



## Analisis dan Implementasi *Honeyd Honeyd* Sebagai *Low Interaction* Terhadap Serangan *Distributed Denial Of Service (DDOS)* dan *Malware*

Ubaidillah <sup>1\*</sup>, Taswanda Taryo <sup>2</sup>, dan Achmad Hindasyah <sup>3</sup>

<sup>1</sup> Universitas Pamulang,, [ubaidillahaidar99@gmail.com](mailto:ubaidillahaidar99@gmail.com)

<sup>2</sup> Universitas Pamulang, [dosen02234@unpam.ac.id](mailto:dosen02234@unpam.ac.id)

<sup>3</sup> Universitas Pamulang, [ahindasyah@gmail.com](mailto:ahindasyah@gmail.com)

\* Korespondensi : [ubaidillahaidar99@gmail.com](mailto:ubaidillahaidar99@gmail.com)

**Sitasi:** Ubaidillah; Taryo, T; dan Hindasyah, A. (2023). Analisis dan Implementasi *Honeyd Honeyd* Sebagai *Low In-teraction* Terhadap Serangan *Distributed Denial Of Service (DDOS)* dan *Malware*. JTIM: Jurnal Teknologi Informasi Dan Multimedia, 5(3), 208-217. <https://doi.org/10.35746/jtim.v5i3.405>

Diterima: 7 September 2023

Direvisi: 3 Oktober 2023

Disetujui: 3 Oktober 2023

Dipublikasi: 8 Oktober 2023

**Abstract:** Every computer device connected to a wide computer network is vulnerable to security risks. These threats encompass vulnerabilities to data, information, resources, and services within the system. These threats include intrusion, eavesdropping, theft of vital data, as well as damage to the network system. These actions are carried out by parties who are not accountable, commonly referred to as intruders or attackers. One method to prevent or anticipate these malicious actions is by utilizing the *honeyd Honeyd* technique. The *honeyd Honeyd* adopts a low-interaction approach, which involves indirect interaction with attackers. This *Honeyd* serves as a decoy or simulated server intentionally presented as a target for attacks. The purpose of this *Honeyd* is to detect and analyze ongoing attacks. In this research, the *honeyd Honeyd* is implemented as a simulated server resembling an authentic server. This server provides various services and opens several ports deliberately prepared as attack targets, such as Port 139, and Port 21. The results of this research unveil the existence of attacks. Signs of these attacks include a surge in network traffic, reaching up to 100 Megabits above the normal level. Another indicator is a sudden spike in CPU usage, reaching 100%. The activities of these attacks can be analyzed through the installed Wireshark application on the *Honeyd* server. Information obtained from this analysis encompasses details about the attacker's activities, enabling more effective preventive, anticipatory, and corrective measures. These steps encompass securing the server, network system, and existing services.

**Keywords:** *Network Security, Honeyd, Honeyd, DDOS Attack, Malware*



**Copyright:** © 2023 oleh para penulis. Karya ini dilisensikan di bawah Creative Commons Attribution-ShareAlike 4.0 International License. (<https://creativecommons.org/licenses/by-sa/4.0/>).

**Abstrak:** Setiap perangkat komputer yang tersambung ke jaringan komputer secara luas rentan terhadap risiko keamanan. Ancaman tersebut meliputi kerentanan terhadap data, informasi, sumber daya, dan layanan yang terdapat dalam sistem. Ancaman-ancaman ini meliputi penyusupan, penyadapan, pencurian data penting, serta kerusakan pada sistem jaringan. Tindakan-tindakan ini dilakukan oleh pihak yang tidak bertanggung jawab, yang sering disebut sebagai intruder atau attacker. Salah satu cara untuk mencegah atau mengantisipasi tindakan buruk ini adalah dengan menggunakan metode *Honeyd honeyd*. *Honeyd honeyd* mengadopsi pendekatan *low-interaction*, yaitu berinteraksi secara tidak langsung dengan *attacker*. *Honeyd* ini berperan sebagai umpan atau *server* tiruan yang sengaja dihadirkan sebagai target serangan. Tujuan dari *Honeyd* ini adalah untuk mendeteksi serta menganalisis serangan yang terjadi. Dalam penelitian ini, *Honeyd honeyd* diimplementasikan sebagai *server* tiruan yang menyerupai *server* asli. *Server* ini menyediakan beberapa layanan dan membuka beberapa port yang sengaja disiapkan sebagai target serangan, seperti Port 139, dan Port 21. Pada penelitian ini, penulis melakukan pembatasan dalam lingkup penelitian yaitu, pengungkapan serangan yang dimaksud adalah serangan berbasis *Distributed Denial of Service (ddos)* dan *Malware*. Tanda-tanda serangan tersebut antara lain terlihat dari lonjakan

lalu lintas jaringan hingga mencapai 100 Megabita di atas tingkat normal. Indikator lainnya adalah peningkatan tiba-tiba pada penggunaan CPU hingga mencapai 100%. Aktivitas serangan ini dapat dianalisis melalui aplikasi *Wireshark* yang telah diinstal pada *server Honeypot*. Informasi yang diperoleh dari analisis ini mencakup detail mengenai aktivitas yang dilakukan oleh *attacker*, sehingga tindakan pencegahan, antisipasi, dan perbaikan dapat dilakukan dengan lebih efektif. Langkah-langkah ini mencakup pengamanan pada *server*, sistem jaringan, dan layanan yang ada."

**Kata kunci :** Keamanan Jaringan, *Honeypot*, *Honeyd*, Serangan DDOS, *Malware*

## 1. Pendahuluan

Serangan *Denial Distributed Of Service* (DDOS) bertujuan untuk membuat layanan jaringan menjadi tidak tersedia bagi pengguna yang sah dengan cara membanjiri sumber daya jaringan dengan lalu lintas palsu[1]. Serangan ini dapat menyebabkan kegagalan sistem, penurunan kinerja, dan kerugian finansial yang signifikan bagi organisasi yang menjadi target. Sementara itu, *malware* merujuk pada perangkat lunak berbahaya yang dirancang untuk merusak, mengganggu, atau mencuri informasi dari sistem komputer[2]. *Malware* dapat memasuki jaringan melalui berbagai metode, seperti email berbahaya, unduhan tidak aman, atau celah keamanan dalam sistem[3]. Untuk melindungi jaringan dari serangan-serangan tersebut, diperlukan strategi keamanan yang efektif. Salah satu pendekatan yang dapat digunakan adalah menggunakan teknologi *Honeypot*[4]. *Honeypot* adalah sistem yang dibuat untuk menarik perhatian penyerang dan menyediakan lingkungan yang terisolasi dan terkendali untuk mempelajari serangan mereka[5]. Dalam konteks ini, *Honeypot* akan diimplementasikan menggunakan perangkat lunak *Honeyd* sebagai metode low interaction[6].

*Honeypot* sebagai sebuah cara yang praktis untuk melindungi asset dari serangan dan penyalahgunaan, serta Teknik data mining menjadi Langkah yang tepat untuk memprediksi dan mengetahui vulnerability kerentanan terhadap arus anomaly yang mencurigakan di dalam traffic lalu lintas jaringan[7]. *Honeypot* dapat mengalihkan penyerang dengan seolah-olah menjadi server asli sehingga dapat menjadi tempat untuk berinteraksi sementara bagi penyerang yang ingin melakukan serangan ke layanan server atau jaringan[8].

*Honeypot low interaction* menggunakan sistem operasi emulasi yang terpasang pada *Honeypot* ketika berinteraksi dengan penyerang[9]. *Honeypot low interaction* memiliki interaksi yang terbatas kepada penyerang[10]. Serangan yang dihadapi biasanya berupa port scanning dan juga digital signature attack[11]. Interaksi pada *Honeypot low interaction* dengan host lain terbatas sehingga kemampuan yang dimiliki terbatas dan penyerang dapat dengan mudah mengenalinya tetapi dibalik terbatasnya *Honeypot low interaction*, memiliki resiko yang rendah[12].

Pada penelitian yang dilakukan [13] dikatakan bahwa *Honeypot honeyd* sebagai solusi keamanan jaringan dan aktivitas serangan pada pengujian serangan berbasis *Internet Control Message Protocol (ICMP)* dan *Scan attack* dengan membuka *port* yang sudah dibuka dan dikonfigurasi sebelumnya, sehingga aktivitas serangan bisa diketahui dan dianalisa.

## 2. Bahan dan Metode

### 2.1. Honeypot

*Honeypot* merupakan sistem tiruan yang dibuat untuk menirukan keaslian layanan layaknya seperti server yang sebenarnya sehingga dapat mengelabui *attacker* yang mencoba menyerang. *Honeypot* merupakan alternatif pengamanan server yang gratis karena tool ini dapat diberdayakan tanpa dipungut biaya[14].

### 2.2. Honeyd

*Honeyd* merupakan suatu program komputer yang bersifat *open source*. cara kerja *honeyd* memungkinkan pengguna untuk membuat dan menjalankan beberapa *virtual host*

dalam jaringan komputer. Dari *virtual host* tersebut pengguna dapat mensimulasikan suatu konfigurasi jaringan komputer untuk meniru beberapa jenis *server*[15].

2.3. Kebutuhan Perangkat Keras

Untuk melangsungkan proses penelitian ini maka perangkat keras dan perangkat lunak harus memenuhi beberapa persyaratan minimum. Komputer yang digunakan dalam analisis dan implementasi *Honeypot honeyd* sebagai *low interaction* terhadap serangan *distributed denial of services* (ddos) dan *malware*, memiliki spesifikasi yang dapat dilihat pada Tabel 1.

Tabel 1. Daftar kebutuhan *hardware*

Nama Perangkat	Spesifikasi	Fungsi
HP Server Prolliant	Processor: GenuineIntel Common KVM processor dual core RAM: 2048 MB	Sebagai <i>Server</i> yang akan diinstalasi dua operating system yaitu (Linux ubuntu server dan Kali Linux) Dalam satu Virtual mesin/VMware

2.4. Kebutuhan Perangkat Lunak

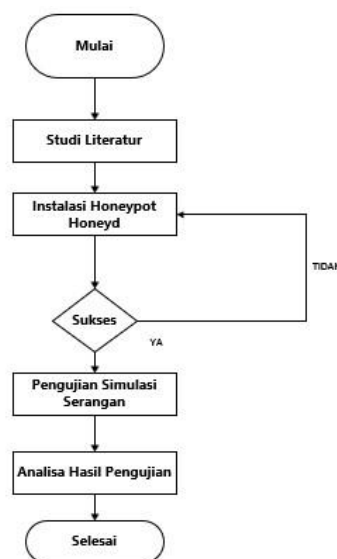
Tabel 2. Daftar Kebutuhan Perangkat Lunak

Perangkat Lunak	Keterangan
OS Ubuntu Server 14.04	Sebagai sistem operasi <i>server Honeyd honeyd</i>
OS Kali Linux 2023.2	Sebagai sistem operasi <i>attacker</i>
Nmap	<i>Tools</i> yang digunakan sebagai sistem port scannig
LOIC	<i>Tools</i> yang digunakan untuk melakukan penyerangan
Wireshark	<i>Tools</i> digunakan untuk monitoring traffic jaringan
Vmware	<i>Software Virtual mesin untuk menjalankan OS secara virtual</i>

2.5. Metode Penelitian

Penelitian ini dalam simulasinya pengimplementasian *Honeypot honeyd* dalam sebuah *virtual mesin* (*Vmware workstation*). Di mana pada rancangan ini ada dua buah *pc* dalam *virtual mesin* yaitu *pc server* yang sudah terinstal *honeyd* dan *pc attacker* yang akan melakukan penyerangan terhadap *pc server*.

2.6. Tahapan penelitian



Gambar 1. Tahapan penelitian

Gambar 1. Tahapan Penelitian adalah gambaran mengenai Langkah-langkah dalam menyelesaikan penelitian. Penjelasan tahapan penelitian :

- Studi literatur
 

Studi literatur merupakan tahap di mana peneliti melakukan pembelajaran dari buku, jurnal, artikel ataupun referensi baik itu dari *online* maupun *offline*, yang berhubungan dengan penelitian tersebut
- Instalasi dan konfigurasi *Honeypot honeyd*

Merupakan tahapan instalasi dan konfigurasi *Honeypot honeyd* ke dalam sistem operasi *Server Linux Ubuntu* berbasis desktop dan membuka beberapa port service diantaranya : *Port 139* dan *Port 21*.
- Pengujian simulasi serangan
 

Merupakan tahapan simulasi penyerangan *Honeypot server* dengan serangan *Distributed Denial Of Service (Ddos)* menggunakan Tools *Loic*, *Nmap* dan Mengirimkan file *malware* kedalam *server* menggunakan *File Transfer Protocol (FTP)*.
- Analisa hasil pengujian
 

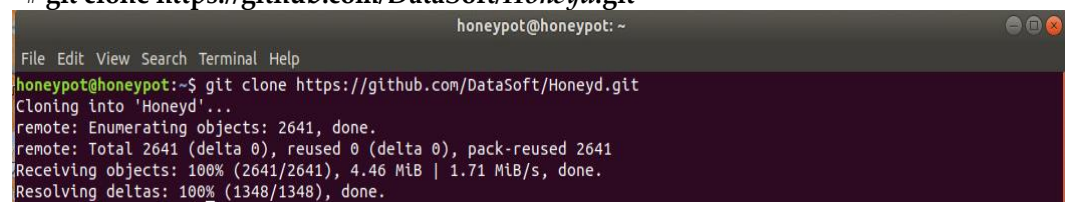
Merupakan tahapan di mana melihat seberapa efektifkah serangan yang sudah dilakukan oleh *attacker* dalam menyerang *server* yang sudah dipersiapkan dan informasi apa saja yang bisa diambil dari serangan tersebut.

### 3. Hasil

#### 3.1. Instalasi *honeyd*

Tahap awal instalasi *honeyd* yaitu melakukan proses penyalinan file *honeyd* ke dalam server *Honeypot* dengan mengetikkan format / perintah :

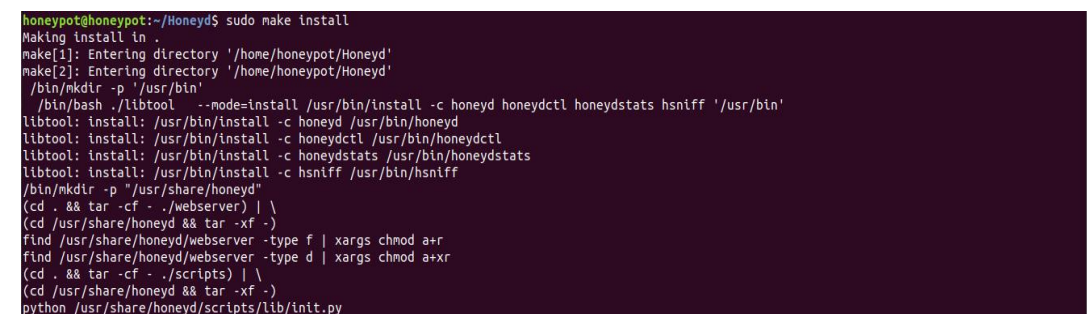
```
# git clone https://github.com/DataSoft/Honeyd.git
```



```
honeypot@honeypot: ~
File Edit View Search Terminal Help
honeypot@honeypot:~$ git clone https://github.com/DataSoft/Honeyd.git
Cloning into 'Honeyd'...
remote: Enumerating objects: 2641, done.
remote: Total 2641 (delta 0), reused 0 (delta 0), pack-reused 2641
Receiving objects: 100% (2641/2641), 4.46 MiB | 1.71 MiB/s, done.
Resolving deltas: 100% (1348/1348), done.
```

Gambar 2. Proses Penyalinan File *honeyd*

Setelah proses penyalinan berhasil maka selanjutnya melakukan instalasi *honeyd* pada server *Honeypot* dengan perintah/format pada terminal linux **#sudo make install**



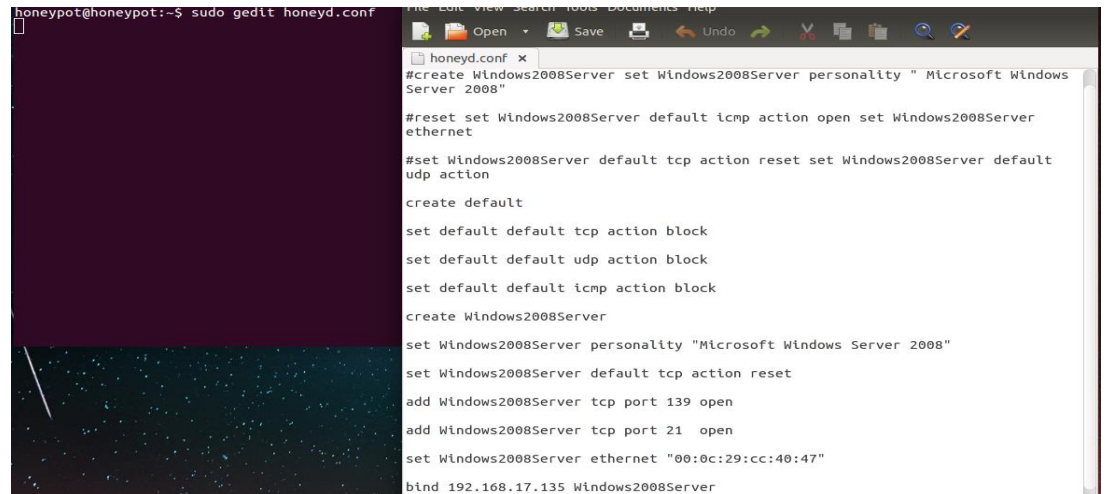
```
honeypot@honeypot:~/Honeyd$ sudo make install
Making install in .
make[1]: Entering directory '/home/honeypot/Honeyd'
make[2]: Entering directory '/home/honeypot/Honeyd'
/bin/mkdir -p '/usr/bin'
/bin/bash ./libtool --mode=install /usr/bin/install -c honeyd honeydctl honeydstats hsniff '/usr/bin'
libtool: install: /usr/bin/install -c honeyd /usr/bin/honeyd
libtool: install: /usr/bin/install -c honeydctl /usr/bin/honeydctl
libtool: install: /usr/bin/install -c honeydstats /usr/bin/honeydstats
libtool: install: /usr/bin/install -c hsniff /usr/bin/hsniff
/bin/mkdir -p "/usr/share/honeyd"
(cd . && tar -cf - ./webserver) | \
(cd /usr/share/honeyd && tar -xf -)
find /usr/share/honeyd/webserver -type f | xargs chmod a+r
find /usr/share/honeyd/webserver -type d | xargs chmod a+rx
(cd . && tar -cf - ./scripts) | \
(cd /usr/share/honeyd && tar -xf -)
python /usr/share/honeyd/scripts/lib/init.py
```

Gambar 3. Hasil instalasi *honeyd*

#### 3.2. Konfigurasi *Honeyd*

Konfigurasi pada *honeyd* memiliki tujuan untuk mendefinisikan berbagai elemen penting. Pertama-tama, terdapat konsep '*personality*'. Konsep ini mengacu pada pengaturan di mana saat perangkat lain terhubung dengan *Honeypot*, *Honeypot* tersebut akan berpura-pura menjadi sistem operasi Windows Server 2008. Dalam template Windows ini, tiga port akan dibuka, yakni 139 dan 21. Port-port ini biasanya digunakan dalam sistem operasi Windows. Tindakan '*action reset*' bertujuan untuk menghentikan lalu lintas yang tidak terkait dengan port yang telah didefinisikan sebagai port terbuka dalam file

konfigurasi. Pengaturan *'set windows ethernet'* digunakan untuk menentukan alamat MAC untuk *Honeypot*. Fitur ini berguna ketika *Honeypot* dijalankan dengan *Static IP*. Dalam konteks penelitian ini, *Honeypot* memegang peran penting sebagai alat utama dalam membangun sistem keamanan jaringan. *Honeypot* dipilih karena mampu mengalihkan serangan yang semula ditujukan ke server utama ke server palsu yang telah dibuat sendiri sesuai dengan konfigurasi *Honeypot*. File *honeyd.conf* merupakan konfigurasi yang diperlukan untuk menciptakan server palsu, sehingga serangan yang seharusnya mengarah ke server utama dapat dialihkan dengan efektif.



```
honeyd@honeypot:~$ sudo gedit honeyd.conf
#create Windows2008Server set Windows2008Server personality " Microsoft Windows
Server 2008"

#reset set Windows2008Server default icmp action open set Windows2008Server
ethernet

#set Windows2008Server default tcp action reset set Windows2008Server default
udp action

create default
set default default tcp action block
set default default udp action block
set default default icmp action block

create Windows2008Server
set Windows2008Server personality "Microsoft Windows Server 2008"
set Windows2008Server default tcp action reset
add Windows2008Server tcp port 139 open
add Windows2008Server tcp port 21 open
set Windows2008Server ethernet "00:0c:29:cc:40:47"

bind 192.168.17.135 Windows2008Server
```

Gambar 4. Konfigurasi *honeyd*

## 4. Pembahasan

### 4.1. Scanning Port Menggunakan Nmap



```
root@kali: ~
File Actions Edit View Help
(root@kali)-[~]
└─# nmap -p 139,21 192.168.17.135
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-28 23:24 EDT
Nmap scan report for 192.168.17.135
Host is up (0.00058s latency).

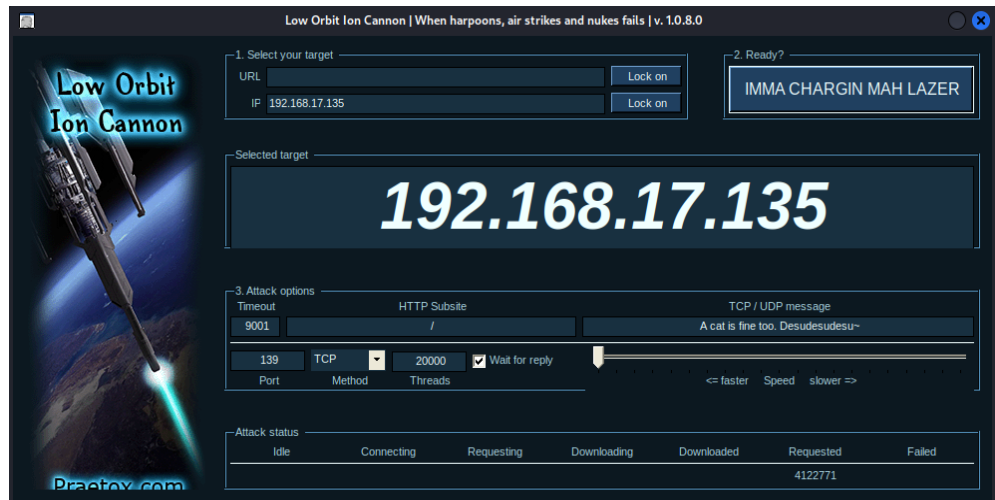
PORT      STATE SERVICE
21/tcp    open  ftp
139/tcp   open  netbios-ssn
MAC Address: 00:0C:29:CC:40:47 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 13.30 seconds
(root@kali)-[~]
```

Gambar 5. Scanning Port Menggunakan Nmap

Pada Gambar 5. Merupakan proses *scanning port* dari pc *attacker* terhadap pc *server* (*Honeypot*) dengan menggunakan *tools nmap* dan dari hasil *scanning* tersebut dapat terlihat ada dua port yang terbuka yaitu *port 21* dan *139* yang akan dijadikan target penyerangan *Distributed denial of service (Ddos)* pada *port 139* dan juga serangan pengiriman *malware* melalui *file transfer protocol (Ftp)* pada *port 21*.

4.2. Serangan Distributed denial of service (ddos) dengan tools Loic

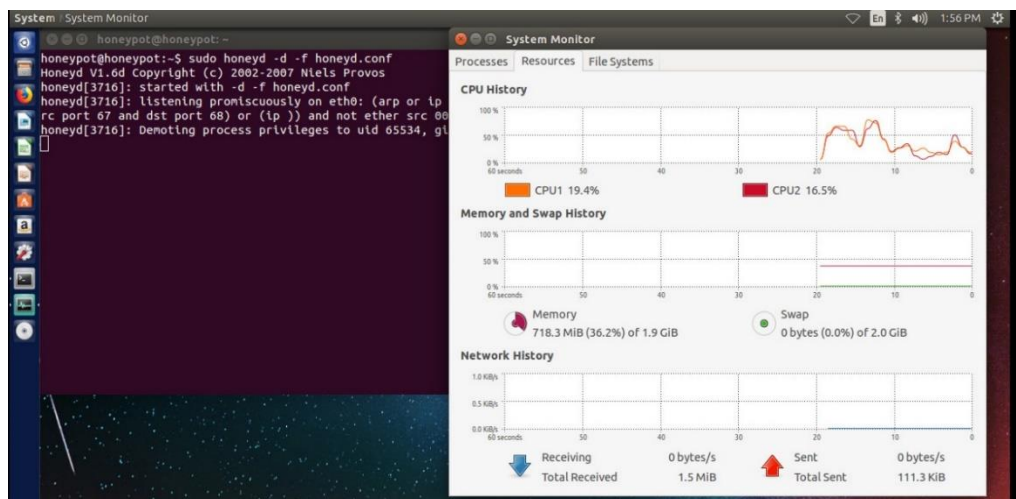


Gambar 6. Serangan Distributed Denial of Services (DDOS) dengan tools Loic

Gambar 6. Merupakan serangan dengan menggunakan tools LOIC (*Low Orbit Ion cannon*) di mana ip address tujuan / ip address server adalah 192.168.17.135, Port 139(*Transmission Control Protocol/TCP*), timeout 9001 dan threads 20000. Kemudian lakukan serangan dengan menekan tombol “*IMMA CHARGIN MAH LAZER*”.

4.3. Hasil serangan Distributed Denial of Services (ddos)

Hasil serangan yang dilakukan oleh *attacker* terhadap pc server *Honeypot honeyd* yang dituju dengan ip address 192.168.17.135 membuat kinerja server menjadi lambat dikarenakan meningkatnya kinerja cpu hingga 99 % dan meningkatnya *traffic* penggunaan bandwidth hingga 646.5 Mib (*Mega byte*) pada saat terjadinya serangan. Adapun perbedaan kondisi *server* sebelum dan sesudah diserang ,bisa dilihat pada Gambar 7 dan 8 dibawah ini.



Gambar 7. Kondisi Server Honeypot honeyd dalam keadaan normal





**Gambar 8.** Kondisi server *Honeypot honeyd* pada saat terjadinya serangan

#### 4.4. Serangan pengiriman malware pada port 21 dengan File transfer Protocol (Ftp)

Pada tahapan ini adalah melakukan serangan dengan mengirimkan *malware* dari pc attacker ke pc server *Honeypot honeyd* (pc target) melalui port 21 dan pengirimannya menggunakan File Transfer Protocol (FTP). Sebelumnya pada gambar 5. Sudah dilakukan scanning port dan terdapat keterangan status port 21 Open.

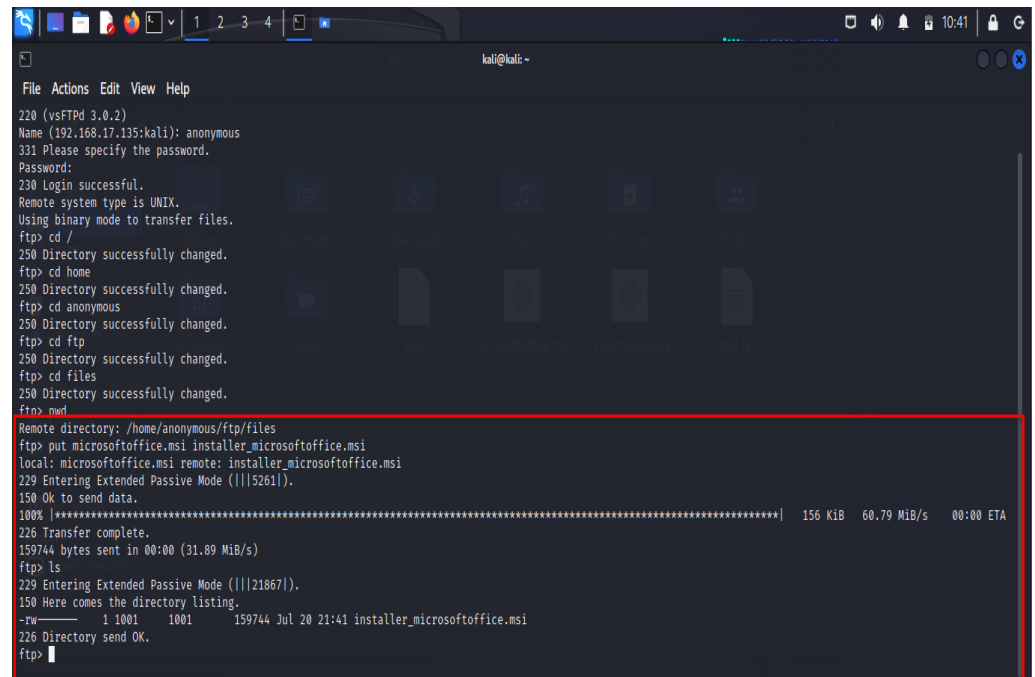
```

root@kali: ~
File Actions Edit View Help
root@kali ~
# ftp 192.168.17.135
Connected to 192.168.17.135.
220 (vsFTPD 3.0.2)
Name (192.168.17.135:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>

```

**Gambar 9.** Attacker melakukan login ke pc server *Honeypot honeyd*

Gambar 9. di mana attacker melakukan login ke pc server *Honeypot honeyd* dengan perintah `#ftp 192.168.17.135` (Ip address server *Honeypot honeyd*) dengan menggunakan user anonymous dan blank password. Pada kondisi ini attacker berhasil login sebagaimana yang terlihat pada gambar 9 dan attacker sudah bisa mengirimkan file *malware* ke pc server *Honeypot honeyd* menggunakan File Transfer Protocol (FTP).

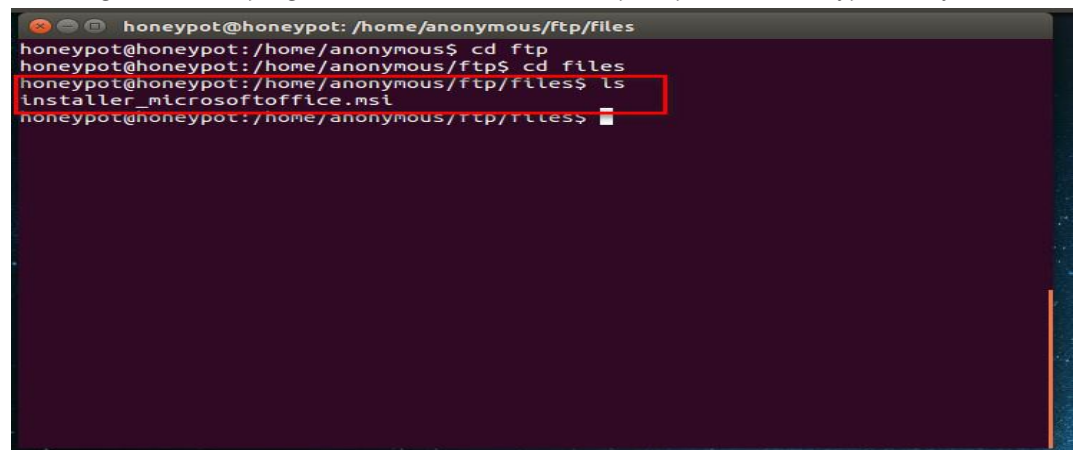


```
File Actions Edit View Help
220 (vsFTPd 3.0.2)
Name (192.168.17.135:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> cd /
250 Directory successfully changed.
ftp> cd home
250 Directory successfully changed.
ftp> cd anonymous
250 Directory successfully changed.
ftp> cd ftp
250 Directory successfully changed.
ftp> cd files
250 Directory successfully changed.
ftp> mwd
Remote directory: /home/anonymous/ftp/files
ftp> put microsoftoffice.msi installer_microsoftoffice.msi
local: microsoftoffice.msi remote: installer_microsoftoffice.msi
229 Entering Extended Passive Mode (|||S261|).
150 Ok to send data.
100% |*****| 156 KiB 60.79 MiB/s 00:00 ETA
226 Transfer complete.
159744 bytes sent in 00:00 (31.89 MiB/s)
ftp> ls
229 Entering Extended Passive Mode (|||21867|).
150 Here comes the directory listing.
-rw-rw-r-- 1 1001 1001 159744 Jul 20 21:41 installer_microsoftoffice.msi
226 Directory send OK.
ftp> |
```

**Gambar 10.** Pengiriman file malware ke pc server Honeypot honeyd

Pada Gambar 10 merupakan proses pengiriman file *malware* dari attacker ke pc server *Honeypot honeyd* dengan menggunakan file transfer protocol (ftp) pada port 21 dan bisa terlihat pada gambar di mana attacker mengirimkan file *malware* pada directory `/home/anonymous/ftp/files` dengan menggunakan perintah `"put microsoftoffice.msi installer_microsoft office.msi"`. pada proses ini attacker berhasil mengirimkn file *malware* ke pc server *Honeypot honeyd* dengan menggunakan file transfer protocol (ftp).

#### 4.5. Pengecekan hasil pengiriman malware dari attacker pada pc server Honeypot honeyd



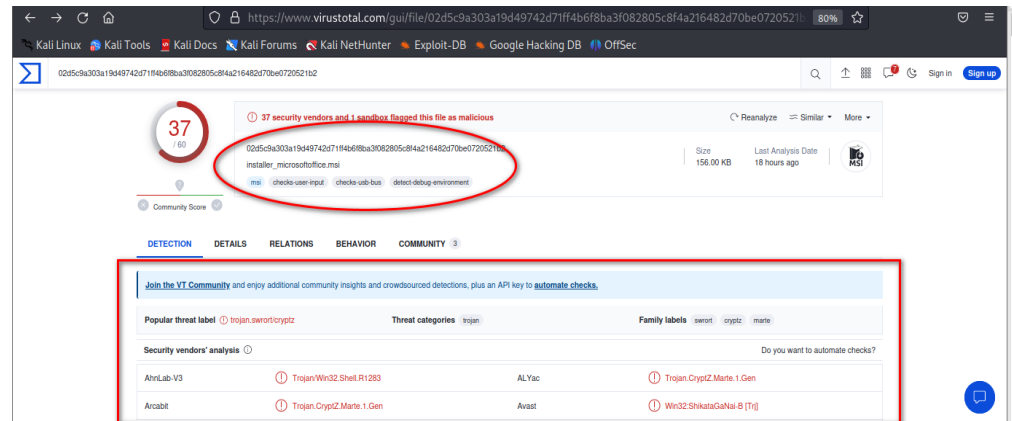
```
honeypot@honeypot: /home/anonymous/ftp/files
honeypot@honeypot:/home/anonymous$ cd ftp
honeypot@honeypot:/home/anonymous/ftp$ cd files
honeypot@honeypot:/home/anonymous/ftp/files$ ls
installer_microsoftoffice.msi
honeypot@honeypot:/home/anonymous/ftp/files$
```

**Gambar 11.** Pengecekan hasil pengiriman malware pada pc server Honeypot honeyd

Gambar 11. Merupakan pengecekan pada sisi pc server *Honeypot honeyd* di mana pada tahapan sebelumnya attacker berhasil mengirimkan files *malware* ke pc server *Honeypot honeyd* dan letak *malware* yang dikirimkan oleh attacker ada pada directory `/home/anonymous/ftp/files` dan file *malware* Bernama `installer_microsoftoffice.msi`.



#### 4.6. Pengecekan jenis malware pada situs virustotal.com



**Gambar 11.** Pengecekan file malware pada situs virustotal.com

Pada Gambar 11. Merupakan tahapan pengecekan file malware yang dikirimkan attacker di situs/website virustotal.com untuk mengetahui jenis malware yang dikirimkan oleh attacker. diketahui hasilnya bahwa file malware yang dikirimkan oleh attacker merupakan jenis "trojan.swort/cryptz", "Trojan/Win32.Shell.R1283", "Trojan.Cryptz.Marte.1.Gen", "Trojan.CryptZ.Marte.1.Gen", "Win32.ShikataGaNai-B". virus / malware ini merupakan kategori malware yang mengumpulkan informasi pribadi dan mengirimkannya ke penyerang kemudian Mengunduh dan menginstal malware tambahan dari server yang dikendalikan oleh penyerang.

#### 5. Kesimpulan

Dari penelitian berupa Analisa dan implementasi *Honeypot honeyd* sebagai *low interaction* maka dapat ditarik kesimpulan sebagai berikut :

- Implementasi *Honeypot honeyd* dapat membantu meningkatkan keamanan pada server dan dapat membantu administrator dalam menganalisa, melakukan Tindakan pencegahan hingga membuat kebijakan terhadap penggunaan jaringan internet.
- Serangan *DDoS (Distributed Denial of Service)* ini merupakan serangan yang berbahaya yang dapat merugikan orang lain untuk itu apapun alasannya serangan *DDoS* ini tidak boleh dilakukan untuk merugikan orang lain atau mengganggu kenyamanan orang lain dalam menggunakan internet.
- Tools LOIC* telah berhasil melakukan serangan *DDoS (Distributed Denial Of Service)* ke Ip target yang telah ditentukan dengan bukti meningkatnya *CPU history* pada server *Honeypot honeyd* dan *traffic bandwidth* yang meningkat.

#### Referensi

- [1] K. Elviani, "ANALISA DAN IMPLEMENTASI HONEYPOT HONEYD PADA JARINGAN WIRELESS DI FAKULTAS TEKNIK UNIVERSITAS ISLAM KUANTAN SINGINGI," vol. 4, no. February, p. 6, 2021.
- [2] R. Hildha Hassan and S. Juli Irzal Ismail, "Implementasi Honeypot Dengan Metode Honeytrap," e-Proceeding Appl. Sci., vol. 6, no. 2, p. 1960, 2020.
- [3] V. A. Manoppo, A. S. . Lumenta, and S. D. . Karouw, "Analisa Malware Menggunakan Metode Dynamic Analysis Pada Jaringan Universitas Sam Ratulangi," J. Tek. Elektro Dan Komput., vol. 9, no. 3, pp. 181–188, 2020.
- [4] N. Bhagat and B. Arora, "Intrusion detection using Honeypots," PDGC 2018 - 2018 5th Int. Conf. Parallel, Distrib. Grid Comput., pp. 412–417, 2018, doi: 10.1109/PDGC.2018.8745761.
- [5] D. K. NURILAH, R. MUNADI, S. SYAHRIAL, and A. BAHRI, "Penerapan Metode Naïve Bayes pada Honeypot Dionaea dalam Mendeteksi Serangan Port Scanning," ELKOMIKA J. Tek. Energi Elektr. Tek. Telekomun. Tek. Elektron., vol. 10, no. 2, p. 309, 2022, doi: 10.26760/elkomika.v10i2.309.
- [6] W. A. Sulaksono and C. E. Suharyanto, "Implementasi Honeypot Sebagai Sistem Keamanan Jaringan Pada Virtual Private Server," InfoTekJar J. Nas. Inform. dan Teknol. Jar., vol. 5, no. 1, pp. 90–95, 2020.

- 
- [7] A. Z. Mardiansyah, Y. M. Abdussyakur, and A. H. Jatmika, "OPTIMASI PORT KNOCKING DAN HONEYPOT MENGGUNAKAN IPTABLES SEBAGAI KEAMANAN JARINGAN PADA SERVER (Port Knocking and Honeypot Optimization using IPTables for Servers Network Security)," vol. 3, no. 2, 2021, [Online]. Available: <http://jtika.if.unram.ac.id/index.php/JTIKA/>
- [8] D. P. Agustino, Y. Priyoatmojo, and N. W. W. Safitri, "Implementasi Honeypot Sebagai Pendeteksi Serangan dan Melindungi Layanan Cloud Computing," *Konf. Nas. Sist. Inform.* 2017, pp. 196–201, 2017.
- [9] I. A. Romadhan, S. Syaifudin, and D. R. Akbi, "Implementasi Multiple Honeypot pada Raspberry Pi dan Visualisasi Log Honeypot Menggunakan ELK Stack," *J. Repos.*, vol. 2, no. 4, pp. 475–484, 2020, doi: 10.22219/repositor.v2i4.114.
- [10] A. Akhriana and A. Irmayana, "Web App Pendeteksi Jenis Serangan Jaringan Komputer Dengan Memanfaatkan Snort Dan Log Honeypot," *CCIT J.*, vol. 12, no. 1, pp. 85–96, 2019, doi: 10.33050/ccit.v12i1.604.
- [11] J. K. Barends, F. Dewanta, N. Bogi, and A. Karna, "Perancangan dan Analisis Intrusion Prevention Sistem Berbasis SNORT dan IPTABLES dengan Integrasi Honeypot pada Arsitektur Software Defined Network," vol. 7, no. 2, p. 163, 2021.
- [12] N. Arkaan and D. V. S. Y. Sakti, "Implementasi Low Interaction Honeypot Untuk Analisa Serangan Pada Protokol SSH," *J. Nas. Teknol. dan Sist. Inf.*, vol. 5, no. 2, pp. 112–120, 2019, doi: 10.25077/teknosi.v5i2.2019.112-120.
- [13] N. Fitriana and F. N. Khasanah, "Honeypot Menggunakan Honeyd Sebagai Solusi Keamanan Jaringan Dari Aktivitas Serangan," *Bina Insa. Ict J.*, vol. 5, no. 2, pp. 143–152, 2018.
- [14] R. Fauzi, Y. Muhyidin, and D. Singasatia, "Sistem Keamanan Jaringan Komputer Berbasis Teknik Intrusion Detection System (IDS) Untuk Mendeteksi Serangan Distributed Denial Of Service (DDOS)," vol. 7, pp. 72–86, 2023.
- [15] A. Aminanto and W. Sulistyono, "Simulasi Sistem Keamanan Jaringan Komputer Berbasis IPS Snort dan Honeypot Artilery," *Aiti*, vol. 16, no. 2, pp. 135–150, 2020, doi: 10.24246/aiti.v16i2.135-150.