JOURNAL OF SOFTWARE ENGINEERING & INTELLIGENT SYSTEMS
ISSN 2518-8739
30th April 2019, Volume 4, Issue 1, JSEIS, CADMEI Copyright © 2016-2019
www.jseis.org

INTRUSION PREVENTION SYSTEM ANALYSIS USING DATABASE RULE AND SIGNATURE ON UNIFIED THREAT MANAGEMENT

[1]IYAN RAHDIAN, [2]WIDYA SILFIANTI

[1,2]Department of Computer Science and Information Technology, Faculty of Information System, Gunadarma University, Depok, Indonesia
Email: [1]iyanrahdian@gmail.com [2]wsilfi@staff.gunadarma.ac.id

ABSTRACT

The use of the internet in the business world is making businesses more effective in improving services and cost efficiency. The internet enables computers to connect to each other with external networks. However, it has the risk of intrusion such as unknown IP addresses entering the network, causing slow connections between networks, even making web pages and applications inaccessible. Network security in this case is very important to detect and block intrusions; A solution to network security is needed such as the Unified Threat Management (UTM). One of the functions of UTM is Intrusion Prevention System (IPS), which has the function of analysing intrusion using methods from database rules and signatures. IPS compares incoming data packets with patterns in database rules and signatures, if it has the same pattern then the package is considered as intrusion and is blocked, if the package does not have the same pattern as the pattern in the database rule and signatures, the data package is not considered as an intrusion. The use of IPS can provide information on intrusion and how to block them, making it easier to improve network security and accuracy in detecting systems infected with DDoS malware in 1000 tests performed, getting accuracy of about 98% with 12 false positives that occur during the experiment.

Keywords: network security; information system security; intruder prevention system (IPS); unified threat management (UTM);

Published: 30th April, 2019

Funding: Authors have no funds.

Article Type: Research Article

1. INTRODUCTION

At this time almost, all activities of human life are related to the internet. The use of internet connected computers to each other, thus facilitating the flow of information. This is possible due to the rapid development of network technology, especially in the use of internet. According to the internetworldstats.com website on June 30, 2018, the number of internet users in the world is dominated by the Asian population, amounting to 49.0%, of the total world internet users [1] as shown in Figure 1.

The use of digital and internet technology in the business world is an attempt to make businesses more effective and efficient [2]. Many benefits and advantages can be obtained through the use of the internet network; of course, there are also problems that might arise, especially in terms of security, such as unknown IP addresses entering the network. Causing a slowdown of connections between networks because of over capacitated bandwidth, making the web pages not working properly and applications inaccessible.

Security is not just about keeping people in the network from the outside world, it also provides access to the network in the desired method [3]. Network security system is necessary in this condition, it can detect intrusions and overcome attacks from intruders, detect activities on the network, and use bandwidth and blocking. One solution is to use Intrusion Prevention System (IPS), IPS is a detection tool that can recognize the presence of intrusions by analysing incoming data packets, then compare them with database rules and signatures, which contain intrusion packet patterns, if the data packet has the same pattern or one pattern that is in the database rule and signatures, then the package is considered as intrusion, and vice versa. If the data package does not have the same pattern with the pattern in the database rule and signatures, then the data package is not considered as intrusion. IPS is an approach that is often used to build computer security systems, IPS combines firewall techniques and intrusion detection system (IDS) methods. This technology can be used to prevent attacks entering the local network by checking and recording all data packets and recognizing packets with sensors when the attack is identified. So IPS acts like a firewall that will allow or block data packets [4].

Corresponding Author: Iyan Rahdian
Email Address: iyanrahdian@gmail.com

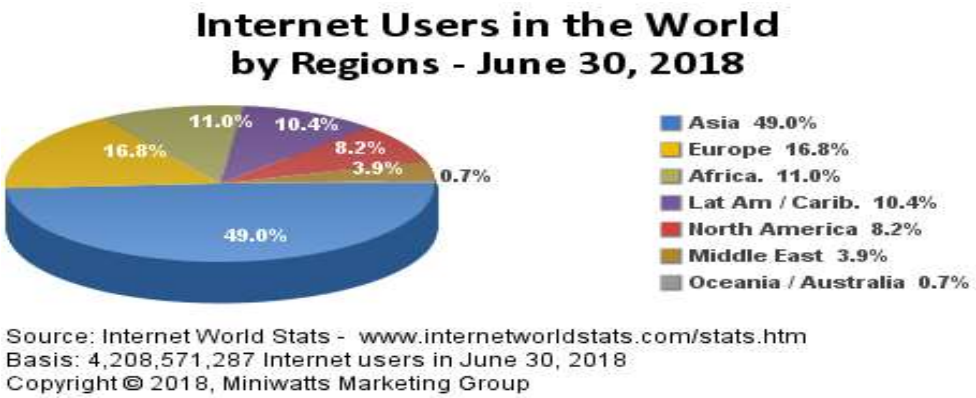

Figure. 1 Number of internet users in the world

As stated by Whitman and Mattord "Information security in this case is protection of information and critical characteristics, including the system of software and hardware used to store and transmit information is also very important" [5]. Internet network security is very important, but the cost of security from this interference is significant, on the other hand the level of network security is difficult to measure, if compared with the costs incurred, many companies are reluctant to pay, to improve network security [6]. A reliable security system, with the main goal of a security system is to build a system that can be relied upon in the face of external threats, or an attack [7].

2. RESEARCH PROCESS

In conducting the preparation of this research process to make it easier to make the expected model, the author describes in 4 stages namely:

a. Identification of Problems
b. Data Collection and Processing
c. Network Security System Modelling
d. Simulation and recommendations

Some quotes are taken from literature reviews and literature studies, such as books, articles, papers, theses and journals. Including other sources of information related to network security material, through the internet as writing guidelines. The author makes the mindset as a systematic writing to achieve the expected goals, including several methods that will be used in determining the variables and models, according to existing sources to be made into a paper.

The author takes a number of previous studies that have relevance to the research conducted. The following are previous studies in Table 1, which have been carried out and used as material for writing references in discussing related research.

Table. 1 Previous research

No	Research Paper	Title	Method	Results	Gap
1	Jung Woo Seo and Sang Jin Lee. [8]	*A study on efficient detection of network-based IP spoofing DDoS and malware-infected Systems.*	The method used is DDoS Malware Finder (DMF) algorithm and network forensics table	Shows detection of DDoS attack mechanism and Algorithm used can analyze real time traffic headers.	The level of response is long to analyze the passing network traffic
2	Shirin Bateni and Ali Asghar Khavasi. [9]	*Design a security firewall policy to filter incoming traffic in packet switched networks using classification methods.*	The method that uses the detection and divider method of network input traffic	The results of the analysis of the research conducted are that security policies on the network firewall provide enough data instructions to the central network.	Adding other qualification s to the network, it will take a long time to learn on the

					running machine.
3	Wu J, Peng D, Li Z, Zhao L and Ling H. [10]	*Network Intrusion Detection Based on a General Regression Neural Network Optimized by an Improved Artificial Immune Algorithm.*	The method that uses the algorithm method of Artificial Immune Algorithm with Elitist Strategies-General Regression Neural Network (AIAE-GRNN).	The results show that this method has a higher resistance and accuracy than other algorithms.	Has a high complexity with other algorithms.
4	Min-Joo Kang and Je-Won Kang. [11]	*Intrusion Detection System Using Deep Neural Network (DNN) for In-Vehicle Network Security.*	The method used is: the method of pre-training the network in depth, followed by the conventional stochastic gradient descent method.	The experimental results show that the proposed technique can provide a response to the current time of the attack with sufficiently accurate detection The average ratio is about 98% when computational complexity.	Network Test-Bed and trial of the Open Car Test-bed and Network Experiments (OCTANE) network in simulations on vehicles are very difficult and very high cost.
5	Wen S, Meng Q, Feng C Ana Tang C. [12]	*Protocol vulnerability detection based on network traffic analysis and binary reverse engineering.*	A method that uses a binary reverse engineering method using genetic algorithms.	The results of the analysis of the research conducted are the results showing that testing fully considers the characteristics of network protocol vulnerability detection.	Using the binary reverse engineering method and the genetic algorithm produces a low test hit rate.

The author explains the differences and similarities of previous researchers as material for writing references and specifies the method to be used:

1. Data used in previous research based on quantitative approaches, with experiments on networks directly using testbed on internal networks and prototypes. Through the DDoS Malware Finder (DMF) algorithm with three phases of extraction, analysis and detection. So that it can indicate the time of the DDos attack and the time of discovery when the local host has been infected with DDos malware.
2. Quantitative approach with real data that is in an organization in the Waikato University network, by designing implementation algorithms and data sets, and comparing incoming data to get a percentage that is easy to understand, to be classified into the specified categories.
3. This research uses a quantitative approach, the use of parameters built by the Deep Neutral Network (DNN), trained with probability-based feature vectors extracted from the network packet vehicles for certain packages, the Deep Neutral Network (DNN) gives the possibility that each class will carry out an attack package analysis so that the sensor can identify who is attacking on a mobile vehicle network such as 3G, 4G and WIFI.
4. The results of the research used are the use of network simulation by designing implementation algorithms and a set of data, and comparing the incoming data to get the number of percentages that are easy to understand, then classified in the specified categories.
5. This research conducts a quantitative process with the use of simulations on computer networks, with a Low-test case hit rate on the network in the protocol. With the first stage: pre-processing stages, second stage: block-based protocol analysis and the last stage: reverse engineering binaries. Consider the characteristics of network protocol vulnerability detection by combining the analysis of network traffic

and reverse binary engineering, then analysing protocol formats that result in effective and efficient attack detection.

a) Identification of Problems

System analysis according to Tata's statement. "Studying the system that runs with all users along with all the problems, the purpose of the system analysis is to get a clear understanding of the existing problems, in addition to clarifying the form of system logic running conceptually, as reference material for drafting proposed systems "[13].

Based on the system analysis and the background that has been stated previously, problems identification that will be examined by the author in this study are as follows:

1. How to detect and overcome network intrusion problems from intruders?
2. How to understand the cause of slow access to certain services because the bandwidth you have is full of unidentified activities?

Of the many problems faced in information technology security, this research is limited to solving problems that exist in parts of network security to ensure that the discussion of this study does not deviate, boundaries are needed. The limitations of this study are as follows: Analysing network security by using Intrusion Prevention System on the network. As well as identifying and evaluating problems, opportunities, obstacles that occur and expected needs so that improvements can be proposed [14].

In accordance with the problems that have been formulated, the objectives of this study are as follows: Provide instructions in implementing network security, detect intrusion, improve network security and overcome network security issues.

b) Data collection and processing

In the network security system modelling phase, it is done using IPS with the database rule method and signature. It consists of three phases, extraction, analysis and detection, in the first stage of extraction in detecting network attacks, by collecting actual time logs on network traffic, gathering network traffic configured in mirroring ports, made to extract detailed information, such as IP addresses and services from ethernet headers. In the second stage analysing the attack with IP addresses that have been extracted and services, then compared with information attributes that are in the database rule and signature. In the third stage of detection based on data extraction, the time interval will be calculated if there is a match between the IP address and service from real time network traffic, with the value that is in the database rule and the signature to determine whether there is an attack or not.

In the process of implementing database rule and signature methods in gathering network traffic information, mirroring ports on layer 3 switches are needed to detect and monitor intrusions based on network traffic analysis. The process is explained in figure 2. Schematic diagram in analysing and collecting data packages in network traffic in real time.

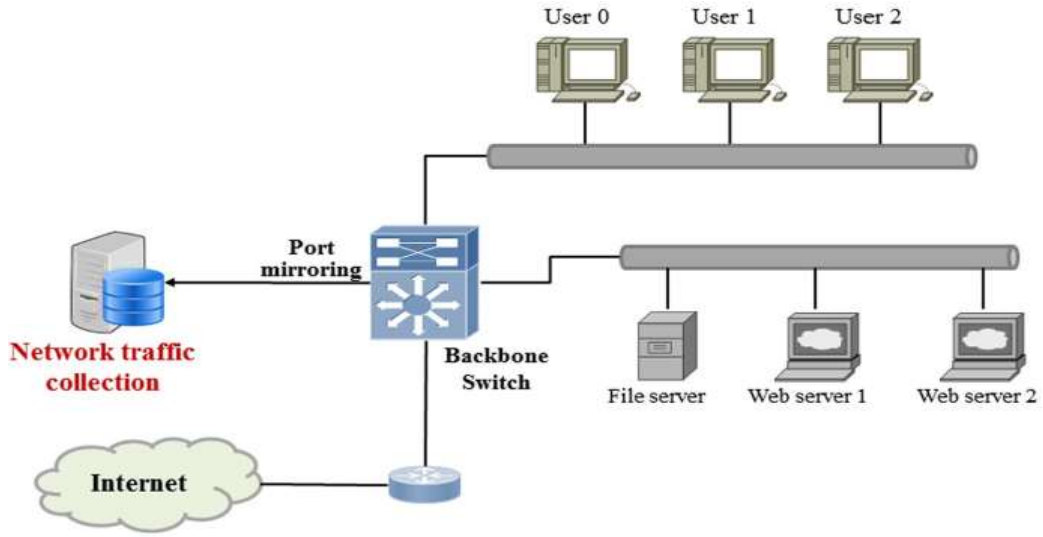

Figure. 2 Schematic diagram of network traffic in real time.

The next process is extracting information, through several protocols shown in Figure 3. A set of protocols used in extracting data packet information in real time.

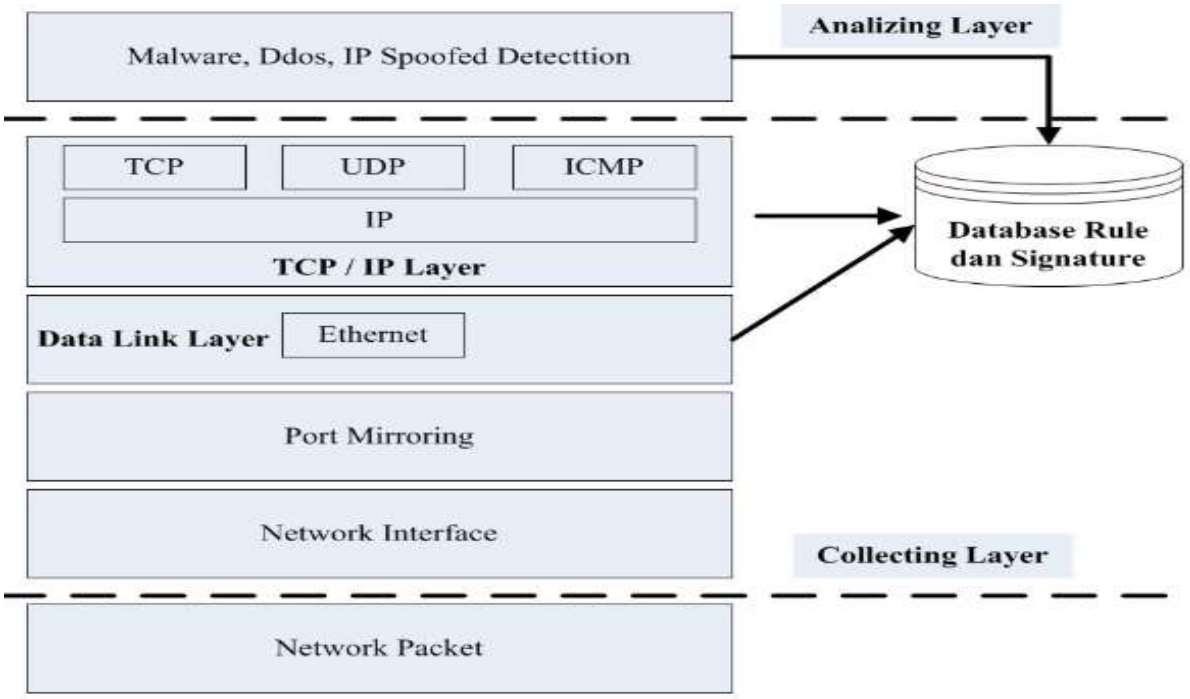

Figure. 3 Group of protocols used in extracting data packet information in real time.

The explanation shown in figure 3. Attribute information by TCP / IP and Ethernet headers are extracted from collected traffic and used as basic data in analysing the database rules and signatures.

As mentioned earlier about the method proposed to detect intrusion attacks is to use database rule methods and signatures, to analyze time and data packets in network traffic, thereby determining DDos, IP-spoofed using IP addresses and services. Then it detects hosts infected with malware, DDos, IP-spoofed and botnets, then calculates the connection time to the destination IP address, and the frequency of connection used.

After intrusion has been detected with the proposed methodology, it is important to find hosts that are infected with malware and eliminate the root cause. As it is not possible to block certain IP addresses on the firewall and even if we block various IP addresses on the network, it will experience a delay or stop as a result of the large volume of traffic generated by malware. Therefore, it is necessary to immediately quarantine the host which results in DDoS attacks to the network. IP-spoofed will cause network resources to be consumed, so web services and intranet services will not run normally, resources will run out over time.

Action needs to be taken against intrusions that have been infected, when the attack is already on an internal network Local Area Network (LAN). By detecting the annoying system, then preventing it before using network resources, it also needs to understand the causes of intrusion by storing logs is very useful to eliminate weak points in network security systems, so that they can understand network traffic flow and use existing information in the log analyzer in analysing infected systems and their tendency to attack.

c) Network Security System Configuration

Unified threat management (UTM) is a new security device that has been developed from a firewall that previously only inspected the origin and destination IP addresses, as well as the origin and destination ports to be broader with features such as Intrusion Prevention System (IPS), Virtual Private Network (VPN), Anti-Spam, Anti-Virus and URL Filtering [15].

In this section we will explain the design and implementation of Intrusion Prevention System (IPS) in Unified Threat Management (UTM), placement of UTM positions is very important, because it is related to accuracy, effectiveness of detection and blocking intrusions. IPS will work together with Firewall in blocking and allowing data communication in accordance with the rules that have been made. If an attack occurs, IPS will call Firewall to block the attack by disconnecting or simply dropping the data packet.

By implementing IPS in UTM, the bridging mode automatically across the entire network, will be directed to all data communications through the IPS system, to be collected and analyzed in the database rule and signature.

Following is the configuration of Fortigate on the core switch to get all data communications over the network.

```
# monitor session 1 source interface fastEthernet0/10 tx
# monitor session 1 source interface fastEthernet0/2 rx
# monitor session 1 source interface fastEthernet0/3 rx
# monitor session 1 source interface port-channel 102 rx
# monitor session 1 destination remote vlan 901 reflector-port fastEthernet0/1
```

Figure. 4 Configure the core switch for port mirroring

In Figure 4. Describe several ports configured to connect between each network with other networks in order to exchange data packets and manage the data circulation. By sorting or filtering the required data to pass through, it will automatically determine the source and destination segments of the data package [16].

It is also necessary to configure Fortigate in port management, which aims to get the log and will be directed to the log analyzer. Figure 5 shows the configuration of Fortigate in port management.

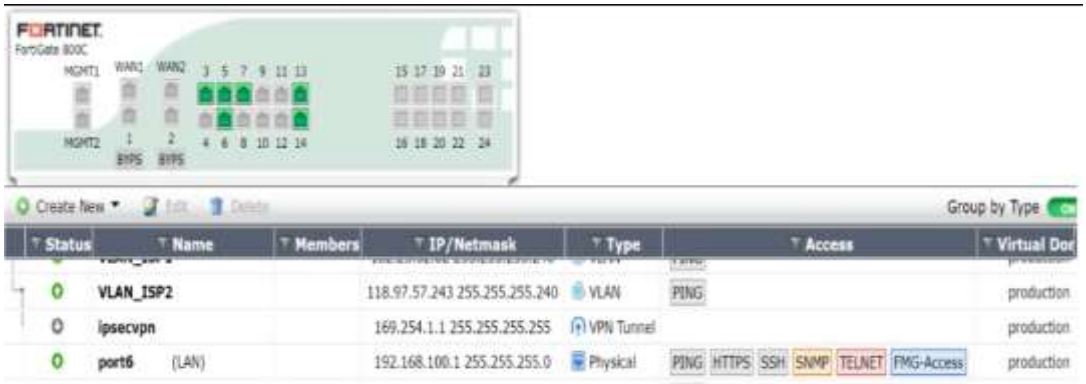

Figure. 5 Configuration of Fortigate for the management port

The explanation in Figure 5. Configuration in port management, describes the ports that will be used such as: ping, https, SSH, telnet, snmp and access to Fortigate manager, and some VLANs that will be logged in the traffic log and IP port management to access Fortigate Manager.

Network security systems using Unified Threat Management (UTM), can be run simultaneously without the need to use a lot of network hardware to perform network security functions. With the UTM, the network security system can be protected with only one hardware [17].

The advantages of the UTM network security system as a network security system are as follows [18]:

- Comprehensive security which includes Firewall, Web Proxy, AntiVirus, AntiSpam, and Intrusion Prevention System.
- UTM system security solutions that can be managed and monitored on one network device management.
- Ease of implementation and integration with other network devices. Includes Firewall, Web Proxy, Antivirus, Anti Spam, and Intrusion Prevention System.

In addition, the client, especially the network administrator, can be easier to check if there is a problem with the network because it only needs to check one device that can be done through a web browser interface so that it makes it easier for network administrators to find problems.

d) Simulation and recommendations

In this study network topology with unified threat management is used. As well as conducting trials of attacks on the Internet and Local Area Networks (LAN) by monitoring network traffic in real-time. The security system will be evaluated by collecting data from various logs and analyzed to see the results.

Data is displayed and collected using information - attribute information that is in the database rule and signatures that are in Unified Threat Management (UTM). Shown in Table 2 are some information attributes that are in the database rule and signatures.

Table. 2 Attribute information of database rules and signatures

Attribute	Type	Feature data	Description
SN	VARCHAR(20)	S00001	Sequence number to traffic
SGN	VARCHAR(20)	G00001	Same group number with the same destination IP
SRCIP	VARCHAR(15)	58.203.201.36	Source IP
SRCPORT	VARCHAR(6)	5312	Source Port
DSTIP	VARCHAR(15)	211.106.66.102	Destination IP
DSTPORT	VARCHAR(6)	80	Destination Port
SRVC	VARCHAR(17)	42781	Service
PT	VARCHAR(8)	TCP	Protocol
AT	DATE	2016.08.12 07:05:28	Destination IP connection time
TIN	FLOAT	2 s	Interval from previous traffic
CND	INTEGER	28 hit	Destination IP connection hits
RATD	FLOAT	136 s	Interval from previous traffic connected to destination IP
CNTI	INTEGER	12 hit	Hits to the destination IP over 3 min
STATE	VARCHAR(20)	Abnormal	Traffic anomaly status

Next is an experiment to detect a system infected with malware after detecting IP spoofed, DDoS based on analysis of real-time traffic. This section examines the system model for the proposed method. By collecting logs on network traffic, configuring several network devices by means of mirroring ports, which are configured in the Layer 3 switch. To detect malware infections based on analysis of traffic directed to network equipment and identify the infected system.

The rule database and signature consist of traffic header attribute information. If there is a match between the IP address and service from real-time traffic with the property value in the Database rule and signature. These results are used to check DDoS-spoofed malware infections. Using the algorithm shown in Table 3. Finding a system infected by malware.

Table. 3 Finding of a system infected by malware.

```
Input : isMalwareddos, macVal          where isMalwareddos is a detection result of algorithm
Output : infectedHost

begin
    j ← ∅
    candidateIP[ ] ← null
    infectedHost ← null
    r[ ][ ] ← EntryPoint(DMF Table)

    if isMalwareddos is true then
      while r is not the end of r do
        i ← ∅,n ← ∅
        cndVal← r[i][10]
        if { macVal == r[i][6] and cndVal ==1 and r≠null } then
        //MAC address is the same and CND field value is 1
            candidateIP[j] ← r[i][2]          //candidateIP array stores the Source IP
            candidateDate[j++] ← r[i][8]      //candidateDate array stores the Access Time
        end
        i ← i + 1
      end

      cmpDate ← null
      foreach { candidateIP.length() ≥ n } do
        if { candidateDate[n] ≥ cmpDate } then
          cmpDate ← candidateDate[n]
          infectedHost ← candidateIP[n]       // infectedHost stores malware infection host
        end
        n ← n + 1
    return infectedHost
end
```

Based on Table 3, it is necessary to find a host that is infected with malware and eliminate the cause. Because IP addresses are spoofed, it is not possible to block certain IP addresses in the firewall and even if we block various IP addresses, the internal network will stop or experience extreme delays as a result of the large volume of traffic generated by malware. Finding an infected host needs to immediately quarantine the host, which results in DDoS attacks on the network.

The following data are used and collected using functions in the UTM Log analyzer during the testing period. In Table 4. Shows the Log analyzer that provides information on the occurrence of intrusion.

Table. 4 Log analyzer intrusion information.

Source IP	Destination IP	Action	Service	Attack ID	Source Port	Destination Port	Attack Name
192.168.59.6	167.99.50.62	Dropped	udp/53413	42781	43603	53413	Netcore.Netis.
50.115.166.167	192.168.59.6	Dropped	udp/53413	42781	32930	53413	Netcore.Netis
184.105.247.251	192.168.59.6	Dropped	udp/5353	26069	5043	5353	Avahi.NULL.UDP .Packet.DoS
111.255.123.91	192.168.59.6	Dropped	udp/53413	42781	49297	53413	Netcore.Netis
206.189.214.35	192.168.59.6	Dropped	udp/53413	42781	41118	53413	Netcore.Netis.
206.189.214.35	192.168.59.6	Dropped	udp/53413	42781	53542	53413	Netcore.Netis.
104.248.189.38	192.168.59.6	Dropped	udp/53413	42781	36289	53413	Netcore.Netis.
104.248.189.38	192.168.59.6	Dropped	udp/53413	42781	52741	53413	Netcore.Netis.
138.68.60.114	192.168.59.6	Dropped	udp/53413	42781	34748	53413	Netcore.Netis.

Table 4. Indicates system monitoring by UTM, detection carried out will be analyzed for an attack. Using sources from IP addresses and services extracted from Ethernet headers, then real-time traffic is compared with attribute information provided in the database rule and signature, to determine the DDoS infection attacks that have occurred with attack ID.

In the database rule and signature, log messages are recorded directly that occur in network traffic, due to violating network policies based on attack ID numbers found in the table log. The log analyzer does not record the type of attack log individually, otherwise the log analyzer records periodically when an attack is in progress, the log analyzer will match to several database rules and signatures.

Description of attacks and descriptions of attack log messages can be found on subtype and attack ID, all attack log messages have the same content column and are explained in figure 6. Detail intrusion log attack.

Figure. 6 Detail intrusion log attack

The results of the DDoS attack attribute analysis indicate that there is communication with IP sources and services used to infiltrate and carry out attacks. Namely a DDoS attack that is strong enough to cause outages to core networks in a gigabit Ethernet environment. The Unified Threat Management (UTM) firewall can detect and quickly respond to attacks before network resources run out when a large volume of DDoS attacks, by ordering the function of the firewall to drop the traffic.

e) Network security accuracy

Assessing accuracy in detecting systems infected with malware using the proposed method, the accuracy test is carried out under the following conditions:

- Installation of unified threat management devices testing and launching DDoS attacks.
- Analysis of attack and false positives features after varying IP addresses from a unified threat management test.
- Analysis of attack and false positives features after replacing network hardware and servers.

The accuracy of detecting a system infected with malware is calculated as follows:

$$\text{Accuracy (\%)} = 1 - \frac{\textit{false positive}s}{\textit{test number}} \times 100$$

False positives can be detected in two cases, the first case is detected because of an error in the network configuration after replacing the server, causing anomalous traffic or communication problems. The second case was detected because of changes in MAC addresses under ARP spoofing and the large number of requests to the server so that memory and processor increased rapidly, resulting in traffic jams or internal network intrusion.

The following are the results of calculating the accuracy of the system that detected DDoS attacks. Which is contained in Table 5. Calculation of the accuracy of system detection.

Table. 5 Calculation of system detection accuracy

Error Ratio	Accuracy (%)	Explanation
12:1000	98.8	TP rate = 0.988, FP = 12
8:600	98.7	TP rate = 0.987, FP = 8
2:400	99.5	TP rate = 0.995, FP = 2
1:100	99.0	TP rate = 0.99, FP = 1
0:50	100	TP rate = 1, FP = 0

The accuracy of detecting systems infected with DDoS malware is assessed in the tests described above and the average is obtained from 1000 runs. The detection accuracy is around 98% of the 12 false positives that occurred during the experiment. (Positive error is detected when there is an anomaly, error with network configuration or when ARP spoofing occurs).

3. CONCLUSION

Based on the analysis, design, implementation and evaluation of the network security system, the conclusions are as follows: The UTM security system serves to secure a comprehensive network including security features consisting of Firewall and Intrusion Prevention System (IPS). The UTM security system can be managed and monitored through a web-based administration program so that it can be done through other computers connected to the network system using a web browser. During implementation UTM has been successfully running in one management console and can be used to generate reports for network security equipment in the form of firewalls, bandwidth and Intrusion Prevention System (IPS). The log analyzer has functioned according to the system requirements so as to facilitate network administrators in monitoring network security, with the following functions: Log analyzers provide detailed report in the form of tables that can be displayed and stored in a certain time (daily, monthly and yearly). The reports produced can be in the form of graphics and have a feature to filter the results of the report that will be displayed. The log analyzer is able to provide a notification in the form of an email to the network administrator when a disturbance occurs that needs to be handled quickly.

ACKNOWLEDGEMENT

Special thanks to Gunadarma University of Indonesia for providing resources and kind support to carry out this research.

REFERENCES

1. World internet stats. *Number of world Internet users on 30 June 2018*. Available at: http://www.internetworldstats.com/stats.htm, [Accessed 20 June 2018].
2. Cavalcante, R. C., I. I. Bittencourt, A. P. Silva, M. Silva, E. Costa and R. *A Survey of Security in Multi-Agent Systems. Expert Systems with Applications.* 2016. *(39): 4835-4846.*
3. Stallings, William . *Cryptography and Network Security: Principles and Practice.* New Jersey: Prentice-Hall. 2015.
4. Raven Alder. *Snort 2.1 Intrusion Detection*, 2016. Second Edition. Rockland, MA 02370: Syngress Publishing, Inc.

5. Whitman, M. E., and H. J. Mattord. *Management of Information Security*. 3rd Edition. Thomson-Course Technology. 2015.
6. Hare, F. and J. Goldstein. *Guide for Conducting Risk Assessment. National Institute of Standards and Technology.* 2015.
7. Cavalcante, R. C., I. I. Bittencourt, A. P. Silva, M. Silva, E. Costa and R. *A Survey of Security in Multi-Agent Systems. Expert Systems with Applications*. (39): 4835-4846. 2015.
8. Jung Woo Seo and Sang Jin Lee. *A study on efficient detection of network-based IP spoofing DDoS and malware-infected Systems.* 2016. Springer Plus 5:1878 DOI 10.1186/s40064-016-3569-3.
9. Shirin Bateni and Ali Asghar Khavasi. *Design a security firewall policy to filter incoming traffic in packet switched networks using classification methods.* 2016. DOI:10.5902/2179-460X21530, ISSN on-line: 2179-460X.
10. Wu J, Peng D, Li Z, Zhao L, Ling H. *Network Intrusion Detection Based on a General Regression Neural Network Optimized by an Improved Artificial Immune Algorithm.* 2015. PLoS ONE 10 (3): e0120976. doi:10.1371/journal.pone.0120976.
11. Min-Joo Kang, Kang J-W. *Intrusion Detection System Using Deep Neural Network for In Vehicle Network Security.* 2016. PLoS ONE 11(6): e0155781. doi:10.1371/journal.pone.0155781.
12. Wen S, Meng Q, Feng C, Tang C. *Protocol vulnerability detection based on network traffic analysis and binary reverse engineering*. 2017. PLoS ONE 12(10): e0186188. https://doi.org/10.1371/journal.pone.0186188.
13. Tata Sutabri. *Analisis Sistem Informasi*. Yogyakarta: Andi. 2017.
14. Jogiyanto. *Analisis dan Desain Sistem Informasi (Pendekatan Terstuktur).* Yogyakarta : Andi. 2015.
15. Miller, Lawrence C. *Next-Generation Firewall for Dummies*. Indianapolis: Wiley Publishing, Inc. 2016.
16. Richard Bejtlich. *The Practice of Network Security Monitoring: Undestanding Incident Detection and Response*. San Fransisco, No Starch Press, Inc. 2017.
17. Firewall. *Unified Threat Management Features* Available at: https://www.firewalls.com/what_is_utm_firewall, [Accessed 10 Desember 2017].
18. Fortinet. *FortiGuard Security Services for FortiGate: Next-Generation Firewalls.* avalable at: https://www.fortinet.com/products/next-generation-firewall.html#services. [Accessed 10 Desember 2018].
19. Mohamad Nurul Huda Monoarfa, Xaverius B.N. Najoan, Alicia A.E. Sinsuw. *Analisa dan Implementasi Network Intrusion Prevention System di Jaringan Universitas Sam Ratulangi*. 2016. E-Journal Teknik Elektro dan Komputer vol. 5 no. 4, ISSN : 2301-8402.
20. B. R. Andrew and J. Esler. *Snort IDS and IPS Toolkit*, 2017, Syngress Publishing, Inc. Burlington.
21. Gallagher, P. D. *Guide for Conducting Risk Assessments*. 2015. National Institute of Standards and Technology.
22. Kouns, J. dan D. Minoli. *Information Technology Risk Management In Enterprise Enviroments*. 2015. John Wiley dan Sons. New Jersey.
23. Werlinger, R., Muldner, K., Hawkey, K., and Beznosov, K. *Preparation, detection, and analysis: the diagnostic work of IT security incident response*. 2015. Emerald.
24. Whitman, M. E., dan H. J. Mattord. *Management of Information Security*. 3rd Edition. 2015. Thomson-Course Technology.
25. Athailah. *Kontrol dan Amankan Koneksi Internet di Jaringan*. 2016. Jakarta: PT.Elex Media Komputindo.
26. Rafiudin, R. *Membangun Firewalll dan Traffic Filtering*. 2016. Yogyakarta: Andi.
27. Whindy, Y. *Kontrol dan Amankan Koneksi Internet di Jaringan.* 2015. Jakarta: PT.Elex Media Koputindo.
28. Paulus, Y. J. *Computer Networking, Pengaturan Jaringan, Keamanan Jaringan, Koneksi dan sharing, Troubleshooting Jaringan.* 2015. Yogyakarta: Andi.
29. Divakaran, D. M., L.Su, Y. S. Liauand V.L.Thing. *SLIC: Self-Learning Intelligent Classifier for Network Traffic. Computer Networks,* 2015. 91,283-297.
30. Goldstein M, Uchida S. *A Comparative Evaluation of Unsupervised Anomaly Detection Algorithms for Multivariate Data*. 2016. PLoS ONE 11(4): e0152173. doi:10.1371/journal.
31. Yeung DY, Ding Y. *Host-Based Intrusion Detection Using Dynamic and Static Behavioral Models. Pattern Recognition*. 2003; 36:229–243. doi: 10.1016/S0031-3203(02)00026-2.
32. Akoglu L, Tong H, Koutra D. *Graph based Anomaly Detection and Description: A Survey. Data Mining and Knowledge Discovery*. 2015; 29(3):626–688. doi: 10.1007/s10618-014-0365-y.
33. Chen JY, Yang DY. *Data security strategy based on artificial immune algorithm for cloud computing*. Appl Math Inform Sci. 2013; 7: 149–153.
34. Gao F, Ru A, Wang J, Mao S. *Knowledge-based detection method for SAR targets. J Syst Eng Electron*. 2014; 25573–579.

35. Sun X, Yan B, Zhang X, Rong C. *An Integrated Intrusion Detection Model of Cluster-Based Wireless Sensor Network*. PLoS ONE 2015; 10(10) doi: 10.1371/journal.pone.0139513.
36. Deepaa AJ, Kavitha V. A. *Comprehensive Survey on Approaches to Intrusion Detection System*. 2012. doi: 10.1016/j.proeng.2012.06.248.
37. Sakib MN, Huang C-T. *Using anomaly detection based techniques to detect HTTP-based botnet C&C traffic*. In: 2016 IEEE international conference on communications (ICC). doi:10.1109/icc.2016.7510883.
38. Zhao D, Traore I, Sayed B, Lu W, Saad S, Ghorbani A, Garant D. *Botnet detection based on traffic behavior analysis and flow intervals*. 2013. Comput Secur 39:2–16. doi:10.1016/j.cose.2013.04.007.

AUTHORS PROFILE

Iyan Rahdian S. Kom., MMSI received a Bachelor degree in Computer Science from Gunadarma University, Depok, Department of Information System in 2004. Received Master of Information Systems Management from Gunadarma University, Depok, in 2018.

Dr. Widya Silfianti received a Bachelor degree of Information Systems from Gunadarma University, Depok, in 1995. Received Master of Information Systems Management from Gunadarma University, Depok, in 1998. Received a Doctorate from Gunadarma University, Depok, in 2010. She is an experienced teacher of computing at Gunadarma University, Depok and has a teaching experience of more than 21 years. She is a Head of System Development Center (SDC) – BAPSI in Gunadarma University