International Journal of Cyber-Security and Digital Forensics (IJCSDF) 8(1): 66-73
The Society of Digital Information and Wireless Communications (SDIWC), 2019 ISSN: 2305-001

Network Forensics Analysis of Man in the Middle Attack Using Live Forensics Method

Dedy Saputra[1], Imam Riadi[2]
[1]*Department of Informatics, Universitas Ahmad Dahlan, Yogyakarta, Indonesia*
[2]*Department of Information System, Universitas Ahmad Dahlan, Yogyakarta, Indonesia*
(dedy1400018017@webmail.uad.ac.id, imam.riadi@is.uad.ac.id)

ABSTRACT
The security of based internet information system is a must to care about. Because the network which is public and global basically are not safe. When the data sent from a personal computer to another personal computer, the data will across several personal computers it will give another user a chance to steal the data. It almost happened every day in the whole world. One of the way to steal the data is Man In The Middle Attack which attacks the server. Intrusion detection system is implemented with sniffing, traffic data watch process, and log traffic snort analyze are open source. Intrusion Detection System Snort analyze all the traffic system to sniff and search for several kinds of cybercrime in the network. The research is implemented with a Live Forensic method which basically has the same traditional forensic technique that is identification of saving, analyze and presentation. This research is expected to get the information such as log with sets the snort into personal computer to detect attack of web server, and then analyze the log file to explore the evidence forensic digital from log snort file. This research generates information in the form of alerts from attacks displayed by IDS Snort that are already installed on the web server. The log file is analyzed using Wireshark for exploration of digital forensics evidence in the form of an IP Address that attacks, when the attack occurred, how the attack occurred, and where the attack occurred. Based on the implementation of IDS Snort to detect Man in the Middle Attack. The results of the exploration of digital forensics evidence are obtained in the form of IP Address and port used by attackers to access the web server. Mitigation of attacks is done by blocking the IP Address and port used by the attacker to access the web server. This research has been successfully carried out.

Keyword: *Ettercap, Forensic, Live, Network, Snort*

I. INTRODUCTION

The development of the internet network is getting huge and wide, the security of internet information system is a must to care about. Because the network which is basically public and global basically are not safe. If someone looks for something that the main purpose is the internet and look for the reference, but the internet will never always give what being promised such as information from the whole world, because there are so many crimes happened on the internet, this crime called cybercrime. That's why the computer system must be complete with the system which can protect the sniffing and intrusion. The system called intrusion detection system (IDS) [1].

Snort IDS is used to detect port scanning on a computer network [2]. In addition to IDS Snort is also used in monitoring wireless network traffic [3]. IDS is a system for identifying the sniffer who tries to attack the system without authorized or legal user but abusing privilege the source of the system. IDS will notify if something suspicious or illegal had happened [4].

Man In The Middle Attack is one of the attacks on the network with open access LAN network. This way it will be done intercepts username and password (ARP Poisoning) by using a computer attacker inside a network multiple computers [5] therefore in their need to take preventive attack detection. [6]

One of the mitigation that can be done to prevent ARP Poisoning is by blocking the attacker IP Address and port used for incoming [7] and [8] Man

In The Middle Attack based evil twin become a dangerous terror for WIFI network users. The attacker will use fake AP (Access Point) with different gateway configuration with legitimate Access Point so the kind of this attack will be difficult to detect. [9] IDS Snort is used for monitoring wireless networks against packet sniffing attacks. [10]

Live Forensic is a method which has the same traditional forensic technique that is identifying the storage, analyst, and presentation. Live forensic is a response from lack of traditional forensic technique which can't get the information from the data and exist information while the system is on a process such as memory activity, network process, file swap, running system process information from the file system. This research uses live forensic technique such as preparation, case simulation, forensic investigation, analyst, and reporting. [9]

Based on the background of the problem, it is important to have network forensic using snort to detect the attack of Man in The Middle Attack. Then the topic of the final project research is Network Forensics Analysis Against Man in The Middle Attack Using Live Forensic Methods.

II. LITERATURE REVIEW

Conducted research about network forensic to detect an attack in the web server which explains about snort IDS configuration where snort works real time [11]. [1] defines that intrusion detection is a watch process of action happened in PC or network and analyze the possibility of an accident. The accident means terror of violation or threat of policy violation computer security, acceptable usage policies or based security practice.

The research conducted by [12] identified that the attack of DDoS in the computer network, discussed network security from DDoS attack, find the attacker, and reconstruct the attack with the analyst of sniffing evidence.

The research conducted by [13] is about package identification in honeynet network ID_SIRTII/CC, identified that parameter of the attack while getting the traffic honeynet data network, investigated package honeynet data, analyst PCAP in the honeynet network. This research is using Tapping Mirroring Method.

The research conducted by [14] is about the security of your account in the browser such as Microsoft Edge, Mozilla Firefox, and Google Chrome, identified the comparison browser for an account while using the private and public the purpose is to find the evidence in storage, USB storage, CD, traffic network and else.

The research conducted by [15] is about additional device traffic network and discuss the attack in traffic network and how to anticipate the attack using an additional device traffic network.

The research conducted by [16] is discussed a survey about the attack of Man in The Middle Attack which is possibly attacker getting the illegal access into a connection between two devices and listened to traffic network. This kind of attack is absolutely wrong because it's almost invisible to the victim's devices. this research using D-H exchange password where two wireless devices sharing their secret password with the safe line between them.

III. RESEARCH METHOD

3.1. Research Subject

Research subject is the subject that will be discussed is Network Forensic Analysis Against Man in The Middle Attack Using Live Forensic Method. The analysis is expected to be one of the ways to increase the security of web server generally especially web server in Universitas Ahmad Dahlan.

3.2. Live Forensic

The research is a case simulation to try to implement the snort to detect the sniffer or an attack. The purpose of a case simulation is to testing the snort to detect the sniffer an attack to the server target that will be used to protect the network with the ability to a response which available with the policy of the safety from IDS Snort. The stages of the research can be seen in Figure 1.

Figure 1. Research Stages

The stages of the research conducted are: [17]

a. Collection

On this stage, the researcher conducted research and some attempt find the evidence, introduction to the sniffing and gather evidence. In the process of detecting the attack, the system will be used is IDS Snort. There are some rules in snort which extracting the package across the network, so if there are suspicious packages and not available with the rules the snort will send the message alert and save it as a log.

b. Examination

These stage need to find the hidden information and published the relevant document. The investigation to a log file using IDS Snort. After the log safe as an alert, then the log will be investigated.

c. Analysis

This stage is used to proof the case and to answer the forensic questions about the attack who's IP's attack, when, where, how, and why the attack happened.

d. Reporting

This stage is the process of writing the report about the data investigation from all the research. Make the report about the attack that happens in the network from the result of the log analysis and after that, the researcher does the reconstruction to the data from the action and make sure not damaging the log.

3.3. Case Scenario

The case scenario in this research is adjusted with a case of bank break-ins using Man in the Middle Attack and the target is web banking. This simulation is using computer device with local network and XAMPP local server. This simulation is exampled the exam test registration page where an attacker will do the sniffing on the web server using Ettercap. The target of the attacker is IP Address web server or the client. When the client access the exam test registration page then the username and the password will be caught by Ettercap and displayed by the client and also username and password.

3.4. The Making of the Scenario

The making of the scenario and experiment can be used to get the digital evidence as the first step before analysis stage. The description of the experiment in the research is shown as follows:

1) Experiment 1: Client access the web server and request to enter the exam test registration page. A client does the request in Figure 2.

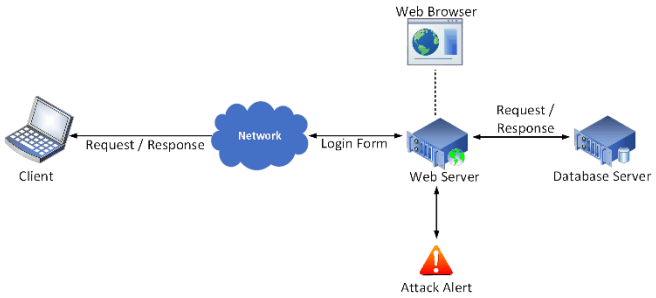

Figure 2. Client Request

Client request the web server and in response by displaying the login page in the web browser to use by the client to fill the username and password.

2) Experiment 2: The attacker will do the attack on the web server using Ettercap and sniffing the data sent by the client to the web server. Attacker's attack can be seen in Figure 3

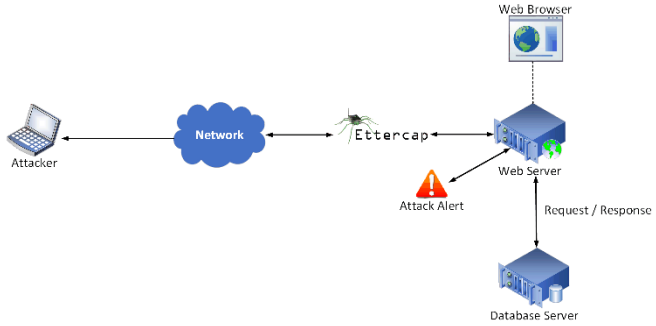

Figure 3. Attacker's Attack

3.5. Testing of Scenario and Experiment

This stage is needed to get the digital evidence. Long testing is not restricted to make it easier in getting and analyze the digital evidence on the next stages. The experiment is suitable with the condition using a local network in the research lab and using XAMPP as a local server. The network design can be seen in Figure 4 and the attack scenario can be seen in Figure 5.

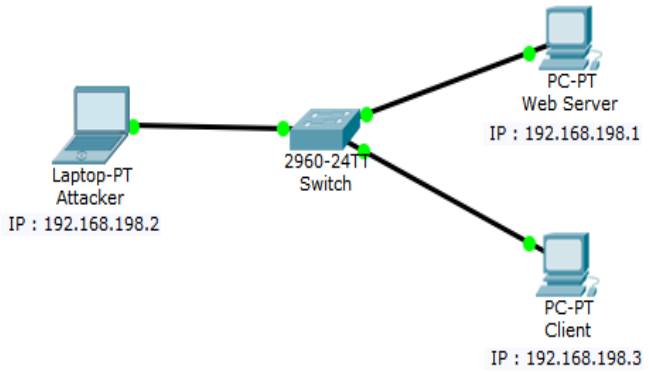

Figure 4. Network Design

At the network design picture, there are two clients. An attacker and web server are connected to each other.

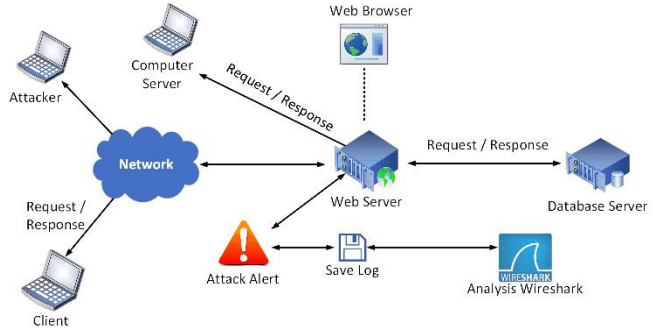

Figure 5. Attack Scenario Web Server

In the attack scenario picture, there are two clients, an attacker and a web server. In the web server, there is the exam test registration page that will be accessed by the client by the web browser. An attacker will do the attack on the web server using Ettercap and sniffing to the network traffic. With the attacker who does sniffing then all request and response made by the client who made the target by the attacker will be recorded on the Ettercap application while snort on the web server will catch all the log and will show the alert from attack by an attacker.

3.6. Digital Evidence Collection

This stages will collect the digital evidence such tested log file by the scenario and experiment which has been determined before. Digital evidence collection such as log file in snort application which has been set in web server before. After getting the evidence the next stages is analyzed the digital evidence. The example of log snort can be seen in Figure 6.

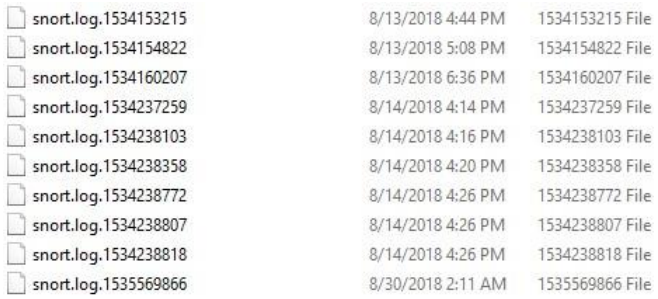

Figure 6. Log Snort

3.7. Analyze the Digital Evidence

After the digital evidence collected, then the next stages are Live Forensic analyze in real time to find the alerts of attack directly. As standard testing, the researcher will be using network analyzer application that has been used for digital forensic analysis, that is *Wireshark.*

3.8. Mitigation

Based on the case of a man in the middle attack on a web server, making a secure web server data by blocking the IP address that carried out the attack. To find out the IP Address that carried out the attack can be seen in the IDS Alert results located in the c:\Snort\log folder. Prevention can also be done by using the XArp application to detect ARP or attack Man In The Middle Attack. The XArp application will display IP, MAC, Host, Vendor, interface, IP status online or not, cache and first seen. A red cross for ARP attack detected status and a green checklist indicates that IP is not being attacked. Flowchart system can be seen in Figure 7.

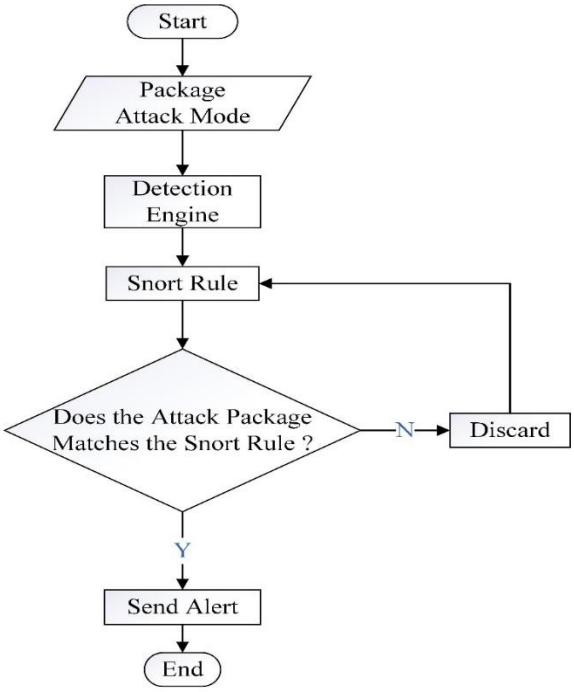

Figure 7. Flowchart System

IV. RESULT AND DISCUSSION

4.1. Live Forensics

a. Collection

At this stage the process of investigating and seeking evidence is conducted. The introduction of the intruders and collecting evidence. Used in intrusion detection system Snort IDS. After the log is stored as an alert, then the log will be researched and examined.

b. Examination

At this stage to do a search and reveal hidden information relevant documentation. The examination was conducted in a log file that has been taken using Snort IDS. After the log is stored as an alert, then the next log will be researched and examined.

c. Analysis

At this stage is used for authentication to the case at hand and answer forensic questions regarding the attacks, IP who carried out the attack, when the attack took place, where the attack occurred, how the attack took place, and why the attack took place.

d. Reporting

This stage is the process of writing data investigation from all the research based on the results of the forensic testing and investigation of the case of Man In The Middle Attack attack.. Make the report about the attack that happens in the network from the result of the log analysis and after that, the researcher does the reconstruction to the data from the action and make sure not damaging the log to found some information that can be used as digital evidence.

4.2. Case Scenario

The process of simulating a Man In The Middle Attack attack is an initial step taken to test Snort IDS configuration in detecting Man In The Middle Attack attacks. The simulation starts with how to prepare the website to test attacks on a server and run XAMPP as a local server. Using 1 computer as a web server as well as for Snort IDS, 1 computer as a client and 1 computer as the web server attacker.

a. Access the Website

Users access the website normally with URL http://192.168.198.1/MITM/index.php . To get full access user must type username and password. When the user clicks the login button then automatically URL, username and password will be captured by Ettercap and displayed on the page Ettercap. The registration exam page of awareness can be seen in Figure 8.

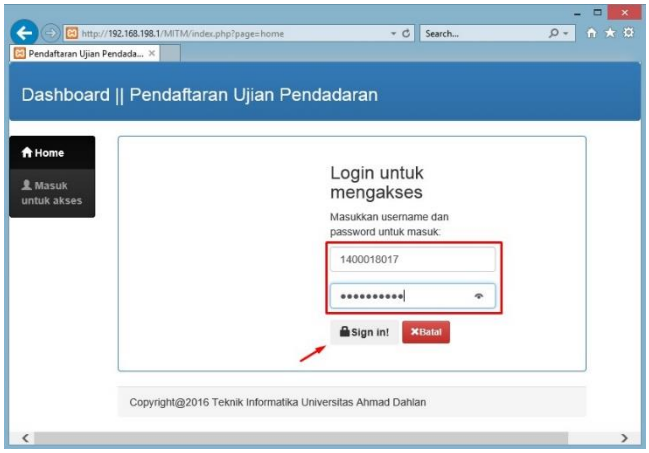

Figure 8. Access the Website

b. Man in the Middle Attack Process

Man In The Middle Attack process was helped by using Ettercap tools. Ettercap is a tool that is used to intercept and capture username and password automatically an IP address that is targeted. The packet capture results from Ettercap can be seen in Figure 9. Ettercap can also be run on Linux terminal by typing the command "Ettercap -i eth0 -T -q -M arp" can be seen in Figure 10.

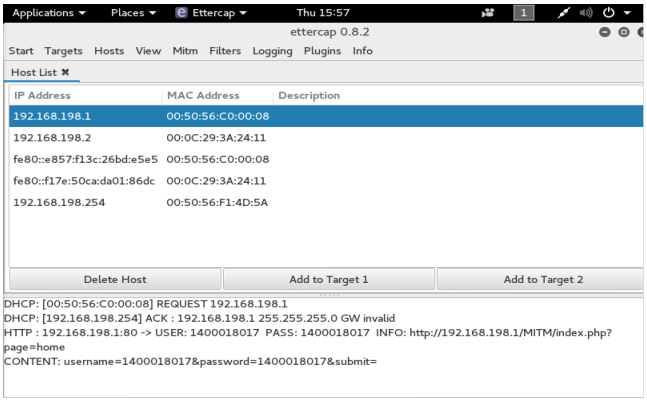

Figure 9. Capture Ettercap

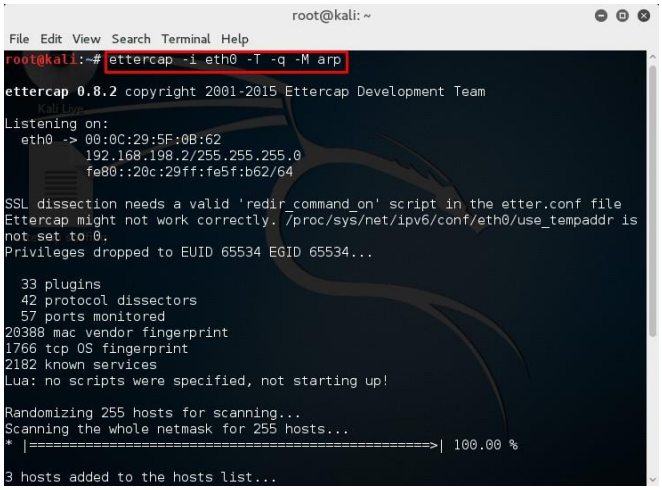

Figure 10. Run Ettercap on Linux Terminal

c. Data Collection

Collection of evidence in this study using the traffic recorded by IDS Snort and stored as a log stored in the folder c:\Snort\log analysis would be conducted to obtain the results of the research.

d. Inspection Logs

The researcher using IDS Snort for detecting intrusion on the network so that if a log file will be taken in the form of a packet capture (PCAP) The parameters need to be installed on snort. Parameters or script that use is " Snort -A console -i2 -c c:\Snort\etc\snort.conf -l c;\Snort\log". So that when detected traffic in accordance with the rules that have been created snort who run the command prompt will display the log and Snort log will be stored in the folder c:\Snort\log. Inspection log can be seen in Figure 11.

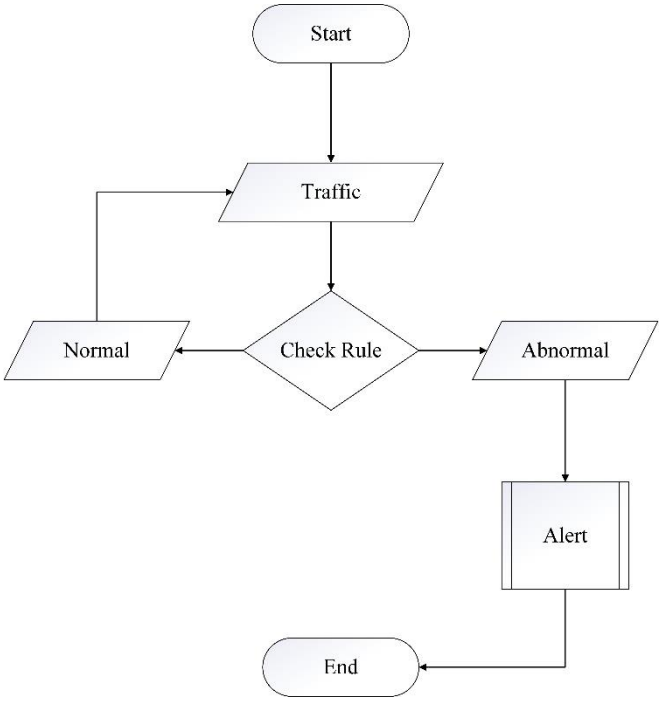

Figure 11. Inspection Log

The snort IDS Alert that detects the attacks of Man In The Middle can be seen in Figure 12.

Figure 12. Alert Snort IDS

Furthermore, IDS Snort Alert will be analyzed by using a network analyzer is Wireshark separately determine the attack occurred. The data log files are managed in check will then be taken in the

form of a packet capture that consists of several log files that the package captured by Snort IDS. The logs will be in an analysis using Wireshark is the data associated with the IP address of the attacker, the port used for entry, as well as the type of data in the attack. This information is very useful in the investigation against attackers and for blocking the port and IP address as measures to protect web servers from Man In The Middle Attack next.

4.3. Analysis and Forensic Investigation

The website that is the example of a Man In The Middle Attack is a site that is built using basic PHP scripts and uses localhost and XAMPP servers. The web application is a login form on the interface which is a gap from the attack of Man In The Middle Attack.

a. The Result of Attack Simulation

Simulated attacks to deliver a strike package Man In The Middle Attack in a network and the attacker can access web pages using the username and password circuitry in getting out of sniffing using Ettercap. Digital evidence found in Man in The Middle Attacks was analyzed by using Wireshark.

In Figure 13 can be seen the results of log analysis using Wireshark.

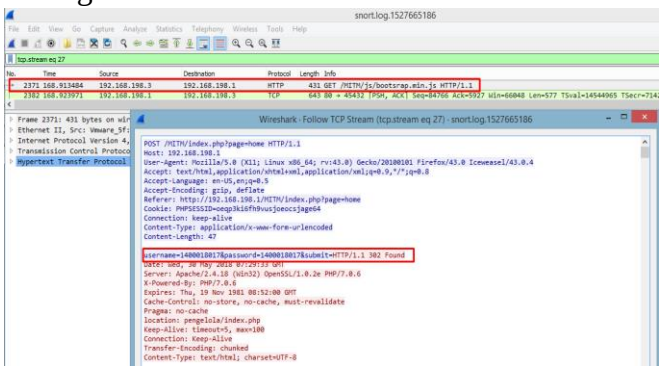

Figure 13. Wireshark Analysis Results

IDS Snort is working on a web server captures all activities that occur in web server and send alerts when there is suspicious activity on the network that matches the rule that has been defined. The results have shown the attacker Wireshark tools managed to get a username and password and access the website page using Iceweasel on Linux times using IP address 192.168.198.3.

b. Mitigation

IDS Snort rule has been set previously. If the traffic according to the rules it will be detected as a Man In The Middle Attack and displayed as an alert on the snort and then stored as a log in the folder c: \ Snort \ log. Figure 14 shown alert Man In The Middle Attack

```
08/01-22:46:52.724393  [**] [1:10000001:0] Terdeteksi MITM Attack [**] [Priority
: 0] {TCP} 192.168.198.2:52676 -> 192.168.100.11:80
08/01-22:46:52.724613  [**] [1:10000001:0] Terdeteksi MITM Attack [**] [Priority
: 0] {TCP} 192.168.198.2:52676 -> 192.168.100.11:80
08/01-22:46:52.861783  [**] [1:10000001:0] Terdeteksi MITM Attack [**] [Priority
: 0] {TCP} 192.168.198.2:52676 -> 192.168.100.11:80
08/01-22:46:52.872043  [**] [1:10000001:0] Terdeteksi MITM Attack [**] [Priority
: 0] {TCP} 192.168.198.2:52676 -> 192.168.100.11:80
08/01-22:46:52.872045  [**] [1:10000001:0] Terdeteksi MITM Attack [**] [Priority
: 0] {TCP} 192.168.198.2:52676 -> 192.168.100.11:80
08/01-22:46:52.872182  [**] [1:10000001:0] Terdeteksi MITM Attack [**] [Priority
: 0] {TCP} 192.168.198.2:52676 -> 192.168.100.11:80
08/01-22:46:52.872235  [**] [1:10000001:0] Terdeteksi MITM Attack [**] [Priority
: 0] {TCP} 192.168.198.2:52676 -> 192.168.100.11:80
08/01-22:46:52.963058  [**] [1:10000001:0] Terdeteksi MITM Attack [**] [Priority
: 0] {TCP} 192.168.198.2:36036 -> 118.98.93.65:80
08/01-22:46:57.868296  [**] [1:10000001:0] Terdeteksi MITM Attack [**] [Priority
: 0] {TCP} 192.168.198.2:52676 -> 192.168.100.11:80
08/01-22:46:58.818589  [**] [1:10000001:0] Terdeteksi MITM Attack [**] [Priority
: 0] {TCP} 192.168.198.2:56418 -> 104.19.198.151:80
08/01-22:46:59.170138  [**] [1:10000001:0] Terdeteksi MITM Attack [**] [Priority
: 0] {TCP} 192.168.198.2:58676 -> 52.37.128.73:443
08/01-22:46:59.778154  [**] [1:10000001:0] Terdeteksi MITM Attack [**] [Priority
: 0] {TCP} 192.168.198.2:55034 -> 205.185.208.52:80
```

Figure 14. Alert MITM Attack

When there is traffic in accordance with the rule will be detected as a MITM Attack and will be displayed as an alert at the command prompt. IP detected attacks can be directly blocked by using the IP Blocker application Firewall 5.0. In addition to using IP Blocker Firewall 5.0, can also use Netcut to block the attacker's IP.

V. CONCLUSION

The conclusion obtained during the detection process of Man In The Middle Attack on a web server is implementation of Intrusion Detection System (IDS) Snort on a web server can assist in providing information to make the detection of Man In The Middle Attack. The log file is stored in the folder log is taken to be analyzed by using Wireshark in order to find the illegal actions that occur on the web server. IP Blocker 5.0 Firewall and Netcut is used to block IP detected an attack against the server. Implementation of tools Ettercap as the attacker is performing Man In The Middle Attack goes well and smoothly. This research has been successfully carried out.

REFERENCES

1 A. P. Wicaksono and Harjono, "Intrusion Detection System With Snort (Intrusion Detection System with Snort)," vol. III, no. 1, pp. 31–34, 2014.

2 M. Anif, S. Hws, and M. D. Huri, "Application of Intrusion Detection System (IDS) with Port Scanning Detection method on Computer Networks at Semarang State Polytechnic," *J. TELE, Vol. 13 Nomor 1*, vol. 13, no. 1, pp. 25–30, 2015.

3 Irwan Agus Sobari, "Design of Wireless Intrusion Detection System Using Snort," vol. XII, no. 1, pp. 1–9, 2015.

4 M. Jannah, Hustinawati, and R. Wildani, "Snort Intrusion System (Ids) Implementation," *UG J.*, vol. 6, no. 05, pp. 1–4, 2012.

5 K. V. A. Prerna Arotea, "Detection and Prevention against ARP Poisoning Attack using Modified ICMP and Voting.pdf." 2015.

6 Y. Mirsky, N. Kalbo, Y. Elovici, and A. Shabtai, "Vesper: Using Echo-Analysis to Detect Man-in-the-Middle Attacks in LANs," no. July, 2018.

7 J. Singh, S. Dhariwal, and R. Kumar, "A Detailed Survey of ARP Poisoning Detection and Mitigation Techniques," no. February, 2017.

8 B. Triandi, "Network Security System in Preventing Data Flooding with IP Blocking and Port Methods," *Semin. Nas. Teknol. Inf. dan Multimed.*, pp. 6–8, 2015.

9 M. S. Ahmad, I. Riadi, and Y. Prayudi, "Forensic Live Investigation from the User's Side to Analyze Man in the Middle Attack Attacks Based on Evil Twin," *Ilk. J. Ilm.*, vol. 9, no. April, pp. 1–8, 2017.

10 F. Teknik, U. N. Surabaya, J. T. Informatika, F. Teknik, U. N. Surabaya, and A. Point, "Wireless Network Monitoring On Packet Sniffing Attack Using IDS Achmad Rizal Fauzi I Made Suartana Abstrak," *J. Manaj. Inform.*, vol. 8, no. 2, pp. 1–17, 2018.

11 D. Mualfah and I. Riadi, "Network Forensics For Detecting Flooding Attack on Web Server," *IJCSIS) Int. J. Comput. Sci. Inf. Secur.*, vol. 15, no. 2, 2017.

12 A. Fadlil, I. Riadi, and S. Aji, "Development of Computer Network Security Systems Based on Network Forensic Analysis," vol. 3, no. July, 2017.

13 S. Budiharjo and F. Riyadi, "Network Forensics on Data Traffic in the Honeynet Network in Indonesia Security Incident Response Team on Internet Infrastructure / Coodrination Center," *ICT*, vol. 5, no. 9, pp. 745–754, 2014.

14 M. Nur Faiz, R. Umar, and A. Yudhana, "Live Forensics Implementation for Browser Comparison on Email Security," *JISKa*, vol. 1, no. 3, pp. 108–114, 2017.

15 R. F. Sri Supatmi, Taufiq Nuzwir Nizar, "Network Forensics Support Devices," *J. Tek. Komput. Unikom – Komputika – Vol. 3, No.2 - 2014 Sist.*, vol. 3, no. 2, pp. 23–28, 2014.

16 J. L. Borade, K. M. Jain, and M. V Jain, "A Survey on an in the Middle Attack," *Int. J. Sci. Technol. Eng.*, vol. 2, no. 09, pp. 277–280, 2016.

17 R. U. Putri and J. E. Istiyanto, "Network Forensic Analysis Case Study of SQL Injection Attack on Server Gadjah Mada University," *Ijccs*, vol. 6, no. 2, pp. 1978–1520, 2012.