FORENSIC NETWORK ANALYSIS AND IMPLEMENTATION OF SECURITY ATTACKS ON VIRTUAL PRIVATE SERVERS

Naikson Fandier Saragih¹, Ridho Agus Wery Nanda Panjaitan², Mufria Jonatan Purba³
¹,²,³Indonesian Methodist University
Jalan Hang Tuah No. 8 Medan, North Sumatra 20152
E-mail: saragihnaiikson@gmail.com

ABSTRACT- PT Kodinglab Integrasi Indonesia's Virtual Private Server (VPS) product requires good quality standards, including security. The challenge that arises is still frequent disruptions to the protection of PT Kodinglab's VPS customers, where it is difficult to identify the source of the attack. Network forensics in the form of dead forensics and live forensics using the NIST method with the stages of collection, examination, Analysis, and reporting are used to find the source of the attack. Data for dead forensics comes from snort tools, and data for live forensics comes from capture Wireshark. The collection stage involves collecting attack data from snort logs and wireshark for life forensics. While the examination dataset stages are further analyzed and mapped. Advanced check on the server via syslog snort.

From the attack testing carried out to obtain information in the form of the attacker's IP address, destination IP address, date of the attack, server time, and type of attack from testing the TCP Flooding and UDP Flooding attacks, all attacks on the customer's VPS can be identified. The information obtained regarding the attacker is in the form of the date and time the attack occurred, the attacker's IP address and the victim's IP address, and the protocol used.

Keywords: Network Forensic, Dead Forensic, Live Forensic, Virtual Private Server, DDos, TCP Flooding, UDP Flooding.

1. INTRODUCTION

PT Kodinglab Integrasi Indonesia, one of the services provided is a Virtual Private Server for customers. Standards are prepared with high quality, especially regarding security in providing information system development and development services, mobile applications, development, e-government, and digital marketing. The Kodinglab server has now accommodated many web applications from government and private agencies using the Docker VPS. However, throughout 2021 there will still be 20 percent security disturbances to VPS customers of PT Kodinglab, such as backdoor and DDoS attacks.

Virtual Private Server (VPS) is one of the virtual machines provided for Internet hosting service providers that have been widely used since 2010. VPS is widely used when website traffic is high and requires more resources when you need Private IP access and create applications based on file sharing, streaming, and MAP Server [1]. Therefore VPS is inseparable from the target of security attacks.

To find the source of the attack, Network Forensic can be used by monitoring and analyzing resource usage, amount of traffic, and user activity, whether the server is on or off. The results of research using Network Forensic, investigators can quickly detect an attack and identify the attacker. In addition, the data needed for the investigation process, among other things, the date of the attack, the time of the attack, the attacker's MAC Address, the attacker's IP Address, the Victim's MAC Address, and the Victim's IP Address, can be presented quickly and precisely so that they can assist investigators in making decisions on attacks that occur [2].

2. RESEARCH CONTENT

2.1 Method

1. Network Forensics

The Network forensic section is a science that focuses on an area of computer networks and devices connected to a network to find attacker information and to find evidence of an attack on a computer network [3]. Network forensic stages can be seen in the image below:

![Figure 1 Forensic Process Model](image)

a. collection

At this stage, it is carried out to obtain evidence according to procedures approved by the authorities.

b. examination

At this stage, it checks the activities that occur on the server.

c. Analysis

This stage is to analyze the data that has been collected to obtain estimates, possibilities, and hypotheses from the data that will potentially become evidence.
d. Reporting

All of the steps above must be well documented to facilitate making reports easy for others to understand from the investigative activities carried out.

1. Live Forensic and Dead Forensic

Live forensics collects data/evidence of attack when the server is on, while Dead forensics collects data/evidence of attack when the server is down, which is generally stored in the snort log.

2. Research Flow

To carry out the research process to get the desired results, the researcher makes a research flow, as shown in Figure 2

[Diagram showing the research flow]

3. System Implementation

This stage is carried out by hiring a VPS service from the herza.id provider. The rented system is a KVM VPS with the Ubuntu 20.04 operating system. The specifications for the VPS that are rented can be seen in Table 1

<table>
<thead>
<tr>
<th>CPU used</th>
<th>Cores 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ram</td>
<td>4GB</td>
</tr>
<tr>
<td>Hard drive</td>
<td>80GB</td>
</tr>
<tr>
<td>Bandwidth</td>
<td>Unlimited</td>
</tr>
<tr>
<td>Operating system</td>
<td>Ubuntu 20.04</td>
</tr>
</tbody>
</table>

Next, install snort on the ubuntu server. Figure 3 shows that snort has been successfully installed.

The image above shows the version of snort that has been successfully installed, namely snort version 2.9.7.0.

In Snort, there are rules to Snort's intelligence. The set rules provide intelligence at the time of protection, so the investigation process depends on rule intelligence. The script below is a configuration for saving rules. When there is an attack on the server, the log of the attack will be stored in the rules.

Next, add the DDoS attack rules with the script below

```bash
=> Added snort rules

alert ICMP any any -> $HOME_NET any (msg:"ICMP Flooding"; detection_filter:tracks by_src, count 30, second 60; sid1000006; rev2;)
alert tcp any any -> $HOME_NET any (msg:"TCP Flooding"; detection_filter: tracks by_src, count 30, second 60; sid1000006; rev2;)
alert udp any any -> $HOME_NET any (msg:"UDP Flooding"; detection_filter: tracks by_src, count 30, second 60; sid1000003; rev1;)
```

From the script above, the following results from changing the snort rules configuration script on the ubuntu server. Figure 4 is the snort rules configuration.

Next, we will install Wireshark on the client’s PC. The following shows the Wireshark that has been successfully installed, shown in Figure 5.
2.4 Attack Testing

After implementing the system and configuring it, we then carry out attack testing to see the snort's response in monitoring data packets. For testing, only use attacks Distributed Denial of Service (DDoS) TCP Flooding and UDP Flooding using the LOIC application. Previously carried out the following tests. The CPU performance conditions in the initial state on the VPS overview tab are shown in Figure 6.

From the picture above, the results of the initial CPU condition data are obtained, which are shown in Table 2.

<table>
<thead>
<tr>
<th>No</th>
<th>Tab</th>
<th>Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Disk Usage</td>
<td>5.6%</td>
</tr>
<tr>
<td>2</td>
<td>Bandwidth</td>
<td>0%</td>
</tr>
<tr>
<td>3</td>
<td>CPUs</td>
<td>1% Used</td>
</tr>
</tbody>
</table>

To get network forensic results in finding evidence of security attacks, researchers conducted DDoS TCP Flooding and UDP Flooding attack scenarios, with information in Table 3.

<table>
<thead>
<tr>
<th>No</th>
<th>Attack Type</th>
<th>Number of Tests</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>TCP Flooding</td>
<td>2</td>
</tr>
<tr>
<td>2</td>
<td>UDP Flooding</td>
<td>2</td>
</tr>
</tbody>
</table>

1. TCP Flooding

An attack that targets the TCP protocol takes advantage of the protocol connection connected to the server by flooding it (flooding). Experiments in making TCP connections that are accommodated by the server in buffers are indeed different. Still, the capacity is no more than a few hundred connections. By sending many packets into TCP, the buffer location will be full and cause the server to not work properly. Figure 7 is a test of the TCP Flooding attack.

In the test above, the LOIC application sends many TCP packets so the server becomes full of these packets. With the "top" tools on Linux Ubuntu, network performance for the CPU and memory running on the server can be seen in Figure 8.

From the picture above, the CPU performance is at 22.4%.

2. UDP Flooding

Testing the second attack is done by testing DDoS attacks with UDP-type flooding using the LOIC application. Figure 9 is a test of the UDP Flooding attack.
The test above shows that LOIC floods User Datagram Protocol requests by sending many UDP packets so that the server becomes full. CPU performance and server memory with the "top" command on Linux ubuntu can be seen in Figure 10.

From the picture above, CPU performance has increased to 42.3%.

2.5 Network Forensics
Network forensics includes a collection stage to deal with previously committed crimes. The focus is to prevent future crimes.

2.3.1 Collections
Retrieval of attack data using snort tools, namely on logsnort and also on wireshark for life forensics. From the testing, carried out to obtain information in the form of the attacker's IP address, destination IP address, date of the attack, server time, and type of attack.

1. Log Data on Snort
a. Log Data for TCP Flooding attacks

Attack trials were carried out twice, each shown in Figure 11 and Figure 12. The first attack was carried out on June 9, and the second on June 16, 2022.

From Figure 11 above, it can be seen that the attacker's IP address is 114.5.144.36, the attack date is June 6, the server was attacked at 09.50, with id 46407, and the type of attack is a TCP attack.

From figure 12 above, it can be seen that the attacker's IP address is 36.72.172.243, the attack date is June 16, the server was attacked at 16.58, with id 64318, and the type of attack is a TCP attack.

b. Log Data for UDP Flooding attacks

Attack trials were carried out twice, respectively shown in figure 13 and figure 14. the first attack was carried out on June 16, and the second on June 18, 2022.

From Figure 13 above, it can be seen that the attacker's IP address is 36.72.172.243, the attack date is June 16, the server was attacked at 17.19, with id 62484, and the type of attack is a UDP attack.
Figure 14 Snort log testing the second UDP Flooding attack

From Figure 14 above, it can be seen that the attacker's IP address is 114.5.147.54, the attack date is June 18, the server was attacked at 12.32, with id 20264, and the type of attack is a UDP attack.

2. Log Data on Wireshark

In this tool, you can see the time, source, destination, and also protocol used.

a. TCP Flooding attack logs

Attack trials were carried out twice, with the results shown in Figure 15 and Figure 16, respectively.

Figure 15 Data packet for testing the TCP Flooding attack first

From Figure 15, it can be seen that the attacker's IP number 50363 is 192.168.1.82, the destination IP is 103.160.63.239, and the protocol is TCP.

Figure 16 Data packet testing the second TCP Flooding attack

From the picture above, it can be seen that the attacker's IP at number 647 is 192.168.252.6, the destination IP is 103.160.63.239, and the protocol is TCP.

b. UDP Flooding Attack Data Logs

Attack trials were carried out twice, with the results shown in Figure 17 and Figure 18, respectively.

Figure 17 First UDP Flooding attack test data packet

From the picture above, it can be seen that the attacker's IP at number 3 is 192.168.1.48, the destination IP is 103.160.63.239, and the protocol is UDP.

Figure 18 Data packet testing the second UDP Flooding attack

From the picture above, it can be seen that the attacker's IP at number 1 is 192.168.252.6, the destination IP is 103.160.63.239, and the protocol is TCP.

2.3.2 Examination

The data obtained forms a dataset and can be analyzed and mapped. Inspection is not only carried out on attack data obtained previously using tools but also checking activities carried out on the server via Syslog, as shown in Figure 19.
From the picture above, the activities carried out on the server will be recorded by snort, which is stored in the syslog, so from the information obtained, the server user can see irregularities if at any time there is a misuse of the server.

2.3.2 Analysis
From stages collection, evidence of an attack has been obtained, and a series of information obtained is evidence that there was an attack on the server, the server's IP address. The Analysis was carried out in the form of a comparison of CPU performance in the initial state before the attack was carried out and when the attack was carried out.

1. Server conditions on ubuntu in an initial state
To see the condition of the CPU on the server, you can do it with the "top" command. After the command is entered, we will see the results, as shown in figure 20 below.

From the picture above, it can be seen that the initial condition of the CPU is at 0.0%, and it can be concluded that the performance of the CPU is in a normal state.

2. Server condition on ubuntu after an attack
After the attack was carried out, the CPU performance condition increased, namely at 43.6%, which can be seen in Figure 21 below.

Thus it can be concluded that the increase in CPU conditions before and after the attack was carried out was 43.6%.

2.3.2 Reports
1. Snort data source
The results of the investigation with the snort data source have occurred on the PVS server from several computers whose complete information can be seen in Table 4

<table>
<thead>
<tr>
<th>No</th>
<th>Attacker IP</th>
<th>The date of the attack</th>
<th>Destination IP</th>
<th>Server Time</th>
<th>ID</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>114.5.1</td>
<td>June 9</td>
<td>103.160.63.239</td>
<td>09:50:00</td>
<td>46</td>
<td>TCP</td>
</tr>
<tr>
<td>2</td>
<td>36.72.1</td>
<td>June 16</td>
<td>103.160.63.239</td>
<td>16:50:45</td>
<td>64</td>
<td>TCP</td>
</tr>
<tr>
<td>3</td>
<td>36.72.1</td>
<td>June 16</td>
<td>103.160.63.239</td>
<td>17:10:55</td>
<td>62</td>
<td>UDP</td>
</tr>
<tr>
<td>4</td>
<td>114.5.1</td>
<td>June 18</td>
<td>103.160.63.239</td>
<td>12:30:03</td>
<td>20</td>
<td>UDP</td>
</tr>
</tbody>
</table>

2. Wireshark data source
The results of the investigation with the Wireshark packet capture data source have been an attack on the PVS server from several computers whose complete information can be seen in Table 5

<table>
<thead>
<tr>
<th>No</th>
<th>time</th>
<th>Attacker IP</th>
<th>Destination IP</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>17:0158</td>
<td>192.168.1.82</td>
<td>103.160.63.239</td>
<td>TCP</td>
</tr>
</tbody>
</table>
3 CONCLUSION

Conclusion

Some conclusions are as follows:

1. Network forensics, in collecting evidence of attacks in the snort log, has been able to identify the attacker in the form of the date of the attack, the time of the attack, the attacker's IP address, the victim's IP address, ID, the protocol can be presented quickly and precisely so that it can assist investigators in making decisions about the attack that occurred on a Virtual Private Server (VPS).

2. Collecting evidence of attacks on wireshark log data in the form of the time of the attack, attacker's IP address, victim's IP address, and protocol.

4 CLOSING

In this study, the authors provide suggestions that are necessary for the next development, which are as follows:

1. The research is also expected to provide recommendations for tools used in detecting and identifying attacks and attackers.

2. Future research also examines how to handle and prevent security attacks on Virtual Private Servers (VPS).

BIBLIOGRAPHY


