LAPORAN ADVANCE NETWORK SECURITY AND PROTOCOLS

Implementasi Honeypot Cowrie untuk Deteksi Pola Penyerangan

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. 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

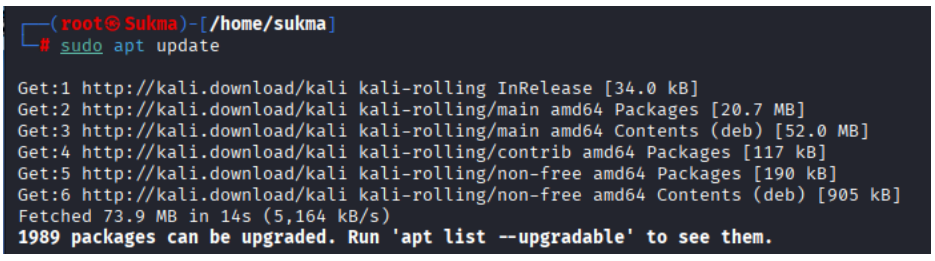
   Sistem Operasi : Ubuntu Server

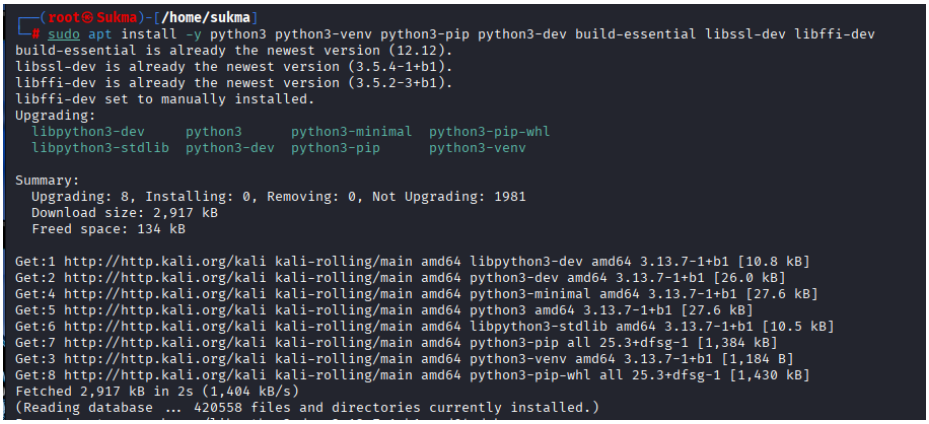
   Digunakan sebagai server yang menjalankan honeypot Cowrie.

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. Persiapan Awal Ubuntu Server

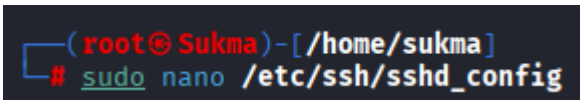
3.1 Update Sistem

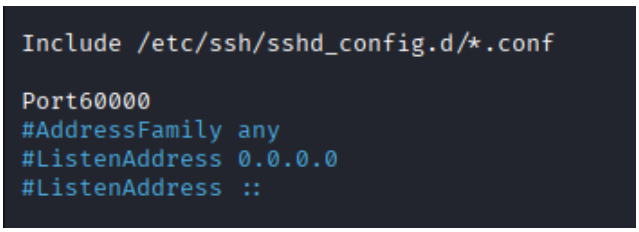




Update dilakukan untuk memastikan sistem berada pada kondisi terbaru dan menghindari konflik dependensi. Selanjutnya dilakukan instalasi beberapa paket pendukung seperti git, python3-venc, python3-pip, dan net-tools. Paket git digunakan untuk mengunduh source code honeypot Cowrie dari repositori resmi, 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.

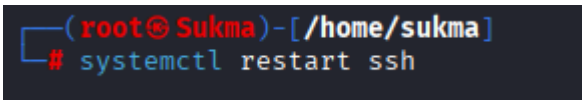
3.2 Mengubah Port Layanan SSH





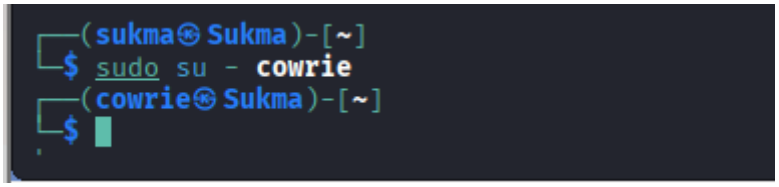
Pada tahap ini dilakukan perubahan konfigurasi layanan SSH dengan mengedit file sshd_config. Port SSH yang sebelumnya menggunakan port default 22 diubah menjadi port 60000. Perubahan ini bertujuan untuk meningkatkan keamanan server dengan mengurangi potensi serangan otomatis yang umumnya menargetkan port standar SSH.

3.3 Restrart Layanan SSH



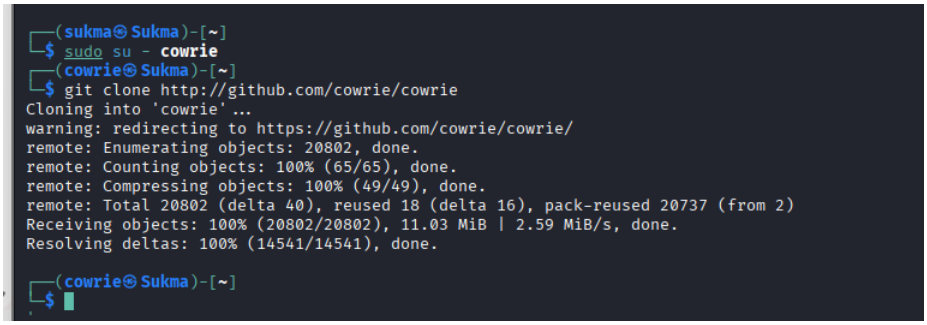
Setelah melakukan perubahan pada konfigurasi port SSH, layanan SSH perlu direstart agar pengaturan baru dapat diterapkan. Proses restart dilakukan menggunakan perintah systemctl restart ssh. Dengan langkah ini, server mulai menerima koneksi SSH melalui port yang telah ditentukan sebelumnya.

3.4 Masuk Ke User Non-Root dan Berpindah ke User Cowrie



Pada tahap ini, sistem tidak dijalankan menggunakan akun root. Pengguna terlebih dahulu masuk menggunakan user biasa, kemudian berpindah ke user khusus bernama cowrie. Penggunaan user non-root bertujuan untuk meningkatkan keamanan sistem dengan membatasi hak akses serta mengurangi risiko apabila terjadi penyalahgunaan atau serangan pada layanan yang dijalankan.

3.5 Clone Source Code Cowrie



Pada tahap ini dilakukan pengunduhan source code Cowrie dengan menggunakan perintah git clone dari repositori resmi GitHub. Proses ini bertujuan untuk memperoleh seluruh file dan struktur program yang diperlukan agar Cowrie dapat diinstal dan dikonfigurasi pada sistem server.

3.6 Setup Virtual Environment Cowrie

```
┌──(cowrie㉿Sukma)-[~]
└─$ cd cowrie

┌──(cowrie㉿Sukma)-[~/cowrie]
└─$ virtualenv --python=python3 cowrie-env
created virtual environment CPython3.13.7.final.0-64 in 1817ms
  creator CPython3Posix(dest=/home/cowrie/cowrie/cowrie-env, clear=False, no_vcs_ignore=False, global=False)
  seeder FromAppData(download=False, pip=bundle, via=copy, app_data_dir=/home/cowrie/.local/share/virtualenv)
    added seed packages: pip==25.3
  activators BashActivator,CShellActivator,FishActivator,NushellActivator,PowerShellActivator,PythonActivator

┌──(cowrie㉿Sukma)-[~/cowrie]
└─$ source cowrie-env/bin/activate
```

```
┌──(cowrie-env)(cowrie㉿Sukma)-[~/cowrie]
└─$ pip install --upgrade pip
Requirement already satisfied: pip in ./cowrie-env/lib/python3.13/site-packages (25.3)

┌──(cowrie-env)(cowrie㉿Sukma)-[~/cowrie]
└─$ pip install -r requirements.txt
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))
  Downloading service_identity-24.2.0-py3-none-any.whl.metadata (5.1 kB)
Collecting tftpy==0.8.6 (from -r requirements.txt (line 10))
  Downloading tftpy-0.8.6-py3-none-any.whl.metadata (5.6 kB)
Collecting treq==25.5.0 (from -r requirements.txt (line 11))
  Downloading treq-25.5.0-py3-none-any.whl.metadata (3.9 kB)
Collecting twisted==25.5.0 (from twisted[conch]==25.5.0→-r requirements.txt (line 12))
  Downloading twisted-25.5.0-py3-none-any.whl.metadata (22 kB)
Collecting urllib3==2.6.3 (from -r requirements.txt (line 13))
  Downloading urllib3-2.6.3-py3-none-any.whl.metadata (6.9 kB)
Collecting cffi≥2.0.0 (from cryptography==46.0.3→-r requirements.txt (line 3))
  Downloading cffi-2.0.0-cp313-cp313-manylinux2014_x86_64.manylinux_2_17_x86_64.whl.metadata (2.6 kB)
Collecting pyasn1<0.7.0,≥0.6.1 (from pyasn1_modules==0.4.2→-r requirements.txt (line 7))
  Downloading pyasn1-0.6.2-py3-none-any.whl.metadata (8.4 kB)
Collecting charset_normalizer<4,≥2 (from requests==2.32.5→-r requirements.txt (line 8))
  Downloading charset_normalizer-3.4.4-cp313-cp313-manylinux2014_x86_64.manylinux_2_17_x86_64.manylinux_2_28_x86_64
.whl.metadata (37 kB)
Collecting certifi≥2017.4.17 (from requests==2.32.5→-r requirements.txt (line 8))
  Downloading certifi-2026.1.4-py3-none-any.whl.metadata (2.5 kB)
Collecting incremental≥24.7.2 (from treq==25.5.0→-r requirements.txt (line 11))
  Downloading incremental-24.11.0-py3-none-any.whl.metadata (9.5 kB)
Collecting multipart (from treq==25.5.0→-r requirements.txt (line 11))
  Downloading multipart-1.3.0-py3-none-any.whl.metadata (4.9 kB)
Collecting typing-extensions≥3.10.0 (from treq==25.5.0→-r requirements.txt (line 11))
  Downloading typing_extensions-4.15.0-py3-none-any.whl.metadata (3.3 kB)
Collecting automat≥24.8.0 (from twisted==25.5.0→twisted[conch]==25.5.0→-r requirements.txt (line 12))
```

Pada tahap ini dilakukan aktivasi virtual environment Cowrie menggunakan perintah source cowrie-env/bin/activate, yang bertujuan untuk memastikan seluruh proses instalasi berjalan dalam lingkungan terisolasi. Setelah virtual environment aktif, dilakukan pembaruan pip serta instalasi seluruh dependensi Cowrie melalui file requirements.txt. Proses ini memastikan semua library yang dibutuhkan Cowrie terpasang dengan benar sehingga sistem siap untuk tahap konfigurasi dan pengoperasian selanjutnya.

3.7 Menyalin File Konfigurasi Cowrie

```
┌──(cowrie-env)(cowrie㉿Sukma)-[~/cowrie]
└─$ cd etc

┌──(cowrie-env)(cowrie㉿Sukma)-[~/cowrie/etc]
└─$ dir cowrie.cfg.dist userdb.example
cowrie.cfg.dist  userdb.example

┌──(cowrie-env)(cowrie㉿Sukma)-[~/cowrie/etc]
└─$ cp cowrie.cfg.dist cowrie.cfg
```

Pada tahap ini dilakukan penyalinan file konfigurasi default Cowrie dengan menyalin file cowrie.cfg.dist menjadi cowrie.cfg di dalam direktori cowrie/etc. File ini selanjutnya digunakan sebagai file konfigurasi utama yang dapat dimodifikasi sesuai kebutuhan sistem sebelum Cowrie dijalankan.

3.8 Instalasi Cowrie

```
┌──(cowrie-env)(cowrie㉿Sukma)-[~/cowrie]
└─$ pip install -e .
Obtaining file:///home/cowrie/cowrie
  Installing build dependencies ... done
  Checking if build backend supports build_editable ... done
  Getting requirements to build editable ... done
  Installing backend dependencies ... done
  Preparing editable metadata (pyproject.toml) ... done
Requirement already satisfied: attrs>=25.4.0 in ./cowrie-env/lib/python3.13/site-packages (from cowrie==2.9.9.dev9+g88b65ffa6) (25.4.0)
Requirement already satisfied: bcrypt>=5.0.0 in ./cowrie-env/lib/python3.13/site-packages (from cowrie==2.9.9.dev9+g88b65ffa6) (5.0.0)
Requirement already satisfied: cryptography>=46.0.3 in ./cowrie-env/lib/python3.13/site-packages (from cowrie==2.9.9.dev9+g88b65ffa6) (46.0.3)
Requirement already satisfied: hyperlink>=21.0.0 in ./cowrie-env/lib/python3.13/site-packages (from cowrie==2.9.9.dev9+g88b65ffa6) (21.0.0)
Requirement already satisfied: idna>=3.11 in ./cowrie-env/lib/python3.13/site-packages (from cowrie==2.9.9.dev9+g88b65ffa6) (3.11)
Requirement already satisfied: packaging>=26.0 in ./cowrie-env/lib/python3.13/site-packages (from cowrie==2.9.9.dev9+g88b65ffa6) (26.0)
Requirement already satisfied: pyasn1_modules>=0.4.2 in ./cowrie-env/lib/python3.13/site-packages (from cowrie==2.9.9.dev9+g88b65ffa6) (0.4.2)
Requirement already satisfied: requests>=2.32.5 in ./cowrie-env/lib/python3.13/site-packages (from cowrie==2.9.9.dev9+g88b65ffa6) (2.32.5)
Requirement already satisfied: service_identity>=24.2.0 in ./cowrie-env/lib/python3.13/site-packages (from cowrie==2.9.9.dev9+g88b65ffa6) (24.2.0)
Requirement already satisfied: tftpy>=0.8.6 in ./cowrie-env/lib/python3.13/site-packages (from cowrie==2.9.9.dev9+g88b65ffa6) (0.8.6)
Requirement already satisfied: treq>=25.5.0 in ./cowrie-env/lib/python3.13/site-packages (from cowrie==2.9.9.dev9+g88b65ffa6) (25.5.0)
Requirement already satisfied: twisted>=25.5.0 in ./cowrie-env/lib/python3.13/site-packages (from twisted[conch]>=25.5.0->cowrie==2.9.9.dev9+g88b65ffa6) (25.5.0)
Requirement already satisfied: cffi>=2.0.0 in ./cowrie-env/lib/python3.13/site-packages (from cryptography>=46.0.3->cowrie==2.9.9.dev9+g88b65ffa6) (2.0.0)
Requirement already satisfied: pyasn1<0.7.0,>=0.6.1 in ./cowrie-env/lib/python3.13/site-packages (from pyasn1_modules>=0.4.2->cowrie==2.9.9.dev9+g88b65ffa6) (0.6.2)
Requirement already satisfied: charset_normalizer<4,>=2 in ./cowrie-env/lib/python3.13/site-packages (from requests>=2.32.5->cowrie==2.9.9.dev9+g88b65ffa6) (3.4.4)
Requirement already satisfied: urllib3<3,>=1.21.1 in ./cowrie-env/lib/python3.13/site-packages (from requests>=2.32.5->cowrie==2.9.9.dev9+g88b65ffa6) (2.6.3)
Requirement already satisfied: certifi>=2017.4.17 in ./cowrie-env/lib/python3.13/site-packages (from requests>=2.32.5->cowrie==2.9.9.dev9+g88b65ffa6) (2026.1.4)
Requirement already satisfied: incremental>=24.7.2 in ./cowrie-env/lib/python3.13/site-packages (from treq>=25.5.0->cowrie==2.9.9.dev9+g88b65ffa6) (24.11.0)
Requirement already satisfied: multipart in ./cowrie-env/lib/python3.13/site-packages (from treq>=25.5.0->cowrie==2.9.9.dev9+g88b65ffa6) (1.3.0)
Requirement already satisfied: typing-extensions>=3.10.0 in ./cowrie-env/lib/python3.13/site-packages (from treq>=25.5.0->cowrie==2.9.9.dev9+g88b65ffa6) (4.15.0)
```

Pada tahap ini dilakukan instalasi Cowrie dengan menjalankan perintah instalasi menggunakan pip di dalam virtual environment. Proses instalasi ini memastikan seluruh modul dan dependensi yang dibutuhkan Cowrie terpasang dengan benar sehingga aplikasi siap untuk dikonfigurasi dan dijalankan sebagai honeypot SSH.

3.9 Modifikasi file konfigurasi Cowrie (cowrie.cfg)

```
[ssh]

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

```
listen_endpoints = tcp:22:interface=0.0.0.0

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

Pada tahap ini dilakukan pengeditan file konfigurasi cowrie.cfg untuk mengatur layanan SSH pada Cowrie. Port layanan diubah menjadi port 22 dengan menyesuaikan parameter listen_endpoints, sehingga Cowrie dapat mensimulasikan layanan SSH pada port standar. Setelah konfigurasi selesai, perubahan disimpan menggunakan kombinasi tombol CTRL+O dan keluar dari editor dengan CTRL+X.

3.10 Mengizinkan Port 22 untuk User Non-Root menggunakan Authbind

```
┌──(root㉿Sukma)-[/home/sukma]
└─# sudo apt-get update && sudo apt-get install authbind -y
Hit:1 http://http.kali.org/kali kali-rolling InRelease
Reading package lists ... Done
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following NEW packages will be installed:
  authbind
0 upgraded, 1 newly installed, 0 to remove and 1981 not upgraded.
Need to get 16.6 kB of archives.
After this operation, 76.8 kB of additional disk space will be used.
Get:1 http://xsrv.moratelindo.io/kali kali-rolling/main amd64 authbind amd64 2.2.0 [16.6 kB]
Fetched 16.6 kB in 1s (11.2 kB/s)
Selecting previously unselected package authbind.
(Reading database ... 80%
```

```
┌──(root㉿Sukma)-[/home/sukma]
└─# sudo touch /etc/authbind/byport/22

┌──(root㉿Sukma)-[/home/sukma]
└─# sudo chown cowrie:cowrie /etc/authbind/byport/22

┌──(root㉿Sukma)-[/home/sukma]
└─# sudo chmod 755 /etc/authbind/byport/22

┌──(root㉿Sukma)-[/home/sukma]
└─#
```

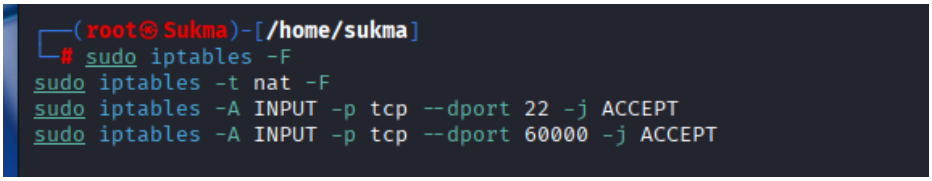
Pada tahap ini dilakukan instalasi dan konfigurasi authbind untuk mengizinkan user non-root menjalankan layanan pada port 22. File izin dibuat pada direktori /etc/authbind/byport/22, kemudian kepemilikan dan

hak akses diatur agar user cowrie dapat menggunakan port tersebut. Penggunaan authbind memungkinkan Cowrie berjalan pada port standar tanpa harus menggunakan hak akses root, sehingga keamanan sistem tetap terjaga.

3.11 Menjalankan Cowrie Menggunakan Authbind

Pada tahap ini Cowrie dijalankan menggunakan authbind agar layanan honeypot dapat berjalan pada port 22 tanpa menggunakan hak akses root. Proses dijalankan melalui perintah authbind --deep cowrie start, dan keberhasilan ditandai dengan layanan Cowrie yang aktif serta munculnya informasi proses pada terminal. Dengan demikian, Cowrie siap menerima koneksi dan merekam aktivitas penyerang.

3.12 Konfigurasi Firewall (iptables)



Pada tahap ini dilakukan konfigurasi firewall dengan membersihkan seluruh aturan iptables yang ada, kemudian mengizinkan akses pada port 22 untuk layanan Cowrie dan port 60000 untuk akses administrator. Langkah ini bertujuan memastikan hanya port yang diperlukan saja yang terbuka, sehingga keamanan server tetap terjaga selama sistem honeypot berjalan.

3.13 Penginstalan LOIC

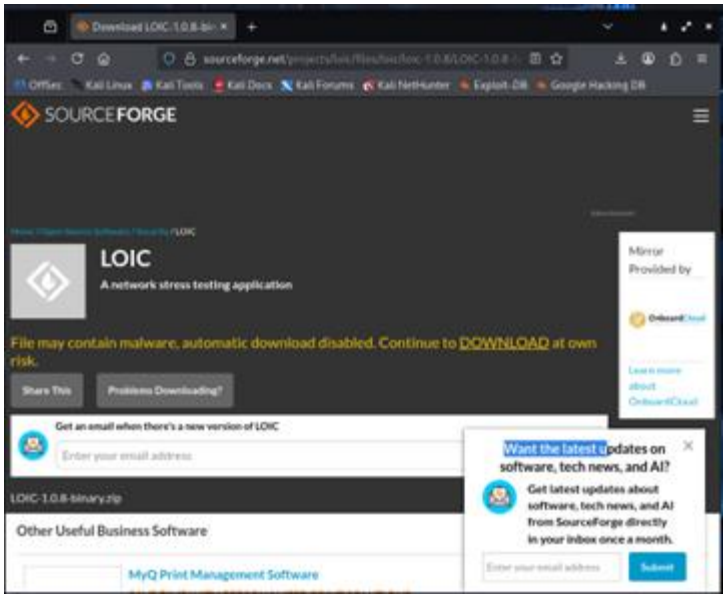
```
┌──(root㉿Aliyah)-[/home/aliyah]
└─# sudo apt update && sudo apt install mono-complete git -y

Hit:1 http://http.kali.org/kali kali-rolling InRelease
1767 packages can be upgraded. Run 'apt list --upgradable' to see them.
Note, selecting 'mono-devel' instead of 'mono-complete'
git is already the newest version (1:2.51.0-1).
The following packages were automatically installed and are no longer required:
  amass-common             libwsutil16
  libbluray2               libx264-164
  libbson-1.0-0t64         libxml2
  libconfig-inifiles-perl  python3-bluepy
  libjs-jquery-ui          python3-click-plugins
  libjs-underscore         python3-gpg
  libmongoc-1.0-0t64       python3-kismetcapturebtgeiger
  libmongocrypt0           python3-kismetcapturefreaklabszigbee
  libplacebo349            python3-kismetcapturertl433
  libportmidi0             python3-kismetcapturertladsb
  librav1e0.7              python3-kismetcapturertlamr
  libtheoradec1            python3-protobuf
  libtheoraenc1            python3-zombie-imp
  libudfread0              samba-ad-dc
  libwireshark18           samba-ad-provision
  libwiretap15             samba-dsdb-modules
Use 'sudo apt autoremove' to remove them.

Installing:
  mono-devel

Installing dependencies:
  libpkgconf3  pkgconf  pkgconf-bin

Summary:
  Upgrading: 0, Installing: 4, Removing: 0, Not Upgrading: 1767
  Download size: 49.9 MB
  Space needed: 174 MB / 26.0 GB available

Get:1 http://http.kali.org/kali kali-rolling/main amd64 libpkgconf3 amd64 1.8.1-4+
b1 [36.8 kB]
Get:2 http://http.kali.org/kali kali-rolling/main amd64 pkgconf-bin amd64 1.8.1-4+
b1 [30.6 kB]
Get:3 http://http.kali.org/kali kali-rolling/main amd64 pkgconf amd64 1.8.1-4+b1 [
26.5 kB]
```

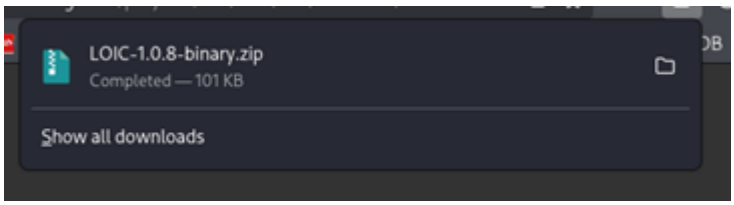
```
┌──(root㉿Aliyah)-[/home/aliyah]
└─# mono --version

Mono JIT compiler version 6.14.1 (tarball Mon Sep  1 13:00:08 UTC 2025)
Copyright (C) Novell, Inc, Xamarin Inc and Contributors. www.mono-project.com
        TLS:
        SIGSEGV:       altstack
        Notifications: epoll
        Architecture:  amd64
        Disabled:      none
        Misc:          softdebug
        Interpreter:   yes
        LLVM:          supported, not enabled.
        Suspend:       hybrid
        GC:            sgen (concurrent by default)

┌──(root㉿Aliyah)-[/home/aliyah]
└─#
```

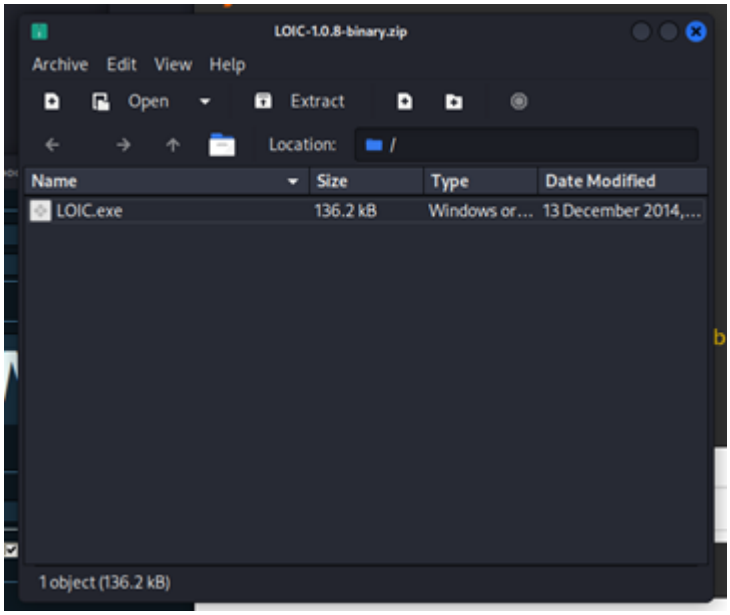
Sebelum masuk ke tahap pengujian serangan dilakukan penginstalan LOIC. Langkah ini bertujuan menyiapkan tools LOIC agar dapat digunakan pada tahap pengujian serangan DDoS. Pada tahap ini dilakukan pembaruan sistem serta instalasi dependensi yang dibutuhkan untuk menjalankan LOIC, yaitu paket mono-complete dan git. Setelah

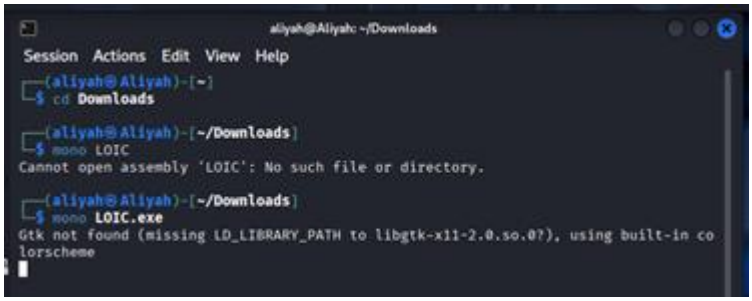
instalasi selesai, dilakukan pengecekan versi Mono untuk memastikan lingkungan runtime telah terpasang dengan benar.

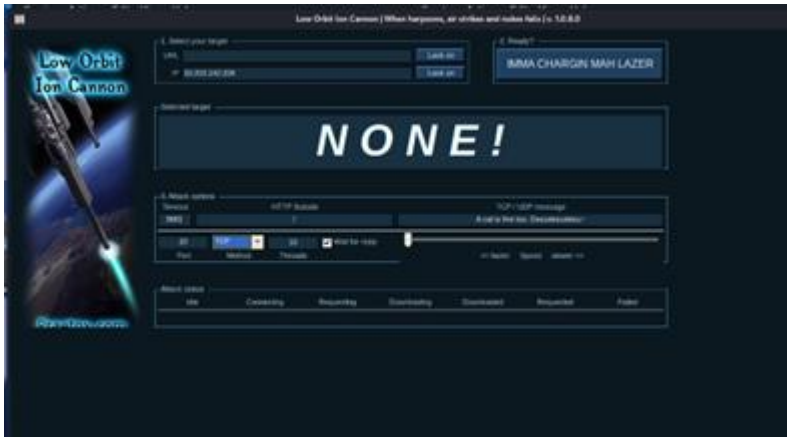
3.14 Mengunduh dan Menjalankan Aplikasi LOIC







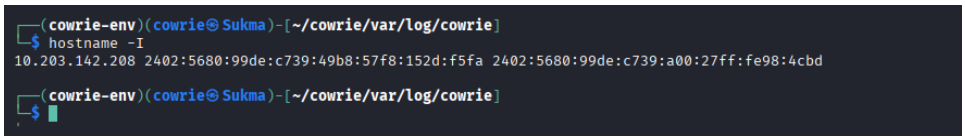




Pada tahap ini dilakukan pengunduhan aplikasi LOIC melalui situs resmi SourceForge. File yang diunduh berupa arsip LOIC-1.0.8-binary.zip, kemudian diekstrak hingga diperoleh file LOIC.exe. Aplikasi dijalankan menggunakan runtime Mono pada sistem Linux. Setelah berhasil dijalankan, antarmuka LOIC muncul yang menandakan aplikasi siap digunakan pada tahap pengujian selanjutnya.

4. Pengujian

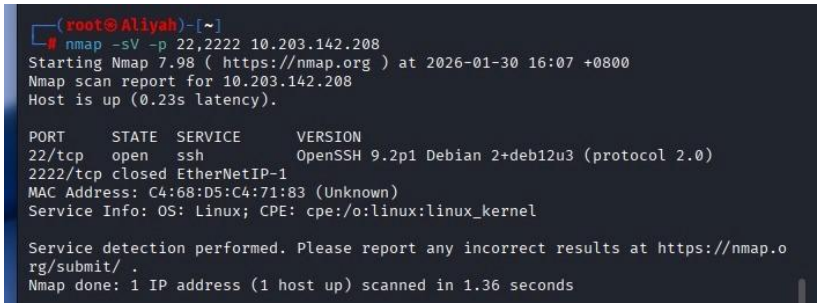
Mengetahui Alamat IP Server



4.1 Individual

- Port Scanning

A. Pengujian Port Scanning Menggunakan Nmap



Pada tahap ini dilakukan pengujian port scanning terhadap IP server menggunakan Nmap untuk mengetahui port yang terbuka pada sistem. Hasil pemindaian menunjukkan bahwa port 22/tcp dalam kondisi terbuka dan menjalankan layanan SSH, sedangkan port 2222/tcp berada dalam kondisi tertutup. Aktivitas pemindaian ini digunakan untuk mengamati bagaimana layanan pada server terdeteksi dari sisi penyerang serta sebagai dasar analisis keamanan pada tahap selanjutnya.

B. Analisis hasil Log file sesudah di lakukan nmap

Pada tahap ini dilakukan analisis terhadap file log Cowrie setelah pengujian port scanning menggunakan Nmap. Berdasarkan log yang dihasilkan, terlihat adanya aktivitas koneksi ke layanan SSH yang berasal dari alamat IP penyerang. Hal ini menunjukkan bahwa Cowrie berhasil merekam percobaan koneksi dan aktivitas pemindaian port, sehingga data log dapat digunakan sebagai bahan analisis pola serangan pada server.

- Brute Force

  Buat File yang berisi daftar Password

```
┌──(root㉿Aliyah)-[~]
└─# echo -e "password\n123456\nadmin\nrood\nqwery" > pass.txt
```

A. Pengujian Brute Force Menggunakan hydra

```
┌──(root㉿Aliyah)-[~]
└─# hydra -l root -P pass.txt 10.203.142.208 ssh
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in mili
tary or secret service organizations, or for illegal purposes (this is non-binding
, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2026-01-30 16:15:11
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recomm
ended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip wait
ing)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 5 tasks per 1 server, overall 5 tasks, 5 login tries (l:1/p:5), ~1 try
per task
[DATA] attacking ssh://10.203.142.208:22/
[22][ssh] host: 10.203.142.208   login: root   password: password
[22][ssh] host: 10.203.142.208   login: root   password: admin
[22][ssh] host: 10.203.142.208   login: root   password: rood
[22][ssh] host: 10.203.142.208   login: root   password: qwery
1 of 1 target successfully completed, 4 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2026-01-30 16:15:25
```

Pada tahap ini dilakukan pengujian brute force attack terhadap layanan SSH pada IP server menggunakan aplikasi Hydra. Pengujian dilakukan dengan memanfaatkan daftar password untuk mencoba proses login secara berulang. Hasil pengujian menunjukkan adanya beberapa kombinasi username dan password yang terdeteksi, serta seluruh aktivitas percobaan login tersebut berhasil direkam oleh sistem Cowrie sebagai data log untuk analisis keamanan.

B. Analisis hasil Log file sesudah di lakukan nmap

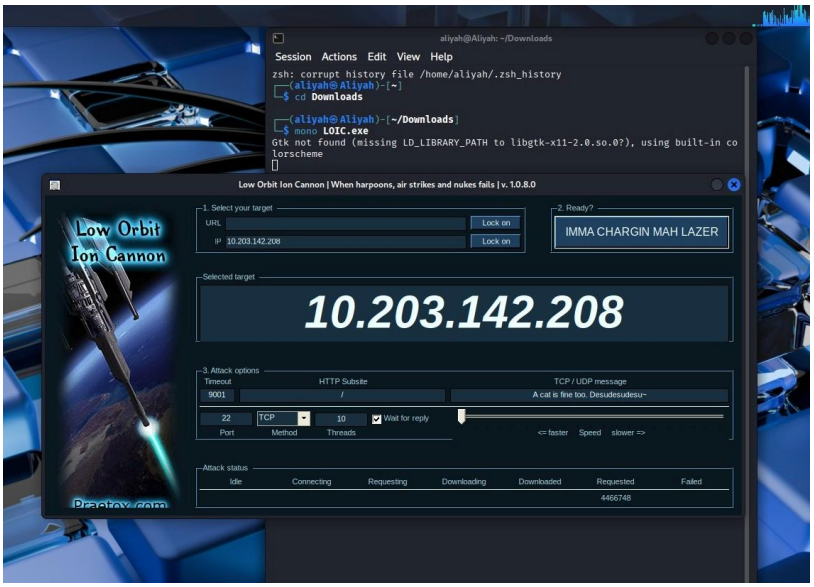
```
┌──(cowrie-env)(cowrie㉿Sukma)-[~/cowrie/var/log/cowrie]
└─$ tail -f cowrie.json
{"eventid":"cowrie.session.connect","src_ip":"10.203.142.101","src_port":58266,"dst_ip":"10.203.142.208","dst_port"
:22,"session":"d80a1ed07bd0","protocol":"ssh","message":"New connection: 10.203.142.101:58266 (10.203.142.208:22) [
session: d80a1ed07bd0]","sensor":"Sukma","uuid":"666a9ffa-fda4-11f0-a021-080027984cbd","timestamp":"2026-01-30T16:1
5:21.472042Z"}
{"eventid":"cowrie.client.version","version":"SSH-2.0-libssh_0.11.3","message":"Remote SSH version: SSH-2.0-libssh_
0.11.3","sensor":"Sukma","uuid":"666a9ffa-fda4-11f0-a021-080027984cbd","timestamp":"2026-01-30T16:15:21.472880Z","s
rc_ip":"10.203.142.101","session":"d80a1ed07bd0","protocol":"ssh"}
{"eventid":"cowrie.client.kex","hassh":"015322ee8471fa8338c558a918183b11","hasshAlgorithms":"diffie-hellman-group-e
xchange-sha1,diffie-hellman-group14-sha1,curve25519-sha256,curve25519-sha256@libssh.org,ecdh-sha2-nistp256,ecdh-sha
2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group18-sha512,diffie-hellman-group16-sha512,diffie-hellman-group-exch
ange-sha256,diffie-hellman-group14-sha256,ext-info-c,kex-strict-c-v00@openssh.com;chacha20-poly1305@openssh.com,aes
256-gcm@openssh.com,aes128-gcm@openssh.com,aes256-ctr,aes192-ctr,aes128-ctr;hmac-sha2-256-etm@openssh.com,hmac-sha2
-512-etm@openssh.com,hmac-sha2-256,hmac-sha2-512;none","kexAlgs":["diffie-hellman-group-exchange-sha1","diffie-hell
man-group14-sha1","curve25519-sha256","curve25519-sha256@libssh.org","ecdh-sha2-nistp256","ecdh-sha2-nistp384","ecd
h-sha2-nistp521","diffie-hellman-group18-sha512","diffie-hellman-group16-sha512","diffie-hellman-group-exchange-sha
256","diffie-hellman-group14-sha256","ext-info-c","kex-strict-c-v00@openssh.com"],"keyAlgs":["ssh-rsa","ssh-ed25519
","ecdsa-sha2-nistp521","ecdsa-sha2-nistp384","ecdsa-sha2-nistp256","sk-ssh-ed25519@openssh.com","sk-ecdsa-sha2-nis
tp256@openssh.com","rsa-sha2-512","rsa-sha2-256"],"encCS":["chacha20-poly1305@openssh.com","aes256-gcm@openssh.com"
,"aes128-gcm@openssh.com","aes256-ctr","aes192-ctr","aes128-ctr"],"macCS":["hmac-sha2-256-etm@openssh.com","hmac-sh
a2-512-etm@openssh.com","hmac-sha2-256","hmac-sha2-512"],"compCS":["none"],"langCS":[""],"message":"SSH client hass
h fingerprint: 015322ee8471fa8338c558a918183b11","sensor":"Sukma","uuid":"666a9ffa-fda4-11f0-a021-080027984cbd","ti
mestamp":"2026-01-30T16:15:21.485655Z","src_ip":"10.203.142.101","session":"d80a1ed07bd0","protocol":"ssh"}
{"eventid":"cowrie.session.closed","duration":"0.7","message":"Connection lost after 0.7 seconds","sensor":"Sukma",
"uuid":"666a9ffa-fda4-11f0-a021-080027984cbd","timestamp":"2026-01-30T16:15:22.192903Z","src_ip":"10.203.142.101","
session":"d80a1ed07bd0","protocol":"ssh"}
{"eventid":"cowrie.session.connect","src_ip":"10.203.142.101","src_port":58280,"dst_ip":"10.203.142.208","dst_port"
:22,"session":"a01687713933","protocol":"ssh","message":"New connection: 10.203.142.101:58280 (10.203.142.208:22) [
session: a01687713933]","sensor":"Sukma","uuid":"666a9ffa-fda4-11f0-a021-080027984cbd","timestamp":"2026-01-30T16:1
```

Pada tahap ini dilakukan analisis terhadap file log Cowrie setelah pengujian brute force menggunakan Hydra.

Berdasarkan log yang dihasilkan, terlihat adanya banyak percobaan koneksi SSH dengan berbagai kombinasi username dan password dari alamat IP penyerang. Cowrie berhasil merekam seluruh aktivitas tersebut, termasuk detail sesi, waktu koneksi, dan metode autentikasi, sehingga log dapat digunakan untuk menganalisis pola serangan brute force pada layanan SSH.

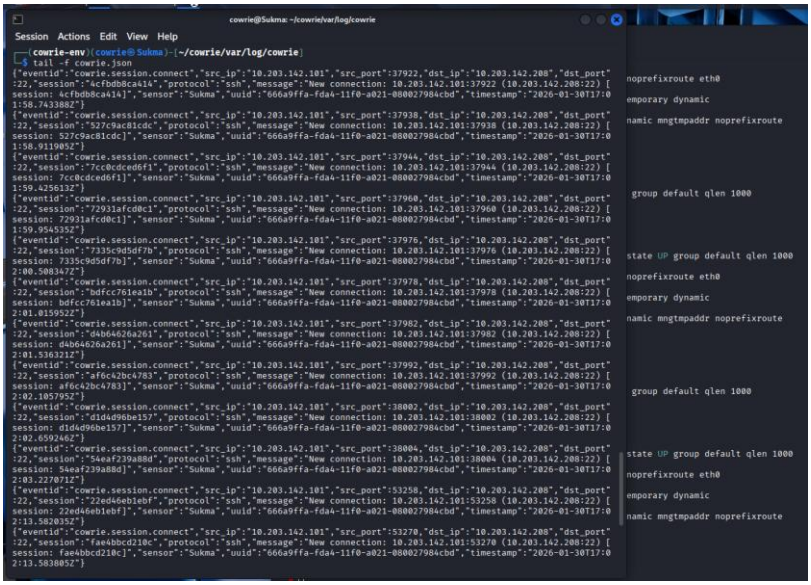
- DDoS

A. Melakukan serangan DdoS Menggunakan LOIC



Pada tahap ini dilakukan pengujian Distributed Denial of Service (DDoS) menggunakan aplikasi LOIC dengan menargetkan alamat IP server Cowrie. Serangan dilakukan dengan mengirimkan trafik secara terus-menerus ke target untuk mensimulasikan kondisi beban tinggi pada layanan. Pengujian ini bertujuan untuk mengamati respons sistem serta memastikan bahwa aktivitas serangan dapat direkam oleh Cowrie sebagai bagian dari data pengujian keamanan.

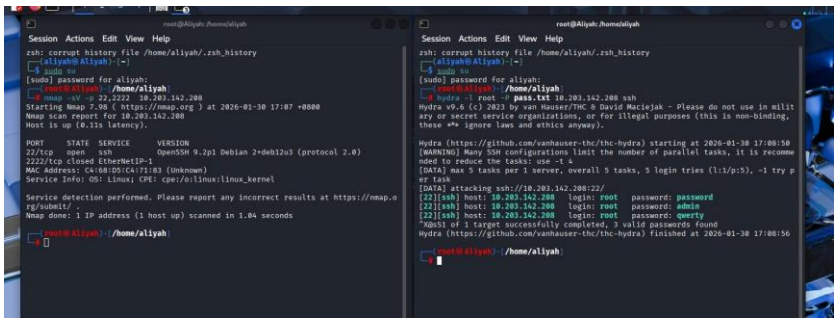
B. Analisis hasil DDoS Menggunakan LOIC



Pada tahap ini dilakukan analisis terhadap file log Cowrie setelah pengujian serangan DDoS menggunakan LOIC. Berdasarkan log yang dihasilkan, terlihat adanya peningkatan koneksi secara masif ke layanan SSH dari alamat IP penyerang dalam waktu yang singkat. Hal ini menunjukkan bahwa Cowrie berhasil merekam aktivitas serangan DDoS dan menyimpannya sebagai data log yang dapat digunakan untuk analisis dampak serta pola serangan terhadap server.

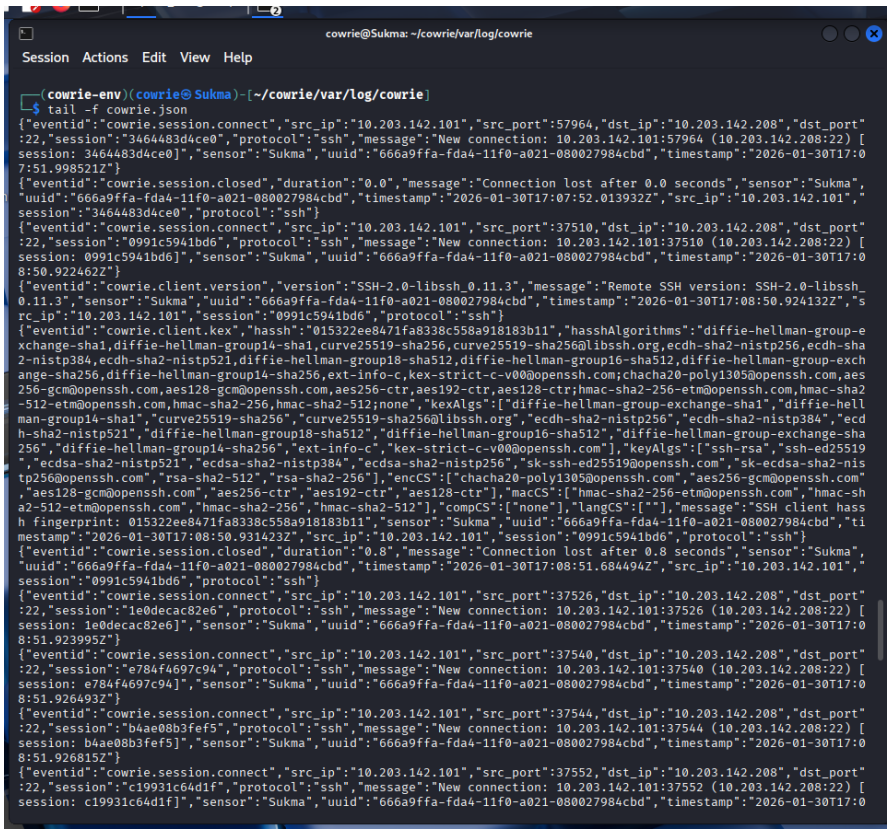
4.2 Double

- Pengujian Port Scanning & Brute Force



Pada tahap ini dilakukan pengujian double attack dengan mengombinasikan dua jenis serangan, yaitu port scanning

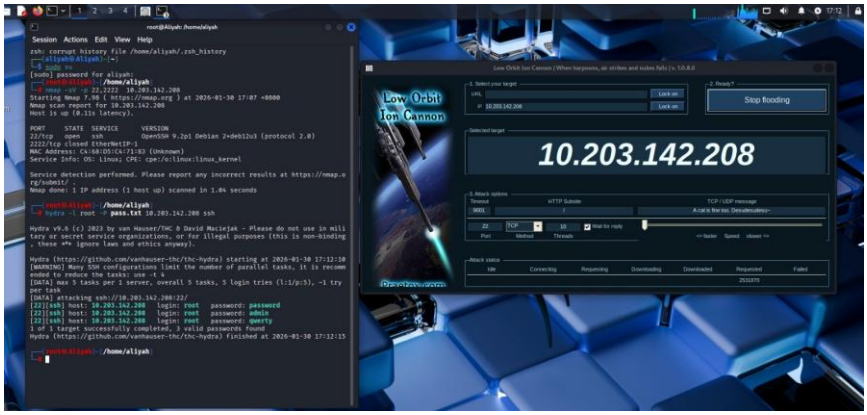
menggunakan Nmap dan brute force attack menggunakan Hydra, yang dijalankan secara berurutan terhadap IP server. Pengujian ini bertujuan untuk mensimulasikan kondisi serangan nyata, di mana penyerang terlebih dahulu melakukan pemindaian port untuk mengidentifikasi layanan aktif, kemudian melanjutkan dengan serangan brute force pada layanan SSH. Seluruh aktivitas serangan tersebut berhasil direkam oleh Cowrie dan tersimpan dalam log sebagai data analisis pola serangan ganda.



Pada tahap ini dilakukan analisis terhadap file log Cowrie setelah pengujian double attack, yaitu kombinasi pemindaian port dan percobaan koneksi berulang ke layanan SSH. Berdasarkan log yang ditampilkan, terlihat adanya banyak sesi koneksi SSH dari alamat IP penyerang dalam waktu yang berdekatan, disertai proses negosiasi protokol dan pertukaran algoritma kriptografi. Hal ini menunjukkan bahwa Cowrie berhasil mendeteksi serta merekam pola serangan ganda secara detail, sehingga data log yang dihasilkan

dapat digunakan untuk menganalisis intensitas dan karakteristik serangan terhadap server.

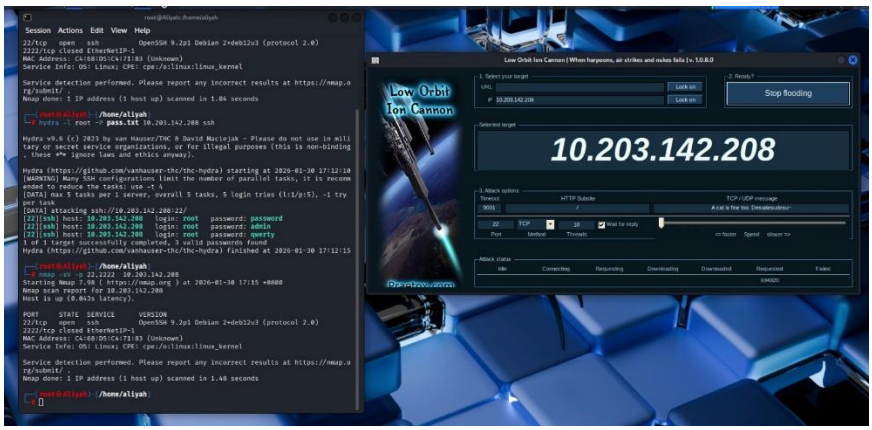
- Brute Force & DDoS



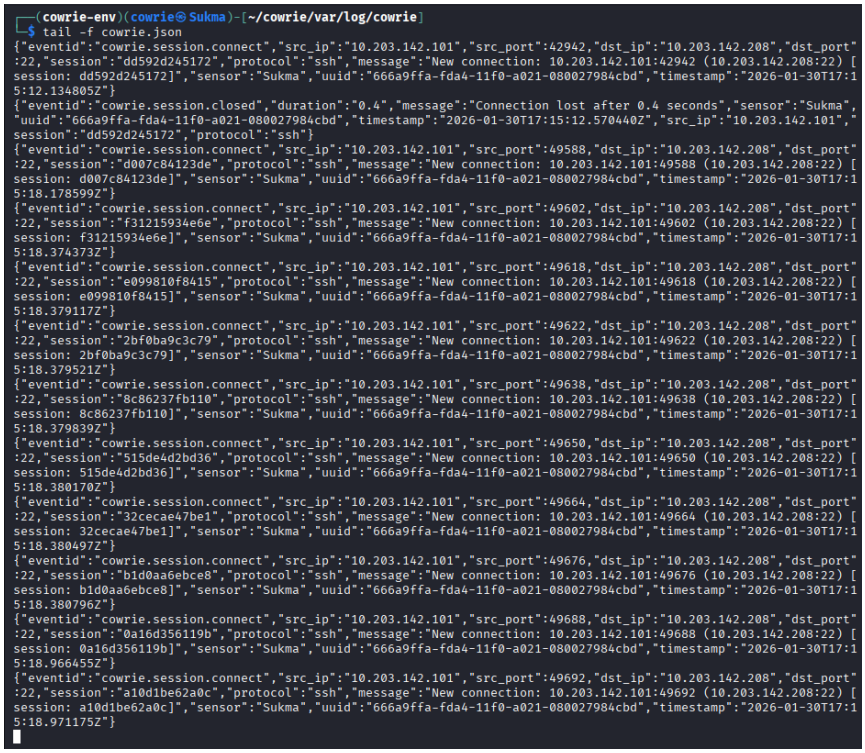
Pada tahap ini dilakukan pengujian double attack dengan mengombinasikan dua jenis serangan, yaitu brute force attack menggunakan Hydra dan serangan DDoS menggunakan LOIC, yang dijalankan terhadap IP server secara bersamaan. Brute force dilakukan untuk mencoba berbagai kombinasi username dan password pada layanan SSH, sementara serangan DDoS bertujuan membanjiri server dengan trafik secara terus-menerus. Pengujian ini mensimulasikan kondisi serangan nyata yang kompleks, di mana penyerang tidak hanya mencoba mengambil alih akses, tetapi juga mengganggu ketersediaan layanan.

Pada tahap ini dilakukan analisis terhadap file log Cowrie setelah pengujian double attack berupa kombinasi brute force SSH dan serangan DDoS. Berdasarkan log yang dihasilkan, terlihat adanya banyak koneksi SSH yang masuk secara berulang dari alamat IP penyerang dalam waktu yang sangat berdekatan, disertai proses negosiasi protokol dan pertukaran algoritma kriptografi. Kondisi ini menunjukkan bahwa server menerima beban koneksi tinggi akibat serangan DDoS, sekaligus percobaan akses berulang akibat brute force. Cowrie berhasil merekam seluruh aktivitas tersebut secara detail, sehingga log yang dihasilkan dapat digunakan untuk menganalisis pola dan intensitas serangan ganda terhadap layanan SSH.

- Port Sccanning & DDoS



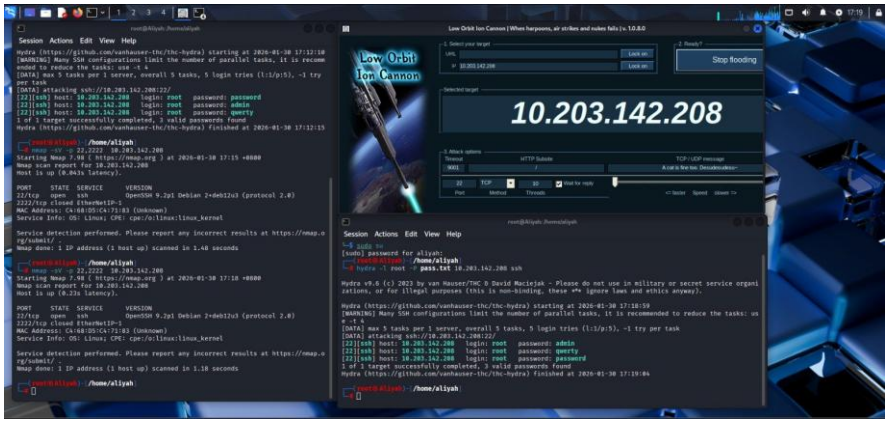
Pada tahap ini dilakukan pengujian double attack dengan mengombinasikan port scanning menggunakan Nmap dan serangan DDoS menggunakan LOIC terhadap IP server. Port scanning digunakan untuk mengidentifikasi port dan layanan yang aktif pada server, sementara serangan DDoS dilakukan untuk membanjiri server dengan trafik secara terus-menerus. Pengujian ini mensimulasikan kondisi serangan nyata, di mana penyerang melakukan pemetaan layanan sekaligus mengganggu ketersediaan server. Seluruh aktivitas serangan berlangsung secara bersamaan dan menjadi bagian dari pengujian ketahanan sistem.



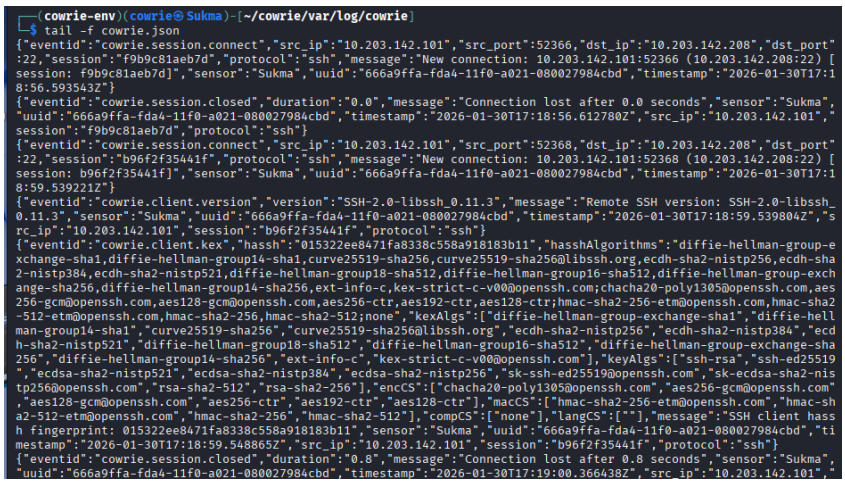
Pada tahap ini dilakukan analisis terhadap file log Cowrie setelah pengujian double attack berupa kombinasi port scanning dan serangan DDoS. Berdasarkan log yang dihasilkan, terlihat adanya banyak koneksi SSH baru dari alamat IP penyerang dengan port sumber yang berbeda-beda dalam waktu yang sangat singkat. Selain itu, terdapat sesi koneksi yang cepat terputus dengan durasi yang pendek, yang menunjukkan adanya lonjakan trafik akibat serangan DDoS. Hasil ini membuktikan bahwa Cowrie berhasil merekam aktivitas pemindaian layanan sekaligus beban koneksi tinggi secara bersamaan, sehingga log yang dihasilkan dapat digunakan untuk menganalisis pola dan intensitas serangan ganda terhadap server.

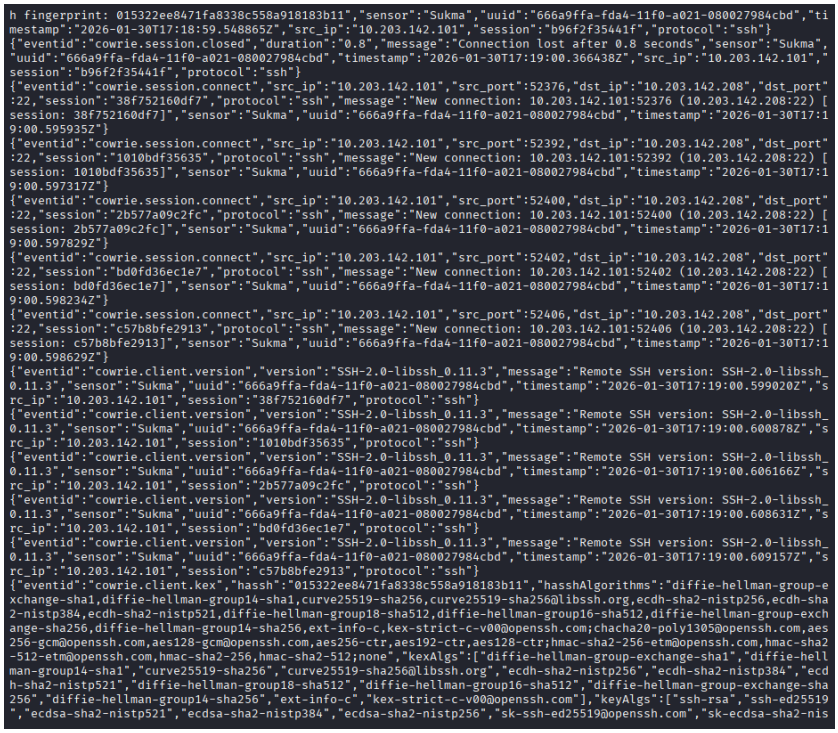
4.3 Multiple

- Port Scanning & Brute Force & DDoS

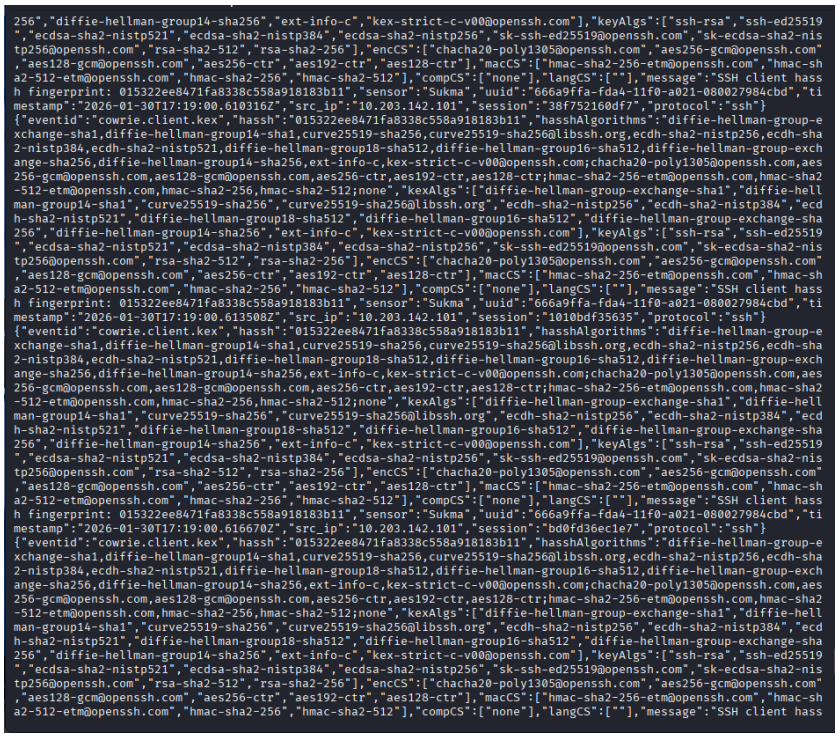


Pada tahap ini dilakukan pengujian multiple attack dengan menjalankan tiga jenis serangan secara bersamaan, yaitu port scanning menggunakan Nmap, brute force SSH menggunakan Hydra, dan serangan DDoS menggunakan LOIC terhadap IP server. Port scanning digunakan untuk mengidentifikasi layanan aktif pada server, brute force dilakukan untuk mencoba berbagai kombinasi kredensial SSH, sementara DDoS bertujuan membanjiri server dengan trafik dalam jumlah besar. Pengujian ini mensimulasikan kondisi serangan kompleks yang mendekati situasi nyata, di mana penyerang melakukan pemetaan layanan, upaya pengambilalihan akses, serta gangguan terhadap ketersediaan layanan secara simultan.





```
h fingerprint: 015322ee8471fa8338c558a918183b11","sensor":"Sukma","uuid":"666a9ffa-fda4-11f0-a021-080027984cbd","ti
mestamp":"2026-01-30T17:18:59.548865Z","src_ip":"10.203.142.101","session":"b96f2f35441f","protocol":"ssh"}
{"eventid":"cowrie.session.closed","duration":"0.8","message":"Connection lost after 0.8 seconds","sensor":"Sukma",
"uuid":"666a9ffa-fda4-11f0-a021-080027984cbd","timestamp":"2026-01-30T17:19:00.366438Z","src_ip":"10.203.142.101","
session":"b96f2f35441f","protocol":"ssh"}
{"eventid":"cowrie.session.connect","src_ip":"10.203.142.101","src_port":52376,"dst_ip":"10.203.142.208","dst_port"
:22,"session":"38f752160df7","protocol":"ssh","message":"New connection: 10.203.142.101:52376 (10.203.142.208:22) [
session: 38f752160df7]","sensor":"Sukma","uuid":"666a9ffa-fda4-11f0-a021-080027984cbd","timestamp":"2026-01-30T17:1
9:00.595935Z"}
{"eventid":"cowrie.session.connect","src_ip":"10.203.142.101","src_port":52392,"dst_ip":"10.203.142.208","dst_port"
:22,"session":"1010bdf35635","protocol":"ssh","message":"New connection: 10.203.142.101:52392 (10.203.142.208:22) [
session: 1010bdf35635]","sensor":"Sukma","uuid":"666a9ffa-fda4-11f0-a021-080027984cbd","timestamp":"2026-01-30T17:1
9:00.597317Z"}
{"eventid":"cowrie.session.connect","src_ip":"10.203.142.101","src_port":52400,"dst_ip":"10.203.142.208","dst_port"
:22,"session":"2b577a09c2fc","protocol":"ssh","message":"New connection: 10.203.142.101:52400 (10.203.142.208:22) [
session: 2b577a09c2fc]","sensor":"Sukma","uuid":"666a9ffa-fda4-11f0-a021-080027984cbd","timestamp":"2026-01-30T17:1
9:00.597829Z"}
{"eventid":"cowrie.session.connect","src_ip":"10.203.142.101","src_port":52402,"dst_ip":"10.203.142.208","dst_port"
:22,"session":"bd0fd36ec1e7","protocol":"ssh","message":"New connection: 10.203.142.101:52402 (10.203.142.208:22) [
session: bd0fd36ec1e7]","sensor":"Sukma","uuid":"666a9ffa-fda4-11f0-a021-080027984cbd","timestamp":"2026-01-30T17:1
9:00.598234Z"}
{"eventid":"cowrie.session.connect","src_ip":"10.203.142.101","src_port":52406,"dst_ip":"10.203.142.208","dst_port"
:22,"session":"c57b8bfe2913","protocol":"ssh","message":"New connection: 10.203.142.101:52406 (10.203.142.208:22) [
session: c57b8bfe2913]","sensor":"Sukma","uuid":"666a9ffa-fda4-11f0-a021-080027984cbd","timestamp":"2026-01-30T17:1
9:00.598629Z"}
{"eventid":"cowrie.client.version","version":"SSH-2.0-libssh_0.11.3","message":"Remote SSH version: SSH-2.0-libssh_
0.11.3","sensor":"Sukma","uuid":"666a9ffa-fda4-11f0-a021-080027984cbd","timestamp":"2026-01-30T17:19:00.599020Z","s
rc_ip":"10.203.142.101","session":"38f752160df7","protocol":"ssh"}
{"eventid":"cowrie.client.version","version":"SSH-2.0-libssh_0.11.3","message":"Remote SSH version: SSH-2.0-libssh_
0.11.3","sensor":"Sukma","uuid":"666a9ffa-fda4-11f0-a021-080027984cbd","timestamp":"2026-01-30T17:19:00.600878Z","s
rc_ip":"10.203.142.101","session":"1010bdf35635","protocol":"ssh"}
{"eventid":"cowrie.client.version","version":"SSH-2.0-libssh_0.11.3","message":"Remote SSH version: SSH-2.0-libssh_
0.11.3","sensor":"Sukma","uuid":"666a9ffa-fda4-11f0-a021-080027984cbd","timestamp":"2026-01-30T17:19:00.606166Z","s
rc_ip":"10.203.142.101","session":"2b577a09c2fc","protocol":"ssh"}
{"eventid":"cowrie.client.version","version":"SSH-2.0-libssh_0.11.3","message":"Remote SSH version: SSH-2.0-libssh_
0.11.3","sensor":"Sukma","uuid":"666a9ffa-fda4-11f0-a021-080027984cbd","timestamp":"2026-01-30T17:19:00.608631Z","s
rc_ip":"10.203.142.101","session":"bd0fd36ec1e7","protocol":"ssh"}
{"eventid":"cowrie.client.version","version":"SSH-2.0-libssh_0.11.3","message":"Remote SSH version: SSH-2.0-libssh_
0.11.3","sensor":"Sukma","uuid":"666a9ffa-fda4-11f0-a021-080027984cbd","timestamp":"2026-01-30T17:19:00.609157Z","s
rc_ip":"10.203.142.101","session":"c57b8bfe2913","protocol":"ssh"}
{"eventid":"cowrie.client.kex","hassh":"015322ee8471fa8338c558a918183b11","hasshAlgorithms":"diffie-hellman-group-e
xchange-sha1,diffie-hellman-group14-sha1,curve25519-sha256,curve25519-sha256@libssh.org,ecdh-sha2-nistp256,ecdh-sha
2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group18-sha512,diffie-hellman-group16-sha512,diffie-hellman-group-exch
ange-sha256,diffie-hellman-group14-sha256,ext-info-c,kex-strict-c-v00@openssh.com;chacha20-poly1305@openssh.com,aes
256-gcm@openssh.com,aes128-gcm@openssh.com,aes256-ctr,aes192-ctr,aes128-ctr;hmac-sha2-256-etm@openssh.com,hmac-sha2
-512-etm@openssh.com,hmac-sha2-256,hmac-sha2-512;none","kexAlgs":["diffie-hellman-group-exchange-sha1","diffie-hell
man-group14-sha1","curve25519-sha256","curve25519-sha256@libssh.org","ecdh-sha2-nistp256","ecdh-sha2-nistp384","ecd
h-sha2-nistp521","diffie-hellman-group18-sha512","diffie-hellman-group16-sha512","diffie-hellman-group-exchange-sha
256","diffie-hellman-group14-sha256","ext-info-c","kex-strict-c-v00@openssh.com"],"keyAlgs":["ssh-rsa","ssh-ed25519
","ecdsa-sha2-nistp521","ecdsa-sha2-nistp384","ecdsa-sha2-nistp256","sk-ssh-ed25519@openssh.com","sk-ecdsa-sha2-nis
```

```
256","diffie-hellman-group14-sha256","ext-info-c","kex-strict-c-v00@openssh.com"],"keyAlgs":["ssh-rsa","ssh-ed25519
","ecdsa-sha2-nistp521","ecdsa-sha2-nistp384","ecdsa-sha2-nistp256","sk-ssh-ed25519@openssh.com","sk-ecdsa-sha2-nis
tp256@openssh.com","rsa-sha2-512","rsa-sha2-256"],"encCS":["chacha20-poly1305@openssh.com","aes256-gcm@openssh.com"
,"aes128-gcm@openssh.com","aes256-ctr","aes192-ctr","aes128-ctr"],"macCS":["hmac-sha2-256-etm@openssh.com","hmac-sh
a2-512-etm@openssh.com","hmac-sha2-256","hmac-sha2-512"],"compCS":["none"],"langCS":[""],"message":"SSH client hass
h fingerprint: 015322ee8471fa8338c558a918183b11","sensor":"Sukma","uuid":"666a9ffa-fda4-11f0-a021-080027984cbd","ti
mestamp":"2026-01-30T17:19:00.610316Z","src_ip":"10.203.142.101","session":"38f752160df7","protocol":"ssh"}
{"eventid":"cowrie.client.kex","hassh":"015322ee8471fa8338c558a918183b11","hasshAlgorithms":"diffie-hellman-group-e
xchange-sha1,diffie-hellman-group14-sha1,curve25519-sha256,curve25519-sha256@libssh.org,ecdh-sha2-nistp256,ecdh-sha
2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group18-sha512,diffie-hellman-group16-sha512,diffie-hellman-group-exch
ange-sha256,diffie-hellman-group14-sha256,ext-info-c,kex-strict-c-v00@openssh.com;chacha20-poly1305@openssh.com,aes
256-gcm@openssh.com,aes128-gcm@openssh.com,aes256-ctr,aes192-ctr,aes128-ctr;hmac-sha2-256-etm@openssh.com,hmac-sha2
-512-etm@openssh.com,hmac-sha2-256,hmac-sha2-512;none","kexAlgs":["diffie-hellman-group-exchange-sha1","diffie-hell
man-group14-sha1","curve25519-sha256","curve25519-sha256@libssh.org","ecdh-sha2-nistp256","ecdh-sha2-nistp384","ecd
h-sha2-nistp521","diffie-hellman-group18-sha512","diffie-hellman-group16-sha512","diffie-hellman-group-exchange-sha
256","diffie-hellman-group14-sha256","ext-info-c","kex-strict-c-v00@openssh.com"],"keyAlgs":["ssh-rsa","ssh-ed25519
","ecdsa-sha2-nistp521","ecdsa-sha2-nistp384","ecdsa-sha2-nistp256","sk-ssh-ed25519@openssh.com","sk-ecdsa-sha2-nis
tp256@openssh.com","rsa-sha2-512","rsa-sha2-256"],"encCS":["chacha20-poly1305@openssh.com","aes256-gcm@openssh.com"
,"aes128-gcm@openssh.com","aes256-ctr","aes192-ctr","aes128-ctr"],"macCS":["hmac-sha2-256-etm@openssh.com","hmac-sh
a2-512-etm@openssh.com","hmac-sha2-256","hmac-sha2-512"],"compCS":["none"],"langCS":[""],"message":"SSH client hass
h fingerprint: 015322ee8471fa8338c558a918183b11","sensor":"Sukma","uuid":"666a9ffa-fda4-11f0-a021-080027984cbd","ti
mestamp":"2026-01-30T17:19:00.613508Z","src_ip":"10.203.142.101","session":"1010bdf35635","protocol":"ssh"}
{"eventid":"cowrie.client.kex","hassh":"015322ee8471fa8338c558a918183b11","hasshAlgorithms":"diffie-hellman-group-e
xchange-sha1,diffie-hellman-group14-sha1,curve25519-sha256,curve25519-sha256@libssh.org,ecdh-sha2-nistp256,ecdh-sha
2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group18-sha512,diffie-hellman-group16-sha512,diffie-hellman-group-exch
ange-sha256,diffie-hellman-group14-sha256,ext-info-c,kex-strict-c-v00@openssh.com;chacha20-poly1305@openssh.com,aes
256-gcm@openssh.com,aes128-gcm@openssh.com,aes256-ctr,aes192-ctr,aes128-ctr;hmac-sha2-256-etm@openssh.com,hmac-sha2
-512-etm@openssh.com,hmac-sha2-256,hmac-sha2-512;none","kexAlgs":["diffie-hellman-group-exchange-sha1","diffie-hell
man-group14-sha1","curve25519-sha256","curve25519-sha256@libssh.org","ecdh-sha2-nistp256","ecdh-sha2-nistp384","ecd
h-sha2-nistp521","diffie-hellman-group18-sha512","diffie-hellman-group16-sha512","diffie-hellman-group-exchange-sha
256","diffie-hellman-group14-sha256","ext-info-c","kex-strict-c-v00@openssh.com"],"keyAlgs":["ssh-rsa","ssh-ed25519
","ecdsa-sha2-nistp521","ecdsa-sha2-nistp384","ecdsa-sha2-nistp256","sk-ssh-ed25519@openssh.com","sk-ecdsa-sha2-nis
tp256@openssh.com","rsa-sha2-512","rsa-sha2-256"],"encCS":["chacha20-poly1305@openssh.com","aes256-gcm@openssh.com"
,"aes128-gcm@openssh.com","aes256-ctr","aes192-ctr","aes128-ctr"],"macCS":["hmac-sha2-256-etm@openssh.com","hmac-sh
a2-512-etm@openssh.com","hmac-sha2-256","hmac-sha2-512"],"compCS":["none"],"langCS":[""],"message":"SSH client hass
h fingerprint: 015322ee8471fa8338c558a918183b11","sensor":"Sukma","uuid":"666a9ffa-fda4-11f0-a021-080027984cbd","ti
mestamp":"2026-01-30T17:19:00.616670Z","src_ip":"10.203.142.101","session":"bd0fd36ec1e7","protocol":"ssh"}
{"eventid":"cowrie.client.kex","hassh":"015322ee8471fa8338c558a918183b11","hasshAlgorithms":"diffie-hellman-group-e
xchange-sha1,diffie-hellman-group14-sha1,curve25519-sha256,curve25519-sha256@libssh.org,ecdh-sha2-nistp256,ecdh-sha
2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group18-sha512,diffie-hellman-group16-sha512,diffie-hellman-group-exch
ange-sha256,diffie-hellman-group14-sha256,ext-info-c,kex-strict-c-v00@openssh.com;chacha20-poly1305@openssh.com,aes
256-gcm@openssh.com,aes128-gcm@openssh.com,aes256-ctr,aes192-ctr,aes128-ctr;hmac-sha2-256-etm@openssh.com,hmac-sha2
-512-etm@openssh.com,hmac-sha2-256,hmac-sha2-512;none","kexAlgs":["diffie-hellman-group-exchange-sha1","diffie-hell
man-group14-sha1","curve25519-sha256","curve25519-sha256@libssh.org","ecdh-sha2-nistp256","ecdh-sha2-nistp384","ecd
h-sha2-nistp521","diffie-hellman-group18-sha512","diffie-hellman-group16-sha512","diffie-hellman-group-exchange-sha
256","diffie-hellman-group14-sha256","ext-info-c","kex-strict-c-v00@openssh.com"],"keyAlgs":["ssh-rsa","ssh-ed25519
","ecdsa-sha2-nistp521","ecdsa-sha2-nistp384","ecdsa-sha2-nistp256","sk-ssh-ed25519@openssh.com","sk-ecdsa-sha2-nis
tp256@openssh.com","rsa-sha2-512","rsa-sha2-256"],"encCS":["chacha20-poly1305@openssh.com","aes256-gcm@openssh.com"
,"aes128-gcm@openssh.com","aes256-ctr","aes192-ctr","aes128-ctr"],"macCS":["hmac-sha2-256-etm@openssh.com","hmac-sh
a2-512-etm@openssh.com","hmac-sha2-256","hmac-sha2-512"],"compCS":["none"],"langCS":[""],"message":"SSH client hass
```


Pada tahap ini dilakukan analisis terhadap file log Cowrie setelah pengujian multiple attack, yaitu kombinasi port scanning, brute force SSH, dan serangan DDoS yang dilakukan secara bersamaan terhadap server. Berdasarkan log yang dihasilkan, terlihat

adanya peningkatan koneksi SSH secara signifikan dari alamat IP penyerang dengan variasi port sumber yang berbeda-beda dalam waktu yang sangat singkat. Selain itu, tercatat pula proses negosiasi protokol SSH, pertukaran algoritma kriptografi, serta sesi koneksi yang cepat terputus akibat tingginya beban trafik. Hasil ini menunjukkan bahwa Cowrie mampu merekam seluruh aktivitas serangan kompleks secara detail, sehingga data log yang dihasilkan dapat dimanfaatkan untuk menganalisis pola, intensitas, dan karakteristik serangan multipel terhadap server.

Hasil Pengujian

No.	Pola Serangan	Nama Pengujian	Kondisi Sebelum (%)	Kondisi Sesudah (%)	Hasil (Terdeteksi atau Tidak Terdeeteksi)
1	Individu	*Port Scanning*	0%	100%	Terdeteksi
2		*Bruteforce*	0%	100%	Terdeteksi
3		*DDoS Attack*	0%	100%	Terdeteksi
4	Double	*Port Scanning & Bruteforce*	0%	100%	Terdeteksi
5		*Bruteforce & DDoS Attack*	0%	100%	Terdeteksi
6		*DDoS Attack & Port Scanning*	0%	100%	Terdeteksi
7	Multiple	*Port Scanning & Bruteforce & DDoS Attack*	0%	100%	Terdeteksi