Investigation of Botnet Attacks using Network Forensic Development Life Cycle Method

Muhammad Ridho Hidayat
Department of Informatics
Universitas Ahmad Dahlan
Yogyakarta of Indonesia

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

ABSTRACT

The development of internet technology is currently growing rapidly, as well as the increasing number of users. Based on the results of the Indonesian Polling study in collaboration with the Indonesian Internet Service Providers Association (APJII), out of a total population of 264 million Indonesians, there are 171.17 million people or around 64.8% who are already connected to the internet. Crime in cyberspace is also growing rapidly, such as botnets spreading on computer networks without knowing who the users are and where they are located. These infected computers are called zombies and they will be controlled by botmasters. One of the motives highlighted was to gain financial gain through a collection of computers that were forcibly taken over.The research uses the Network Forensic Development Life Cycle (NFDLC) method which focuses on 5 stages, Initiation, Acquisition, Implementation, Operations, and Disposition. This study uses Wazuh forensic tools that focus on monitoring attacks that enter the server by placing a wazuh agent on the server whose task is to monitor attacks that enter the computer server and then report to the wazuh manager then it will be processed into visual attack data.The experimental results, it is proven that the Network Forensic Development Life Cycle (NFDLC) method can detect botnet attacks while simultaneously monitoring incoming attacks with the results recorded in real-time in the form of a table containing 25 types of attacks that have attack levels from the lowest level 3 to the highest level. 15, the highest number of attacks was recorded with the number reaching 927 attacks and for the lowest attack, 1 attack was recorded.

Keywords

Botnet, NFDLC, Server, Wazuh, Realtime

1. INTRODUCTION

The need for computer networks has grown rapidly in various sectors of life. Internet technology is currently developing rapidly, as well as the increasing number of users[1]. Based on the results of the Indonesian Polling study in collaboration with the Association of Indonesian Internet Service Providers (APJII), out of a total population of 264 million people in Indonesia, there are 171.17 million people or around 64.8 percent who are already connected to the internet.[2]. The internet is no longer only used as a means of exchanging information but has begun to be used for commercial purposes, for example as a means of payment transactions. This of course causes a large amount of valuable data to be circulated more and more through the internet network[3]. However, from time to time more and more internet security holes are obtained and abused by electronic criminals. One of them is botnet[4]. A study showed that about 40% of the 800 million computers connected to the internet were infected with botnets. These infected computers are called zombies and they will be controlled by botmasters[5]. Therefore there must be security against crime from cyberspace, the branch of science that studies cybercrime security is digital forensics, the method that can be used is using the network forensic development life cycle (NFDLC) method.

1.1 Study Literature

1.1.1 Previous Study

Septian Geges, Waskitho Wibisono, and Tohari Ahmad, (2013) have conducted digital forensic research entitled "Identification of moments through monitoring group activity in DNS Traffic" [6]. In this study the botnet detection mechanism by monitoring DNS traffic to detect botnets, namely by monitoring group activity in DNS queries sent simultaneously by bots distributed in the network, the mechanism provided can detect botnets effectively when bots try to connect to the command server. and control (C&C) the botnet or migrate to another C&C server.

Rahmadani Hadianto and Tito Waluyo Purboyo (2018) have conducted digital forensic research entitled “a survey paper on botnet attacks and defenses in software-defined networking.” With this system, botmasters can enter and spread infections through the SDN control plane as unauthorized computers. This issue is considered as Integrity in the CIA triad (Confidentiality, Integrity, and Availability) which is used for evaluation of SDN security performance [7]. Integrity in the CIA triad means a condition in which information is kept accurate and consistent unless official changes are made.

Aisyatul Karima (2013) has conducted digital forensic research entitled "Anomaly detection for the identification of Kraken and Conficker botnets using a rule-based approach". Botnets consist of various types with their respective behaviors that make it difficult for users to classify the types of botnets that can be used in botnet detection [8]. The researcher proposes a new rule-based intrusion detection to detect botnets, especially for Kraken and Conficker detection using anomaly detection. Rule-based is obtained from real network traffic through observation techniques [9]. With these observations, the rule set can provide significant results compared to the implementation of the Intrusion Detection System, such as that found in Snort.

Septian Geges, Waskitho Wibisono, (2015). Has carried out digital forensic research entitled "Development of prevention of distributed andial of service (DDOS) attacks network resources by integrating network behavior analysis and client puzzles." This study proposes a mechanism to secure web services by filtering and validating requests received for access network resources [10]. This filtration and validation are carried out using a combination of Network Behavior Analysis (NBA) and Client Puzzle (CP) methods. The NBA method is the first layer of defense to detect whether a DDoS attack is taking place by measuring the network density. From the NBA method, an IP Address is obtained that needs to be validated by the CP method as a second layer of defense.

Tika Hairani, (2018). Has conducted digital forensic research entitled "Botnet Detection Using the K-Nearest Neighbor Algorithm". This study classifies network traffic information that contains botnets using the K-Nearest Neighbor algorithm [11]. The algorithm calculates the distance for each feature in the dataset and then identifies the type of flow based on the majority of a certain neighbor value (k value). The test results in this study is an accuracy of 92.57% where the k value is determined according to the system default, which is 5. The best k value in this study cannot be determined because the tests carried out to determine the k value get results with quite far apart values.

1.1.2 Digital Forensics

Digital forensics (English: Digital forensics) (also known as digital forensic science) is a branch of forensic science, especially for the investigation and discovery of digital device content, and is often associated with computer crimes.[12]. The term digital forensics was originally synonymous with computer forensics but has now been expanded to investigate all devices that can store digital data. Forensics in general is a scientific process for collecting, analyzing, and presenting evidence in court[13]. In general, a forensic stage is carried out with the assumption that the data that has been collected will be used as evidence in court. Therefore, after the collection of evidence, forensic practitioners maintain and control the evidence to prevent modification. Digital forensics is divided into several sections as shown in Figure 1.

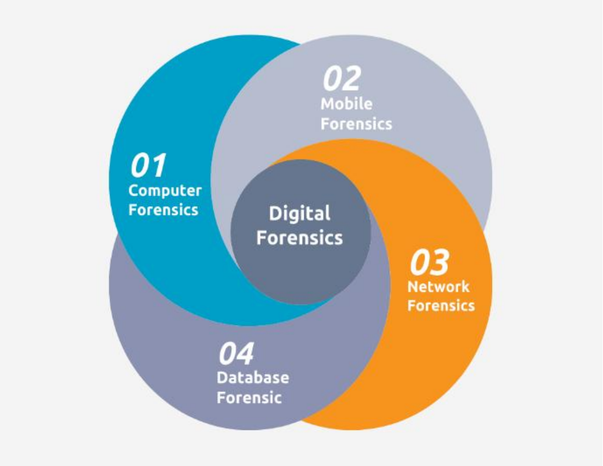


Figure 1. Digital Forensic Section

1. *Computer Forensics*
   Computer Forensics is to describe the current state of digital artifacts, such as computer systems, storage media, or electronic documents[14]. Disciplines typically include computers, embedded systems (digital devices with basic computing power and onboard memory), and static memory (such as USB pen drives).
2. *Mobile Forensics*
   Mobile device forensics is a sub-branch of digital forensics concerned with the recovery of digital evidence or data from mobile devices[15]. It differs from Computer forensics in that a mobile device will have an inbuilt communication system (eg GSM) and usually, a proprietary storage mechanism.
3. *Network Forensics*
   Network forensics relating to the monitoring and analysis of computer network traffic, both local and WAN/internet, to gather information, gathering evidence, or detecting intrusions[16].
4. *Database Forensic*
   Database forensics is the branch of digital forensics that deals with the forensic study of databases and investigating metadata using database contents, log files, and RAM data to establish a timeline or recover relevant information.

1.1.3 Bots and Botnets

Bots are defined as small program code designed to perform their functions automatically[17]. In their use, bots can be very useful if they are used properly, for example in terms of indexing/spidering websites.

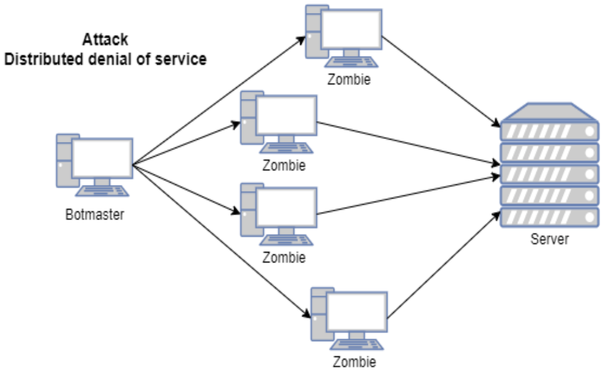


Figure 2. Botnet Topology

Figure 2, it can be seen that the initial topology of botnet attacks is often used by botmasters to attack the target server that will be infected using a computer that has been sent by the bot and becomes a zombie that can be moved and ordered by the botmaster.

1.1.4 Bone Monitoring Tools

Botnet attacks can be monitored using several tools, namely:

1. *WordPress Security Scan*
   WordPress Security Scan For users who use a CMS like WordPress, this tool is very useful to use. WordPress Security Scan can check WordPress server security, plugin security, and hosting area [18]. how to use it is easy. just enter the website after opening the WordPress Security Scan tool.
2. *Wow*
   Wow is a tool that provides deeper security visibility features into infrastructure by monitoring hosts at the operating system as well as at the application level [19]. Wazuh consists of 2 (two) parts, namely Wazuh-Server and Wazuh-Agent. Wazuh server is a device that is used as agent management and monitoring system dashboard, both file integrity, intrusion, and logs. Meanwhile, the Wazuh agent is a device that is installed on the endpoint device to read the system, collect logs and send them to the Wazuh server.
3. *Zed Attack Proxy (ZAP)*
   Zed Attack Proxy is an integrated penetration testing tool to find vulnerabilities in web applications in an easy way, ZAP provides an automatic scanner to find attack vulnerabilities against the web [20].

Proxy (ZAP) It is designed to be used by people with various security experiences and thus is ideal for developers and pentesters who are new to pentesting activities [22].

ZAP provides an automated scanner as well as a set of tools that make it possible to find website security vulnerabilities manually.

4. *Wireshark*

   *Wireshark/Ethereal*is a Network Analyzer that is widely used by network administrators to analyze network performance and is also a Vaccination tool (Vaccine technician) [23]. Wireshark is much preferred because of its interface that uses a Graphical User Interface (GUI) or a graphical display.

1.1.5 Network Forensic Development Life Cycle

Network Forensic Development Life Cycle(NFDLC) is based on the Information Systems Development Life Cycle (ISDLC) [24]. In addition, the life cycles that will assist in developing the framework mentioned later on in the ISDLC method performed Specific modifications that result in the NFDLC results are summarized in Table 1.

Table 1. Modification of ISDLC to NFDLC

Additional ISDLC (Life Cycle)	Additional NFDLC Procedure
Initiation phase/ early risk assessment.	Determine what aspects of the network will guarantee digital forensic protection.
Acquisition/Development Phase.	Adhere to Evidence Rules in system requirements Implement published forensic checklists [ie31, 32, 33].
Implementation Stage.	Perform basic testing Perform networkverification/calibration/mechanism tests Perform.
Disposition Phase Operation Phase.	verification/calibration audit.
Maintenance.	Entering the chain of storage procedures / storage of evidence goods.

Table 1 five stages must be achieved to benefit from the NFDLC. They are initiation, acquisition or development, implementation, operation or maintenance, and disposition [25]. An overview of the Network Forensic Development Life Cycle flow can be seen in Figure 3.

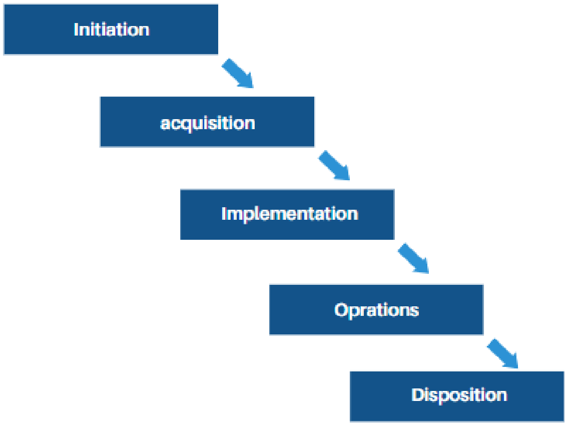


Figure 3. Forensic Network Development Life Cycle

2. Methodology

2.1 Research Scenario

The initial stage of the simulation process in this research is to create case scenarios based on actual cases, the case raised in this research is Digital Forensics Against Botnet Attacks Using the Network Forensic Development Life Cycle (NFDLC) Method. The attack scenario in this research plan is illustrated.

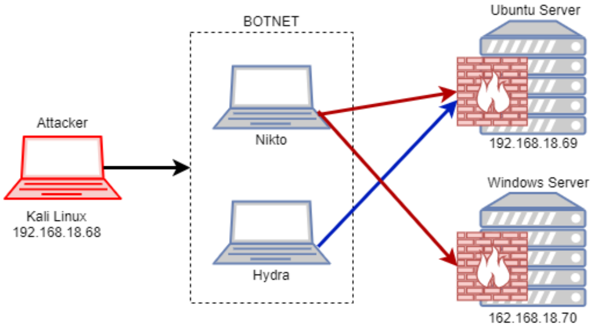


Figure 4. Attack Scenario Simulation

Figure 4 the attack scenario shows the flow of the attack process from the attacker then attacking to infect sending bots to a laptop or PC after that it is continued by controlling the laptop or PC that has been attacked to attack the webserver. Windows Server 2012 has a Web Server Service that has WordPress installed and then on Ubuntu Server 20.04 it has a Web Server service that has Joomla installed and SSH for remote access. Then the Firewall will use Modsecurity as a Web Application Firewall (WAF) then Network traffic will be monitored by Zeek as the Network Intrusion Detection System, then OSSEC as the Host Intrusion Detection System. So that every attack launched by the attacker will pass through the firewall and will be stopped if it is considered dangerous.

The attacker uses the Kali Linux OS which is controlled by a botnet to attack the targeted website running on Windows Server 2012 and Ubuntu Server, another attack that will be carried out is an attack on SSH on Ubuntu Server 20.04

2.2 Research Stages

Botnet obtained after digital investigative analysis. The investigation is used for the object of research, namely the botmaster's attack on the server making the target a bot that can be controlled by the botmaster. The analysis phase uses the Network Forensics Development Life Cycle (NFDLC) method in Figure 5.

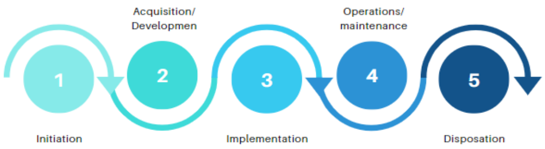


Figure 5. Implementation Stages

Figure 5, the NFDLC method shows the analysis stages of the Network Forensics Development Life Cycle (NFDLC) method which can be described in 5 stages, namely:

1. *Initiation*

Determine aspects of research tools and materials to be used in research.

2. *Acquisition/Development*
   Is the process of setting up the system, carrying out installation, verification, and calibration so that it can be used in research containing evidence rules in systems that develop systems, verify, and calibrate.
3. *Implementation*
   Basic testing of the platform by verifying the basic network mechanism for making workflows, scenarios, and flowcharts that will be carried out in the research.
4. *Operations/maintenance*
   It is the main process carried out in this research, such as conducting attacks and monitoring attacks, including verification and measurement of network usages, such as traffic, bandwidth, and data content.
5. *Disposition*
   Carry out a series of procedures to secure evidence and the final stage of research is securing evidence obtained from the final results of monitoring attacks.

2.2.1 *Initiation*

Initiation is the process of determining aspects of the network and equipment for Digital Forensic Protection that will be used in research.

1. Needs Analysis
   There are several pieces of equipment which are divided into two parts, namely software (software) and hardware (hardware) which are described in Table 2:

Table 2. Research Tools and Materials

No	Tools and materials	Type	status	Information
1	Asus Laptops	X453SA	Hardware	Research Forum
2	VirtualBox	6.1	Software	Virtual Operating System
3	Kali Linux	2.6	Software	Attack Media
4	Ubuntu Server	64-bit	Software	Attack Object
5	Windows Server	2012	Software	Attack Object
6	Wazuh	V4.1.5	Software	Forensic Tools
7	XAMPP	7.3	Software	Forensic Tools

2. Network topology
   In this study, the topology used is a star type because this network is under the needs of the attack process and network monitoring. The function of the star topology is as a liaison between one computer and another in a computer network, as can be seen in Figure 6.

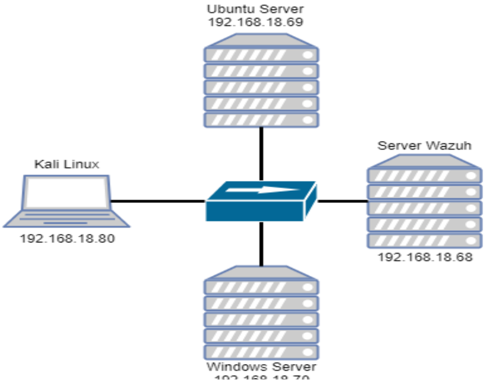


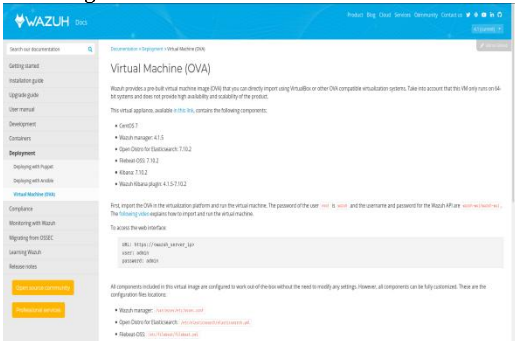
Figure 6. Network Topology

Figure 6 provides information on the network structure used in the study, as for the devices that are used there are four devices, namely, Kali Linux as an attacker who will send a botnet to the Ubuntu server and Windows server as a target to be attacked using a botnet sent by Kali Linux. , then the wazuh server will play a role in providing information on incoming attacks to the Ubuntu server and windows server.

2.2.2 *Acquisition*

It is the process of setting up the system, carrying out installation, verification, and calibration so that it can be used in research.

1. *Install Wazuh Manager*
   The initial stage of monitoring with Wazuh, related to early access, you can use the OVA file that has been provided on the official Wazuh website at the following link:



Virtual Machine (OVA)

Wazuh provides a pre-built virtual machine image (OVA) that you can directly import using VirtualBox or other OVA compatible virtualization systems. Take into account that this VM only runs on 64-bit systems and does not provide high availability and scalability of the product.

This virtual appliance, available in this link, contains the following components:

- CentOS 7
- Wazuh manager: 4.1.5
- Open Distro for Elasticsearch: 7.10.2
- Filebeat-OSS: 7.10.2
- Kibana: 7.10.2
- Wazuh Kibana plugin: 4.1.5-7.10.2

First, import the OVA in the virtualization platform and run the virtual machine. The password of the user root is wazuh and the username and password for the Wazuh API are wazuh-wui:wazuh-wui. The following video explains how to import and run the virtual machine.

To access the web interface:

```
URL: https://<wazuh_server_ip>
user: admin
password: admin
```

All components included in this virtual image are configured to work out-of-the-box without the need to modify any settings. However, all components can be fully customized. These are the configuration files locations:

- Wazuh manager: /var/ossec/etc/ossec.conf
- Open Distro for Elasticsearch: /etc/elasticsearch/elasticsearch.yml
- Filebeat-OSS: /etc/filebeat/filebeat.yml

Figure 7 Wazuh Install Process

Figure 7, the import file manager can run WAZUH MANAGER Virtual Machine with root username and wazuh password.

2. *Install Wazuh Agent*
   At the stage after entering the elasticsearch dashboard, the next step is to install WAZUH AGENT which can be found on the dashboard. Installation of wazu agent is done for windows server and Ubuntu server then, when you want to do the installation, the user is asked to choose the operating system and architecture that is the initial destination of the agent installation. .deb files

2.2.3 *Implementation.*

The basic testing process for making workflows and flowcharts will be carried out in research.

1. *Monitoring Workflow*

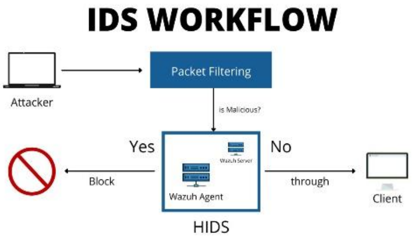


Figure 8 Monitoring Workflow

Figure 8 the general network monitoring process through the Intrusion Detection System (IDS) is carried out using the WAZUH service. In the early stages of the scenario when the attacker carries out the attack process in the form of the Bruteforce method, the process will be accommodated at the packet filtering stage. At this stage, IP addresses are collected for the early detection of suspicious packets. Then the packet is forwarded to the Wazuh Agent for the next IP Address scanning stage.

2. *Investigation Flowchart*

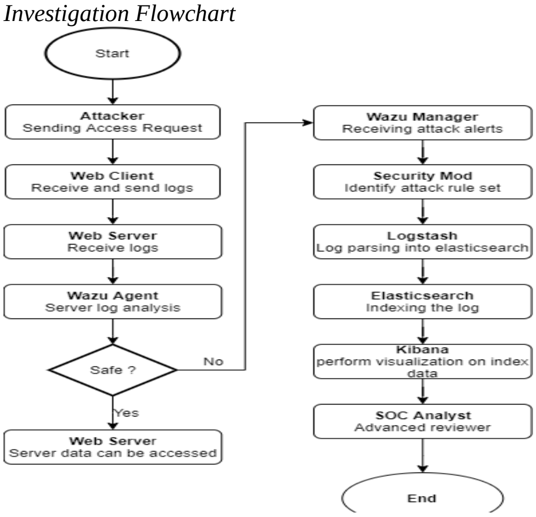


Figure 9 Flowchart ofAttack Scenario

Figure 9 the flowchart model illustrates the attack analysis process using the Host Intrusion Detection System Service, WAZUH. In the initial scenario, the attacker sends an access request to the website. Then from the website is forwarded to the webserver where the access assessment process occurs before the data on the server can be fully accessed in the wazuh agent. Then in the assessment, there are 2 results, if the access is safe, then the log is returned to the server to be processed into secure access. If the log is malicious, then the attack log is forwarded to Wazuh Manager to analyze the attack model rule set in the security mod. After reviewing the analysis of the attack model, logs and alerts are then sent to logstash which will be processed and decomposed into an elasticsearch format.

Then at the last stage, the visualization data from the kibana is sent to the SOC Analyst for further review.

2.2.3.1 Operations

Operationsare the main process carried out in this study such as carrying out attacks and monitoring attacks. At this stage is the discussion of attack case simulations and verification of monitoring botnet attacks. In general, there are two stages in the attack process using botnets, namely sending commands from the Botnet Master and executing commands from the Botnet Master to the target.

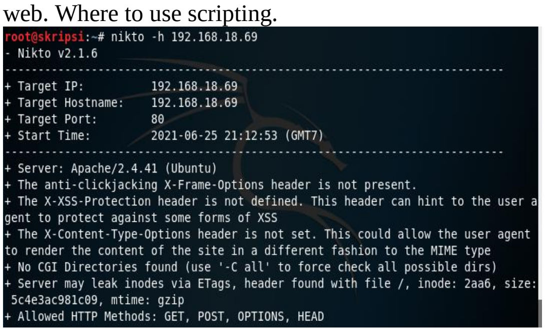
1. *Assault Simulation*

Command Botmasters are actors responsible for controlling and sending commands to bot clients via the C&C infrastructure. The command sent is to perform a web scanning attack using Nikto and a Brute Force SSH attack using Hydra.

The execution of the attack at this stage carried out an attack method on the Linux server with web attacks and SSH services. In this case, the attack method with the target IP will be tested, namely 192.168.18.69.

2. *Attack Execution*

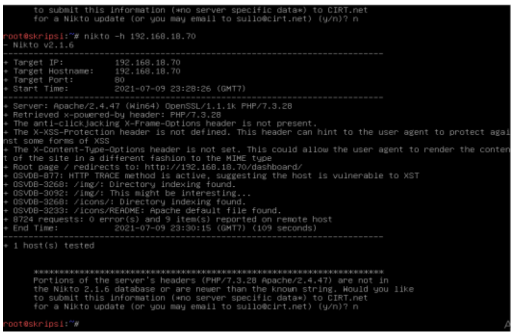
Attacks on Ubuntu Server use NIKTO to perform the scanning/reconnaissance process on the target web. Where to use scripting.



```
root@skripsi:~# nikto -h 192.168.18.69
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.18.69
+ Target Hostname:    192.168.18.69
+ Target Port:        80
+ Start Time:         2021-06-25 21:12:53 (GMT7)
---------------------------------------------------------------------------
+ Server: Apache/2.4.41 (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user a
gent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent
to render the content of the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Server may leak inodes via ETags, header found with file /, inode: 2aa6, size:
 5c4e3ac981c09, mtime: gzip
+ Allowed HTTP Methods: GET, POST, OPTIONS, HEAD
```

Figure 10 Attack on Ubuntu Server

Attacks to Windows Server web scanning attacks using Nikto will send web attacks such as Cross-Site Scripting (XSS), Local File Inclusion (LFI), Command Injection, SQL Injection, and Cross-Site Request Forgery (CSRF). The impact of these attacks is that attackers can take over the system, database leaks, and the system becomes inaccessible.

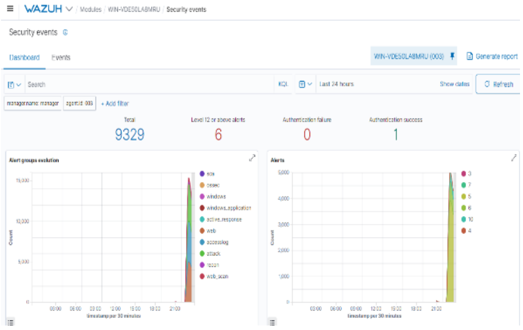


```
      to submit this information (*no server specific data*) to CIRT.net
      for a Nikto update (or you may email to sullo@cirt.net) (y/n)? n

root@skripsi:~# nikto -h 192.168.18.70
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.18.70
+ Target Hostname:    192.168.18.70
+ Target Port:        80
+ Start Time:         2021-07-09 23:28:26 (GMT7)
---------------------------------------------------------------------------
+ Server: Apache/2.4.47 (Win64) OpenSSL/1.1.1k PHP/7.3.28
+ Retrieved x-powered-by header: PHP/7.3.28
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect agai
nst some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the conten
t of the site in a different fashion to the MIME type
+ Root page / redirects to: http://192.168.18.70/dashboard/
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ OSVDB-3268: /img/: Directory indexing found.
+ OSVDB-3092: /img/: This might be interesting...
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ 8724 requests: 0 error(s) and 9 item(s) reported on remote host
+ End Time:           2021-07-09 23:30:15 (GMT7) (109 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested


      *********************************************************************
      Portions of the server's headers (PHP/7.3.28 Apache/2.4.47) are not in
      the Nikto 2.1.6 database or are newer than the known string. Would you like
      to submit this information (*no server specific data*) to CIRT.net
      for a Nikto update (or you may email to sullo@cirt.net) (y/n)? n

root@skripsi:~#
```

Figure 11 Attack on Windows Server

3. *Result of windows attack and Ubuntu Server.*

The results of scanning windows server, display the results as shown in Figure 12.

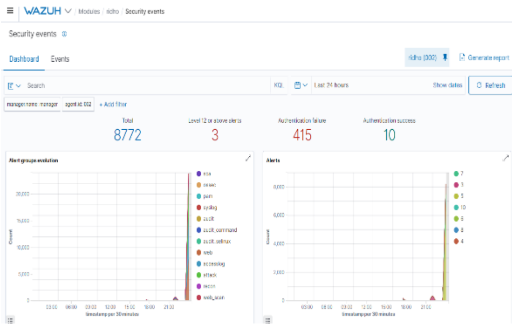


Total 9329
Level 12 or above alerts 6
Authentication failure 0
Authentication success 1

Figure 12 Results of Scanning Windows

Figure 12 scanning monitoring windows server which has a scan result of 9329 with an alert level of 6 alerts. In the alert group graph, there is a high webscan progress with the monitoring model capturing attack activity in second place when web scanning is carried out. For alerts, there are 4 alert results where the 4th level at the top is the main activity and background attacks are at level 7 related to attack service.

The results of scanning the Ubuntu server, display the results as shown in Figure 13.



WAZUH / Modules / ridho / Security events

Security events

Dashboard | Events

ridho (002) | Generate report

Search | KQL | Last 24 hours | Show dates | Refresh

manager.name: manager | agent.id: 002 | + Add filter

Total	Level 12 or above alerts	Authentication failure	Authentication success
8772	3	415	10

Figure 13 Scanned Ubuntu Results

Figure 13 shows the results of the scanning monitoring Linux server which has a scan result of 8772 with an alert level of 3 alerts, then there are 415 Authentication failures and 10 Authentication successes. In the alert group graph, there is a high webscan progress with the monitoring model capturing attack activity in second place when web scanning is carried out. For alerts, there are 4 alert results where the 4th level at the top is the main activity and background attacks are at level 7 related to attack service.

2.2.3.2 Disposition.

Despotitions is the final stage of the research, which is the final process of securing evidence obtained from the final results of monitoring botnet attacks on the server. After disposition, attackers can recapitulate data from all the data they want to get. The results of attacks that can be reported in tabular form can be seen in the table3.

Table 3. Results of all Monitoring

Rule ID	Description	Level	count
31104	Common weattack	6	927
31105	XXS (Cross Site Scripting) attempt	6	762
5716	Sshd: authentication failed	5	223
31166	Shellshock attack attempt	6	178
31153	Multiple common web attacks from samesource ip	10	102
31154	Multiple XXS (Cross Site Scripting) samesource ip	10	84
31516	Suspicious URL acces	6	64
2502	Syslog: User missed the password more than time	10	42
5758	Maximum authentication attempts exceeded	8	32
5720	sshd: Multiple authentication tailures	10	31
5501	PAM: Login session opened	3	17
5402	Successful sudo to ROOT executed	3	12
31103	SQL injection attempt	7	8
31168	Shellshock attack detected	15	7
40111	Multiple authentication failures	10	6
5551	PAM: Multiple Failed logins in small priod of time	10	6
31106	A web attack returned code 200(sucsess)	6	5
31110	PHP CGI bin vulnerability attempt	6	5
504	Ossec Agent disconnected	3	2
30306	Apache: Attempt to acces forbidden directory index	5	1
30316	Apache: Multiple ivalid URL requests from same source	10	1
60106	Windows logon success	3	1
61138	New Windows Service Created	5	1

Table 3 is a record of all attacks that were successfully recorded by agents placed on the ubuntu server and windows server, in the attack records wazuh was able to recognize and group incoming attacks based on the type and level of the attack as shown in the table from the results of monitoring carried out agent wazu on these two servers.

3. CONCLUSION

Server security by using the Network Forensic Development Life Cycle (NFDL) method, resulting in a system that can minimize botnet attacks that enter the server, incoming attacks can be monitored starting from the time of the attack that enters the server, the type of attack, the level of attack and the number of attacks that enter the server. can be recorded and seen visually by the manager. Based on the results of botnet countermeasures research carried out by the wazuh system, it can monitor attacks that enter the server in real-time, in the form of a table containing 25 types of attacks that have attack levels from the lowest level 3 to the highest level 15, the highest number of attacks recorded with the number reaching 927 attacks. and for the lowest attack recorded 1 attack.

4. REFERENCES

[1] Anwar, N., & Riadi, I. (2017). WhatsApp Messenger Forensic Investigation Analysis Smartphone Against Web-Based WhatsApp. Scientific Journal of Computer Electrical Engineering and Informatics, 3(1), 1.https://doi.org/10.26555/jiteki.v3i1.6643

[2] Damayanti, M. (2015). Simulation of Botnet Attacks on HTTP Protocol Scientific Articles.

[3] Endicott-Popovsky, BE, & Frincke, DA (2006). Embedding forensic capabilities into networks: Addressing inefficiencies in digital forensics investigations. Proceedings of the 2006 IEEE Workshop on Information Assurance, 2006, 133–139.https://doi.org/101.1109/iaw.2006.1652087

[4] Endicott-popovsky, BE, Frincke, DA, & Ieee, AS (2006). Embedding Forensic Capabilities into Networks: Overcoming Inefficiencies in Digital Forensic Investigations. 99352, 133–139.

[5] Endicott-popovsky, B., Frincke, DA, & Taylor, CA (2007). Theoretical Framework for Organizational Forensic Readiness Networks. 2, 1–11.

[6] Geges, S., Wibisono, W., & Ahmad, T. (2013). Identify Botnets Through Monitoring Group activity on DNS Traffic. Journal of Engineering Pomits Vol. 2, No. 1, (2013) ISSN: 2337-3539 (2301-9271 Print), 2(1), 1–6.http://digilib.its.ac.id/public/ITS-paper-30350-5109100179-Paper.pdf

[7] Geges, S., & Wibisono, W. (2015). Development of Prevention of Distributed Denial of Service (DDoS) Attacks on Network Resources With Integration of Network Behavior Analysis and Client Puzzle. JUTI:

Scientific Journal of Information Technology, 13(1), 53.https://doi.org/10.12962/j24068535.v13i1.a388

[8] Hadianto, R., & Purboyo, TW (2018a). A Survey Paper on Botnet Attacks and Defenses in Software Defined Networking. International Journal of Applied Engineering Research, 13(1), 483–489.http://www.ripublication.com

[9] Hadianto, R., & Purboyo, W. (2018b). Network. 13, 483–489.

[10] Karima, A. (2012). Anomaly detection to identify Kraken and Conficker botnets uses a rule-based approach. 2012(Semantics), 274–281.

[11] Rosalina, V., Herli, D., Information, FT, Kingdom, US, Information, FT, Kingdom, US, Forensics, D., Model, P., Framework, Z., & Clark, JG (2015)). Digital Forensic Stages Model Development To Support. 0–5.

[12] R. Montasari, "Review and Assessment of the Existing Digital Forensic Investigation Process Models," Int. J. Comput. Appl., vol. 147, no. 7, pp. 1–9, 2016.

[13] I. Riadi, S. Sunardi, and AA Kadim, "Monitoring Mobile Native Application Logs Using the Grr Rapid Response Framework," J. Buana Inform., vol. 10, no. 1, p. 1, 2019, doi:10.24002/jbi.v10i1.1909.

[14] D. Hariyadi, U. Jenderal, and A. Yani, "Identification of Conversation Evidence for the Dual Apps Whatsapp Application on," no. November, 2018, doi:10.13140/RG.2.2.20253.56805.

[15] I. Riadi, R. Umar, and IM Nasrulloh, "Digital Forensic Analysis on Frozen Solid State Drives Using the National Institute of Justice (Nij) Method," Elinvo (Electronics, Informatics, Vocat. Educ., vol. 3, no. 1, p. 70–82, 2018, doi:10.21831/info.v3i1.19308.

[16] R. Umar and Sahiruddin, "Nist Method For Forensic Analysis Of Digital Evidence On Android Devices," Pros. SENDU_U_2019, matter. 978–979, 2019.

[17] RY Prasongko, A. Yudhana, and A. Fadil, "Forensic analysis of the cocoatalk application using the national institute standard technology method," Semin. Nas. information. 2018 (semnasIF 2018) UPN "Veteran" Yogyakarta, 24 Novemb. 2018 ISSN 1979-2328, vol. 2018, no. November, p. 129–133, 2018.

[18] H. Nurhairani and I. Riadi, "Analysis of Mobile Forensics on Twitter Application using the National Institute of Justice (NIJ) Method," int. J. Comput. app., vol. 177, no. 27, p. 35–42, 2019, doi:10.5120/ijca2019919749.

[19] B. Carrier, "Open {Source} {Digital} {Forensics} {Tools}: {The} {Legal} {Argument}," no. October, 2002.

[20] Buyens, Jim. 2001. Web Database Development. Elex Media Komputindo. Jakarta

[21] PW Setyaningsih, Y. Prayudi, and B. Sugiantoro, "Management of Digital Evidence from the Acquisition of Dfxml," J. Tek. Inform., vol. 11, no. 1, p. 47–54, 2018, doi:10.15408/jti.v11i1.6680.

[22] MN Faiz, R. Umar, and A. Yudhana, "Analysis of Live Forensics for Comparison of Email Security on Proprietary Operating Systems," Ilk. J. Ilm., vol. 8, no. 3, p. 242–247, 2016, doi:10.33096/ilkom.v8i3.79.242-247.

[23] A. Yudhana, I. Riadi, and I. Anshori, "Analysis of Digital Evidence for Facebook Messenger Using the Nist Method," It J. Res. Dev., vol. 3, no. 1, p. 13–21, 2018, doi:10.25299/itjrd.2018.vol3(1).1658.

[24] Raka, Z. D, "4523/Kom-D/Sd-S1/2021 Analysis of P3Sps Violations on Bigo Live Application Shows," 2021.

[25] AN Ichsan and I. Riadi, "Mobile Forensic on Android-based IMO Messenger Services using Digital Forensic Research Workshop (DFRWS) Method," 2021.