CyberSecurity dan Forensik Digital e-ISSN: 2615-8442
Vol. 5, No. 1, Mei 2022, hlm. 23-31

ANALISIS FORENSIK TERHADAP SERANGAN DDOS *PING OF DEATH* PADA SERVER

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

Abstrak

Kemajuan teknologi yang terus berkembang bisa menjadi sebuah ancaman salah satunya pada bidang dunia maya dimana terdapat beberapa kejahatan cyber dengan caranya yaitu menurunkan kinerja web server Anda dengan membanjiri lalu lintas jaringan. Terlepas dari apa telah Anda lakukan untuk meningkatkan kinerja web server Anda, peretas masih dapat mensimulasikan lebih banyak pengguna daripada yang dapat ditangani oleh web server itu sendiri. Pada data IDSIRTI bulan oktober 2020 total serangan mencapai 66 juta dan serangan DDoS dilakukan berdasarkan klasifikasi anomali mencapai 6 juta serangan. Peningkatan ancaman dan serangan terhadap keamanan sistem meningkat karena didukung oleh kemudahan akses dan ketersediaan sumber daya yang lebih mudah didapatkan. Banyak tahapan yang dapat dilakukan pelaku kejahatan *cyber* untuk memuluskan langkahnya mendapatkan informasi sebanyak mungkin pada target salah satunya adalah DDoS. Untuk memuluskan langkahnya biasanya dilakukan dengan menggunakan metode untuk membanjiri *source* pada perangkat jaringan. *Web server* merupakan salah satu bagian dari sebuah jaringan dan seiring jalanya perkembangan zaman banyak sekali *web* yang tersebar atau bertebaran di internet dan bisa diakses, serangan intrusi sangat tidak diinginkan pada sistem karena bisa membahayakan kerahasiaan dan ketersediaan sumber daya yang ada jenis serangan terhadap sebuah *web server* menghabiskan sumber (*resource*) yang dimiliki.Masalah datang dimulai ketika paket data yang datang sangat banyak dan harus di analisis terhadap sebuah data. Pada penelitian ini akan melakukan sebuah serangan DDOS *Ping of death* pada sebuah *web server* yang dimana hasil dari sebuah penyerangan tersebut akan menciptakan data record yang terekam pada *software snorby,* data tersebut dibutuhkan untuk menjalankan forensik agar dapat mengumpulkan bukti digital dengan menggunakan metode forensik (NIST) yang meliputi *collection, examination, analysis, reporting*. Berdasarkan dari percobaan pengujian tahapan pemeriksaan menghasilkan bukti data oleh *snorby* tahapan analisis mendapatkan adanya serangan yang dilakukan oleh alamat IP 192.168.177.2 dengan jenis serangan DDOS *Ping of death* dan menyerang *web server* dengan alamat IP 103.229.73.105.

Kata kunci: *Web Server,Forensic,NIST, DDoS, Ping of death*

ANALYSIS FORENSIC DDOS *PING OF DEATH* ATTACK ON SERVER

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 handled. IDSIRTI data October 2020, total attacks reached 66 million and DDoS attacks carried out based on anomaly classification reached 6 million attacks. Increased 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 informationas possible on the target, 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. Based on the testing experiment, the inspection stage produced evidence of

data by Snorby, the analysis stage found an attack carried out by the IP address 192.168.177.2 with the type of DDOS attack Ping of death.

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

1. PENDAHULUAN

Pada era teknologi informasi, terdapat bidang forensik yang mampu membuktikan tindak kejahatan berdasarkan serangkaian tahapan seperti mengidentifikasi, menguji, menganalisis, serta dapat mendokumentasikan bukti yang terdapat pada sumber serta hasil analisa yang dilakukan. Forensik perlu dilakukan dengan tujuan membantu administrator jaringan untuk mempermudah dalam menemukan rancang untuk mencatat segala kejadian yang ada pada sistem. analisis forensik perlu dilakukan dengan tujuan untuk menemukan bukti berdasarkan sumber serangan, waktu kejadian, serta dampak dari serangan DDOS *ping of death*, mendapatkan sejumlah bukti forensik dengan temuan kunci utama dan bukti pendukung analisis pada penelitian forensik ini, aplikasi Wireshark sebagai analisis paket secara *offline*, mendapatkan barang bukti berupa hasil rekaman paket (Ridho, 2017).

analisis paket secara *offline*, mendeteksi kemungkinan *ip address*s yang bertanggung jawab atas serangan di antara paket yang tertangkap menggunakan snorby. Penelitian ini menjelaskan tentang alat yang dapat mendeteksi serangan DDoS ataupun mengurangi serangan yang muncul pada jaringan, kerangka forensik disajikan dengan mempertimbangkan data yang tercatat pada data yang tersimpan.

Serangan DDoS (*Distributed Denial of Service*). Serangan yang mengakibatkan sistem keamanan jaringan diserang mengalami gangguan. Gangguan tersebut bisa berupa kegagalan sistem, halt, error request bahkan kerusakan hardware server tersebut. Setelah melihat masalah masalah pada sistem keamanan jaringan (Wahanani et al., 2016).

DDoS telah dikenal untuk komunitas jaringan sejak awal 1980. Target serangan DDoS bisa ditujukan ke berbagai jaringan, bisa ke *routing device, web, electronic mail*, atau *server domain name system*. Serangan ini bertujuan membuat server *shutdown, reboot, crash*, atau *"not responding"*.

Saran selanjutnya yaitu melakukan penelitian analisis paket secara *offline* dengan menggunakan aplikasi selain wireshark dan *network miner*, seperti Microsoft Network Monitor dan NetIntercept (generator, 2021).

pembaruan pada penelitian ini terdapat pada *tools*, *tools* yang digunakan yaitu mengunakan snorby untuk melakukan olah forensik, seragan yang dilakukan menggunakan DDoS *Ping of death* yang akan menyerang web Ada dua tahapan dalam penelitian ini yang pertama melakukan simulasi serangan dengan jenis seragan DDoS (*Distributed Denial of Service*) *ping of death* pada web, yang kedua melakukan analisis forensik mengunakan metode National Institute of Standards Technology (NIST), Penelitian ini difokuskan pada serangan *ping of death* dengan melihat aktivitas data *traffic* jaringan menggunakan *tools* pada *software* snorby.

2. TINJAUAN PUSTAKA

2.A. Digital Forensik

Digital forensik adalah kombinasi disiplin ilmu hukum dan pengetahuan komputer dalam mengumpulkan dan menganalisa data dari sistem komputer, jaringan, komunikasi nirkabel, dan perangkat penyimpanan sehingga dapat dibawa sebagai barang bukti di dalam penegakan hukum. Dapat disimpulkan bahwa digital forensik adalah penggunaan teknik analisis dan investigasi untuk mengidentifikasi, mengumpulkan, memeriksa dan menyimpan bukti/informasi yang secara magnetis tersimpan/disandikan pada komputer atau media penyimpanan digital sebagai alat bukti dalam mengungkap kasus kejahatan yang dapat dipertanggungjawabkan secara hukum (Saputra & Widiyasono, 2017).

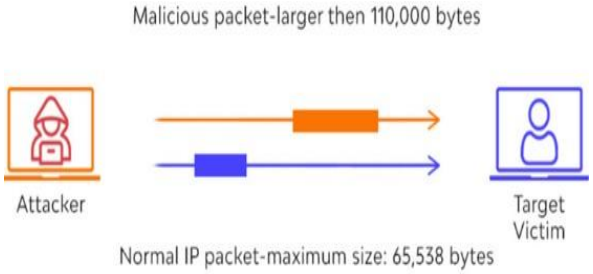
Komponen dalam suatu model digital forensik melibatkan tiga komponen yang dikelola sedemikian rupa sehingga menjadi sebuah tujuan akhir dengan segala kelayakan serta hasil yang berkualitas. Ketiga komponen tersebut yaitu :

a. Manusia (*People*), Diperlukan kualifikasi untuk mencapai manusia yang berkualitas. Memang mudah untuk belajar komputer forensik, tetapi untuk menjadi ahlinya, dibutuhkan lebih dari sekedar pengetahuan dan pengalaman.
b. Peralatan (*Equipment*), Diperlukan sejumlah perangkat atau alat yang tepat untuk mendapatkan sejumlah bukti yang dapat dipercaya dan bukan sekedar bukti palsu
c. Aturan (*Protocol*), Diperlukan dalam munurut menggali, mendapatkan, menganalisis, dan akhirnya menyajikan dalam bentuk laporan yang akurat, diperlukan pemahaman yang baik dalam segi hukum etika, kalau perlu dalam menyelesaikan sebuah kasus (Du et al., 2017).

2.B. *Ping of death*

ping of death yaitu serangan paling lama dan sering digunakan orang pada serangan ini dengan menggunakan utility ping disebuah sistem operasi. saat fragmentasi dilakukan, setiap fragmen IP perlu membawa informasi tentang bagian mana dari paket IP asli yang dikandungnya. Informasi ini menurut disimpan di bidang *Fragment Offset*, di header IP.

Bidang ini panjangnya 13 bit, dan berisi offset data dalam fragmen IP saat ini, dalam paket IP asli. Offset diberikan dalam satuan 8 bits. Ini memungkinkan offset maksimum 65.528 ((213-1)*8). Kemudian saat menambahkan 20 bits header IP, maksimumnya adalah 65.548 bits, yang melebihi ukuran bingkai maksimum. Artinya, fragmen IP dengan offset maksimum harus memiliki data yang tidak lebih dari 7 bits, atau akan melebihi batas panjang paket maksimum. Pengguna yang berniat jahat dapat mengirim fragmen IP dengan offset maksimum dan dengan lebih banyak data dari 8 bits (sebesar yang dimungkinkan oleh lapisan fisik) (Walad, 2020).



Gambar 1. cara kerja ping of death

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

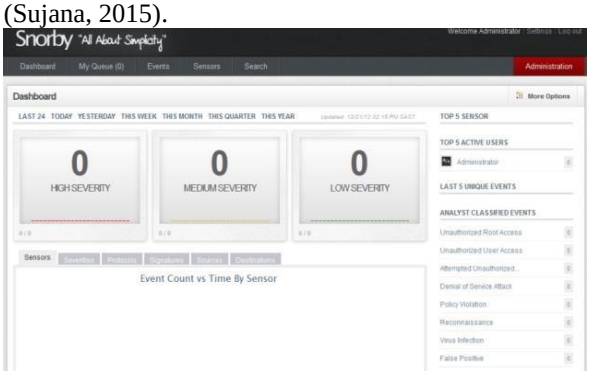
Serangan DDOS biasanya melibatkan penyerang mengirimkan pesan untuk mengeksploitasi kerentanan tertentu yang mengarah kepada ketidakstabilan atau kelumpuhan sistem bisnis. Penyerang juga dapat melakukan DDOS dengan mengirim sejumlah besar pesan normal dengan cepat ke *node* tunggal, tujuannya adalah untuk menghabiskan sumber daya sistem sehingga menyebabkan kegagalan sistem bisnis. bandwidth jaringan. Berikut ini adalah langkah-langkah yang terjadi pada serangan terdistribusi:

a. Penyerang mengirimkan perintah “eksekusi” yang berupa pesan ke program kontrol utama.
b. Program kontrol utama menerima pesan berupa perintah "eksekusi" dan kemudian menyebarkan perintah penyerangan untuk tiap daemon serangan yang berada di bawah kendalinya.
c. Begitu menerima perintah serangan, daemon serangan memulai serangan terhadap target (Geges & Wibisono, 2015.).

Meskipun tampaknya pelaku utama serangan DDoS hanya melancarkan aksinya dengan mengirim perintah eksekusi, namun sebenarnya dia benar-benar harus melakukan perencanaan demi serangan DDoS yang berhasil. Penyerang harus menyusup semua host komputer dan jaringan di mana para daemon harus terpasang. Penyerang harus mempelajari topologi jaringan target dan mencari celah keamanan dan kecendrungan sistem yang dapat dimanfaatkan untuk melancarkan serangan.

2.D. Snorby

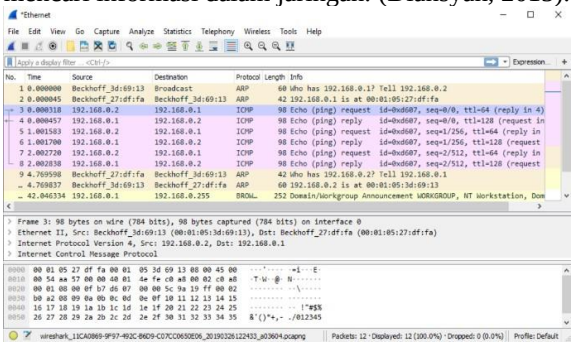
Snorby adalah *frontend web application* (yang ditulis dalam Bahasa ruby on rails) untuk monitoring keamanaan jaringan yang bersangkutan dengan *system network intrusion detection* seperti snort. Administrator dalam melakukan tuning terhadap rule yang diimplementasikan untuk menjalankan snorby (Sujana, 2015).



Gambar 2. Aplikasi snorby

2.E. Wireshark

Wireshark banyak digunakan dalam memecahkan *troubleshooting* dijaringan untuk memeriksa keamanan jaringan, men-*debug* implementasi protocol jaringan dalam *software* mereka, melakukan *debugging* implementasi paket protocol, dan banyak digunakan untuk sniffer atau mencari data-data privasi dijaringan dan juga sebagai media atau tool yang dapat dipakai untuk mencari informasi dalam jaringan. (Diansyah, 2015).



Gambar 3. Aplikasi wireshark

Manfaat dari penggunaan aplikasi wireshark ini yaitu sebagai berikut :

a. Menangkap informasi atau data paket yang dikirim dan diterima dalam jaringan komputer.
b. Mengetahui aktivitas yang terjadi dalam jaringan komputer.
c. Mengetahui dan menganalisa kinerja jaringan komputer yang dimiliki seperti kecepatan akses/shere data dan koneksi jaringan ke internet.
d. Mengamati keamanan dari jaringan komputer. Kegunaan wireshark, beberapa kegunaan wireshark diantaranya, wireshark digunakan oleh seorang network administrator untuk menganalisis lalu lintas dalam jaringannya (Hanipah & Dhika, 2020).

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

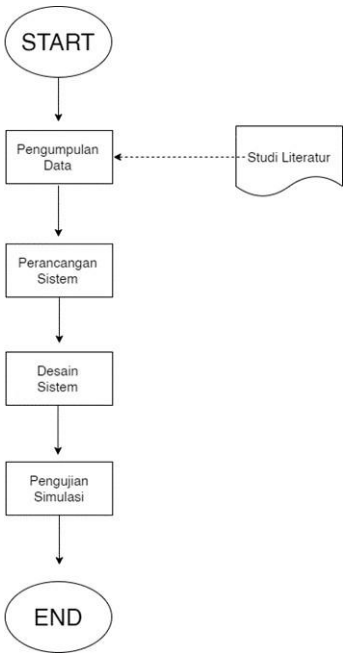
National Institute of Standards and Technology (NIST) adalah badan nasional non regulator dari bagian administrasi teknologi Amerika Serikat. Misi dari badan ini adalah untuk mendorong dan membuat pengukuran, standar, dan teknologi untuk meningkatkan produktivitas, mendukung perdagangan, dan memperbaiki kualitas hidup semua orang. Program cybersecurity NIST berupaya memungkinkan pengembangan lebih besar dan penerapan teknologi dan metodologi keamanan yang inovatif dan praktis untuk meningkatkan kemampuan negara mengatasi tantangan keamanan komputer dan informasi saat ini dan masa depan.

Tahapan pada metode NIST adalah:

1. *Collection* (Pengumpulan data). Pengumpulan barang bukti dengan proses identifikasi, pengumpulan, pengambilan, dan perekaman barang bukti.
2. *Examination* (Akuisisi data). Pengumpulan barang bukti dilakukan pengujian agar tidak ada perubahan informasi pada barang bukti.
3. *Analysis.* Pemeriksaan untuk mendapatkan bukti terkait dengan kasus tersebut.
4. *Reporting* (Pembuatan laporan). Pelaporan hasil investigasi yang didapatkan dari penyelidikan berisi tentang hasil analisis barang bukti sehingga bukti tersebut membantu proses penyidikan untuk menemukan tersangka (Nofiyan & Mushlihudin, 2020).

3. METODOLOGI

3.A. Tahapan Penelitian



Gambar 4. Tahapan Penelitian

Tahapan peneilitian ini berisikan tahapan-tahapan penelitian yang akan dilakukan, tahapan penelitian ini berdasarkan tahapan metode penelitian yang tercantum pada gambar 4.

3.B. Metode Penelitian

Metode penelitian adalah cara yang digunakan peneliti untuk mencapai tujuan penelitian. Metode penelitian ini dilakukan beberapa bagian diantaranya:

1. Waktu dan Lokasi. Waktu penelitian pada tanggal 20 Desember 2021 sampai tanggal 23 Januari 2022. Lokasi penelitian ini dilakukan pada area Perumahan Nusa Tamanlanrea Indah.
2. Instrumentasi
   a.Perangkat keras (hardware)
   1) 2 laptop dengan spesifikasi intel i5/i7
   b. Perangkat lunak (*software*)
   1) Microsoft Windows 10 Professional 64-bit, sebagai Sistem Operasi
   2) Kali Linux, sebagai sistem operasi
   3) Hping3
   4) Wireshark
   5) Snorby
   6) Nmap
   3. Cara Pengumpulan Data

Pengumpulan data hasil penelitian dilakukan dengan cara melakukan simulasi serangan yang tertuju pada web dan mengolah data recod yang terdapat pada snorby dan wireshark .

3.C. Simulasi Serangan

Simulasi serangan pada penlitian ini dilakukan dengan bebara tahapan yaitu:

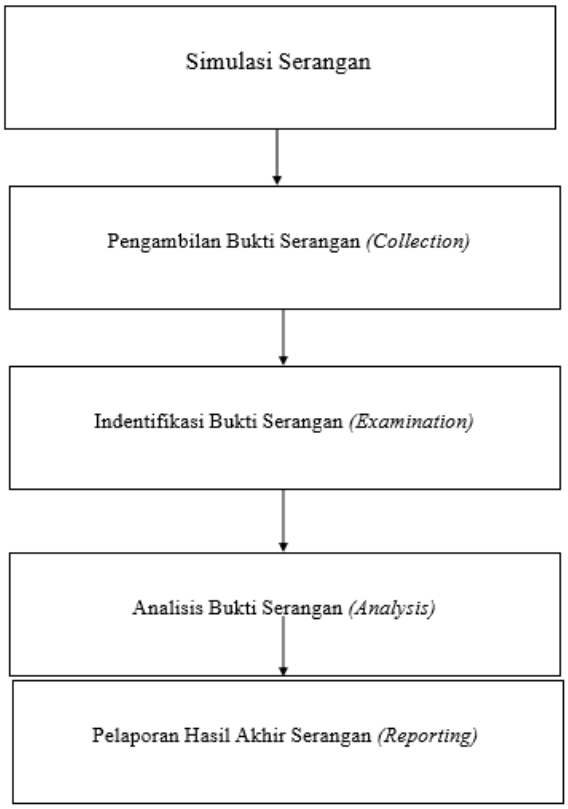
1. *Information Gathering*. *Information Gathering* adalah proses pengumpulan informasi yang dilakukan untuk menemukan informasi target, pada peneletian ini penulis akan melakukan *Information Gathering* pada sebuah web cakrawalaide.com.
2. *Vulnerabillity Assesment.*Merupakan metode untuk melakukan Identifikasi mendeteksi dan mempelajari kelemahan target, pada penelitian ini penulis menggunakan cmd untuk mendapatkan *Ip addresss* web dan menggunakan Nmap untuk mencari iphosting yang terbuka untuk melakukan penyerangan.
3. *Exploitaiton. Explotation* adalah metode untuk menyerang suatu target dengan informasi yang sudah diapat pada saat *Information Gathering* dan *vulnerability assesment*, pada penelitian ini penulis akan melakukan serangan *ping of death* penyeragan pada web dilakukan dengan mengunakan *software* Hping3 yang terdapat pada sistem operasi kali linux.

3.D. Forensik NIST (National Institute of Standars Technology)

Metode dari National Institute of Standards Technology (NIST) digunakan untuk melakukan tahapan analisis terhadap bukti digital atau tahapan untuk mendapatkan informasi dari bukti digital. Pada tahap awal data yang didapat dikumpulkan dan diperiksa, kemudian tahap ekstraksi atau pembuatan image data dari SSD dan diubah menjadi format yang dapat diproses oleh tool forensik. Selanjutnya data diterjemahkan menjadi informasi melalui analisis, hasil pada tahap ini menjadi bukti analogi dari pengetahuan ke dalam tindakan menggunakan informasi yang didapatkan dari analisis dalam pelaporan.(Saad et al., 2020)

1. Pengumpulan *(Collection)* :
   tahapan ini, akan mengumpulkan data-data yang diperoleh dari rekaman paket data dan pengamatan lalu lintas secara langsung maupun tidak langsung pada jaringan komputer.
2. Pengujian (*Examinitaion*) :
   pada langkah ini, akan ada proses identifikasi data yang dapat digunakan sebagai bukti digital. Setelah ditentukan data akan diambil proses pengambilan data akan diuji secara forensik
3. Analisa (*Analysis*) :
   data yang telah di ambil akan di analisis untuk mencari hal-hal yang dapat digunakan sebagai bukti terkhusus jaringan komputer, hal yang akan menjadi bukti digital.
4. Laporan (*Reporting*) :
   tahap akhir ini langkah forensik lalu lintas metarouter adalah pelaporan hasil analisis forensik dari awal hingga akhir dalam bentuk laporan tertulis sehingga dapat memberikan rekomendasi untuk perbaikan kebijakan, pedoman, prosedur, alat, dan aspek lain dari forensik.

Bukti digital yang telah didapatkan pada penelitian ini diperoleh dari hasil semulasi serangan yang telah dilakukan pada tahapan awal penelitian, ada tahapan forensik mengacu pada 4 tahapan langkah kerja forensik dari NIST *collection, exemination, analysis, reporting* dari 4 langkah metode ini langkah kerja pada penelitian ini dibagi menjadi 5 tahapan penelitian dan dapat dilihat pada gambar 5.



Gambar 5. Tahapan Penelitian

4. HASIL DAN PEMBAHASAN

4.A. Hasil Penelitian

Adapun hasil Simulasi serangan dan pengumpulan bukti forensik yang dilakukan :

Table 1. Pengujian Simulasi serangan

Tahapan	*Tools*	Tanggal/Waktu
Information Gathering	-	27 Januari 2022/12 : 00 WITA
Vulnarabilltiy Assement	Nmap	30 Januari 2022/ 21 : 31 – 1 : 11WITA
Explotation	Hping3	31 Januari 2022/ 01 : 12 – 02 : 59WITA

Tabel 2. Pengumpulan Data Barang Bukti Serangan

Tahapan	*Tools*	Tanggal/Waktu
Pengumpulan *(Collection)*	Snorby&Wireshark	32 Januari 2022/12 : 00 WITA
Pengujian *(Examinitaion)*	Snorby&Wireshark	32 Januari 2022/ 21 : 31 – 1 : 11 WITA
Analisa *(Analysis)*	Snorby&Wireshark	32 Januari 2022/ 01 : 12 – 02 : 59 WITA
Laporan *(Reporting)*	Snorby&Wireshark	32 Januari 2022/12 : 00 WITA

4.B. Simulasi Serangan

a. Information Gathering

Information Gathering difokuskan untuk dapat mengumpulkan informasi secukupnya mengenai sistem target, pada penelitian ini target yang di dapat pada saat mealkukan *Information Gathering* adalah website Cakrawalaide.com dimana web adalah website salah satu UKM yang berada pada kampus UMI dan masih memiliki kerentanan firewall yang cukup rendah untuk ditembus.

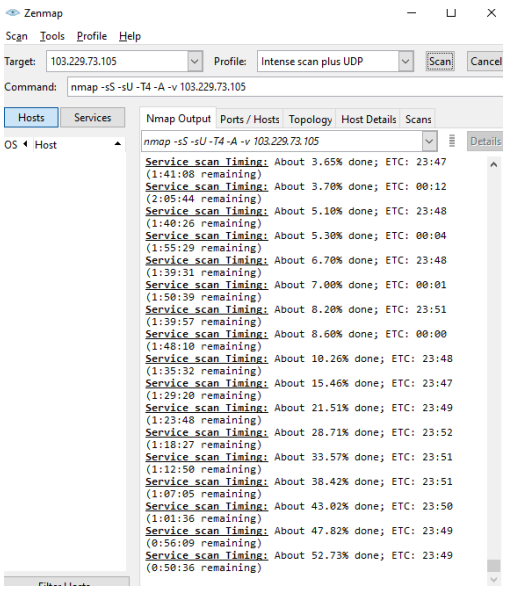
b. Vulnerabillity Assesment

Langkah ini merupakan lanjutan dari proses *Information Gathering*, tujuan melakukan proses ini untuk mengidentifikasi kelemahan yang kemungkinan dapat dimanfaatkan untuk proses eksploitasi, pada tahapan penelitian ini *vulnerabillity assessment* dilakukan pada web target dengan cara yang pertama mendapatkan *IP Address* web tersebut menggunakan CMD, perintah yang dimasukan dalam CMD adalah sebagai berikut (ping cakrawalaide.com) dan hasilnya dapat dilihat pada gambar 6.

```
Microsoft Windows [Version 10.0.19043.1466]
(c) Microsoft Corporation. All rights reserved.

C:\Users\beban>ping cakrawalaide.com

Pinging cakrawalaide.com [103.229.73.105] with 32 bytes of data:
Reply from 103.229.73.105: bytes=32 time=38ms TTL=57
Reply from 103.229.73.105: bytes=32 time=53ms TTL=57
Reply from 103.229.73.105: bytes=32 time=30ms TTL=57
Reply from 103.229.73.105: bytes=32 time=31ms TTL=57

Ping statistics for 103.229.73.105:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 30ms, Maximum = 53ms, Average = 38ms

C:\Users\beban>
```

Gambar 6. Hasil Perintah CMD

Berikutnya menggunakan Nmap untuk mendapatkan kerentanan pada web target dengan cara memasukan *Ip address* web *target* kedalam Nmap dan melakukan perintah UDP scan pada Nmap, cara melakukan vulanerabillity assessment pada Nmap dapat dilihat pada gambar 7.



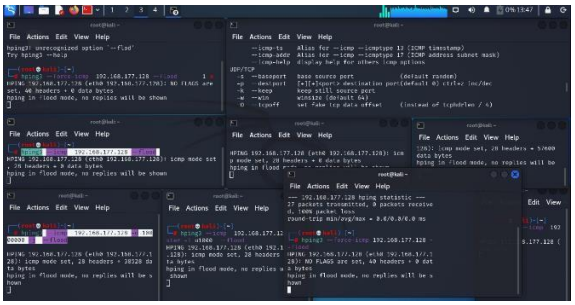
Gambar 7. vulnerabillity assessment pada Nmap

Pada gambar 7 bisa dilihat Nmap sedang melakukan pencarian keretanan pada web target, dengan cara memasukan *IP address* 103.229.73.105 *vulnerabillity assessment* dilakukan pada jam 21 : 31 WITA dan selesai pada jam 01 : 11 WITA scaning pada Nmap memakan waktu 2 jam sampai mendapatkan open port dari *IP Address* 103.229.73.105 dari scanning tersebut mendapatkan hasil 1000 port yang terbuka selanjutkan akan diseleksi lagi oleh Nmap untuk menentukan port mana yang paling rentan untuk diserang hasil akhir nmap mendapati port 53 dapat diserang.

c. *Exploitation*

tujuan dari tahapan ini adalah eksploitasi terhadap kelemahan sistem *(vulnerabilities system)* yang sudah didapatkan pada tahapan sebelumnya. Pada tahapan penelitian ini penulis akan mulai melakukan serangan DDoS dimana DDoS ini adalah sebuah serangan *flooding* yang bertujuan untuk menghabiskan re*source* dari sebuah *web server* serangan yang dilakukan adalah serangan DDosS bertipe *ping of death* yang akan mengirimkan paket ICMP yang berlebih pada layer 3 OSI pada sebuah web server dan bisa mengakibatkan *server down.*

Penyerangan dilakukan dalam sebuah laptop yang sudah terinstall system operasi Kali linux didalam kali linux tersebut terdapat sebuah *software* Hping3 untuk melakukan penyerangan, penyerangan tersebut dapat dilihat pada gambar 8.



Gambar 8. Penyerangan ping of death pada Hping3

Dari gambar 8 dilihat penyerangan dilakukan sebanyak 5x dengan membuka root terminal pada kali linux dan memasukan perintah diterminal penyerangan dilakukan pada jam 01 : 12 WITA dan web target down pada waktu 02 : 59,

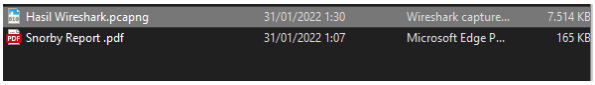
4.C. Forensik NIST (National Institute of Standars Technology)

Pada pengumpulan bukti forensik akan dilakukan 4 tahapan pengumpulan, pengujian, analisa, laporan olah data bukti forensik menggunakan 2 *tools* yang pertama mengunakan *Software* snorby yang kedua menggunakan *software* wireshark.

A. Pengumpulan (*Collection*).

Dalam tahapan pengumpulan data yang akan dijadikan bukti forensik pada lalu lintas jaringan,

terdapat 2 data yang didapatkan dari snorby dan wireshark hasil data tersebut di simpan dalam format .pcapng , .pdf bisa dilihat pada gambar 9.



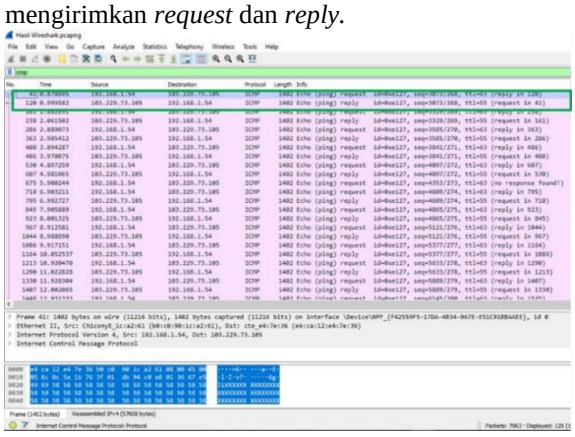
Gambar 9. Hasil Bukti Serangan Snorby & Wireshark

Gambar 9 menampilkan hasil tangkapan dengan nama (Hasil Wireshark) yang di lakukan pada tanggal dan bulan 31 Januari 2022 dengan file type pcapng yang didapat dari wireshark dan hasil capture dengan nama snorby report pada tanggal dan bulan yang sama, file type pdf didapatkan daei snorby.

B. Pengujian (*Examination*)

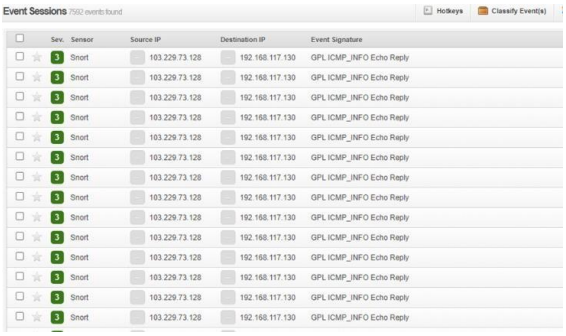
Tahapan pengujian atau pemeriksaan ini dilakukan untuk mengetahui atau mengidentifikasi serangan *ping of death* pada web target dengan *ip address* 103.229.73.105 menggunakan 2 *tools* wireshark dan snorby.

Hal pertama yang dilakukan adalah melakukan olah data pada file Hasil Wireshark.pcapng yang telah didapatkan pada saat tahap pengumpulan data. Data yang dicari disini adalah data yang berprotocol ICMP pada wireshark dapat dilihat pada gambar 10. Dari gambar 10 dan nomor 120 bisa dilihat bahwa terjadi serangan pada *ip address* 103.229.73.105 dimana *ip address* tersebut merupakan *ip address* dari Cakrawalaide.com dengan protocol ICMP yang mengirimkan *request* dan *reply.*



Gambar 10. Hasil bukti Serangan Wireshark

Selanjutnya adalah melakukan pemeriksaan pada, *tools* Snorby yang didapatkan pada saat melakukan *scanning* jaringan hasil pemeriksaan snorby dapat dilihat pada gambar 11.



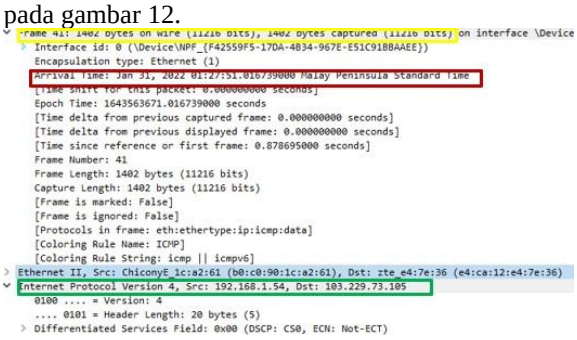
Gambar 11. Hasil Bukti Serangan snorby

Pada gambar 11 diatas dapat dilihat terjadi serangan ICMP pada *tools* snorby dengan keterangan ICMP_INFO *Echo reply* dengan ip addres yang sama 103.229.73.128.

C. Analisa (*Analysis*)

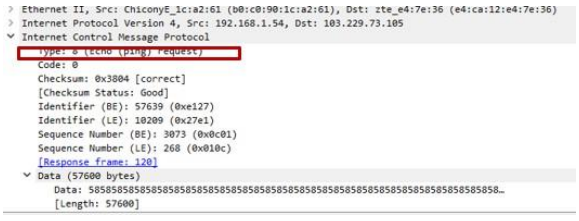
Setelah melakuan tahapan pengumpulan dan pemeriksaan serta ditemukanya serangan *ping of death* yang berprotocol ICMP maka akan dilakukan analisis pada penyerangan ICMP tersebut mulai dari *ip addresss* penyerang dan berapa banyak paket yang dikirim pada web target, untuk melakukan analisis ini akan digunakan *tools* wireshark dan snorby.

Hal pertama yang dilakukan adalah melakukan anlisis pada *tools* wireshak hasilnya dapat dilihat pada gambar 12.



Gambar 12. Hasil Analisa Pada Wireshark

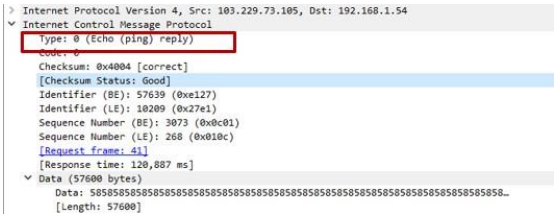
Dari hasil gambar 13 ditandai dengan warna merah bisa dilihat bahwa serangan terjadi pada Bulan Januari 31, 2022 pada jam 01:27, tanda warna kuning paket yang diterima 1402 byte atau 11216 bits dari sumber *ip address* 192.168.1.54 dengan tujuan yang tertuju pada *ip addresss* 103.229.73.105 yang ditandai dengan warna hijau.



Gambar 13. ICMP Request

Hasil analisis dari gambar 14 pada tanda diwarnai merah menjelaskan type pesan ICMP diatas adalah 8, bahwa type 8 adalah *echo request*,

yaitu pesan ketika meminta untuk menghubungkan ke *Ip address* korban.



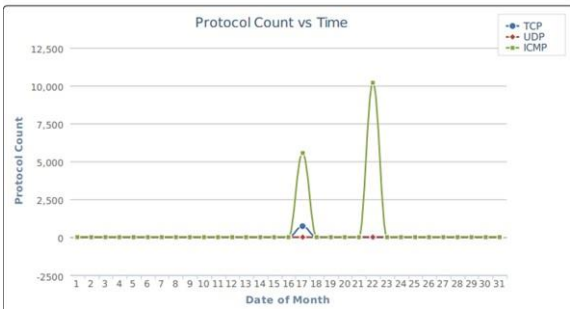
Gambar 14. ICMP Reply

Hasil analisis dari gambar 14 pada tanda diwarnai merah menjelaskan type pesan ICMP diatas adalah 0, bahwa type 0 adalah *echo reply*, yaitu menjawab pesan dari request Ping pada gambar 14 sehingga bisa menghubungkan ke *Ip address* korban.

Selanjutnya dengan menggunakan *tools* snorby dengan melihat file pada tahapan pengumpulan data snorby report.pdf pada saat melakukan scaning lalu lintas jaringan pada snorby, ada berapa hasil yang di dapatkan dalam melakukan analisis pada snorby.

Protocols

TCP Count	UDP Count	ICMP Count	Total
723	6	15749	16479



Gambar 15. Hasil Analisis Snorby Protocol Count

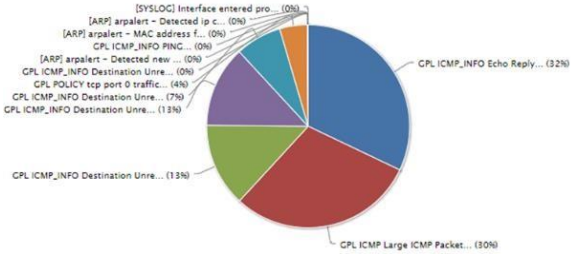
Kode hijau menandakan penyerangan bertipe ICMP dan terhitung 10.000 paket data yang dikirim Web server, penyerangan dilakukan sebanyak 15749 yang berhasil dikirim pada target.

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

Gambar 16. Hasil Analisis Snorby jenis Serangan

Ada 2 jenis serangan yang dilakukan yang pertama jenis serangan dengan ket ICMP_INFO *Echo reply* yang presentasi penyranganya 32.09% yang terhitung sebanyak 5288 kali serangan yang kedua ICMP_LARGE Packet dengan presentasi penyeraganya 29.76% yang terhitung sebanyak 4904 kali serangan.



Gambar 17. Hasil Snorby Diagram Report

Dari hasil gambar diatas bisa dilihat bahwa penyeranga ICMP yang berhasil dilakukan adalah 32% dan 30% sendangkan yang tidak berhasil sebanyak 7% dan 13%.

D. Pelaporan (*Reporting*)

Setelah melakukan 3 tahapan pengumpulan, pengujian dan anailisa yang sudah dilakukan, tahapan terakhir adalah membuat laporan data forensik yang sudah dianalisa pada penelitian ini dan akan dilihat pada tabel berikut

Tabel 3. Pelaporan Bukti Serangan

No.	Data	Ket	BuktiDigital
1	*Ip addresss penyerang*	Ya	Gambar 13
2	Penyaragan *Ping of death*	Ya	Gambar 11,16,17
3	Banyaknya *byte ping of death*	Ya	Gambar 16,14,15
4	Presentase Penyerangan *ping of death*	Ya	Gambar 17,18
5	Penyeragan *ping of death* yang gagal	Ya	Gambar 18

Dari hasil pelaporan diatas penulis mendapatkan hasil pelaporan penyeragan yang terjadi pada web cakrawalaide.com dengan *ip addresss* 103.229.73.105, didapatkan hasil penyerangan dari *Ip address* 192.168.1.54 dengan jenis serangan *ping of death* berprotokol ICMP paket yang diterima perpaket 1408 byte/ 1126 bit dan dilakukan penyerangan sebanyak sebanyak 15749 kali serangan yang dilakukan dengan presentase keterangan GCL_ICMP-INFO Echo Replay berhasil dilakukan 32% dan GCL_ICMP- LARGE ICMP Packet 30% dan gagal melakuka serangan ICMP 7% dan 13%.

5. KESIMPULAN

Berdasarkan hasil yang di peroleh uji coba maka penulis berkesimpulan, antara lain :

1. Metode NIST yang meliputi pengumpulan, pengujian, analisa, pelaporan dapat dipertahankan ataupu diulang, berdasarkan simulasi penyerangan yang dilakukan berhasil mendapatkan barang bukti digital baik dengan pengamatan secara tidak langsung dari tahapan

pemeriksaan meggunakan wireshark dan snorby.

2. Simulasi serangan DDoS *ping of death* berhasil dilakukan dengan bantuan *tools* Hping3 untuk exploit, Nmap untuk melakukan vulnareabilitiy pada web target dan berhasil membuat web server down.
3. Penelitian menghasilkan barang bukti dari implementasi tahapan-tahapan pada metode National Institute of Standards and Technology (NIST). Tahapan pertama adalah collection (pengumpulan data) file capture HasilWireshark.pcapng dan Snorby Report pada saat menggunakan Wireshark Dan Snorby

DAFTAR PUSTAKA

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