SATIN – Science and Information Technology Monitoring on the STMIK Amik Riau Server by Using Suricata via Telegram Bot Notifications. 5(1).

[17] Dewi, E. K., Harini, D., & Miftachurohmah, N. (2017). Snort Ids As Forensic Tools Network Universitas Nusantara Pgri Kediri. (January), 411–418.

[18] Gunawan, G. B., Sukarno, P., & Putrada, A. G. (2018). Denial of Service (DoS) Attack Detection on Wifi-Based Smartlock Devices Using SNORT IDS. E-Proceeding of Engineering, 5(3), 7875–7884

[19] Inscrição, C. D. E. (2018). Detection and prevention of attacks on the network using snort on linux ubuntu. 2018.

[20] Sudradjat, B. (2017). Intruder Detection and Prevention System On Computer Networks Using Snort and Firewalls. JISAMAR (Journal of Information Systems, Applied, Management, Accounting and Research), 1(1), 10–24.

[21] Syaimi, A., Utami, P., Lidyawati, L., & Ramadhan, Z. (2013). Design and Analysis of Network Intrusion Prevention System Performance Using Snort IDS and Honeyd. Journal of Electrical Engineering ©Electrical

[22] Rahmatulloh, A., & MSN, F. (2017). Implementation of Load Balancing Web Server using Haproxy and File Synchronization on the Academic Information System of Siliwangi University. National Journal of Information Technology and Systems, 3(2), 241–248.

[23] Ridho, F., Yudhana, A., & Riadi, I. (2016). Router Forensic Analysis To Detect Distributed Danial of Service (DDoS) Attacks In Real Time. 2(1), 111–116.

[24] Purba, W. W., & Efendi, R. (2021). Design and analysis of computer network security systems using SNORT. Aiti, 17(2), 143–158.

[25] Riadi, I., Istiyanto, J. E., Ashari, A., & Subanar. (2013). *Log Analysis Techniques using Clustering in Network Forensics*. *10*(7).

[26] Pratama, I. P. A. E. (2014). Computer Networking (1st ed.). Bandung: Bandung Informatics Engineering | Itenas Online Journal of the National Institute of Technology Jurnal Reka Elkomika, 1(4), 2337–2439.