Network Forensics For Detecting Flooding Attack On Web Server

By Imam Riadi

(IJCSIS) International Journal of Computer Science and Information Security,
Vol.15, No. 2, February 2017

Network Forensics For Detecting Flooding Attack On Web Server

DESTI MUALFAH
Department of Informatics
Islamic University of Indonesia
Yogyakarta, Indonesia
desti.mualfah@gmail.com

IMAM RIADI
Department of Information System
Ahmad Dahlan University
Yogyakarta, Indonesia
imam.riadi@is.uad.ac.id

***Abstract*- Flooding attack is one of the serious threats of network security on Web servers that resulted in the loss of bandwidth and overload for the user and the service provider web server. The first step to recognizing the network flooding attack is by applying the detection system Intrusion Detection System (IDS) like Snort. Snort is an open source system that can be used to detect flooding attacks using special rules owned by Snort. All activities are recorded on Snort are stored in a log file that records all activity on network traffic. Log files are used at this stage of the investigation to the forensic process model method to find evidence. The results of this research scenario analysis obtained 15 IP Address recorded perform illegal actions on web server. This research has successfully detected flooding attack on the network by performing forensics on web server.**

Keyword: Flooding, IDS, Snort, Network Forensics

I. INTRODUCTION

In this era, the increase in threats and attacks on network security is increasing because the web server is supported by the ease of access and resource availability are more easily lead to hacker has vulnerabilities for hacking web servers. Web server is an application server with the content contained on HTTP or HTTPS from the browser and send it back in the form of pages[1].

The web server will record data every of the visitor in the form of log files on the web server[2]. The data log file will be very helpful in case of problems on the web server[3]. In this regard, there is a field of computer technology, the network forensic (forensic network) is a branch of digital forensics[4], using the technique scientifically proven to collect, use, identifying, testing,

Analyzing, documenting and over and can present digital evidence from several sources of digital evidence to network events on finding source of the attack[5].

There are many possible attacks on a web server, one of which is a flooding attack. Flooding attack is an attack indicated[6] or stop services carried from one computer or to many computers simultaneously, by spending resources (resource) owned by that computer until the computer is not able to function properly[7]. Making it necessary to do the search step to finding the lights and reconstructed the attack action through evidence analysis attack. To combat this, the Intrusion Detection System (IDS)[8], which can be used for detection and identification of flooding attacks such as Snort IDS[9]. Snort can detect intruders with a rule that has been owned by Snort by way of a packet sniffer to see the data traffic on computer networks[10].

Detection of flooding attack on a web server as done with the forensic evidence in forensic process model approach, namely forensic methods to gather information, examination, analysis, and reports[5]. Therefore, the topics raised in this research is the detection of flooding attack on a web server[11], including flooding attack detection process and the reconstruction of the characteristics of the log file that has been recorded by Intrusion Detection System (IDS) Snort[12]. The detection process is done with the aim to help network administrators to minimize manual tasks undertaken in the search for evidence of an attack on the data of each visitor who is deliberately flooding attack on a web server[13].

Forensic research network with the network computers contained in the Bureau of Information and Communication Technology (ICT)[14], University of Muhammadiyah Magelang. From the description of the ICT network administrator, University of Muhammadiyah Magelang most attacks are attacking flooding. therefore required an investigation and forensic investigation network in the University of Muhammadiyah Magelang.

II. BASIC THEORY

A. Network Forensic

Network forensics is defined in [19] as capture, recording, and analysis of network events in order to discover the source of security attacks or other problem incidents. In other words, network forensics involves capturing, recording and analyzing of network traffic. The network data is derived from the existing network security appliances such as firewall or

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

intrusion detection system, examined for attack characterization, and investigated to trace back to the attacker. In many cases, certain crimes which do not break network security policies but might be legally prosecutable. Those crimes can be handled only by network forensics.

B. Model Process Forensic

The template is used to format your paper and style the text. All margins, column widths, line spaces, and text fonts are prescribed; please do not alter them. You may note peculiarities. For example, the head margin in this template measures proportionately more than is customary. This measurement and others are deliberate, using specifications that anticipate your paper as one part of the entire proceedings, and not as an independent document. Please do not revise any of the current designations.

C. Intrusion Detection System (IDS)

The software application or hardware device that can detect suspicious activity in a network system. Intrusion Detection System (IDS)[11]. Intrusion Detection System (IDS) can perform inspections of inbound and outbound traffic in a system or network, do the analysis and find evidence of experiments (infiltration)[15].Intrusion Detection System (IDS) are passive which can only detect the presence of an intruder to inform the network administrator that there is an attack or disruption to the network. Intrusion Detection System (IDS) is divided into two types, namely[16]:

- Network-based Intrusion Detection System (NIDS)

  All traffic flowing into a network will be analyzed to find whether there was an attempted attack or intrusion into the network system.

- Host-based Intrusion Detection System (HIDS)

  Activities of a host of individual networks will be monitored if they are in an attempted attack or intrusion into it or not.

D. Snort

Snort is a software to detect instruction on the system[17], capable of analyzing in real-time traffic and logging IP Address, able to analyze the port and detect all sorts of attacks from outside[18]. Snort works in three modes package as shown in figure 1, namely:

- Packet sniffer mode

  In a packet sniffer mode, Snort works as a sniffer to see the data traffic on computer networks.

- Packet Logger

  None of the packets on the network will be analyzed.

- Intrusion Detection Mode

  In this mode, Snort will serve to detect attacks made through a computer network.

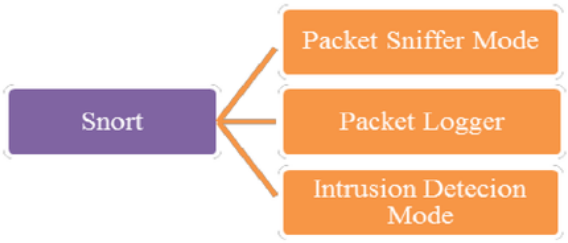

Figure 1: Snort detection

III. METHODOLOGY

Flooding attack detection configuration phase consists of Intrusion Detection System (IDS) Snort. This configuration is performed to detect flooding attack on a web server, after configuration Intrusion Detection System (IDS) Snort the next step flooding conduct simulated attacks to test whether the Intrusion Detection System (IDS) Snort has been successfully installed. Snort log files can be saved in a file p.cap, it will be analyzed to obtain the results of the forensic evidence of the intruder on a web server.

A. Intrusion Detection System (IDS) Snort Configuration

Configuration phase Intrusion Detection System (IDS) Snort performed to detect any demand (request) data, either by request or attack. after configuring snort, then the next rule configuration in accordance with the rules that have been owned by the snort to detect attacks flooding.

B. Flooding Attack Scenario

Phase flooding attack scenario was conducted to test whether the configuration Intrusion Detection System (IDS) Snort on the web server has been successfully installed. The simulation was performed using the LOIC tool used to test Intrusion Detection System (IDS) Snort to detect attacks flooding. The drill began with the sending IP packets on a target and selected the port will be attacked.

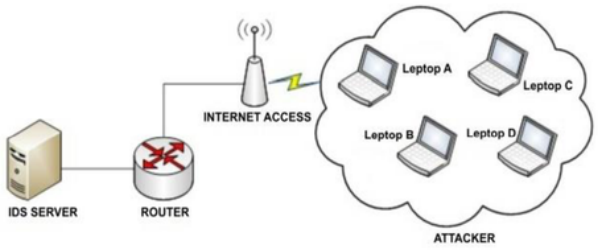

Figure 2: Simulation Flooding attack

Scenario of flooding attack as show by figure 2, carried out from several directions that connected to the Internet, by using the LOIC tool. The server Muh University of Mgl is targeted Flooding attack simulation to test whether the Snort IDS has worked well. During the simulation, flooding attacks carried out for about 15 minutes. During the simulated attack lasted

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

flooding a target server running IDS Snort to capture traffic and will get Snort log file shaped p.cap file.

IV. IMPLEMENTATION & RESULT

Phase analysis was used to reconstruct the results of Snort logfile to obtain evidence. Muh University of Mgl network topology is distributed (dispersed), the development of a star topology. ICT Muh University of Mgl into the center once the division of bandwidth in each faculty. The topology can be seen in figure 3.

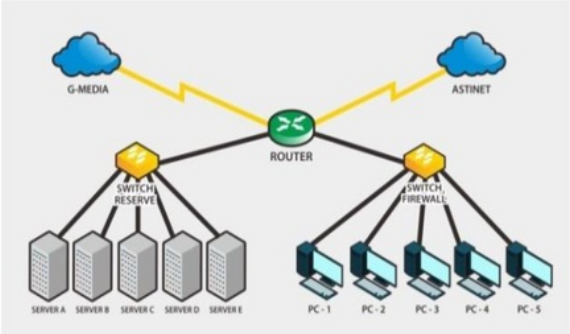

Figure 3: Topology University of Muhammadiyah Magelang

A. Implemetation Model Process Forensic

Implementation of network forensics process model in the architectural design of network forensics in detecting flooding attack on a web server Muh University Mgl. Detection of flooding attacks seen in figure 4.2. The simulation process cases that are trying to attack the target web server and Intrusion Detection System (IDS) Snort detects an intruder attempted flooding attacks by matching rules / rule that has been owned by Snort. Intrusion Detection System (IDS) Snort will record all activities towards the delivery of data to the target server. Thus the log file will be stored in a log file Snort. So the intruder will be analyzed to look for forensic evidence by using Wireshark to reconstruct characteristics of log files contained on Snort.

B. Model Process Forensic

The results of this analysis have four stages Model Process Forensic:

- Phase Collection

  Collection evidence in this study used recordings of traffic IDS. IDS is implemented for about three months during the study. IDS reconstruction process begins after the catch traffic deemed a predetermined rule. The process of taking payload as flooding attack file in this study as figure 4.

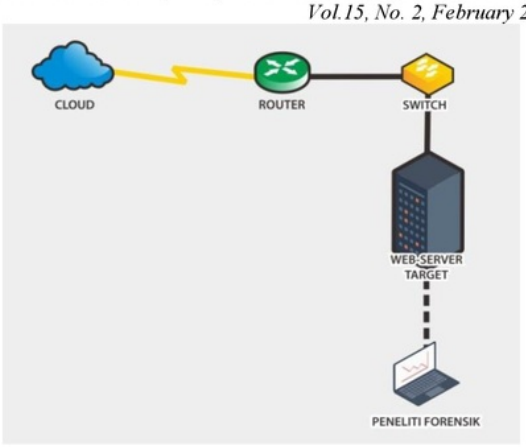

Figure 4: Data Collection Stages

- Phase Examination

  Intrusion Detection System (IDS) used Snort forensic investigators in examining the log file found on Snort in the capture (p.cap) b entering parameters to be plugged into Snort. The inspection process is going through a phase in figure 5.

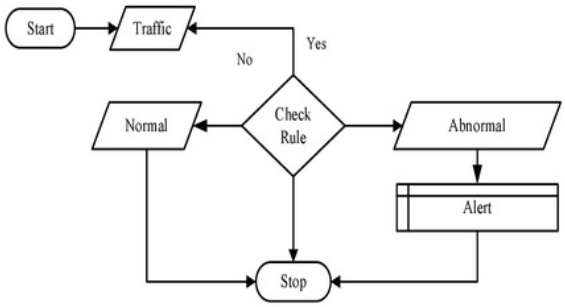

Figure 5. Detection IDS Snort

- Phase Analysis

  At this stage of the analysis of log files will be checked, the log files that have been recovered will be examination one by one to determine changes in the network and to see a timestamp. Flooding attacks will be visible when the request to the web server University of Muhammadiyah Magelang increased capture traffic that is an anomaly. Then flooding attacks are sent from the attacker so that traffic will increase. In addition to traffic conducted investigator using a remote SSH, also can be in the graphic user requesting increased in figure 6.

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

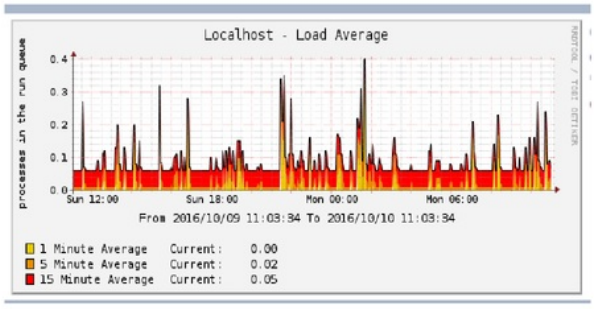

Figure 6: Load Average

After the Snort log files are recorded, the log file will be taken and analyzed using Wireshark to have this forensic evidence. In the picture seen demand exceed 30 packets in one second. When detected, the Snort rules will give a warning message in the alerts as shown in figure 7.

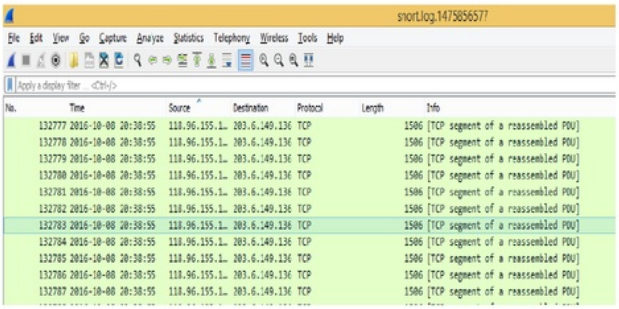

Figure 7: Log Snort in Wireshark

With the help of filters ip.src == flooding attack will then be analyzed to select the rows one by one to open the menu on UDP follow that will result in Figure 8.

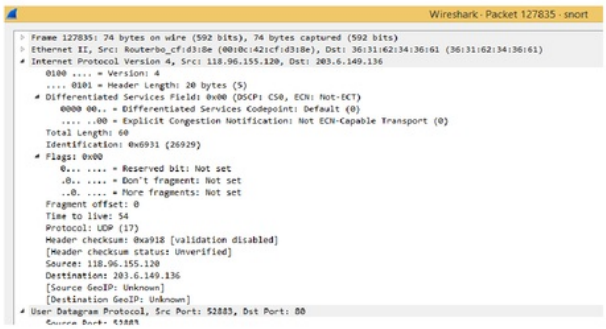

Figure 8: UDP Follow

From the collection of the line can have one line to perform analysis on any part of the frame that represents a frame in an attack packet flooding of IP address 118.96.155.120 has a length (length) range in the 70s Bytes (74 Bytes). On the Internet Protocol Version 4, to read as 118.96.55.120 IP source and destination IP address visible 203.6.149.136 with 20 Bytes header length and the total length of 60. on the part of the user datagram protocol, source port reads as 52 883 and destination port read as 80. If the filter is returned to the ip.src == 118.96.55.120 and investigated in another frame, the source port is immutable, but still in a great range (ports 51000-64000). log file analysis results obtained 15 IP address that has acted illegally flooding attacks web servers.

In addition, the analysis continued with statistics module endpoint in Wireshark used to collect attack packets contained in log files Intrusion Detection System (IDS) Snort during the attack simulation. In Figure 9 below explains that the IP address has a different load on each package and at different speeds in each of its bytes.

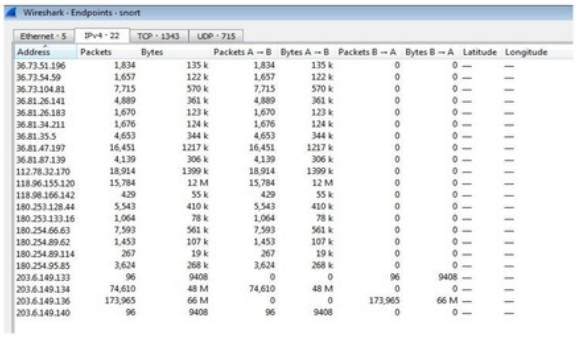

Figure 9:Statistic Endpoint Snort

- Phase Reporting

  At the reporting stage is the last stage in the forensic process model. This stage was the presentation of all the findings in this study. Based on the analysis that has been done then obtained 15 IP address which becomes the findings in this research scenario, as shown in Table 10.

V. CONCLUSION

IDS system that is applicable to the scenario of this study have worked as expected, the system can record the activities of the network in the form of log files with the extension p.cap the file can be analyzed with Wireshark tool. Based on the analysis that has been done, it was found that 15 IP address web servers perform illegal actions, which led to overload traffic.

By applying the forensic process model, IDS systems on a web server can be used to help meet the needs of forensics at the Muh University of Mgl, other than that the administrator can monitor and prevent future attacks.

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

TABLE 10 FILE LOG SNORT

No.	Timestamp	Source	Dest. IP	Protokol	Source Port	Dest. Port	Payload
1	7/10/2016 17:26	203.6.149.140	203.x.x.136	ICMP	-	-	40ddf957603e0e006e69746f72696e6763616374692d6d6f…
2	7/10/2016 16:32	112.78.32.170	203.x.x.136	UDP	52658	80	697320666966e6520746f6f2e204465737564657375646573...
3	8/10/2016 19:28	36.73.51.196	203.x.x.136	UDP	58894	80	697320666966e6520746f6f2e204465737564657375646573...
4	8/10/2016 20:36	118.96.155.120	203.x.x.136	UDP	52882	80	697320666966e6520746f6f2e204465737564657375646573...
5	8/10/2016 19:45	180.253.133.16	203.x.x.136	UDP	60052	80	697320666966e6520746f6f2e204465737564657375646573...
6	8/10/2016 20:26	180.253.128.44	203.x.x.136	UDP	63749	80	697320666966e6520746f6f2e204465737564657375646573…
7	8/10/2016 20:09	180.254.95.85	203.x.x.136	UDP	53820	80	697320666966e6520746f6f2e204465737564657375646573...
8	8/10/2016 20:15	180.254.89.62	203.x.x.136	UDP	61246	80	697320666966e6520746f6f2e204465737564657375646573...
9	8/10/2016 20:51	180.254.66.63	203.x.x.136	UDP	54948	80	697320666966e6520746f6f2e204465737564657375646573...
10	8/10/2016 20:07	36.73.104.81	203.x.x.136	UDP	53817	80	697320666966e6520746f6f2e204465737564657375646573...
11	8/10/2016 20:08	36.73.54.59	203.x.x.136	UDP	53814	80	697320666966e6520746f6f2e204465737564657375646573...
12	8/10/2016 20:20	36.81.87.139	203.x.x.136	UDP	63748	80	697320666966e6520746f6f2e204465737564657375646573...
13	8/10/2016 20:25	36.81.26.141	203.x.x.136	UDP	63756	80	697320666966e6520746f6f2e204465737564657375646573...
14	10/10/2016 6:34	36.81.47.197	203.x.x.136	UDP	55291	80	697320666966e6520746f6f2e204465737564657375646573...
15	10/10/2016 6:34	36.81.35.5	203.x.x.136	UDP	56328	80	697320666966e6520746f6f2e204465737564657375646573...

REFERENCES

[1] J. D. Ndibwile and A. Govardhan, "Web Server Protection against Application Layer DDoS Attacks using Machine Learning and Traffic Authentication," pp. 261–267, 2015.

[2] A. Iswardani and I. Riadi, "Denial Of Service Log Analysis Using Density K-Means Method," vol. 83, no. 2, pp. 299–302, 2016.

[3] T. A. Cahyanto and Y. Prayudi, "Web Server Logs Forensic Investigation to Find Attack's Digital Evidence Using Hidden Markov Models Method ," *Snati*, pp. 15–19, 2014.

[4] K. K. Sindhu and B. B. Meshram, "Digital Forensics and Cyber Crime Datamining," vol. 2012, no. July, pp. 196–201, 2012.

[5] R. Utami Putri and J. E. Istiyanto, "Network Forensic Analysis Case Studies SQL Injection Attacks on Server Universitas Gadjah Mada," *Int. J. Comput. Sci. Secur.*, vol. 6, no. 2, 2012.

[6] R. K. Idowu, R. C. M, and Z. A. L. I. Othman, "Denial Of Service Attack Detection Using Trapezoidal Fuzzy Reasoning Spiking Neural P," vol. 75, no. 3, pp. 397–404, 2015.

[7] E. Lee, "Detection Of Flooded Areas From Multitemporal Sar Images 2016 Second International Conference on Science Technology Engineering And Management," 2016.

[8] V. Shah and A. K. Aggarwal, "Heterogeneous fusion of IDS alerts for detecting DOS attacks," *Proc. - 1st Int. Conf. Comput. Commun. Control Autom. ICCUBEA 2015*, pp. 153–158, 2015.

[9] A. Dewiyana, A. Hadi, U. Mara, U. Mara, and U. Mara, "IDS Using Mitigation Rules Approach to Mitigate ICMP Attacks," 2013.

[10] A. Saboor, M. Akhlaq, and B. Aslam, "Experimental Evaluation of Snort against DDoS Attacks under Different Hardware Configurations," pp. 31–37, 2013.

[11] N. M. Lanke and C. H. R. Jacob, "Detection of DDOS Attacks Using Snort Detection," vol. 2, no. 9, pp. 13–17, 2014.

[12] A. I. Technology, T. Nadu, and T. Nadu, "Flow Based Multi Feature

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

Inference Model For Detection Of DDoS Attacks In Network Immune," vol. 67, no. 2, pp. 519–526, 2014.
[13] S. Sharma, "On Selection of Attributes for Entropy Based Detection of DDoS," pp. 1096–1100, 2015.
[14] "Guide to Integrating Forensic Techniques into Incident Response."
[15] "Introduction to Snort A . Sniffer Mode," pp. 1–11.
[16] H. Toumi, A. Eddaoui, and M. Talea, "Cooperative Intrusion Detection System Framework Using Mobile Agents For Cloud Computing," vol. 70, no. 1, 2014.
[17] H. A. D. Eugene C. Ezin, "Java-Based Intrusion Detection System in a Wired Network," vol. 9, no. 11, 2011
[18] B. Khadka, C. Withana, A. Alsadoon, and A. Elchouemi, "Distributed Denial of Service attack on Cloud : Detection and Prevention," 2015.
[19] Nguyen, K., Tran, D., Ma., & Shama, D. (2014) An Approach to Detect Network Attacks Applied for Network Forensics, 655-660.

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

Network Forensics For Detecting Flooding Attack On Web Server

ORIGINALITY REPORT

4%

SIMILARITY INDEX

PRIMARY SOURCES

1	article.wn.com Internet	33 words —	1%
2	digilib.uin-suka.ac.id Internet	28 words —	1%
3	Pilli, E.S.. "Network forensic frameworks: Survey and research challenges", Digital Investigation, 201010 Crossref	27 words —	1%
4	www.jatit.org Internet	20 words —	1%
5	Mohd Nazri Ismail, Mohd Taha Ismail. "Framework of Intrusion Detection System via Snort Application on Campus Network Environment", 2009 International Conference on Future Computer and Communication, 2009 Crossref	16 words —	1%

EXCLUDE QUOTES OFF

EXCLUDE MATCHES OFF

EXCLUDE BIBLIOGRAPHY OFF