

# **LAPORAN ADVANCE NETWORK SECURITY AND PROTOCOLS**

Implementasi Honeypot Cowrie untuk Deteksi Pola Penyerangan  
Double Attack



**DISUSUN OLEH**

**KELOMPOK 3**

**NAMA**

**NIM**

**NUR ALIYAH AMALIANI**

**105841106923**

**SUKMA WARDIA NINGSIH**

**105841112723**

**PROGRAM STUDI INFORMATIKA**

**FAKULTAS TEKNIK**

**UNIVERSITAS MUHAMMADIYAH MAKASSAR**

**2026**

## 1. Pendahuluan

Pada praktikum ini dilakukan implementasi honeypot Cowrie sebagai sistem deteksi dini terhadap serangan jaringan, khususnya serangan dengan pola penyerangan ganda (*Double Attack*). Honeypot Cowrie dipilih karena mampu mensimulasikan layanan SSH palsu dan mencatat aktivitas penyerang secara detail tanpa membahayakan sistem asli.

Pengujian difokuskan pada kombinasi serangan port scanning, brute force, dan DDoS, yang dijalankan secara bersamaan untuk melihat bagaimana sistem honeypot merespon aktivitas penyerang pada berbagai lapisan

## 2. Lingkungan dan topologi pengujian

pengujian dilakukan menggunakan dua mesin virtual dengan peran yang berbeda, yaitu:

### a. Mesin penyerang (attacker)

Sistem Operasi : Kali linux

Digunakan untuk melakukan simulasi serangan

### b. Mesin Target

Sistem Operasi : Ubuntu Server

Digunakan sebagai server yang menjalankan honeypot Cowrie.

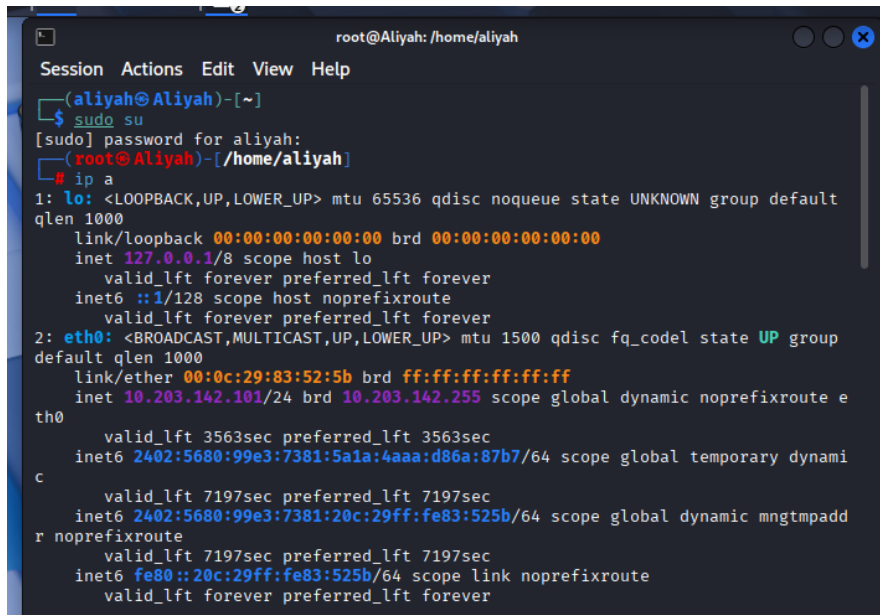
Kedua mesin dikonfigurasi berada dalam satu jaringan agar dapat saling berkomunikasi secara langsung. Konfigurasi jaringan dilakukan dengan menyamakan mode network adapter pada kedua mesin Virtual.

## 3. Konfigurasi Jaringan Awal

### a. Pengecekan IP Address pada Ubuntu Server

```
(cowrie-env) sukma@ubuntu:~/cowrie$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:16:75:6b brd ff:ff:ff:ff:ff:ff
    inet 10.203.142.37/24 metric 100 brd 10.203.142.255 scope global dynamic enp0s3
        valid_lft 3241sec preferred_lft 3241sec
    inet6 2402:5680:99e3:7381:a00:27ff:fe16:756b/64 scope global dynamic mngtmpaddr noprefixroute
        valid_lft 6844sec preferred_lft 6844sec
    inet6 fe80::a00:27ff:fe16:756b/64 scope link
        valid_lft forever preferred_lft forever
```

b. Pengecekan IP Address pada Kali Linux

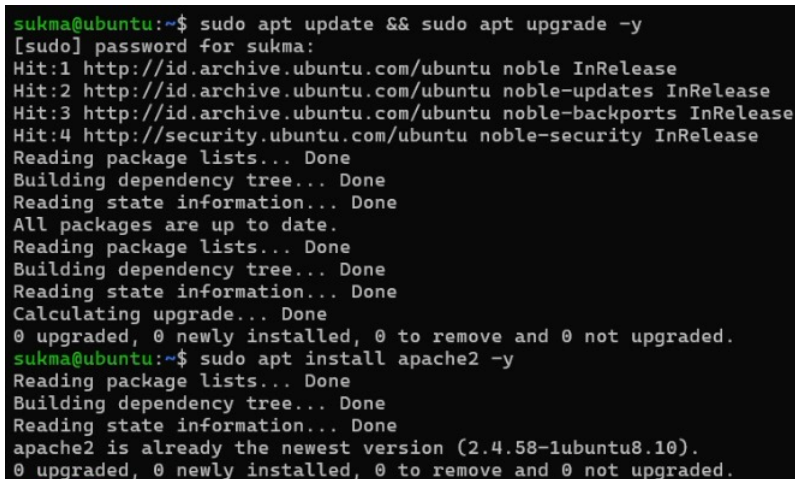


```
root@Aliyah: /home/aliyah
Session Actions Edit View Help
(aliyah@Aliyah)~
$ sudo su
[sudo] password for aliyah:
(aliyah@Aliyah)~
# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:83:52:5b brd ff:ff:ff:ff:ff:ff
    inet 10.203.142.101/24 brd 10.203.142.255 scope global dynamic noprefixroute eth0
        valid_lft 3563sec preferred_lft 3563sec
    inet6 2402:5680:99e3:7381:5a1a:4aaa:d86a:87b7/64 scope global temporary dynamic
    inet6 2402:5680:99e3:7381:20c:29ff:fe83:525b/64 scope global dynamic mngtmpaddr noprefixroute
        valid_lft 7197sec preferred_lft 7197sec
    inet6 fe80::20c:29ff:fe83:525b/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

Langkah ini bertujuan untuk memastikan bahwa kedua mesin berada dalam satu subnet jaringan. Apabila mesin tidak berada dalam satu subnet, proses pengujian seperti port scanning dan serangan jaringan tidak dapat dilakukan

## 4. Persiapan Awal Ubuntu Server

### 4.1 Update Sistem



```
sukma@ubuntu:~$ sudo apt update && sudo apt upgrade -y
[sudo] password for sukma:
Hit:1 http://id.archive.ubuntu.com/ubuntu noble InRelease
Hit:2 http://id.archive.ubuntu.com/ubuntu noble-updates InRelease
Hit:3 http://id.archive.ubuntu.com/ubuntu noble-backports InRelease
Hit:4 http://security.ubuntu.com/ubuntu noble-security InRelease
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
All packages are up to date.
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Calculating upgrade... Done
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
sukma@ubuntu:~$ sudo apt install apache2 -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
apache2 is already the newest version (2.4.58-1ubuntu8.10).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
```

```

0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
sukma@ubuntu:~$ sudo apt update
sudo apt install git python3-venv python3-pip net-tools -y
Hit:1 http://id.archive.ubuntu.com/ubuntu noble InRelease
Hit:2 http://id.archive.ubuntu.com/ubuntu noble-updates InRelease
Hit:3 http://id.archive.ubuntu.com/ubuntu noble-backports InRelease
Hit:4 http://security.ubuntu.com/ubuntu noble-security InRelease
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
All packages are up to date.
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
git is already the newest version (1:2.43.0-1ubuntu7.3).
git set to manually installed.
The following additional packages will be installed:
  binutils binutils-common binutils-x86-64-linux-gnu build-essential bzip2
  cpp cpp-13 cpp-13-x86-64-linux-gnu cpp-x86-64-linux-gnu dpkg-dev
  fakeroot g++ g++-13 g++-13-x86-64-linux-gnu g++-x86-64-linux-gnu gcc
  gcc-13 gcc-13-base gcc-13-x86-64-linux-gnu gcc-x86-64-linux-gnu
  javascript-common libalgorithm-diff-perl libalgorithm-diff-xs-perl
  libalgorithm-merge-perl libasan8 libatomic1 libbinutils libcc1-0
  libctf-nobfd0 libctf0 libdpkg-perl libexpat1-dev libfakeroot

```

Update dilakukan untuk memastikan sistem berada pada kondisi terbaru dan menghindari konflik dependensi. Selanjutnya dilakukan instalasi beberapa paket pendukung seperti git, python3-venv, python3-pip, dan net-tools. Paket git digunakan untuk mengunduh source code honeypot Cowrie dari repositori resmi, sedangkan python3-venv dan python3-pip digunakan untuk membuat serta mengelola virtual environment Python. Paket net-tools digunakan sebagai alat bantu dalam proses pengecekan jaringan selama tahap konfigurasi dan pengujian.

#### 4.2 Instalasi Honeypot Cowrie

```

sukma@ubuntu:~$ git clone https://github.com/cowrie/cowrie.git
cd cowrie
Cloning into 'cowrie'...
remote: Enumerating objects: 20802, done.
remote: Counting objects: 100% (65/65), done.
remote: Compressing objects: 100% (49/49), done.
remote: Total 20802 (delta 40), reused 18 (delta 16), pack-reused 20737 (from 2)
Receiving objects: 100% (20802/20802), 11.03 MiB | 2.99 MiB/s, done.
Resolving deltas: 100% (14541/14541), done.

```

Pada tahap ini dilakukan pengunduhan source code honeypot Cowrie dari repositori resmi GitHub menggunakan perintah git clone. Setelah proses pengunduhan selesai, sistem berpindah ke direktori Cowrie untuk melanjutkan proses instalasi.

#### 4.3 Instalasi Dependensi Python

```
sukma@ubuntu:~/cowrie$ python3 -m venv cowrie-env
source cowrie-env/bin/activate
(cowrie-env) sukma@ubuntu:~/cowrie$ pip install --upgrade pip
pip install -r requirements.txt
Requirement already satisfied: pip in ./cowrie-env/lib/python3.12/site-packages (24.0)
Collecting pip
  Downloading pip-25.3-py3-none-any.whl.metadata (4.7 kB)
  Downloading pip-25.3-py3-none-any.whl (1.8 MB)
    1.8/1.8 MB 3.8 MB/s eta 0:00:00
Installing collected packages: pip
  Attempting uninstall: pip
    Found existing installation: pip 24.0
    Uninstalling pip-24.0:
      Successfully uninstalled pip-24.0
  Successfully installed pip-25.3
Collecting attrs==25.4.0 (from -r requirements.txt (line 1))
  Downloading attrs-25.4.0-py3-none-any.whl.metadata (10 kB)
Collecting bcrypt==5.0.0 (from -r requirements.txt (line 2))
  Downloading bcrypt-5.0.0-cp39-abi3-manylinux_2_34_x86_64.whl.metadata (10 kB)
Collecting cryptography==46.0.3 (from -r requirements.txt (line 3))
  Downloading cryptography-46.0.3-cp311-abi3-manylinux_2_34_x86_64.whl.metadata (5.7 kB)
Collecting hyperlink==21.0.0 (from -r requirements.txt (line 4))
  Downloading hyperlink-21.0.0-py2.py3-none-any.whl.metadata (1.5 kB)
Collecting idna==3.11 (from -r requirements.txt (line 5))
  Downloading idna-3.11-py3-none-any.whl.metadata (8.4 kB)
Collecting packaging==26.0 (from -r requirements.txt (line 6))
  Downloading packaging-26.0-py3-none-any.whl.metadata (3.3 kB)
Collecting pyasn1_modules==0.4.2 (from -r requirements.txt (line 7))
  Downloading pyasn1_modules-0.4.2-py3-none-any.whl.metadata (3.5 kB)
Collecting requests==2.32.5 (from -r requirements.txt (line 8))
  Downloading requests-2.32.5-py3-none-any.whl.metadata (4.9 kB)
Collecting service_identity==24.2.0 (from -r requirements.txt (line 9))
```

Melakukan pembuatan virtual environment Python menggunakan perintah `python3 -m venv cowrie-env`. Virtual environment ini digunakan untuk mengisolasi seluruh dependensi Cowrie agar tidak bercampur dengan paket Python pada sistem utama.

Setelah virtual environment diaktifkan, dilakukan pembaruan pip dan instalasi seluruh library Python yang dibutuhkan oleh Cowrie melalui file `requirements.txt`. Proses ini mencakup instalasi berbagai modul pendukung seperti `twisted`, `cryptography`, dan `hyperlink` yang merupakan komponen utama dalam operasi honeypot Cowrie.

#### 4.4 Konfigurasi Awal Cowrie

```
(cowrie-env) sukma@ubuntu:~/cowrie$ cp etc/cowrie.cfg.dist etc/cowrie.cfg
(cowrie-env) sukma@ubuntu:~/cowrie$ sudo nano /etc/ssh/sshd_config^C
(cowrie-env) sukma@ubuntu:~/cowrie$ sudo nano /etc/ssh/sshd_config
```

Pada tahap ini dilakukan penyalinan file konfigurasi bawaan Cowrie menggunakan perintah `cp etc/cowrie.cfg.dist etc/cowrie.cfg`. Proses ini bertujuan untuk membuat file konfigurasi aktif (`cowrie.cfg`) yang nantinya akan digunakan sebagai dasar pengaturan honeypot Cowrie.

Selanjutnya, dilakukan pengeditan file konfigurasi layanan SSH Ubuntu Server melalui file `/etc/ssh/sshd_config`. Konfigurasi ini

diperlukan untuk menyesuaikan pengaturan layanan SSH asli agar tidak berbenturan dengan layanan SSH palsu yang dijalankan oleh honeypot Cowrie.

```
# =====
# SSH Specific Options
# =====
[ssh]

# Enable SSH support
# (default: true)
enabled = true

# Public and private SSH key files. If these don't exist, they are created
# automatically.
rsa_public_key = ${honeypot:state_path}/ssh_host_rsa_key.pub
rsa_private_key = ${honeypot:state_path}/ssh_host_rsa_key
ecdsa_public_key = ${honeypot:state_path}/ssh_host_ecdsa_key.pub
ecdsa_private_key = ${honeypot:state_path}/ssh_host_ecdsa_key
ed25519_public_key = ${honeypot:state_path}/ssh_host_ed25519_key.pub
ed25519_private_key = ${honeypot:state_path}/ssh_host_ed25519_key

# Public keys supported are: ssh-rsa, ecdsa-sha2-nistp256, ssh-ed25519
public_key_auth = ssh-rsa, ecdsa-sha2-nistp256, ssh-ed25519

# listen_endpoints = systemd:domain=INET:index=0
# For both IPv4 and IPv6: listen_endpoints = tcp6:2222:interface=
# Listening on multiple endpoints is supported with a single space
# e.g listen_endpoints = "tcp:2222:interface=0.0.0.0 tcp:1022:interface=0.0.0.0"
# use authbind for port numbers under 1024

listen_endpoints = tcp:22:interface=0.0.0.0

# Enable the SFTP subsystem
# (default: true)
sftp_enabled = true
```

Cowrie dikonfigurasi untuk berjalan pada port 22 sebagai server jebakan SSH.

#### 4.5 Pengamanan SSH Asli Ubuntu Server

```
(cowrie-env) sukma@ubuntu:~/cowrie$ sudo nano /etc/ssh/sshd_config

#
# For changes to take effect, run:
#
#   systemctl daemon-reload
#   systemctl restart ssh.socket
#
Port 2222
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key
```

Pada tahap ini dilakukan pengamanan layanan SSH asli pada Ubuntu Server. Pengamanan ini bertujuan untuk mencegah konflik antara layanan SSH asli dengan layanan SSH palsu yang dijalankan oleh honeypot Cowrie serta meminimalkan risiko serangan langsung terhadap layanan SSH asli.



dilakukan pengeditan file konfigurasi SSH Ubuntu Server melalui file `/etc/ssh/sshd_config`. Pada konfigurasi ini, port SSH asli diubah dari port default menjadi port lain, yaitu **port 2222**, dengan cara mengaktifkan baris konfigurasi **port 2222**. Dengan demikian, port 22 dapat digunakan oleh honeypot Cowrie sebagai server jebakan yang akan menerima dan merekam aktivitas penyerang. Setelah di konfigurasi simpan perubahan dengan menekan CTRL + O enter dan keluar dengan CTRL + X.

setelah keluar retart SSH dengan perintah berikut:

```
(cowrie-env) sukma@ubuntu:~/cowrie$ sudo nano /etc/ssh/sshd_config
(cowrie-env) sukma@ubuntu:~/cowrie$ sudo systemctl restart ssh
```

#### 4.6 Verifikasi Port Aktif

```
(cowrie-env) sukma@ubuntu:~/cowrie$ sudo ss -tulnp | grep -E '22|2222'
[sudo] password for sukma:
tcp        LISTEN     0            4096               0.0.0.0:2222      0.0.0.0:*        users:((("sshd",pid=1129,fd=3),("systemd",pid=1,fd=93)))
tcp        LISTEN     0            50                0.0.0.0:22        0.0.0.0:*        users:((("twisted",pid=2399,fd=8)))
tcp        LISTEN     0            4096                :::2222           [::]:*          users:((("sshd",pid=1129,fd=4),("systemd",pid=1,fd=94)))
(cowrie-env) sukma@ubuntu:~/cowrie$ client_loop: send disconnect: Connection reset
```

Port 22 digunakan oleh Cowrie dan port 2222 digunakan oleh SSH asli Ubuntu server

#### 4.7 Menjalankan Honeypot Cowrie

Cowrie dijalankan oleh user cowrie dalam mode foreground

```
last login: Sun Jan 10 10:30:53 2026 from 10.253.243.100
sukma@ubuntu:~$ tail -f ~/cowrie/var/log/cowrie/cowrie.log
2026-01-28T15:47:45.118986Z [-] Python Version 3.12.3 (main, Jan 8 2026, 11:38:58) [GCC 13.3.0]
2026-01-28T15:47:45.118937Z [-] Twisted Version 25.5.0
2026-01-28T15:47:45.118944Z [-] Cowrie Version 2.9.9.dev9g08b65ffa6
2026-01-28T15:47:45.118950Z [-] Sender UUID: 802a4c27-fc60-11f0-8bd6-0800271675db
2026-01-28T15:47:45.124563Z [-] Loaded output engine: jsonlog
2026-01-28T15:47:45.125736Z [twisted.scripts.twisted_unix.UnixAppLogger#info] twisted 25.5.0 (/home/sukma/cowrie/cowrie-env/bin/python3 3.12.3) starting up.
2026-01-28T15:47:45.125813Z [twisted.scripts.twisted_unix.UnixAppLogger#info] reactor class: twisted.internet.epollreactor.EPollReactor.
2026-01-28T15:47:45.133022Z [-] CowrieSSHFactory starting on 2222
2026-01-28T15:47:45.133585Z [cowrie.ssh.factory.CowrieSSHFactory#info] Starting factory <cowrie.ssh.factory.CowrieSSHFactory object at 0x7f194e32a630>
2026-01-28T15:47:45.252883Z [-] Ready to accept SSH connections
```

Ini menunjukkan bahwa cowrie telah aktif dan siap menerima koneksi SSH.

### 5. Simulasi Serangan dari Kali linux

Sebelum melakukan seranga pastikan terlebih dahulu bahwa tools yang digunakan sudah tersedia.

```
(root@Aliyah) ~/home/aliyah
# nmap --version
hydra -h
hping3 --help

Nmap version 7.98 ( https://nmap.org )
Platform: x86_64-pc-linux-gnu
Compiled with: liblua-5.4.8 openssl-3.5.4 libssh2-1.11.1 libz-1.3.1 libpcap-1.10.5 nmap-libdnet-1.18.0 ipv6
Compiled without:
Available nsock engines: epoll poll select
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).

Syntax: hydra [[-l LOGIN|-L FILE] [-p PASS|-P FILE]] [-c C FILE] [-e nsr] [-o FI
LE] [-t TASKS] [-M FILE [-T TASKS]] [-w TIME] [-W TIME] [-f] [-s PORT] [-x MIN:MAX
:CHARSET] [-c TIME] [-ISOUvVd46] [-m MODULE_OPT] [service://server[:PORT]/OPT]]

Options:
-R      restore a previous aborted/crashed session
-I      ignore an existing restore file (don't wait 10 seconds)
-S      perform an SSL connect
-s PORT if the service is on a different default port, define it here
-l LOGIN or -L FILE login with LOGIN name, or load several logins from FILE
-p PASS or -P FILE try password PASS, or load several passwords from FILE
-x MIN:MAX:CHARSET password bruteforce generation, type "-x -h" to get help
-y      disable use of symbols in bruteforce, see above
-r      use a non-random shuffling method for option -x
-e nsr try "n" null password, "s" login as pass and/or "r" reversed login
-u      loop around users, not passwords (effective! implied with -x)
-c FILE colon separated "login:pass" format, instead of -L/-P options
-M FILE list of servers to attack, one entry per line, ':' to specify port
-D XoFY Divide wordlist into Y segments and use the Xth segment.
-o FILE write found login/password pairs to FILE instead of stdout
-b FORMAT specify the format for the -o FILE: text(default), json, jsonv1
-f / -F exit when a login/pass pair is found (-M: -f per host, -f global)
-t TASKS run TASKS number of connects in parallel per target (default: 16)
-T TASKS run TASKS connects in parallel overall (for -M, default: 64)
-w / -W TIME wait time for a response (32) / between connects per thread (0)
-c TIME wait time per login attempt over all threads (enforces -t 1)
-4 / -6 use IPv4 (default) / IPv6 addresses (put always in [] also in -M)
-v / -V / -d verbose mode / show login-pass for each attempt / debug mode
-O      use old SSL v2 and v3
```

Berdasarkan hasil verifikasi, tools Nmap, Hydra, dan Hping3 telah terinstal dan dapat dijalankan pada sistem Kali Linux. Nmap digunakan untuk melakukan *port scanning*, Hydra digunakan untuk simulasi serangan *brute force* pada layanan SSH, dan Hping3 digunakan untuk mensimulasikan peningkatan lalu lintas jaringan (*DDoS*).

Setelah itu kita masuk ke simulasi serangan double.

## 5.1 Simulasi Serangan Port Scanning Dan Brute Force

### a. Kali linux (Attacker)

```
root@Aliyah:~/home/aliyah
# ssh root@10.283.142.37
Warning: Permanently added '10.283.142.37' (SSH-2.0-Debian) to the list of known hosts.
root@10.283.142.37's password:
Permission denied, please try again.
root@10.283.142.37's password:
Permission denied, please try again.
root@10.283.142.37's password:
Permission denied (publickey,password).

root@Aliyah:~/home/aliyah
# nmap -t 10.283.142.37
Starting Nmap 7.98 ( https://nmap.org ) at 2026-01-30 01:53 +0800
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 1.58 seconds

root@Aliyah:~/home/aliyah
# nmap -t 10.283.142.37
Starting Nmap 7.98 ( https://nmap.org ) at 2026-01-30 01:53 +0800
Nmap scan report for 10.283.142.37
Host is up (0.075s latency).
Not shown: 997 closed tcp ports (conn-refused)
port      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
2222/tcp  open  EtherIP-1
MAC Address: CA:68:05:CA:7E:83 (Unknown)
Nmap done: 1 IP address (1 host up) scanned in 1.16 seconds
```

Pada tahap ini, penyerang menggunakan Kali Linux untuk melakukan port scanning dan brute force attack terhadap server target. Pemindaian port dengan Nmap menunjukkan bahwa layanan



SSH aktif pada port 22 dan 2222. Setelah port target teridentifikasi, dilakukan percobaan koneksi SSH menggunakan akun root dengan berbagai kombinasi autentikasi.

Meskipun akses tidak sepenuhnya berhasil, koneksi tetap diterima oleh honeypot Cowrie dan diarahkan ke sistem palsu. Hal ini menunjukkan bahwa honeypot berhasil mendeteksi dan menangkap aktivitas serangan tanpa memberikan akses ke sistem asli.

## b. Ubuntu Server (Target)

```
(cowrie-env) sukma@ubuntu:~/cowrie$ cd ~/cowrie
authbind twisted -n cowrie
/home/sukma/cowrie/cowrie-env/lib/python3.12/site-packages/twisted/conch/ssh/transport.py:118: CryptographyDeprecationWarning: TripleDES has been moved to cryptography.hazmat.decrepit.ciphers.algorithms.TripleDES and will be removed from cryptography.hazmat.primitives.ciphers.algorithms in 48.0.0.
  b"new-ctc". (algorithms.TripleDES, 24, modes.CBC)
/home/sukma/cowrie/cowrie-env/lib/python3.12/site-packages/twisted/conch/ssh/transport.py:117: CryptographyDeprecationWarning: TripleDES has been moved to cryptography.hazmat.decrepit.ciphers.algorithms.TripleDES and will be removed from cryptography.hazmat.primitives.ciphers.algorithms in 48.0.0.
  b"new-ctc". (algorithms.TripleDES, 24, modes.CBC)
2026-01-29T05:59:06+0000 [-] Reading configuration from ['/home/sukma/cowrie/etc/cowrie.cfg.dist', '/home/sukma/cowrie/etc/cowrie.cfg']
2026-01-29T05:59:06+0000 [-] Python Version 3.12.3 (main, Jan 8 2026, 11:30:58) [GCC 13.3.0]
2026-01-29T05:59:06+0000 [-] Twisted Version 25.5.0
2026-01-29T05:59:06+0000 [-] Cowrie Version 2.9.9.dev9+g8bb65ffa6
2026-01-29T05:59:06+0000 [-] Sensor UUID: 862a8c2f-fc6b-11f6-8bde-88082716756b
2026-01-29T05:59:06+0000 [-] Loaded output engine: jsonlog
2026-01-29T05:59:06+0000 [twisted.scripts._twisted_unix.UnixAppLogger#info] twisted 25.5.0 (/home/sukma/cowrie/cowrie-env/bin/python3 3.12.3) starting up.
2026-01-29T05:59:06+0000 [twisted.scripts._twisted_unix.UnixAppLogger#info] reactor class: twisted.internet.epollreactor.EPollReactor.
2026-01-29T05:59:06+0000 [-] CowrieSSHFactory starting on 22
2026-01-29T05:59:06+0000 [cowrie.ssh.factory.CowrieSSHFactory#info] Starting factory <cowrie.ssh.factory.CowrieSSHFactory object at 0x795dada615b>
2026-01-29T05:59:09+0000 [cowrie.ssh.factory.CowrieSSHFactory] New connection: 10.203.142.101:51814 (10.203.142.37:22) [session: 10f1283469e6]
2026-01-29T05:59:09+0000 [HoneyPotSSHTransport 0, 10.203.142.101] Remote SSH version: SSH-2.0-OpenSSH_10.2p1 Debian-3
2026-01-29T05:59:09+0000 [HoneyPotSSHTransport 0, 10.203.142.101] SSH client hash: fingerprint: eac3d66858b0ded80ae32f78a75356
2026-01-29T05:59:09+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#debug] outgoing: b'aa128-ctc' b'aa128-ctc' b'none'
2026-01-29T05:59:09+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#debug] incoming: b'aa128-ctc' b'aa128-ctc' b'none'
2026-01-29T05:59:09+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#debug] NEW KEYS
2026-01-29T05:59:09+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#debug] starting service b'ssh-userauth'
2026-01-29T05:59:09+0000 [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'root' trying auth b'none'
2026-01-29T05:43:13+0000 [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'root' trying auth b'none'
2026-01-29T05:43:16+0000 [HoneyPotSSHTransport 3, 10.203.142.101] Could not read etc/userdb.txt, default database activated
2026-01-29T05:43:16+0000 [HoneyPotSSHTransport 3, 10.203.142.101] Login attempt [b'root' b'123'] succeeded
2026-01-29T05:43:16+0000 [HoneyPotSSHTransport 3, 10.203.142.101] Initialized emulated server as architecture: linux-x64-lsb
2026-01-29T05:43:16+0000 [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'root' authenticated with b'password'
2026-01-29T05:43:16+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#debug] starting service b'ssh-connection'
2026-01-29T05:43:16+0000 [cowrie.ssh.connection.CowrieSSHConnection#debug] got channel b'session' request
2026-01-29T05:43:16+0000 [cowrie.ssh.connection.CowrieSSHConnection#debug] got global b'no-more-sessions@openssh.com' request
2026-01-29T05:43:17+0000 [twisted.conch.ssh.session#info] Handling pty request: b'sterm-256color' (46, 82, 9, 0)
2026-01-29T05:43:17+0000 [SSHChannel session (0) on SSHService b'ssh-connection' on HoneyPotSSHTransport 3, 10.203.142.101] Terminal Size: 82 46
2026-01-29T05:43:17+0000 [SSHChannel session (0) on SSHService b'ssh-connection' on HoneyPotSSHTransport 3, 10.203.142.101] request-env: COLORTERM=truecolor
2026-01-29T05:43:17+0000 [SSHChannel session (0) on SSHService b'ssh-connection' on HoneyPotSSHTransport 3, 10.203.142.101] request-env: LANG=en_US.UTF-8
2026-01-29T05:43:17+0000 [twisted.conch.ssh.session#info] Getting shell
2026-01-29T05:43:21+0000 [HoneyPotSSHTransport 3, 10.203.142.101] CMD: whoami
2026-01-29T05:43:21+0000 [HoneyPotSSHTransport 3, 10.203.142.101] Command found: whoami
2026-01-29T05:43:42+0000 [HoneyPotSSHTransport 3, 10.203.142.101] CMD: uname -a
2026-01-29T05:43:42+0000 [HoneyPotSSHTransport 3, 10.203.142.101] Command found: uname -a
2026-01-29T05:43:56+0000 [HoneyPotSSHTransport 3, 10.203.142.101] CMD: ls
2026-01-29T05:43:56+0000 [HoneyPotSSHTransport 3, 10.203.142.101] Command found: ls
2026-01-29T05:44:09+0000 [HoneyPotSSHTransport 3, 10.203.142.101] CMD: ls /root
2026-01-29T05:44:09+0000 [HoneyPotSSHTransport 3, 10.203.142.101] Command found: ls /root
2026-01-29T05:44:14+0000 [HoneyPotSSHTransport 3, 10.203.142.101] CMD: exit
2026-01-29T05:44:14+0000 [twisted.conch.ssh.session#info] exitCode: 0
2026-01-29T05:44:14+0000 [cowrie.ssh.connection.CowrieSSHConnection#debug] sending request b'exit-status'
2026-01-29T05:44:14+0000 [HoneyPotSSHTransport 3, 10.203.142.101] Closing TTY Log: var/lib/cowrie/tty/4ba47a77d8ee2e349a907f186e80e5e2e9cc39fed91dd63f4dbffc9f8d5acc6 after 57.3 seconds
2026-01-29T05:44:14+0000 [cowrie.ssh.connection.CowrieSSHConnection#info] sending close 0
2026-01-29T05:44:14+0000 [cowrie.ssh.session.HoneyPotSSHSession#info] remote close
2026-01-29T05:44:14+0000 [HoneyPotSSHTransport 3, 10.203.142.101] got remote error: code 11 reason: b'disconnected by user'
2026-01-29T05:44:14+0000 [HoneyPotSSHTransport 3, 10.203.142.101] avatar root logging out
2026-01-29T05:44:14+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#info] connection lost
2026-01-29T05:44:14+0000 [HoneyPotSSHTransport 3, 10.203.142.101] Connection lost after 0.2 seconds
2026-01-29T05:48:42+0000 [twisted.internet.base#info] Received SIGINT, shutting down.
2026-01-29T05:48:42+0000 [-] (TCP Port 22 Closed)
2026-01-29T05:48:42+0000 [cowrie.ssh.factory.CowrieSSHFactory#info] Stopping factory <cowrie.ssh.factory.CowrieSSHFactory object at 0x77948f34707b>
2026-01-29T05:48:42+0000 [twisted.internet.base#info] Main loop terminated.
2026-01-29T05:48:42+0000 [twisted.scripts._twisted_unix.UnixAppLogger#info] Server Shut Down.
```

Berdasarkan hasil pengujian pada sisi target, honeypot Cowrie berhasil mendeteksi dan merekam seluruh aktivitas serangan yang masuk melalui layanan SSH. Setiap koneksi dari penyerang tercatat secara detail, mulai dari alamat IP sumber, metode autentikasi yang digunakan, hingga percobaan login menggunakan akun root.

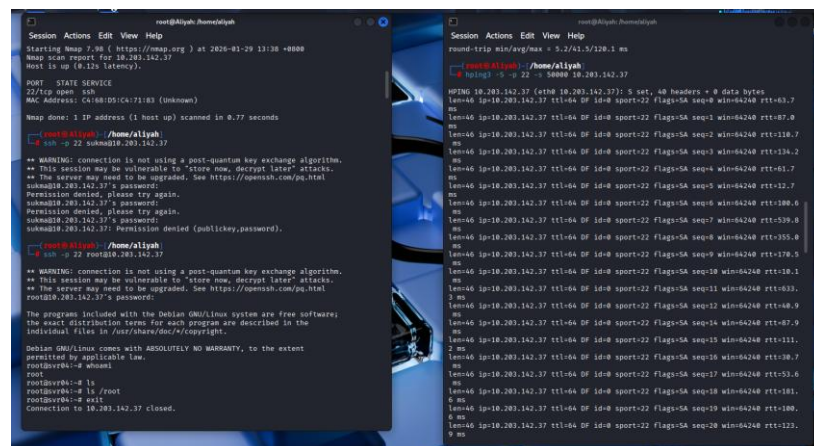
Setelah autentikasi diterima oleh sistem palsu, aktivitas penyerang seperti identifikasi pengguna, pengecekan sistem operasi,

serta perintah dasar lainnya terekam sepenuhnya dalam log Cowrie. Hal ini menunjukkan bahwa honeypot mampu menipu penyerang dengan menyediakan lingkungan tiruan tanpa memberikan akses ke server asli.

Data yang diperoleh dari proses ini berupa log aktivitas lengkap yang dapat digunakan untuk analisis pola serangan, perilaku penyerang, serta efektivitas mekanisme deteksi honeypot terhadap serangan port scanning dan brute force.

## 5.2 Simulasi Serangan Brute Force Dan Ddos

### a. Kali linux (Attacker)



The image shows two terminal windows from a Kali Linux machine. The left window displays the output of an Nmap scan for IP 10.203.142.37, identifying it as a 22/tcp open ssh. It then shows a brute force attack using 'crackmapexec ssh' with a list of usernames and passwords, resulting in a 'Permission denied' message. The right window shows a 'hping3' command being used to perform a SYN flood attack on the same IP address, with a list of IP addresses and ports being scanned.

Pada tahap ini, penyerang melakukan dua jenis serangan secara berurutan, yaitu brute force SSH dan DDoS (SYN flood) terhadap server target. Serangan brute force dilakukan dengan mencoba beberapa kombinasi kata sandi pada akun root untuk menguji kerentanan autentikasi layanan SSH.

Setelah itu, serangan DDoS dilakukan menggunakan teknik SYN flood untuk mengirimkan paket dalam jumlah besar ke port SSH target. Tujuan dari serangan ini adalah untuk meningkatkan beban jaringan dan mengganggu ketersediaan layanan.

Dari sisi penyerang, sistem target tetap dapat dijangkau, namun menerima lonjakan trafik yang signifikan. Aktivitas ini digunakan untuk mengamati respons dan pencatatan serangan oleh honeypot pada sisi server target.

## b. Ubuntu server (Target)

- Brute force

```
2026-01-29T05:50:05+0000 [cowrie.ssh.transport.HoneyPotSSHTransportInfo] connection lost
2026-01-29T05:50:05+0000 [HoneyPotSSHTransport,1,10.203.142.101] Connection lost after 14.4 seconds
2026-01-29T05:51:34+0000 [cowrie.ssh.factory.CowrieSSHFactory] New connection: 10.203.142.101:40858 (10.203.142.37:22) [session: 30f08dc290]
2026-01-29T05:51:34+0000 [HoneyPotSSHTransport,1,10.203.142.101] Remote SSH version: SSH-2.0-openssh.10.102 Ubuntu-7
2026-01-29T05:51:34+0000 [HoneyPotSSHTransport,1,10.203.142.101] SSH client hash fingerprint: eeca260858b9d0e08becf2778a75356
2026-01-29T05:51:34+0000 [cowrie.ssh.transport.HoneyPotSSHTransportDebug] hex alg=b'curve25519-sha256' key alg=b'ssh-ed25519'
2026-01-29T05:51:34+0000 [cowrie.ssh.transport.HoneyPotSSHTransportDebug] outgoing: b'aa128-ctr' b'hmac-sha2-256' b'none'
2026-01-29T05:51:34+0000 [cowrie.ssh.transport.HoneyPotSSHTransportDebug] incoming: b'aa128-ctr' b'hmac-sha2-256' b'none'
2026-01-29T05:51:34+0000 [cowrie.ssh.transport.HoneyPotSSHTransportDebug] NEW KEX
2026-01-29T05:51:37+0000 [cowrie.ssh.sshuserauth.HoneyPotSSHUserAuthServiceDebug] b'root' trying auth b'none'
2026-01-29T05:51:37+0000 [cowrie.ssh.sshuserauth.HoneyPotSSHUserAuthServiceDebug] b'root' trying auth b'password'
2026-01-29T05:51:37+0000 [HoneyPotSSHTransport,1,10.203.142.101] Could not read etc/usersh.cty, default database activated
2026-01-29T05:51:37+0000 [HoneyPotSSHTransport,1,10.203.142.101] Login attempt (b'root' b'123') succeeded
2026-01-29T05:51:37+0000 [HoneyPotSSHTransport,1,10.203.142.101] Initialized emulated server as architecture: linux-x64-ssh
2026-01-29T05:51:37+0000 [cowrie.ssh.sshuserauth.HoneyPotSSHUserAuthServiceDebug] b'root' authenticated with b'password'
2026-01-29T05:51:37+0000 [cowrie.ssh.session.HoneyPotSSHSessionInfo] starting service b'ssh-connection'
2026-01-29T05:51:37+0000 [cowrie.ssh.session.HoneyPotSSHSessionInfo] get channel b'session' request
2026-01-29T05:51:37+0000 [cowrie.ssh.session.HoneyPotSSHSessionInfo] channel open
2026-01-29T05:51:37+0000 [cowrie.ssh.connection.CowrieSSHConnectionDebug] got global b'no-more-sessions@openssh.com' request
2026-01-29T05:51:37+0000 [twisted.conch.ssh.sessionInfo] Handling pty request: b'style=36color' (46, 12, 8, 0)
2026-01-29T05:51:37+0000 [SSHChannel session (0)] on SSHService b'ssh-connection' on HoneyPotSSHTransport,1,10.203.142.101 Terminal Size: 82 46
2026-01-29T05:51:37+0000 [SSHChannel session (0)] on SSHService b'ssh-connection' on HoneyPotSSHTransport,1,10.203.142.101 request_env: COLUMNS=terminal
2026-01-29T05:51:37+0000 [SSHChannel session (0)] on SSHService b'ssh-connection' on HoneyPotSSHTransport,1,10.203.142.101 request_env: LANG=en_US.UTF-8
2026-01-29T05:51:37+0000 [twisted.conch.ssh.sessionInfo] Getting shell
2026-01-29T05:51:45+0000 [HoneyPotSSHTransport,1,10.203.142.101] CMD: whoami
2026-01-29T05:51:45+0000 [HoneyPotSSHTransport,1,10.203.142.101] Command found: whoami
2026-01-29T05:51:50+0000 [HoneyPotSSHTransport,1,10.203.142.101] CMD: ls
2026-01-29T05:51:50+0000 [HoneyPotSSHTransport,1,10.203.142.101] Command found: ls
2026-01-29T05:51:54+0000 [HoneyPotSSHTransport,1,10.203.142.101] CMD: ls /root
2026-01-29T05:51:54+0000 [HoneyPotSSHTransport,1,10.203.142.101] Command found: ls /root
2026-01-29T05:51:58+0000 [HoneyPotSSHTransport,1,10.203.142.101] CMD: exit
2026-01-29T05:51:58+0000 [twisted.conch.ssh.sessionInfo] exitCode: 0
2026-01-29T05:51:58+0000 [cowrie.ssh.connection.CowrieSSHConnectionDebug] sending request b'exit-status'
2026-01-29T05:51:58+0000 [HoneyPotSSHTransport,1,10.203.142.101] Closing TTY Log: var/lib/cowrie/tty/cacaa34a3e7b28ee5841a0e017ae387c53ccccebae7d08586d0ec
2026-01-29T05:51:58+0000 [cowrie.ssh.connection.CowrieSSHConnectionInfo] sending close 0
2026-01-29T05:51:58+0000 [cowrie.ssh.session.HoneyPotSSHSessionInfo] remote close
2026-01-29T05:51:58+0000 [HoneyPotSSHTransport,1,10.203.142.101] Got remote error: code 11 reason: b'disconnected by user'
2026-01-29T05:51:58+0000 [HoneyPotSSHTransport,1,10.203.142.101] avatar root logging out
```

Pada sisi Ubuntu Server, honeypot Cowrie berhasil mendeteksi percobaan brute force pada layanan SSH. Log menunjukkan adanya upaya autentikasi berulang menggunakan akun root hingga salah satu percobaan berhasil.

Setelah berhasil login, seluruh aktivitas penyerang di dalam sistem palsu terekam dengan baik, termasuk perintah dasar seperti whoami, pwd, dan ls. Hal ini menunjukkan bahwa Cowrie mampu mencatat proses serangan brute force beserta aktivitas lanjutan penyerang setelah memperoleh akses ke honeypot.

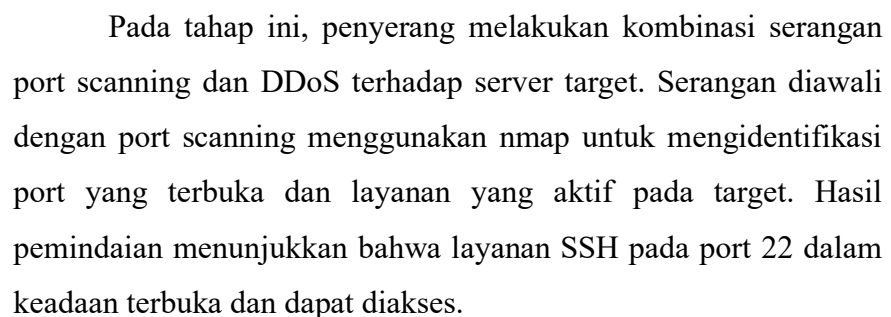
- DDos

```
sukma@ubuntu: ~/cowrie
06:05:33.942436 IP 10.203.142.101.5271 > 10.203.142.37.22: Flags [S], seq 976013419, win 512, length 0
06:05:33.942436 IP 10.203.142.101.5272 > 10.203.142.37.22: Flags [S], seq 1748485141, win 512, length 0
06:05:33.942437 IP 10.203.142.101.5273 > 10.203.142.37.22: Flags [S], seq 718706627, win 512, length 0
06:05:33.942437 IP 10.203.142.101.5274 > 10.203.142.37.22: Flags [S], seq 1972132294, win 512, length 0
06:05:33.942437 IP 10.203.142.101.5275 > 10.203.142.37.22: Flags [S], seq 1070201818, win 512, length 0
06:05:33.942437 IP 10.203.142.101.5276 > 10.203.142.37.22: Flags [S], seq 595503018, win 512, length 0
06:05:33.942437 IP 10.203.142.101.5277 > 10.203.142.37.22: Flags [S], seq 1049276921, win 512, length 0
06:05:33.942460 IP 10.203.142.37.22 > 10.203.142.101.5270: Flags [S], seq 2585626279, win 64240, options [mss 1460]
06:05:33.942693 IP 10.203.142.37.22 > 10.203.142.101.5271: Flags [S], seq 340373644, ack 976013420, win 64240, options [mss 1460]
06:05:33.942747 IP 10.203.142.37.22 > 10.203.142.101.5272: Flags [S], seq 3803907033, ack 1748485142, win 64240, options [mss 1460]
06:05:33.943104 IP 10.203.142.37.22 > 10.203.142.101.5273: Flags [S], seq 4009130042, ack 718706628, win 64240, options [mss 1460]
06:05:33.943456 IP 10.203.142.37.22 > 10.203.142.101.5274: Flags [S], seq 2146579717, ack 1972132295, win 64240, options [mss 1460]
06:05:33.943632 IP 10.203.142.37.22 > 10.203.142.101.5275: Flags [S], seq 1031483704, ack 1070201819, win 64240, options [mss 1460]
06:05:33.943812 IP 10.203.142.37.22 > 10.203.142.101.5276: Flags [S], seq 3265050472, ack 595503019, win 64240, options [mss 1460]
06:05:33.944018 IP 10.203.142.37.22 > 10.203.142.101.5277: Flags [S], seq 4117070642, ack 1949275922, win 64240, options [mss 1460]
06:05:33.944480 IP 10.203.142.101.5276 > 10.203.142.37.22: Flags [S], seq 1217526062, win 512, length 0
06:05:33.944487 IP 10.203.142.101.5279 > 10.203.142.37.22: Flags [S], seq 1423346555, win 512, length 0
06:05:33.944487 IP 10.203.142.101.5280 > 10.203.142.37.22: Flags [S], seq 559600785, win 512, length 0
06:05:33.944487 IP 10.203.142.101.5281 > 10.203.142.37.22: Flags [S], seq 446631404, win 512, length 0
06:05:33.944487 IP 10.203.142.101.5282 > 10.203.142.37.22: Flags [S], seq 1993717122, win 512, length 0
06:05:33.944487 IP 10.203.142.101.5283 > 10.203.142.37.22: Flags [S], seq 923018499, win 512, length 0
06:05:33.944487 IP 10.203.142.101.5284 > 10.203.142.37.22: Flags [S], seq 793857110, win 512, length 0
06:05:33.944487 IP 10.203.142.101.5285 > 10.203.142.37.22: Flags [S], seq 576453064, win 512, length 0
06:05:33.944613 IP 10.203.142.37.22 > 10.203.142.101.5270: Flags [S], seq 117572564, ack 1217526063, win 64240, options [mss 1460]
06:05:33.944650 IP 10.203.142.37.22 > 10.203.142.101.5279: Flags [S], seq 3252340298, ack 1423346556, win 64240, options [mss 1460]
06:05:33.945267 IP 10.203.142.37.22 > 10.203.142.101.5280: Flags [S], seq 1392515316, ack 559600786, win 64240, options [mss 1460]
06:05:33.945404 IP 10.203.142.37.22 > 10.203.142.101.5281: Flags [S], seq 3588622839, ack 446631405, win 64240, options [mss 1460]
06:05:33.945528 IP 10.203.142.37.22 > 10.203.142.101.5282: Flags [S], seq 1081378428, ack 1993717123, win 64240, options [mss 1460]
06:05:33.945658 IP 10.203.142.37.22 > 10.203.142.101.5283: Flags [S], seq 1168525688, ack 923018499, win 64240, options [mss 1460]
06:05:33.945802 IP 10.203.142.37.22 > 10.203.142.101.5284: Flags [S], seq 1192824099, ack 793857111, win 64240, options [mss 1460]
06:05:33.946243 IP 10.203.142.37.22 > 10.203.142.101.5285: Flags [S], seq 1521618999, ack 576453065, win 64240, options [mss 1460]
06:05:33.946549 IP 10.203.142.101.5286 > 10.203.142.37.22: Flags [S], seq 473215305, win 512, length 0
06:05:33.946549 IP 10.203.142.101.5287 > 10.203.142.37.22: Flags [S], seq 75624867, win 512, length 0
06:05:33.946549 IP 10.203.142.101.5288 > 10.203.142.37.22: Flags [S], seq 694651999, win 512, length 0
06:05:33.946550 IP 10.203.142.101.5289 > 10.203.142.37.22: Flags [S], seq 571665052, win 512, length 0
06:05:33.946550 IP 10.203.142.101.5290 > 10.203.142.37.22: Flags [S], seq 719763085, win 512, length 0
06:05:33.946550 IP 10.203.142.101.5291 > 10.203.142.37.22: Flags [S], seq 6434306, win 512, length 0
06:05:33.946550 IP 10.203.142.101.5292 > 10.203.142.37.22: Flags [S], seq 1313902350, win 512, length 0
06:05:33.946550 IP 10.203.142.101.5293 > 10.203.142.37.22: Flags [S], seq 1542913915, win 512, length 0
06:05:33.946570 IP 10.203.142.37.22 > 10.203.142.101.5286: Flags [S], seq 2027482356, ack 473215306, win 64240, options [mss 1460]
06:05:33.946690 IP 10.203.142.37.22 > 10.203.142.101.5287: Flags [S], seq 4016030208, ack 75624868, win 64240, options [mss 1460]
06:05:33.946799 IP 10.203.142.37.22 > 10.203.142.101.5288: Flags [S], seq 2889338576, ack 694651991, win 64240, options [mss 1460]
06:05:33.947245 IP 10.203.142.37.22 > 10.203.142.101.5289: Flags [S], seq 2848986653, ack 571665053, win 64240, options [mss 1460]
```

Pada tahap ini, Ubuntu Server menerima serangan DDos berupa pengiriman paket SYN secara masif ke port SSH. Hal ini

Serangan ini menyebabkan peningkatan trafik jaringan yang signifikan pada port target. Meskipun layanan SSH masih merespons paket SYN, pola trafik yang terekam menunjukkan adanya upaya pembajakan jaringan. Data ini membuktikan bahwa sistem berhasil mendeteksi aktivitas DDoS dan dapat digunakan untuk menganalisis karakteristik serangan berbasis flood terhadap layanan SSH.

**a. Kali linux (Attacker)**



secara terus-menerus ke port SSH untuk membanjiri layanan dan meningkatkan beban jaringan.

Dari sisi penyerang, target tetap dapat dijangkau namun menerima trafik yang sangat tinggi. Kombinasi serangan ini digunakan untuk menguji kemampuan sistem target, khususnya honeypot, dalam mendeteksi pola serangan berlapis yang dimulai dari pengintaian port hingga pembanjiran layanan.

## b. Ubuntu Server (Target)

```
06:10:15.835868 IP 10.203.142.37.22 > 10.203.142.101.46794: Flags [S], seq 1265511897, ack 1120885861, win 64240, options [msg 1460], length 0
06:10:15.834462 IP 10.203.142.101.46785 > 10.203.142.37.22: Flags [S], seq 1658911855, win 512, length 0
06:10:15.835131 IP 10.203.142.37.22 > 10.203.142.101.46785: Flags [S], seq 1779117691, ack 1658911855, win 64240, options [msg 1460], length 0
06:10:15.835267 IP 10.203.142.101.46786 > 10.203.142.37.22: Flags [S], seq 182188409, win 512, length 0
06:10:15.835282 IP 10.203.142.37.22 > 10.203.142.101.46786: Flags [S], seq 1341787837, ack 182188410, win 64240, options [msg 1460], length 0
06:10:15.835307 IP 10.203.142.101.46787 > 10.203.142.37.22: Flags [S], seq 123727246, win 512, length 0
06:10:15.835358 IP 10.203.142.37.22 > 10.203.142.101.46787: Flags [S], seq 312734366, ack 752372461, win 64240, options [msg 1460], length 0
06:10:15.835367 IP 10.203.142.101.46788 > 10.203.142.37.22: Flags [S], seq 116151351, win 512, length 0
06:10:15.835452 IP 10.203.142.37.22 > 10.203.142.101.46788: Flags [S], seq 1818953367, ack 116151351, win 64240, options [msg 1460], length 0
06:10:15.835267 IP 10.203.142.101.46789 > 10.203.142.37.22: Flags [S], seq 1494214080, win 512, length 0
06:10:15.835317 IP 10.203.142.37.22 > 10.203.142.101.46789: Flags [S], seq 1265959715, ack 1494214081, win 64240, options [msg 1460], length 0
06:10:15.835267 IP 10.203.142.101.46788 > 10.203.142.37.22: Flags [S], seq 1573910382, win 512, length 0
06:10:15.835459 IP 10.203.142.37.22 > 10.203.142.101.46788: Flags [S], seq 1573910382, win 64240, options [msg 1460], length 0
06:10:15.835368 IP 10.203.142.101.46761 > 10.203.142.37.22: Flags [S], seq 1886712966, win 512, length 0
06:10:15.835791 IP 10.203.142.37.22 > 10.203.142.101.46761: Flags [S], seq 3835882328, ack 1886712961, win 64240, options [msg 1460], length 0
06:10:15.835368 IP 10.203.142.101.46762 > 10.203.142.37.22: Flags [S], seq 1886712966, win 512, length 0
06:10:15.836424 IP 10.203.142.37.22 > 10.203.142.101.46762: Flags [S], seq 2796918161, ack 488569759, win 64240, options [msg 1460], length 0
06:10:15.835368 IP 10.203.142.101.46763 > 10.203.142.37.22: Flags [S], seq 1886712966, win 512, length 0
06:10:15.836398 IP 10.203.142.37.22 > 10.203.142.101.46763: Flags [S], seq 1679978034, ack 1584734215, win 64240, options [msg 1460], length 0
06:10:15.836722 IP 10.203.142.101.46764 > 10.203.142.37.22: Flags [S], seq 445631075, win 512, length 0
06:10:15.836739 IP 10.203.142.37.22 > 10.203.142.101.46764: Flags [S], seq 1413222885, ack 445631076, win 64240, options [msg 1460], length 0
06:10:15.836722 IP 10.203.142.101.46765 > 10.203.142.37.22: Flags [S], seq 761764157, win 512, length 0
06:10:15.837068 IP 10.203.142.37.22 > 10.203.142.101.46765: Flags [S], seq 1584881166, ack 761764153, win 64240, options [msg 1460], length 0
06:10:15.836722 IP 10.203.142.101.46766 > 10.203.142.37.22: Flags [S], seq 1689724346, win 512, length 0
06:10:15.837161 IP 10.203.142.37.22 > 10.203.142.101.46766: Flags [S], seq 1431327958, ack 1689724347, win 64240, options [msg 1460], length 0
06:10:15.836722 IP 10.203.142.101.46767 > 10.203.142.37.22: Flags [S], seq 2428382385, win 512, length 0
06:10:15.837238 IP 10.203.142.37.22 > 10.203.142.101.46767: Flags [S], seq 2938851798, ack 2428382382, win 64240, options [msg 1460], length 0
06:10:15.836722 IP 10.203.142.101.46768 > 10.203.142.37.22: Flags [S], seq 663971786, win 512, length 0
06:10:15.837161 IP 10.203.142.37.22 > 10.203.142.101.46768: Flags [S], seq 1431431855, ack 663971787, win 64240, options [msg 1460], length 0
06:10:15.836722 IP 10.203.142.101.46769 > 10.203.142.37.22: Flags [S], seq 1877989268, win 512, length 0
06:10:15.837178 IP 10.203.142.37.22 > 10.203.142.101.46769: Flags [S], seq 1286687231, ack 1877989269, win 64240, options [msg 1460], length 0
06:10:15.836722 IP 10.203.142.101.46770 > 10.203.142.37.22: Flags [S], seq 2871239778, win 512, length 0
06:10:15.837480 IP 10.203.142.37.22 > 10.203.142.101.46770: Flags [S], seq 958469769, ack 287239777, win 64240, options [msg 1460], length 0
06:10:15.836723 IP 10.203.142.101.46771 > 10.203.142.37.22: Flags [S], seq 1446337394, win 512, length 0
06:10:15.837511 IP 10.203.142.37.22 > 10.203.142.101.46771: Flags [S], seq 622249662, ack 1446337395, win 64240, options [msg 1460], length 0
06:10:15.837633 IP 10.203.142.101.46772 > 10.203.142.37.22: Flags [S], seq 1452488533, win 512, length 0
06:10:15.837646 IP 10.203.142.37.22 > 10.203.142.101.46772: Flags [S], seq 3588938438, ack 1452488534, win 64240, options [msg 1460], length 0
06:10:15.837633 IP 10.203.142.101.46773 > 10.203.142.37.22: Flags [S], seq 1423892397, win 512, length 0
06:10:15.837732 IP 10.203.142.37.22 > 10.203.142.101.46773: Flags [S], seq 839712786, ack 1423892398, win 64240, options [msg 1460], length 0
06:10:15.837633 IP 10.203.142.101.46774 > 10.203.142.37.22: Flags [S], seq 1118616709, win 512, length 0
06:10:15.838061 IP 10.203.142.37.22 > 10.203.142.101.46774: Flags [S], seq 3985393577, ack 1118616709, win 64240, options [msg 1460], length 0

06:10:15.858239 IP 10.203.142.37.22 > 10.203.142.101.46829: Flags [S], seq 1756980472, ack 1704566804, win 64240, options [msg 1460], length 0
06:10:15.849788 IP 10.203.142.101.46830 > 10.203.142.37.22: Flags [S], seq 1613197048, win 512, length 0
06:10:15.858242 IP 10.203.142.37.22 > 10.203.142.101.46830: Flags [S], seq 3582829226, ack 1613197049, win 64240, options [msg 1460], length 0
06:10:15.849788 IP 10.203.142.101.46831 > 10.203.142.37.22: Flags [S], seq 2065580935, win 512, length 0
06:10:15.858451 IP 10.203.142.37.22 > 10.203.142.101.46831: Flags [S], seq 688871649, ack 2065580936, win 64240, options [msg 1460], length 0
06:10:15.849788 IP 10.203.142.101.46832 > 10.203.142.37.22: Flags [S], seq 958469769, win 512, length 0
06:10:15.858642 IP 10.203.142.37.22 > 10.203.142.101.46832: Flags [S], seq 2589564271, ack 1861672897, win 64240, options [msg 1460], length 0
06:10:15.849788 IP 10.203.142.101.46833 > 10.203.142.37.22: Flags [S], seq 1229878266, win 512, length 0
06:10:15.858672 IP 10.203.142.37.22 > 10.203.142.101.46833: Flags [S], seq 3868967620, ack 1229878267, win 64240, options [msg 1460], length 0
06:10:15.849788 IP 10.203.142.101.46834 > 10.203.142.37.22: Flags [S], seq 983264622, win 512, length 0
06:10:15.858618 IP 10.203.142.37.22 > 10.203.142.101.46834: Flags [S], seq 468882604, ack 983264623, win 64240, options [msg 1460], length 0
06:10:15.849788 IP 10.203.142.101.46835 > 10.203.142.37.22: Flags [S], seq 312151975, win 512, length 0
06:10:15.858936 IP 10.203.142.37.22 > 10.203.142.101.46835: Flags [S], seq 2258815621, ack 312151976, win 64240, options [msg 1460], length 0
06:10:15.831257 IP 10.203.142.101.46836 > 10.203.142.37.22: Flags [S], seq 1224667258, win 512, length 0
06:10:15.851276 IP 10.203.142.37.22 > 10.203.142.101.46836: Flags [S], seq 1134488558, ack 1224667259, win 64240, options [msg 1460], length 0
06:10:15.851257 IP 10.203.142.101.46837 > 10.203.142.37.22: Flags [S], seq 347532981, win 512, length 0
06:10:15.851480 IP 10.203.142.37.22 > 10.203.142.101.46837: Flags [S], seq 4165286278, ack 347532982, win 64240, options [msg 1460], length 0
06:10:15.851257 IP 10.203.142.101.46838 > 10.203.142.37.22: Flags [S], seq 1338388049, win 512, length 0
06:10:15.851880 IP 10.203.142.37.22 > 10.203.142.101.46838: Flags [S], seq 3636581899, ack 1338388050, win 64240, options [msg 1460], length 0
06:10:15.851257 IP 10.203.142.101.46839 > 10.203.142.37.22: Flags [S], seq 1748892627, win 512, length 0
06:10:15.852843 IP 10.203.142.37.22 > 10.203.142.101.46839: Flags [S], seq 1428816752, ack 1748892628, win 64240, options [msg 1460], length 0
06:10:15.851257 IP 10.203.142.101.46840 > 10.203.142.37.22: Flags [S], seq 998998667, win 512, length 0
06:10:15.852135 IP 10.203.142.37.22 > 10.203.142.101.46840: Flags [S], seq 3582481938, ack 998998668, win 64240, options [msg 1460], length 0
06:10:15.851257 IP 10.203.142.101.46841 > 10.203.142.37.22: Flags [S], seq 2838388295, win 512, length 0
06:10:15.852216 IP 10.203.142.37.22 > 10.203.142.101.46841: Flags [S], seq 1748892627, ack 2838388296, win 64240, options [msg 1460], length 0
06:10:15.851257 IP 10.203.142.101.46842 > 10.203.142.37.22: Flags [S], seq 548642141, win 512, length 0
06:10:15.852290 IP 10.203.142.37.22 > 10.203.142.101.46842: Flags [S], seq 886289984, ack 548642142, win 64240, options [msg 1460], length 0
06:10:15.851257 IP 10.203.142.101.46843 > 10.203.142.37.22: Flags [S], seq 697799838, win 512, length 0
06:10:15.852360 IP 10.203.142.37.22 > 10.203.142.101.46843: Flags [S], seq 2161981812, ack 697799831, win 64240, options [msg 1460], length 0
06:10:15.852427 IP 10.203.142.101.46844 > 10.203.142.37.22: Flags [S], seq 1748892627, win 512, length 0
06:10:15.852436 IP 10.203.142.37.22 > 10.203.142.101.46844: Flags [S], seq 12694769, ack 2090189511, win 64240, options [msg 1460], length 0
06:10:15.852427 IP 10.203.142.101.46845 > 10.203.142.37.22: Flags [S], seq 1989718453, win 512, length 0
06:10:15.852566 IP 10.203.142.37.22 > 10.203.142.101.46845: Flags [S], seq 3829522466, ack 1989718454, win 64240, options [msg 1460], length 0
06:10:15.852428 IP 10.203.142.101.46846 > 10.203.142.37.22: Flags [S], seq 797883311, win 512, length 0
06:10:15.852581 IP 10.203.142.37.22 > 10.203.142.101.46846: Flags [S], seq 796588589, ack 797883312, win 64240, options [msg 1460], length 0
06:10:15.852428 IP 10.203.142.101.46847 > 10.203.142.37.22: Flags [S], seq 1864985718, win 512, length 0
06:10:15.852662 IP 10.203.142.37.22 > 10.203.142.101.46847: Flags [S], seq 3677294859, ack 1864985717, win 64240, options [msg 1460], length 0
06:10:15.852428 IP 10.203.142.101.46848 > 10.203.142.37.22: Flags [S], seq 318872296, win 512, length 0
06:10:15.852763 IP 10.203.142.37.22 > 10.203.142.101.46848: Flags [S], seq 1620951858, ack 318872297, win 64240, options [msg 1460], length 0
06:10:15.852428 IP 10.203.142.101.46849 > 10.203.142.37.22: Flags [S], seq 621245238, win 512, length 0
06:10:15.853629 IP 10.203.142.37.22 > 10.203.142.101.46849: Flags [S], seq 3483926215, ack 621245239, win 64240, options [msg 1460], length 0
```

Pada sisi Ubuntu Server, serangan port scanning dan DDoS terdeteksi melalui log jaringan yang menunjukkan lonjakan paket SYN secara masif ke port SSH. Log memperlihatkan banyak koneksi masuk dengan flag [S] dalam waktu yang sangat singkat, yang menandakan adanya upaya pembanjiran trafik ke layanan target.

Aktivitas ini menunjukkan bahwa setelah tahap pengintaian port dilakukan oleh penyerang, serangan dilanjutkan dengan DDoS

untuk mengganggu ketersediaan layanan. Meskipun layanan masih merespons sebagian permintaan, pola trafik yang terekam mencerminkan tekanan jaringan yang tinggi akibat serangan flood.

Hasil ini membuktikan bahwa sistem target, khususnya honeypot yang diimplementasikan, mampu mendeteksi dan mencatat serangan berlapis yang dimulai dari port scanning hingga serangan DDoS. Data log yang dihasilkan dapat digunakan untuk analisis karakteristik serangan serta sebagai dasar evaluasi keamanan layanan SSH.



## Format Hasil Pengujian

### Hasil Pengujian Penyerangan

No.	Pola Serangan	Nama Pengujian	Kondisi Sebelum (%)	Kondisi Sesudah (%)	Hasil (Terdeteksi atau Tidak Terdeeteksi)
1	Double	<i>Port Scanning &amp; Bruteforce</i>	0%	100%	Terdeteksi
2		<i>Bruteforce &amp; DDoS Attack</i>	0%	100%	Terdeteksi
3		<i>DDoS Attack &amp; Port Scanning</i>	0%	100%	Terdeteksi