CyberSecurity and Digital Forensics e-ISSN: 2615-8442
Vol. 5, No. 1, May 2022, p.23-31

FORENSIC ANALYSIS OF DDOS PING OF DEATH ATTACKS ON SERVERS

Muhammad Adam[1], Erick Irawadi Alwi[2], Ihwana As'ad[3]

[1,3]Teknik Informatika, Fakultas Ilmu Komputer, Universitas Muslim Indonesia
[2]Sistem Informasi, Fakultas Ilmu Komputer, Universitas Muslim Indonesia

Email: [1]warzone729@gmail.com , [2]Erick.alwi@umi.ac.id , [3]ihwana.asad@umi.ac.id

Abstract

Technological advances that continue to develop become a threat, which one is in the digital world where there are several cyber crimes by reducing the performance of your web server by flooding network traffic. Regardless of what you have done to improve the performance of your web server, hackers can still simulate more users than the web server itself can handle. IDSIRTI data for October 2020, total attacks reached 66 million and DDoS attacks carried out based on anomaly classification reached 6 million attacks. Increasing threats and attacks on system security are increasing because they are supported by easier access and the availability of resources that are easier to obtain. There are many stages that cyber criminals can smoothen their steps to get as much information as possible on the target, of which one is DDoS. To smooth the steps are usually done by using a method to flood the source on the network device. The web server is one part of a network and as the times progress, there are lots of webs that are scattered on the internet and can be accessed , intrusion attacks are very undesirable on the system because they can endanger the confidentiality and availability of resources. spend the resources they have..The problem starts when the data packets come in are very large and must be analyzed against a data. In this study, DDoS Ping of death attack will be carried out on a web server where the results of an attack will create a data record that is recorded on the Snorby software, the data is needed to run forensics in order to collect evidence cyber crime using forensic methods (NIST). which is includes collection, examination, analysis, reporting.

***Keywords**: Web Server, Forensic, NIST, DDoS, Ping of death*

1. INTRODUCTION

In the era of information technology, there is a field of forensics that is able to prove a crime based on a series of stages such as identifying, testing, analyzing, and being able to document the evidence contained at the source and the results of the analysis carried out. Forensics needs to be done with the aim of helping network administrators to make it easier to find designs to record all events that occur on the system. forensic analysis needs to be carried out with the aim of finding evidence based on the source of the attack, the time of occurrence, and the impact of the DDOS ping of death attack, obtaining a number of forensic evidence with the main key findings and supporting evidence for analysis in this forensic research, Wireshark application as offline package analysis, Obtain evidence in the form of a recorded package(Ridho, 2017).

offline packet analysis, detect possible ip addresses responsible for attack among packets caught using snorby. This research describes a tool that can detect DDoS attacks or mitigate attacks that appear on the network, a forensic framework is presented by considering the data recorded in the stored data.

DDoS (Distributed Denial of Service) attacks. The attack resulted in the network security system being attacked experiencing disruption. These disturbances can be in the form of system failures, halts, error requests and even damage to the server hardware. After seeing the problems with the network security system(Wahanani et al., 2016).

DDoS has been known to the network community since the early 1980s. The target of a DDoS attack can be directed at various networks, whether it be routing devices, web, electronic mail, or domain name system servers. This attack aims to make the server shutdown, reboot, crash, or "not responding".

The next suggestion is to do offline packet analysis research using applications other than wireshark and network miner, such as Microsoft Network Monitor and NetIntercept.(generators, 2021).

the update in this research is in the tools, the tools used are using snorby to carry out forensic processing, attacks carried out using DDoS Ping of death which will attack the web There are two stages in this research, the first is to simulate attacks with the type of DDoS (Distributed Denial of Defence) attack. Service) ping of death on the web, the second

performs forensic analysis using the National Institute of Standards Technology (NIST) method. This research is focused on the ping of death attack by looking at network traffic data activity using tools in the Snorby software.

2. LITERATURE REVIEW

2.A. Digital Forensics

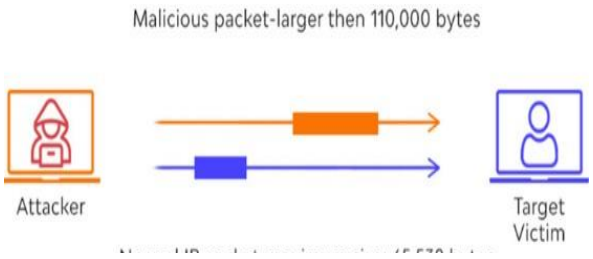
Digital forensics is a combination of legal disciplines and computer knowledge in collecting and analyzing data from computer systems, networks, wireless communications, and storage devices so that they can be brought as evidence in law enforcement. It can be concluded that digital forensics is the use of analytical and investigative techniques to identify, collect, examine and store evidence/information that is magnetically stored/encoded on a computer or digital storage media as evidence in exposing criminal cases that can be legally justified.(Saputra & Widiyasono, 2017).

Components in a digital forensic model involve three components that are managed in such a way as to become an end goal with all feasibility and quality results. These three components are:

a. Human (People), Qualifications are needed to achieve quality human beings. It's easy to learn computer forensics, but becoming an expert requires more than just knowledge and experience.
b. Equipment (Equipment), Required a number of appropriate devices or tools to get some evidence that can be trusted and not just fake evidence
c. Rules (Protocol), Required in order to explore, obtain, analyze, and finally present in the form of an accurate report, a good understanding in terms of ethical law is needed, if necessary in resolving a case(Du et al., 2017).

2.B. *Ping of death*

*ping of death*namely the longest attack and often used by people in this attack by using the ping utility in an operating system. when fragmentation is performed, each IP fragment needs to carry information about which part of the original IP packet it contains. This information is stored in the Fragment Offset field, in the IP header. This field is 13 bits long, and contains the data offset in the current IP fragment, in the original IP packet. The offset is given in units of 8 bits. This allows a maximum offset of 65,528 ((213-1)*8). Then when adding 20 bits of IP header, the maximum is 65,548 bits, which exceeds the maximum frame size. This means that the IP fragment with the maximum offset must have no more than 7 bits of data, or it will exceed the maximum packet length limit.(Walad, 2020).



Picture1. how the ping of death works

2.C. *Distributed Denial of Service*(DDoS)

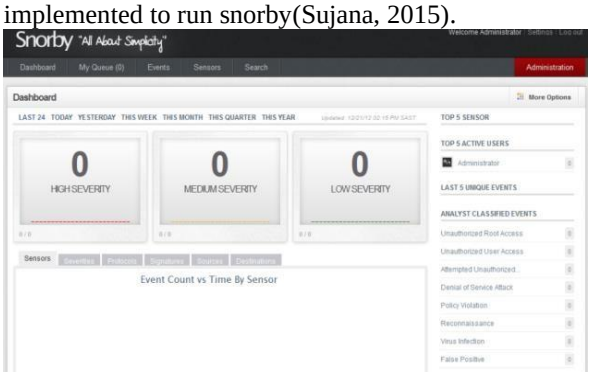
A DDOS attack usually involves the attacker sending messages to exploit certain vulnerabilities leading to instability or crashing of business systems. Attackers can also perform DDOS by sending a large number of normal messages quickly to a single node, the goal is to exhaust system resources causing business system failure. network bandwidth. The following are the steps that occur in a distributed attack:

a. The attacker sends an "execute" command in the form of a message to the main control program.
b. The main control program receives messages in the form of "execute" commands and then issues attack commands to each attack daemon under its control.
c. Upon receiving an attack command, the attack daemon initiates an attack on the target(Geges & Wibisono, 2015.).

While it may seem that the main culprit of a DDoS attack is simply carrying out his actions by sending execution orders, he actually has to do the planning for a successful DDoS attack. The attacker has to infiltrate all the host computers and networks where the daemons have to be attached. The attacker must study the target network topology and look for security holes and system trends that can be exploited to launch an attack.

2.D. Snorby

Snorby is a frontend web application (written in ruby on rails) for monitoring network security related to network intrusion detection systems such as snort. Administrator in tuning the rules that are implemented to run snorby(Sujana, 2015).

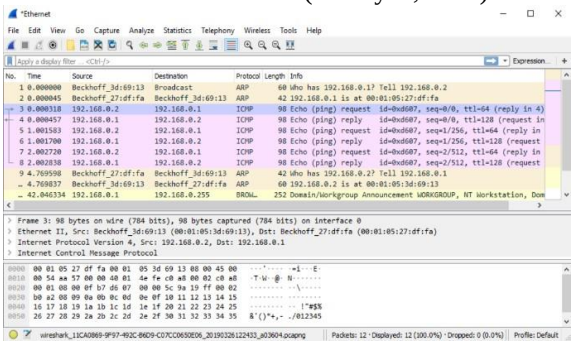


Picture2. snorby app

2.E. Wireshark

Wireshark is widely used in solving network troubleshooting to check network security, debugging network protocol implementations in their software, debugging protocol packet implementations, and is widely used for sniffer or searching for privacy data on networks and also as a

medium or tool that can be used to search for information on the network.(Diansyah, 2015).



Picture3. wireshark application

The benefits of using the Wireshark application are as follows:

a. Capturing information or data packets sent and received in a computer network.
b. Know the activities that occur in computer networks.
c. Knowing and analyzing the performance of a computer network that is owned, such as access speed/share data and network connection to the internet.
d. Observing the security of computer networks. Uses of wireshark, some of the uses of wireshark include, wireshark is used by a network administrator to analyze traffic in his network(Hanipah & Dhika, 2020).

2.F. NIST (National Institute of Standards Technology)

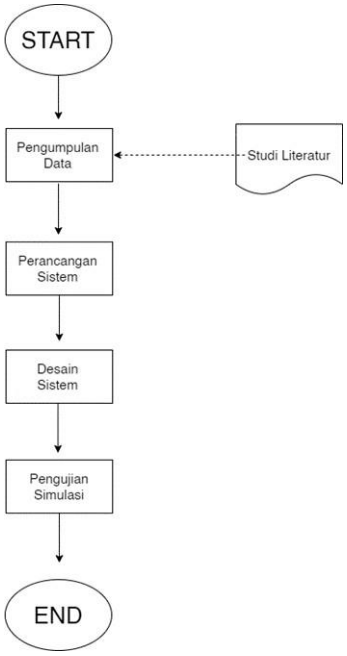
National Institute of Standards and Technology(NIST) is the non-regulatory national agency of the United States Technology Administration. The agency's mission is to promote and create measures, standards, and technologies to improve productivity, shamang trade, and improve the quality of life for all people. NIST's cybersecurity program seeks to enable the greater development and application of innovative and practical security technologies and methodologies to enhance countries' capabilities to address current and future computer and information security challenges.

The stages in the NIST method are:

1. *collection*(Data collection). Collection of evidence with the process of identifying, collecting, retrieving, and recording evidence.
2. *examination*(data acquisition). The collection of evidence is tested so that there is no change in the information on the evidence.
3. *Analysis.*Examination to obtain evidence related to the case.
4. *reporting*(Report preparation). Reporting on the results of the investigation obtained from the investigation contains the results of the analysis of evidence so that the evidence helps the investigation process to find the suspect(Nofiyan & Mushlihudin, 2020).

3. METHODOLOGY

3.A. Research Stages



Picture4. Research Stages

The stages of this research contain the stages of the research that will be carried out, the stages of this research are based on the stages of the research method listed in Figure 4.

3.B. Research methods

The research method is the method used by researchers to achieve research objectives. This research method is carried out in several parts including:

1. Time and Location. The time of research is from 20 December 2021 to 23 January 2022. The location of this research is in the Nusa Tamanlanrea Indah Housing area.
2. Instrumentation
   a. Hardware
   1) 2 laptops with Intel i5/i7 specifications
   b. Software (software)
   1) Microsoft Windows 10 Professional 64-bit, as Operating System
   2) Kali Linux, as the operating system
   3) Hping3
   4) Wireshark
   5) Snorby
   6) Name
   3. Methods of Data Collection

Research data collection was carried out by simulating attacks aimed at the web and processing the recorded data contained in snorby and wireshark.

3.C. Attack Simulation

Attack simulation in this research is carried out in several stages, namely:

1. *Information Gathering. Information Gathering*is the process of gathering information that is carried out to find target information, in this research the author will conduct Information Gathering on a web Horizonide.com.
2. *Vulnerability Assessment.*Is a method for identifying, detecting and studying target weaknesses, in this study the author uses cmd to get web Ip addresses and uses Nmap to find open hosting for attacks.
3. *Exploitaiton. Exploitation*is a method for attacking a target with information that has been obtained during the Information Gathering and vulnerability assessment, in this study the author will carry out a ping of death attack on the web carried out using the Hping3 software found on the Kali Linux operating system.

3.D. NIST (National Institute of Standards Technology) Forensics

The method from the National Institute of Standards Technology (NIST) is used to carry out the stages of analyzing digital evidence or the steps to obtain information from digital evidence. In the initial stages the data obtained is collected and examined, then the stage of extracting or creating an image data from the SSD and converting it into a format that can be processed by forensic tools. Furthermore, the data is translated into information through analysis, the results at this stage are evidence of the analogy of knowledge into action using the information obtained from the analysis in reporting.(Saad et al., 2020)

1. Collection (Collection):

this stage, will collect data obtained from data packet recordings and traffic observations directly or indirectly on computer networks.

2. Testing (Examinitaion):

in this step, there will be a process of identifying data that can be used as digital evidence. After the data is determined, the data collection process will be forensicly tested

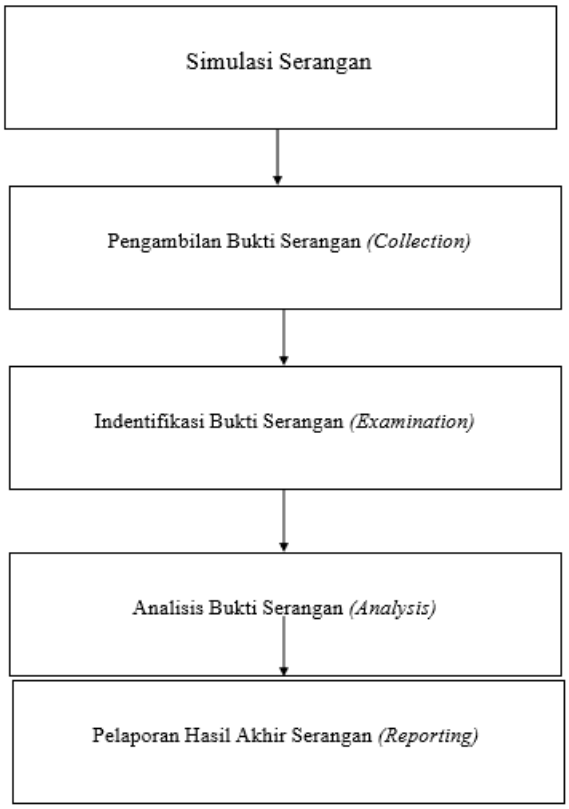
3. Analysis (Analysis):

The data that has been taken will be analyzed to look for things that can be used as evidence specifically for computer networks, things that will become digital evidence.

4. Report (Reporting):

the final stage of this metarouter traffic forensics step is reporting the results of the forensic analysis from start to finish in the form of a written report so that it can provide recommendations for improving policies, guidelines, procedures, tools, and other aspects of forensics.

The digital evidence that has been obtained in this study was obtained from the results of initial attacks that were carried out in the early stages of the research, there are forensic stages referring to the 4 stages of forensic work steps from NIST collection, exemination, analysis, reporting of the 4 steps of this method work steps in this study divided into 5 stages of research and can be seen in Figure 5.



Picture5. Research Stages

4. RESULTS AND DISCUSSION

4.A. Research result

The results of the attack simulation and collection of forensic evidence were carried out:

Table 1. Attack Simulation Testing

Stages	*Tools*	Date/Time
Information Gathering	-	27 January 2022/12: 00 WITA
Vulnarability Assessment	Name	January 30 2022/ 21 : 31 – 1 : 11 WITA
Exploitation	Hping3	31 January 2022/ 01 : 12 – 02 : 59 WITA

Table 2. Collection of Attack Evidence Data

Stages	*Tools*	Date/Time
Collection *(Collection)*	Snorby&Wireshark	January 32nd 2022/12 : 00 WITA
Testing *(Examination)*	Snorby&Wireshark	32 January 2022/ 21 : 31 – 1 : 11 WITA
Analysis	Snorby&Wireshark	32 January 2022/ 01 : 12 – 02 : 59 WITA

Stages	***Tools***	**Date/Time**
Reporting	Snorby&Wireshark	January 32nd 2022/12 : 00 WITA

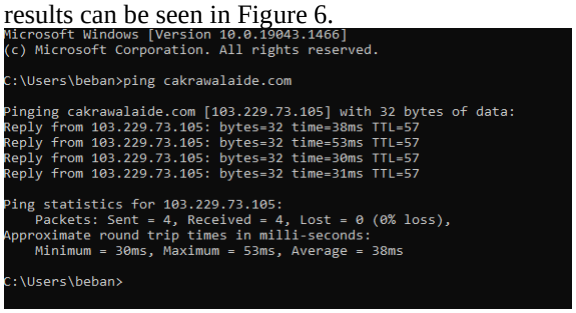
4.B. Attack Simulation

a. Information Gathering

*Information Gathering*focused on being able to collect sufficient information about the target system, in this study the target that was obtained when carrying out the Information Gathering was the Cakrawalaide.com website where the website is the website of one of the UKM that is on the UMI campus and still has a firewall vulnerability that is low enough to be penetrated.

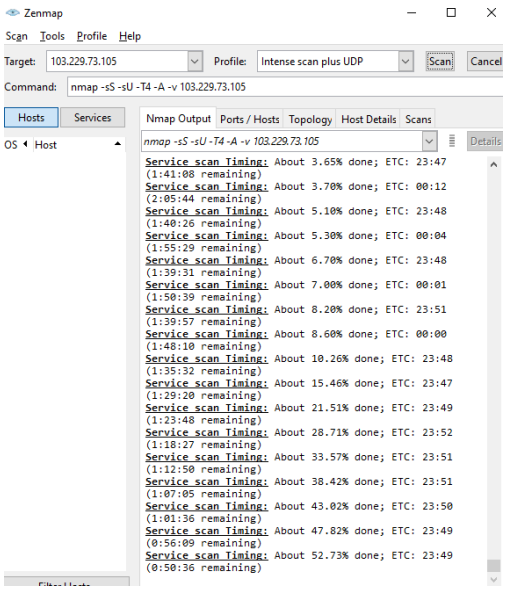
b. Vulnerability Assessment

This step is a continuation of the Information Gathering process, the purpose of carrying out this process is to identify weaknesses that might be exploited for the exploitation process, at this research stage a vulnerability assessment is carried out on the target web by first getting the IP Address of the web using CMD, the command entered in CMD is as follows (ping Horizonide.com) and the results can be seen in Figure 6.



Picture6. CMD Command Result

Next, use Nmap to find vulnerabilities on the target web by entering the target web's IP address into Nmap and performing a UDP scan command on Nmap. How to do a vulnerability assessment on Nmap can be seen in Figure 7.



Picture7. vulnerability assessment on Nmap

In Figure 7 you can see Nmap is conducting a vulnerability search on the target web, by entering the IP address 103.229.73.105 the vulnerability assessment was carried out at 21:31 WITA and finished at 01:11 WITA scanning on Nmap took 2 hours to get an open port From the IP address 103.229.73.105, the scanning results show that 1000 open ports will then be selected again by Nmap to determine which ports are the most vulnerable to attack. The final result is that Nmap finds port 53 can be attacked.

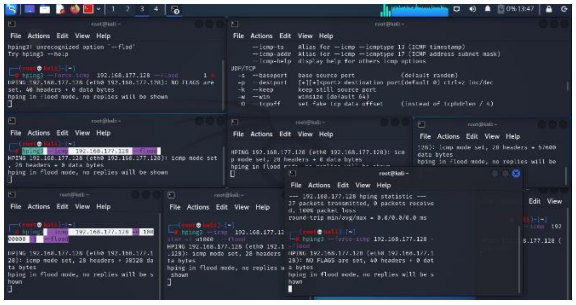
c. *Exploitation*

the purpose of this stage is the exploitation of system weaknesses (system vulnerabilities) that have been obtained in the previous stage. At this stage of research the author will start carrying out DDoS attacks where this DDoS is a flooding attack that aims to spend the resources of a web server. The attack being carried out is a ping of death type DDosS attack which will send excess ICMP packets at layer 3 OSI on a web. server and can result in server downtime.

The attack was carried out on a laptop that had the Kali Linux operating system installed. In Kali Linux, there was an Hping3 software to carry out the attack, the attack can be seen in Figure 8.

Picture8. Ping of death attack on Hping3

From Figure 8 it can be seen that the attack was carried out 5 times by opening the root terminal on Kali Linux and entering commands in the terminal



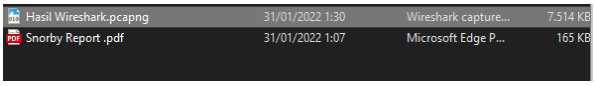
the attack was carried out at 01:12 WITA and the target web was down at 02:59,

4.C. NIST (National Institute of Standards Technology) Forensics

In collecting forensic evidence, there will be 4 stages of collection, testing, analysis, data processing reports for forensic evidence using 2 tools, the first is using Snorby software, the second is using Wireshark software.

A. Collection (Collection).

In the data collection stage that will be used as forensic evidence on network traffic, there are 2 data obtained from snorby and wireshark.



Picture9. Evidence of Snorby & Wireshark Attack Results

Figure 9 shows the capture results with the name (Wireshark Results) which were carried out on

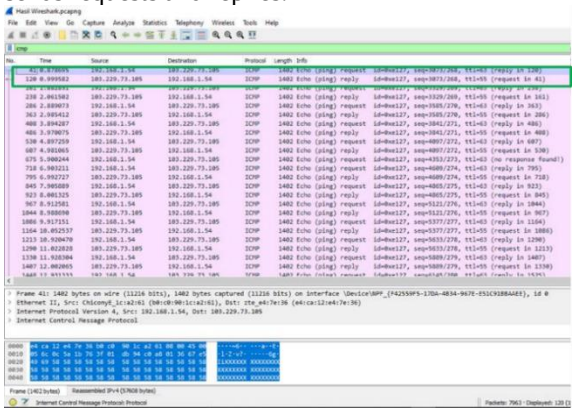
the date and month of January 31 2022 with the pcapng file type obtained from Wireshark and the capture results with the name snorby report on the same date and month, file type pdf obtained from Snorby.

B. Testing (Examination)

This testing or checking stage is carried out to find out or identify the ping of death attack on the target web with the ip address 103.229.73.105 using 2 tools wireshark and snorby.

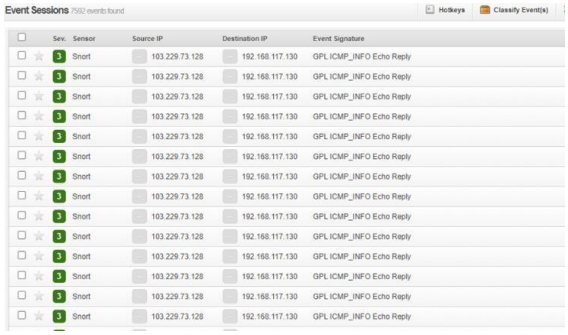
The first thing to do is process the data in the Wireshark.pcapng Results file that was obtained during the data collection stage. The data sought here is data with the ICMP protocol on Wireshark, which can be seen in Figure 10.

From figure 10 and number 120 it can be seen that there was an attack on the ip address 103.229.73.105 where the ip address is the ip address of Cakrawalaide.com with the ICMP protocol that sends requests and replies.



Picture10. Wireshark Attack Proof Results

The next step is to check the Snorby tools obtained when scanning the network, the results of the Snorby inspection can be seen in Figure 11.



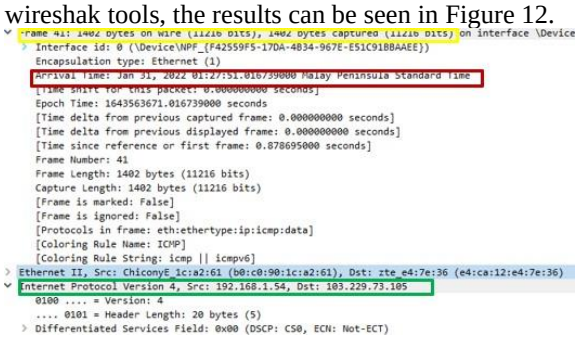
Picture11. Proof of Snorby Attack Results

In Figure 11 above, you can see that there was an ICMP attack on the snorby tool with the information ICMP_INFO Echo reply with the same ip address 103.229.73.128.

C. Analysis

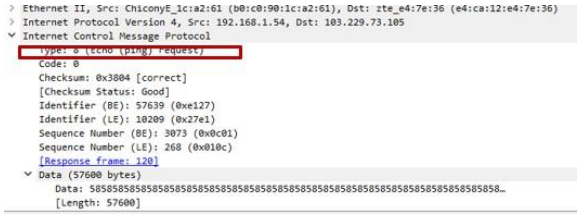
After carrying out the stages of collection and inspection and finding the ping of death attack with the ICMP protocol, an analysis of the ICMP attack will be carried out starting from the attacker's ip addresses and how many packets were sent on the target web, to carry out this analysis wireshark and snorby tools will be used.

The first thing to do is to do an analysis on the wireshak tools, the results can be seen in Figure 12.



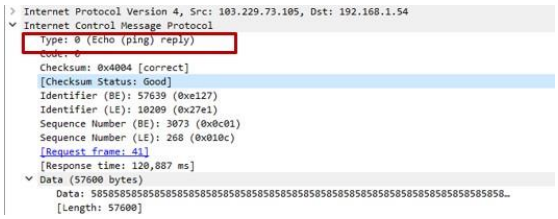
Picture12. Analysis Results on Wireshark

From the results of Figure 13 marked in red it can be seen that the attack occurred on January 31, 2022 at 01:27, the yellow packet received 1402 bytes or 11216 bits from the source ip address 192.168.1.54 with the destination addressing the ip addresses 103.229.73.105 which is marked in green.



Picture13. ICMP Request

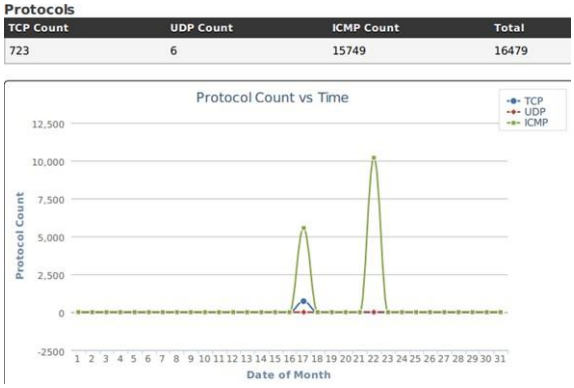
The results of the analysis from Figure 14 on the sign colored red explain that the type of ICMP message above is 8, that type 8 is an echo request, which is a message when asking to connect to the victim's IP address.



Picture14. ICMP Reply

The results of the analysis from Figure 14 on the sign colored red explain that the ICMP message type above is 0, that type 0 is an echo reply, which is an answer to the message from the Ping request in Figure 14 so that it can connect to the victim's IP address.

Furthermore, by using the Snorby tool by looking at the file at the Snorby report.pdf data collection stage when scanning network traffic on Snorby, how many results are obtained in conducting an analysis on Snorby.



Picture15. Snorby Protocol Count Analysis Results

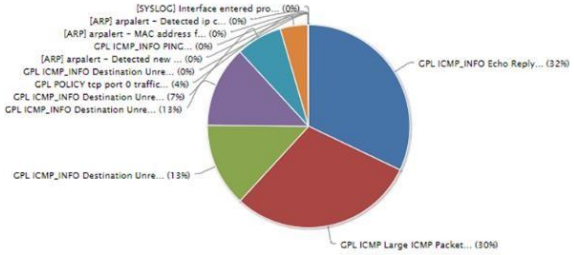
The green code indicates an ICMP type attack and counting 10,000 data packets sent by the Web server, 15,749 attacks were successfully sent to the target.

Top 15 Signatures

Signature Name	Percentage	Event Count
GPL ICMP_INFO Echo Reply	32.09%	5288
GPL ICMP Large ICMP Packet	29.76%	4904
GPL ICMP_INFO Destination Unreachable Destination Host Unknown	13.31%	2194
GPL ICMP_INFO Destination Unreachable Host Unreachable	12.96%	2136
GPL ICMP_INFO Destination Unreachable Network Unreachable	7.35%	1211
GPL POLICY tcp port 0 traffic	4.39%	723
GPL ICMP_INFO Destination Unreachable Port Unreachable	0.07%	12

Picture16. Snorby analysis results of attack types

There are 2 types of attacks carried out, the first is the type of attack with the ICMP_INFO Echo reply ket, which has a presentation of 32.09% which has counted 5288 attacks.



Picture17. Snorby Diagram Report results

From the results of the picture above it can be seen that the ICMP attacks that were successful were 32% and 30%, while those that were not successful were 7% and 13%.

D. Reporting

After carrying out the 3 stages of collection, testing and analysis that have been carried out, the final stage is to make a forensic data report that has been analyzed in this study and will be seen in the following table

Table 3. Reporting of Evidence of Attack

No.	Data	Ket	Digital Proof
1	*Attacker IP addresses*	Yes	Figure 13
2	Ping of death skimming	Yes	Figure 11,16,17
3	The number of bytes of ping of death	Yes	Figure 16,14,15
4	Attack Percentage *ping of death*	Yes	Figure 17.18
5	Ping of death raid which failed	Yes	Figure 18

From the results of the report above, the author gets the results of the attack reporting that occurred on the jasaide.com web with the ip address 103.229.73.105, the results of the attack from the IP address 192.168.1.54 with the type of ping of death attack with the ICMP protocol packets received per packet 1408 bytes/1126 bits and 15749 attacks were carried out with the percentage of information GCL_ICMP-INFO Echo Replay successfully carried out 32% and GCL_ICMP-LARGE ICMP Packet 30% and failed to carry out ICMP attacks 7% and 13%.

5. CONCLUSION

Based on the results obtained from the trial, the authors conclude, among others:

1. The NIST method which includes collection, testing, analysis, reporting can be maintained or repeated, based on attack simulations that have been carried out successfully obtained digital evidence either by indirect observation of the inspection stage using wireshark and snorby.
2. The ping of death DDoS attack simulation was successfully carried out with the help of Hping3 tools for exploits, Nmap to perform vulnerabilities on the target web and succeeded in bringing down the web server.
3. The research produced evidence of the implementation of the stages in the National Institute of Standards and Technology (NIST) method. The first stage is collection (collection of data) file capture ResultsWireshark.pcapng and Snorby Report when using Wireshark and Snorby

BIBLIOGRAPHY

Diansyah, T. M. (2015). ANALISA PENCEGAHAN AKTIVITAS ILEGAL DIDALAM JARINGAN MENGGUNAKAN WIRESHARK. Jurnal TIMES.

Du, X., Le-Khac, N.-A., & Scanlon, M. (2017). Evaluation of Digital Forensic Process Models with Respect to Digital Forensics as a Service. ArXiv:1708.01730 [Cs]. http://arxiv.org/abs/1708.01730

Geges, S., & Wibisono, W. (2015). PENGEMBANGAN PENCEGAHAN SERANGAN DISTRIBUTED DENIAL OF SERVICE (DDOS) PADA SUMBER DAYA JARINGAN DENGAN INTEGRASI NETWORK BEHAVIOR ANALYSIS DAN CLIENT PUZZLE | Geges | JUTI: Jurnal Ilmiah Teknologi Informasi.

generator, metatags. (2021). Identifikasi Bukti Forensik Jaringan Virtual Router Menggunakan Metode NIST | Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi). https://jurnal.iaii.or.id/index.php/RESTI/article/view/2784

Hanipah, R., & Dhika, H. (2020). Analisa Pencegahan Aktivitas Ilegal Didalam Jaringan Dengan Wireshark. DoubleClick: Journal of Computer and Information Technology, https://doi.org/10.25273/doubleclick.v4i1.568

Nofiyan, A., & Mushlihudin, M. (2020). Analisis Forensik pada Web Phishing Menggunakan Metode National Institute Of Standards And Technology (NIST). Jurnal Sarjana Teknik Informatika

Ridho, F. (2017). Analisis Forensik Router Untuk Mendeteksi Serangan Distributed Danial of Service (DDoS) Secara Real Time. Annual Research Seminar (ARS).

Saad, S. K., Umar, R., & Fadlil, A. (2020). Analisis Forensik Aplikasi Dropbox Pada Android Menggunakan Metode NIST. Seri Prosiding Seminar Nasional Dinamika Informatika, http://prosiding.senadi.upy.ac.id/index.php/senadi/article/view/138

Saputra, A., & Widiyasono, N. (2017). Analisis Digital Forensik pada File Steganography (Studi kasus: Peredaran Narkoba). Jurnal Teknik Informatika Dan Sistem Informasi.

Sujana, A. P. (2015). Perangkat Pendukung Forensik Lalu Lintas Jaringan. TEKNIK KOMPUTER, Volume 03 No. 1. http://komputika.tk.unikom.ac.id/jurnal/perangkat-pendukung-forensik.

Wahanani, H. E., Nugroho, B., & Prakoso, G. I. (2016). ANALISA SERANGAN SMURF DAN PING OF DEATH DENGAN METODE SUPPORT VECTOR MACHINE (SVM). Scan : Jurnal Teknologi Informasi Dan Komunikasi.

Walad, I. (2020). Analisis Denial Of Service Attack Pada Sistem Keamanan Web [Thesis, Universitas Sumatera Utara]. https://repositori.usu.ac.id/handle/123456789/28240

Walad, I. (2020). Denial Of Service Attack Analysis on Web Security Systems [Thesis, University of North Sumatra]. https://repositori.usu.ac.id/handle/123456789/28240