

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:

- Mesin penyerang (attacker)

Sistem Operasi : Kali linux

Digunakan untuk melakukan simulasi serangan

- Mesin Target

Sistem Operasi : Ubuntu Server

Digunakan sebagai server yang menjalankan honeypot Cowrie.

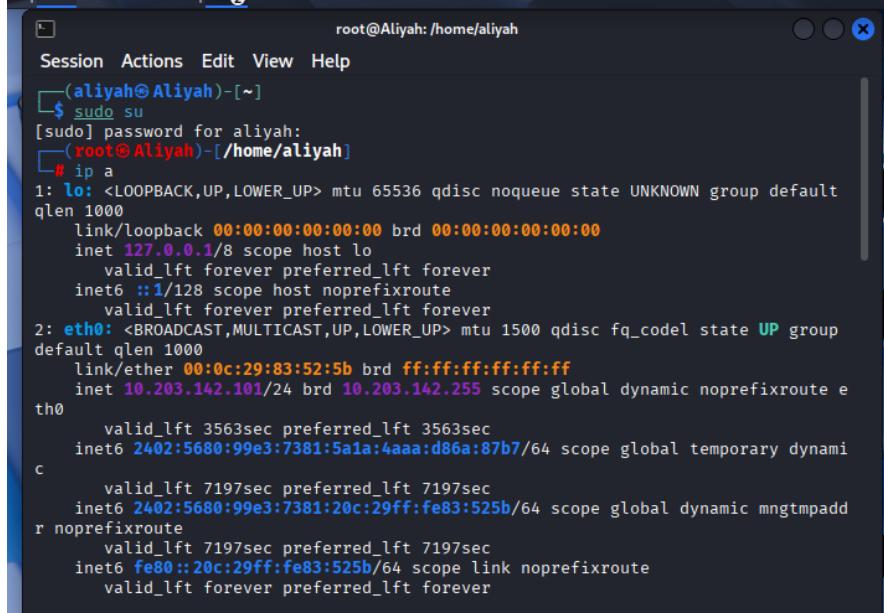
Kedua mesin dikonfigurasi berada dalam satu jaringan agar dapat saling berkomunikasi secara langsung. Konfigurasi jaringan dilakukan dengan menyamakan mode network adapter pada kedua mesin Virtual.

3. Konfigurasi Jaringan Awal

- 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 mngrtmpaddr 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

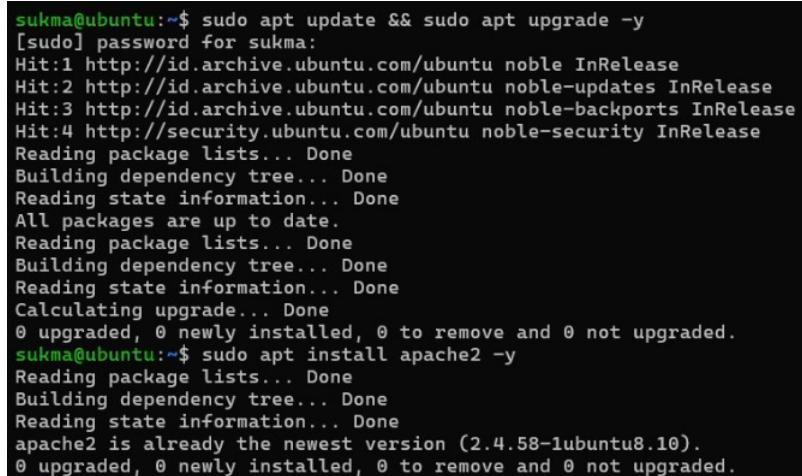


```
root@Aliyah:/home/aliyah
Session Actions Edit View Help
[aliyah@Aliyah] ~
$ sudo su
[sudo] password for aliyah:
[root@Aliyah] /home/aliyah
# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
qlen 1000
    link/loopback brd 00:00:00:00:00:00
    inet 127.0.0.1/8 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 2402:5680:99e3:7381:20c:29ff:fe83:525b/64 scope global temporary dynamic
r
        valid_lft 7197sec preferred_lft 7197sec
        inet6 2402:5680:99e3:7381:20c:29ff:fe83:525b/64 scope global dynamic mngtmpadd
r
        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-venc, 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-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:int
# 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 restart SSH dengan perintah berikut:

```
(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:(("twistd",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

```
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, 11:30:58) [GCC 13.3.0]
2026-01-28T15:47:45.118987Z [-] Twisted Version 25.5.0
2026-01-28T15:47:45.118984Z [-] Cowrie Version 2.9.9.dev9+g88bd5ffa6
2026-01-28T15:47:45.118985Z [-] Using configuration file: /home/sukma/cowrie/cowrie-env/bin/python3 3.12.3) starting up.
2026-01-28T15:47:45.124543Z [-] Loaded output engine: json
2026-01-28T15:47:45.125736Z [twisted.scripts._twistd_unix.UnixAppLogger#info] twistd 25.5.0 (/home/sukma/cowrie/cowrie-env/bin/python3 3.12.3) starting up.
2026-01-28T15:47:45.125813Z [twisted.scripts._twistd_unix.UnixAppLogger#info] reactor class: twisted.internet.epollreactor.EPollReactor.
2026-01-28T15:47:45.133062Z [-] 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 serangan pastikan terlebih dahulu bahwa tools yang digunakan sudah tersedia.

```
[root@Aliyah]# [root@Aliyah]# /home/aliyah]
# nmap --version
hydra -h
hpings3 --help

Nmap version 7.98 ( https://nmap.org )
Platform: x86_64-pc-linux-gnu
Compiled with: liblhu-5.4.8 openssl-1.3.5.4 libssh2-1.11.1 libz-1.3.1 libpcre2-10.46
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/TuC & 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 FILE] [-e nsr] [-o FILE] [-t TASKS] [-M FILE [-T TASKS]] [-w TIME] [-f] [-s PORT] [-x MIN:MAX :CHARSET] [-c TIME] [-ISOv4v6d4] [-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   choose a password space by specifying type -x "h" to get help
-y           use a non-random shuffling method for option -x
-z           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:~/homework/aliyah
Session Actions Edit View Help
x
[+] root@aliyah: /home/aliyah
[+] root@aliyah: /home/aliyah
ssh root@10.28.1.142 -p 37
The authenticity of host '10.28.1.142 (37.10.28.1.142.37)' can't be established.
The key fingerprint is SHA256:KzJLwQWfPjXqkVnDg9WfRIV0mAEH85
This host key is known by this host under the following other names/addresses:
  /sshKnownHosts2 [hashed name]
Are you sure you want to continue connecting (yes/no/[Fingerprint])? yes
Warning: Permanently added '10.28.1.142.37' (EDD5559) to the list of known hosts.
root@10.28.1.142:37% password:
root@10.28.1.142:37% password:
Permission denied, please try again.
root@10.28.1.142:37% password:
root@10.28.1.142:37% Permission denied (publickey,password).

[+] root@aliyah: /home/aliyah
[+] root@aliyah: /home/aliyah
[+] root@aliyah: /home/aliyah
ssh -p 10.28.1.142 -p 37

Starting Nmap 7.98 ( https://nmap.org ) at 2026-01-30 01:53 +0800
NSE: 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 1.56 seconds
[+] root@aliyah: /home/aliyah
[+] root@aliyah: /home/aliyah
[+] root@aliyah: /home/aliyah
ssh -p 10.28.1.142 -p 37

Starting Nmap 7.98 ( https://nmap.org ) at 2026-01-30 01:53 +0800
NSE: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap scan report for 10.28.1.142.37
Host is up (0.017s latency).
Nmap shown 1 port instead of 2 (tcp ports conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    closed http
2222/tcp  open  EtherNetPTP-1
MAC Address: C4:6E:D5:C4:71:83 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 1.16 seconds

root@aliyah:~/homework/aliyah
Session Actions Edit View Help
Connection to 10.28.1.142.37 closed.
[+] root@aliyah: /home/aliyah
[+] ssh -p 22 root@10.28.1.142 -p 37

** WARNING: connection is not using a post-quantum key exchange algorithm.
** This session may be vulnerable to "store now, decrypt later" attacks.
** The server may need to be upgraded. See https://openSSH.com/qtls.
root@10.28.1.142:37% password:

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
root@10.28.1.142:37% whoami
root@10.28.1.142:37% whoami
root@10.28.1.142:37% exit
Connection to 10.28.1.142.37 closed.

[+] root@aliyah: /home/aliyah
[+] ssh -p 22 root@10.28.1.142 -p 37

** WARNING: connection is not using a post-quantum key exchange algorithm.
** This session may be vulnerable to "store now, decrypt later" attacks.
** The server may need to be upgraded. See https://openSSH.com/qtls.
root@10.28.1.142:37% password:

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
root@10.28.1.142:37% whoami
root@10.28.1.142:37% uname -a
Linux scrub 3.2.64+ #1 SMP Debian 3.2.68-1+deb7u1 x86_64 GNU/Linux
root@10.28.1.142:37% ls
root@10.28.1.142:37% cd /root
root@10.28.1.142:37% exit
Connection to 10.28.1.142.37 closed.
```

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 mendekripsi dan menangkap aktivitas serangan tanpa memberikan akses ke sistem asli.

b. Ubuntu Server (Target)

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)

```

Session Actions Edit View Help
Starting Nmap 7.98 ( https://nmap.org ) at 2026-01-29 13:38 +0800
Nmap scan report for 10.203.142.37
Host is up (0.02s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.77 seconds

root@alayah:~# nmap -sV 10.203.142.37
PORT      STATE SERVICE
22/tcp    open  ssh
MAC Address: C4:0B:D5:C4:71:03 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.77 seconds

root@alayah:~# ssh -p 22 sukma01@10.203.142.37
root@alayah:~# ssh -p 22 sukma01@10.203.142.37

** WARNING: connection is not using a post-quantum key exchange algorithm.
** This session may be vulnerable to "store now, decrypt later" attacks.
** The password may need to be upgraded. See https://openSSH.com/pq.html
sukma01@10.203.142.37's password:
Permission denied, please try again.
sukma01@10.203.142.37: Permission denied (publickey,password).
sukma01@10.203.142.37: Permission denied (publickey,password).

root@alayah:~# ssh -p 22 root@10.203.142.37
root@alayah:~# ssh -p 22 sukma01@10.203.142.37

** WARNING: connection is not using a post-quantum key exchange algorithm.
** This session may be vulnerable to "store now, decrypt later" attacks.
** The password may need to be upgraded. See https://openSSH.com/pq.html
root@10.203.142.37's password:
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual program's documentation /etc/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY; to the extent
permitted by applicable law,
root@alayah:~# whoami
root
root@alayah:~# ls
root@alayah:~# rm -rf /root
root@alayah:~# exit
Connection to 10.203.142.37 closed.

Session Actions Edit View Help
round-trip min/avg/max = 5.2/41.5/128.1 ms
root@alayah:~# ping -s 800000 10.203.142.37
PING 10.203.142.37 (10.203.142.37) 56(84) bytes of data.
lens=64 ip=10.203.142.37 ttl=64 DF id=4 sport=>2 Flags=SA seq=0 win=64240 rtt=63.7 ms
lens=64 ip=10.203.142.37 ttl=64 DF id=4 sport=>2 Flags=SA seq=1 win=64240 rtt=87.9 ms
lens=64 ip=10.203.142.37 ttl=64 DF id=8 sport=>2 Flags=SA seq=2 win=64240 rtt=110.7 ms
lens=64 ip=10.203.142.37 ttl=64 DF id=8 sport=>2 Flags=SA seq=3 win=64240 rtt=134.2 ms
lens=64 ip=10.203.142.37 ttl=64 DF id=8 sport=>2 Flags=SA seq=4 win=64240 rtt=161.7 ms
lens=64 ip=10.203.142.37 ttl=64 DF id=8 sport=>2 Flags=SA seq=5 win=64240 rtt=182.7 ms
lens=64 ip=10.203.142.37 ttl=64 DF id=8 sport=>2 Flags=SA seq=6 win=64240 rtt=198.6 ms
lens=64 ip=10.203.142.37 ttl=64 DF id=8 sport=>2 Flags=SA seq=7 win=64240 rtt=209.8 ms
lens=64 ip=10.203.142.37 ttl=64 DF id=8 sport=>2 Flags=SA seq=8 win=64240 rtt=235.8 ms
lens=64 ip=10.203.142.37 ttl=64 DF id=8 sport=>2 Flags=SA seq=9 win=64240 rtt=278.5 ms
lens=64 ip=10.203.142.37 ttl=64 DF id=8 sport=>2 Flags=SA seq=10 win=64240 rtt=308.1 ms
lens=64 ip=10.203.142.37 ttl=64 DF id=8 sport=>2 Flags=SA seq=11 win=64240 rtt=633.3 ms
lens=64 ip=10.203.142.37 ttl=64 DF id=8 sport=>2 Flags=SA seq=12 win=64240 rtt=448.9 ms
lens=64 ip=10.203.142.37 ttl=64 DF id=8 sport=>2 Flags=SA seq=14 win=64240 rtt=487.9 ms
lens=64 ip=10.203.142.37 ttl=64 DF id=8 sport=>2 Flags=SA seq=15 win=64240 rtt=511.1 ms
lens=64 ip=10.203.142.37 ttl=64 DF id=8 sport=>2 Flags=SA seq=16 win=64240 rtt=538.7 ms
lens=64 ip=10.203.142.37 ttl=64 DF id=8 sport=>2 Flags=SA seq=17 win=64240 rtt=536.6 ms
lens=64 ip=10.203.142.37 ttl=64 DF id=8 sport=>2 Flags=SA seq=18 win=64240 rtt=535.1 ms
lens=64 ip=10.203.142.37 ttl=64 DF id=8 sport=>2 Flags=SA seq=19 win=64240 rtt=530.0 ms
lens=64 ip=10.203.142.37 ttl=64 DF id=8 sport=>2 Flags=SA seq=20 win=64240 rtt=523.9 ms

```

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

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

```
sukman@ubuntu: ~/cowrie
```

06:05:33.9342436 IP 10.263.142.101.5271 > 10.263.142.37.22: Flags [S], seq 976813149, win 512, length 0
06:05:33.9342436 IP 10.263.142.101.5272 > 10.263.142.37.22: Flags [S], seq 1774885141, win 512, length 0
06:05:33.9342436 IP 10.263.142.101.5273 > 10.263.142.37.22: Flags [S], seq 7179806227, win 512, length 0
06:05:33.9342436 IP 10.263.142.101.5274 > 10.263.142.37.22: Flags [S], seq 1774885142, win 512, length 0
06:05:33.9342437 IP 10.263.142.101.5275 > 10.263.142.37.22: Flags [S], seq 1878301818, win 512, length 0
06:05:33.9342437 IP 10.263.142.101.5276 > 10.263.142.37.22: Flags [S], seq 595593618, win 512, length 0
06:05:33.9342437 IP 10.263.142.101.5277 > 10.263.142.37.22: Flags [S], seq 1949275921, win 512, length 0
06:05:33.9342446 IP 10.263.142.101.5278 > 10.263.142.37.22: Flags [S], seq 2585626271, ack 13194789571, win 64248, options [mss 1460]
06:05:33.9342446 IP 10.263.142.101.5279 > 10.263.142.37.22: Flags [S], seq 12913967833, ack 17488481342, win 64248, options [mss 1460]
06:05:33.9342446 IP 10.263.142.101.5279 > 10.263.142.37.22: Flags [S], seq 12913967833, ack 17488481342, win 64248, options [mss 1460]
06:05:33.9433034 IP 10.263.142.101.5272 > 10.263.142.37.22: Flags [S], seq 4099138482, ack 1710786268, win 64248, options [mss 1460]
06:05:33.9434956 IP 10.263.142.101.5274 > 10.263.142.37.22: Flags [S], seq 2146597179, ack 1973133295, win 64248, options [mss 1460]
06:05:33.9434956 IP 10.263.142.101.5274 > 10.263.142.37.22: Flags [S], seq 2146597179, ack 1973133295, win 64248, options [mss 1460]
06:05:33.9434956 IP 10.263.142.101.5275 > 10.263.142.37.22: Flags [S], seq 5364358507, ack 1569583219, win 64248, options [mss 1460]
06:05:33.9443138 IP 10.263.142.101.5277 > 10.263.142.37.22: Flags [S], seq 41176796462, ack 1949275922, win 64248, options [mss 1460]
06:05:33.9449486 IP 10.263.142.101.5278 > 10.263.142.37.22: Flags [S], seq 1281756268, win 512, length 0
06:05:33.9449487 IP 10.263.142.101.5279 > 10.263.142.37.22: Flags [S], seq 1423345658, win 512, length 0
06:05:33.9449487 IP 10.263.142.101.5280 > 10.263.142.37.22: Flags [S], seq 12913967833, ack 17488481342, win 64248, options [mss 1460]
06:05:33.9449487 IP 10.263.142.101.5281 > 10.263.142.37.22: Flags [S], seq 4466158184, win 512, length 0
06:05:33.9449487 IP 10.263.142.101.5282 > 10.263.142.37.22: Flags [S], seq 1993717122, win 512, length 0
06:05:33.9449487 IP 10.263.142.101.5283 > 10.263.142.37.22: Flags [S], seq 293015097, win 512, length 0
06:05:33.9449487 IP 10.263.142.101.5284 > 10.263.142.37.22: Flags [S], seq 793857111, win 512, length 0
06:05:33.9449487 IP 10.263.142.101.5285 > 10.263.142.37.22: Flags [S], seq 12913967833, ack 17488481342, win 64248, options [mss 1460]
06:05:33.9449513 IP 10.263.142.101.5278 > 10.263.142.37.22: Flags [S], seq 1177525644, ack 1215726639, win 64248, options [mss 1460]
06:05:33.9449682 IP 10.263.142.101.5279 > 10.263.142.37.22: Flags [S], seq 3252349248, ack 1343945556, win 64248, options [mss 1460]
06:05:33.9452657 IP 10.263.142.101.5280 > 10.263.142.37.22: Flags [S], seq 1393515316, ack 559690786, win 64248, options [mss 1460]
06:05:33.9452657 IP 10.263.142.101.5281 > 10.263.142.37.22: Flags [S], seq 3093515316, ack 559690786, win 64248, options [mss 1460]
06:05:33.9452657 IP 10.263.142.101.5282 > 10.263.142.37.22: Flags [S], seq 15165179842, ack 559690786, win 64248, options [mss 1460]
06:05:33.9456580 IP 10.263.142.101.5283 > 10.263.142.37.22: Flags [S], seq 1168255688, ack 392150698, win 64248, options [mss 1460]
06:05:33.9458920 IP 10.263.142.101.5284 > 10.263.142.37.22: Flags [S], seq 1192824899, ack 793857111, win 64248, options [mss 1460]
06:05:33.9462407 IP 10.263.142.101.5285 > 10.263.142.37.22: Flags [S], seq 18213967833, ack 975980965, win 64248, options [mss 1460]
06:05:33.9462407 IP 10.263.142.101.5286 > 10.263.142.37.22: Flags [S], seq 12913967833, ack 17488481342, win 64248, options [mss 1460]
06:05:33.9462407 IP 10.263.142.101.5287 > 10.263.142.37.22: Flags [S], seq 755248687, win 512, length 0
06:05:33.9462407 IP 10.263.142.101.5288 > 10.263.142.37.22: Flags [S], seq 755248687, win 512, length 0
06:05:33.9462407 IP 10.263.142.101.5289 > 10.263.142.37.22: Flags [S], seq 696451996, win 512, length 0
06:05:33.9465550 IP 10.263.142.101.5290 > 10.263.142.37.22: Flags [S], seq 5716658502, win 512, length 0
06:05:33.9465550 IP 10.263.142.101.5291 > 10.263.142.37.22: Flags [S], seq 601135956, win 512, length 0
06:05:33.9465550 IP 10.263.142.101.5292 > 10.263.142.37.22: Flags [S], seq 1319942359, win 512, length 0
06:05:33.9465550 IP 10.263.142.101.5293 > 10.263.142.37.22: Flags [S], seq 1542913916, win 512, length 0
06:05:33.9465765 IP 10.263.142.101.5294 > 10.263.142.37.22: Flags [S], seq 2927482356, ack 473215396, win 64248, options [mss 1460]
06:05:33.9465765 IP 10.263.142.101.5295 > 10.263.142.37.22: Flags [S], seq 2927482356, ack 473215396, win 64248, options [mss 1460]
06:05:33.9467966 IP 10.263.142.101.5296 > 10.263.142.37.22: Flags [S], seq 2809338576, ack 516656583, win 64248, options [mss 1460]
06:05:33.9472445 IP 10.263.142.101.5297 > 10.263.142.37.22: Flags [S], seq 284988653, ack 571665853, win 64248, options [mss 1460]

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

terlihat dari log jaringan yang menunjukkan banyak paket dengan flag [S] yang datang secara terus-menerus dari alamat IP penyerang dalam waktu singkat.

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 pembanjiran jaringan. Data ini membuktikan bahwa sistem berhasil mendeteksi aktivitas DDoS dan dapat digunakan untuk menganalisis karakteristik serangan berbasis flood terhadap layanan SSH.

5.3 Simulasi Serangan Port Scanning Dan Ddos

a. Kali linux (Attacker)

Pada tahap ini, penyerang melakukan kombinasi serangan port scanning dan DDoS terhadap server target. Serangan diawali dengan port scanning menggunakan nmap untuk mengidentifikasi port yang terbuka dan layanan yang aktif pada target. Hasil pemindaian menunjukkan bahwa layanan SSH pada port 22 dalam keadaan terbuka dan dapat diakses.

Setelah port target berhasil diidentifikasi, penyerang melanjutkan dengan serangan DDoS menggunakan teknik SYN flood. Serangan ini dilakukan dengan mengirimkan paket SYN

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)

```

06:18:15.835066 IP 10.283.142.37.22 > 10.283.142.101.46754: Flags [S], seq 23668510967, ack 1326885061, win 642408, options [mss 1460], length 0
06:18:15.835067 IP 10.283.142.101.46755 > 10.283.142.37.22: Flags [S], seq 1658919555, win 512, length 0
06:18:15.835068 IP 10.283.142.37.22 > 10.283.142.101.46754: Flags [S], seq 1326885061, win 642408, options [mss 1460], length 0
06:18:15.835267 IP 10.283.142.101.46756 > 10.283.142.37.22: Flags [S], seq 1821880899, win 512, length 0
06:18:15.835268 IP 10.283.142.37.22 > 10.283.142.101.46754: Flags [S], seq 13417877897, ack 1821880899, win 642408, options [mss 1460], length 0
06:18:15.835269 IP 10.283.142.101.46757 > 10.283.142.37.22: Flags [S], seq 13273438667, ack 7523724041, win 642408, options [mss 1460], length 0
06:18:15.835270 IP 10.283.142.37.22 > 10.283.142.101.46758: Flags [S], seq 1161551351, win 512, length 0
06:18:15.835271 IP 10.283.142.101.46759 > 10.283.142.37.22: Flags [S], seq 2265995711, win 512, length 0
06:18:15.835272 IP 10.283.142.37.22 > 10.283.142.101.46760: Flags [S], seq 1694216089, win 512, length 0
06:18:15.835273 IP 10.283.142.101.46761 > 10.283.142.37.22: Flags [S], seq 1265033051, ack 1949214081, win 642408, options [mss 1460], length 0
06:18:15.835274 IP 10.283.142.37.22 > 10.283.142.101.46762: Flags [S], seq 1573910383, win 512, length 0
06:18:15.835275 IP 10.283.142.101.46763 > 10.283.142.37.22: Flags [S], seq 1886712998, win 512, length 0
06:18:15.835276 IP 10.283.142.37.22 > 10.283.142.101.46764: Flags [S], seq 1821880899, win 642408, options [mss 1460], length 0
06:18:15.835277 IP 10.283.142.101.46765 > 10.283.142.37.22: Flags [S], seq 1573910383, ack 1821880899, win 642408, options [mss 1460], length 0
06:18:15.835278 IP 10.283.142.37.22 > 10.283.142.101.46766: Flags [S], seq 1588671795, ack 1976415628, win 642408, options [mss 1460], length 0
06:18:15.835279 IP 10.283.142.101.46767 > 10.283.142.37.22: Flags [S], seq 1886712998, win 512, length 0
06:18:15.835280 IP 10.283.142.37.22 > 10.283.142.101.46768: Flags [S], seq 1821880899, win 642408, options [mss 1460], length 0
06:18:15.835281 IP 10.283.142.101.46769 > 10.283.142.37.22: Flags [S], seq 1886712998, ack 1821880899, win 642408, options [mss 1460], length 0
06:18:15.835282 IP 10.283.142.37.22 > 10.283.142.101.46770: Flags [S], seq 1799691916, ack 4045692918, win 642408, options [mss 1460], length 0
06:18:15.835283 IP 10.283.142.101.46771 > 10.283.142.37.22: Flags [S], seq 1821880899, win 642408, options [mss 1460], length 0
06:18:15.835284 IP 10.283.142.37.22 > 10.283.142.101.46772: Flags [S], seq 1384742109, ack 1821880899, win 642408, options [mss 1460], length 0
06:18:15.835285 IP 10.283.142.101.46773 > 10.283.142.37.22: Flags [S], seq 448631975, win 512, length 0
06:18:15.835286 IP 10.283.142.37.22 > 10.283.142.101.46774: Flags [S], seq 2083929385, ack 1821880899, win 642408, options [mss 1460], length 0
06:18:15.835287 IP 10.283.142.101.46775 > 10.283.142.37.22: Flags [S], seq 1873729346, ack 1821880899, win 642408, options [mss 1460], length 0
06:18:15.835288 IP 10.283.142.37.22 > 10.283.142.101.46776: Flags [S], seq 1889729346, win 512, length 0
06:18:15.835289 IP 10.283.142.101.46777 > 10.283.142.37.22: Flags [S], seq 2280828281, win 512, length 0
06:18:15.835290 IP 10.283.142.37.22 > 10.283.142.101.46778: Flags [S], seq 2933817958, ack 2028832882, win 642408, options [mss 1460], length 0
06:18:15.835291 IP 10.283.142.101.46779 > 10.283.142.37.22: Flags [S], seq 1821880899, win 642408, options [mss 1460], length 0
06:18:15.835292 IP 10.283.142.37.22 > 10.283.142.101.46780: Flags [S], seq 1821880899, ack 6639717107, win 642408, options [mss 1460], length 0
06:18:15.835293 IP 10.283.142.101.46781 > 10.283.142.37.22: Flags [S], seq 1877999268, win 512, length 0
06:18:15.835294 IP 10.283.142.37.22 > 10.283.142.101.46782: Flags [S], seq 2673299779, win 512, length 0
06:18:15.835295 IP 10.283.142.101.46783 > 10.283.142.37.22: Flags [S], seq 995869789, ack 2673299779, win 642408, options [mss 1460], length 0
06:18:15.835296 IP 10.283.142.37.22 > 10.283.142.101.46784: Flags [S], seq 1821880899, ack 1821880899, win 642408, options [mss 1460], length 0
06:18:15.835297 IP 10.283.142.101.46785 > 10.283.142.37.22: Flags [S], seq 1822294662, ack 1044337395, win 642408, options [mss 1460], length 0
06:18:15.835298 IP 10.283.142.37.22 > 10.283.142.101.46786: Flags [S], seq 1821880899, win 512, length 0
06:18:15.835299 IP 10.283.142.101.46787 > 10.283.142.37.22: Flags [S], seq 1823890297, win 512, length 0
06:18:15.835300 IP 10.283.142.37.22 > 10.283.142.101.46788: Flags [S], seq 1821880929, win 642408, options [mss 1460], length 0
06:18:15.835301 IP 10.283.142.101.46789 > 10.283.142.37.22: Flags [S], seq 1310617049, win 512, length 0
06:18:15.835302 IP 10.283.142.37.22 > 10.283.142.101.46790: Flags [S], seq 1821880929, ack 1118016768, win 642408, options [mss 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 Terdeteksi)
1	Double	<i>Port Scanning & Bruteforce</i>	0%	100%	Terdeteksi
2		<i>Bruteforce & DDoS Attack</i>	0%	100%	Terdeteksi
3		<i>DDoS Attack & Port Scanning</i>	0%	100%	Terdeteksi