

TUGAS BESAR
ADVANCE NETWORK SECURITY
“Implementasi Honeypot Sebagai Pendeteksi Serangan Vps”



OLEH:

UMMUL MU'MININ

105841117323

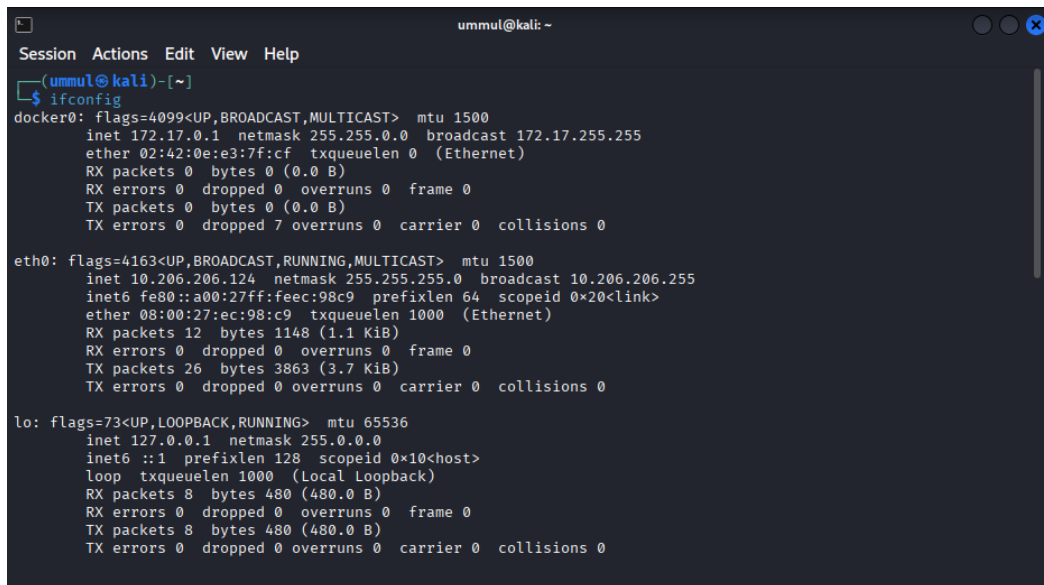
RIRIN YULANDARI

105841117923

PROGRAM STUDI INFORMATIKA
FAKULTAS TEKNIK
UNIVERSITAS MUHAMMADIYAH MAKASSAR
2026

A. INDIVIDUAL

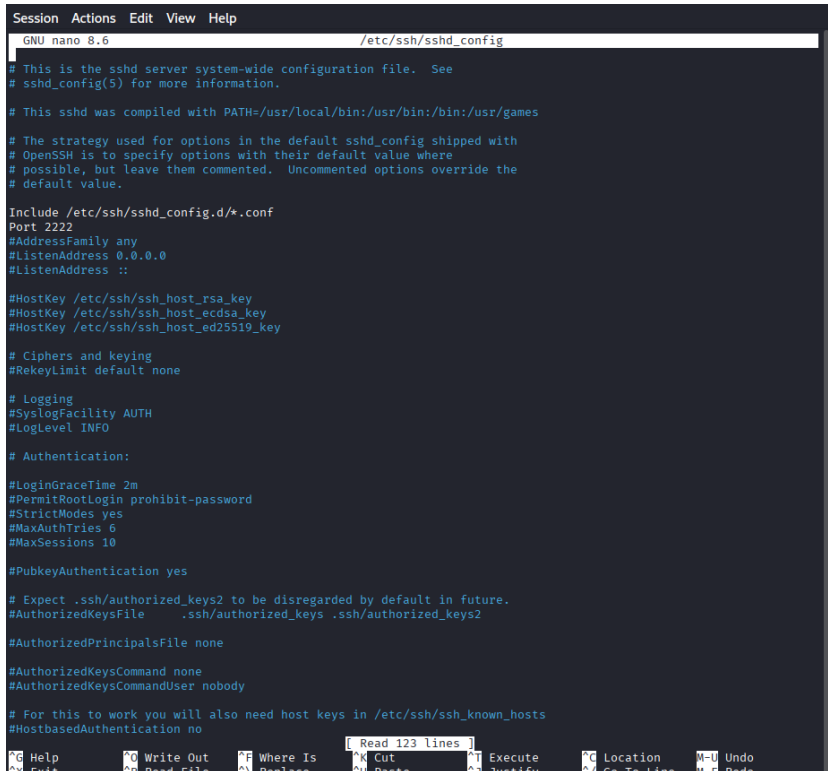
1. Cek ip



```
ummul@kali: ~  
Session Actions Edit View Help  
(ummul@kali)-[~]  
$ ifconfig  
docker0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500  
    inet 172.17.0.1 netmask 255.255.0.0 broadcast 172.17.255.255  
    ether 02:42:0e:e3:7f:cf txqueuelen 0 (Ethernet)  
    RX packets 0 bytes 0 (0.0 B)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 0 bytes 0 (0.0 B)  
    TX errors 0 dropped 7 overruns 0 carrier 0 collisions 0  
  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 10.206.206.124 netmask 255.255.255.0 broadcast 10.206.206.255  
    inet6 fe80::a00:27ff:feec:98c9 prefixlen 64 scopeid 0x20<link>  
    ether 08:00:27:ec:98:c9 txqueuelen 1000 (Ethernet)  
    RX packets 12 bytes 1148 (1.1 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 26 bytes 3863 (3.7 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
    inet 127.0.0.1 netmask 255.0.0.0  
    inet6 ::1 prefixlen 128 scopeid 0x10<host>  
    loop txqueuelen 1000 (Local Loopback)  
    RX packets 8 bytes 480 (480.0 B)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 8 bytes 480 (480.0 B)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Langkah awal yang paling krusial dalam prosedur pengujian ini adalah melakukan verifikasi alamat jaringan pada laptop target (ummul@kali) dengan mengeksekusi perintah `ifconfig` untuk memastikan target sudah terhubung secara benar ke dalam infrastruktur jaringan yang sama dengan penyerang. Berdasarkan hasil pembacaan pada antarmuka jaringan utama `eth0`, teridentifikasi bahwa target memiliki alamat IPv4 10.206.206.124, yang nantinya akan ditetapkan sebagai titik tuju tunggal bagi seluruh simulasi serangan.

2. Ubah port



```
Session Actions Edit View Help
GNU nano 8.6 /etc/ssh/sshd_config
# This is the sshd server system-wide configuration file. See
# sshd_config(5) for more information.
# This sshd was compiled with PATH=/usr/local/bin:/usr/bin:/bin:/usr/games
# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented. Uncommented options override the
# default value.
Include /etc/ssh/sshd_config.d/*.conf
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
# Ciphers and keying
#RekeyLimit default none
# Logging
#SyslogFacility AUTH
#LogLevel INFO
# Authentication:
#LoginGraceTime 2m
#PermitRootLogin prohibit-password
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10
#PubkeyAuthentication yes
# Expect .ssh/authorized_keys2 to be disregarded by default in future.
#AuthorizedKeysFile .ssh/authorized_keys .ssh/authorized_keys2
#AuthorizedPrincipalsFile none
#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody
# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
#HostbasedAuthentication no
^H Help ^O Write Out ^F Where Is ^L Read 123 lines ^T Execute ^G Location M-U Undo
^X Exit ^R Read File ^N Replace ^M Cut ^J Justify ^_ Go To Line M-F Redo
```

Langkah selanjutnya dalam konfigurasi keamanan jaringan adalah melakukan perubahan pada port standar layanan SSH guna meningkatkan aspek keamanan melalui metode pengaburan (*security by obscurity*). Proses ini dilakukan dengan mengakses file konfigurasi utama melalui perintah `nano /etc/ssh/sshd_config`. Di dalam editor tersebut, baris parameter Port diubah nilainya dari port standar 22 menjadi port baru, yaitu 2222. Modifikasi ini bertujuan untuk meminimalisir risiko serangan *brute-force* otomatis yang umumnya menargetkan port *default* layanan komunikasi terenkripsi.

3. Install Docker

```

(ummul@kali)-[~]
$ sudo apt update && sudo apt install docker.io docker-compose -y
Hit:1 https://packages.microsoft.com/repos/code stable InRelease
Hit:2 http://http.kali.org/kali kali-rolling InRelease
1961 packages can be upgraded. Run 'apt list --upgradable' to see them.
Upgrading:
  libnl-3-200  libnl-genl-3-200  libnl-route-3-200  libperl5.40  perl  perl-base  perl-modules-5.40

Installing:
  docker-compose  docker.io

Installing dependencies:
  containerd      docker-cli      libintl-xs-perl  libproc-processtable-perl  python3-pycriu
  criu            libcompell      libmodule-find-perl  libsort-naturally-perl      runc
  docker-buildx  libintl-perl    libnet9          needrestart              tini-static

Suggested packages:
  containernetworking-plugins  btrfs-progs  rinse      xfsprogs  | zfsutils-linux
  docker-doc                   debootstrap  rootlesskit  zfs-fuse

Summary:
  Upgrading: 7, Installing: 17, Removing: 0, Not Upgrading: 1954
  Download size: 110 MB
  Space needed: 432 MB / 5,671 MB available

Get:1 http://xsr.v.moratelindo.io/kali kali-rolling/main amd64 libperl5.40 amd64 5.40.1-7 [4,317 kB]
Get:6 http://http.kali.org/kali kali-rolling/main amd64 containerd amd64 1.7.24-ds1-10 [33.6 MB]
Get:2 http://kali.download/kali kali-rolling/main amd64 perl amd64 5.40.1-7 [267 kB]
Get:4 http://kali.download/kali kali-rolling/main amd64 perl-modules-5.40 all 5.40.1-7 [3,012 kB]
Get:5 http://http.kali.org/kali kali-rolling/main amd64 runc amd64 1.3.3+ds1-2 [6,686 kB]
Get:7 http://kali.download/kali kali-rolling/main amd64 tini-static amd64 0.19.0-6 [277 kB]
Get:8 http://http.kali.org/kali kali-rolling/main amd64 docker.io amd64 27.5.1+dfsg4-1 [23.2 MB]
Get:3 http://xsr.v.moratelindo.io/kali kali-rolling/main amd64 perl-base amd64 5.40.1-7 [1,679 kB]
Get:18 http://xsr.v.moratelindo.io/kali kali-rolling/main amd64 libintl-perl all 1.35-1 [690 kB]
Get:24 http://xsr.v.moratelindo.io/kali kali-rolling/main amd64 python3-pycriu all 4.2-1 [44.3 kB]
Get:9 http://http.kali.org/kali kali-rolling/main amd64 libnet9 amd64 1.3+dfsg-3 [51.3 kB]
Get:10 http://kali.download/kali kali-rolling/main amd64 libnl-genl-3-200 amd64 3.12.0-2 [18.8 kB]
Get:11 http://kali.download/kali kali-rolling/main amd64 libnl-route-3-200 amd64 3.12.0-2 [200 kB]
Get:12 http://kali.download/kali kali-rolling/main amd64 libnl-3-200 amd64 3.12.0-2 [62.2 kB]
Get:13 http://kali.download/kali kali-rolling/main amd64 libcompell amd64 4.2-1 [64.2 kB]
Get:15 http://http.kali.org/kali kali-rolling/main amd64 docker-buildx amd64 0.19.3+ds1-4 [13.9 MB]
Get:16 http://http.kali.org/kali kali-rolling/main amd64 docker-cli amd64 27.5.1+dfsg4-1 [7,650 kB]
Get:17 http://kali.download/kali kali-rolling/main amd64 docker-compose amd64 2.32.4-3 [13.5 MB]
Get:14 http://mirror.primelink.net.id/kali kali-rolling/main amd64 criu amd64 4.2-1 [557 kB]
Get:19 http://mirror.primelink.net.id/kali kali-rolling/main amd64 libintl-xs-perl amd64 1.35-1 [15.3 kB]
Get:20 http://kali.download/kali kali-rolling/main amd64 libmodule-find-perl all 0.17-1 [10.7 kB]
Get:21 http://http.kali.org/kali kali-rolling/main amd64 libproc-processtable-perl amd64 0.637-1+b1 [42.3 kB]
Get:22 http://kali.download/kali kali-rolling/main amd64 libsort-naturally-perl all 1.03-4 [13.1 kB]
Get:23 http://kali.download/kali kali-rolling/main amd64 needrestart all 3.11-1 [68.6 kB]
Fetched 110 MB in 33s (3.368 kB/s)

```

Setelah berhasil melakukan verifikasi alamat IP target, langkah krusial berikutnya dalam membangun infrastruktur pengujian adalah melakukan instalasi perangkat lunak *Docker* pada sistem operasi Kali Linux. Proses ini diawali dengan menjalankan perintah sinkronisasi repositori melalui `sudo apt update`, yang segera dilanjutkan dengan instalasi paket utama `docker.io` dan `docker-compose` untuk memungkinkan pengelolaan kontainer secara efisien. Selama proses berlangsung, sistem secara otomatis mengunduh berbagai dependensi teknis seperti `containerd`, `runc`, dan `docker-buildx` dengan total ukuran unduhan sekitar 110 MB guna memastikan seluruh fungsionalitas virtualisasi dapat berjalan optimal. Instalasi Docker ini merupakan pondasi utama dalam skenario pengujian, karena nantinya layanan Honeypot Cowrie akan dijalankan di dalam lingkungan kontainer yang terisolasi dari sistem utama.

4. Aktifkan cowrie

```
(ummul@kali)-[~]
$ sudo docker run -p 22:2222 cowrie/cowrie
/cowrie/cowrie-env/lib/python3.11/site-packages/twisted/conch/ssh/transport.py:110: CryptographyDeprecationWarnin
g: 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"3des-cbc": (algorithms.TripleDES, 24, modes.CBC),
/cowrie/cowrie-env/lib/python3.11/site-packages/twisted/conch/ssh/transport.py:117: CryptographyDeprecationWarnin
g: 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"3des-ctr": (algorithms.TripleDES, 24, modes.CTR),
2026-01-27T15:18:59+0000 [-] Reading configuration from ['/cowrie/cowrie-git/etc/cowrie.cfg.dist']
2026-01-27T15:19:00+0000 [-] Python Version 3.11.2 (main, Apr 28 2025, 14:11:48) [GCC 12.2.0]
2026-01-27T15:19:00+0000 [-] Twisted Version 25.5.0
2026-01-27T15:19:00+0000 [-] Cowrie Version 2.9.9.dev1+g7d81de406
2026-01-27T15:19:00+0000 [-] Sensor UUID: 80ea96c2-fab7-11f0-bb6a-ee532cd24139
2026-01-27T15:19:00+0000 [-] Loaded output engine: jsonlog
2026-01-27T15:19:00+0000 [twisted.scripts._twistd_unix.UnixAppLogger#info] twistd 25.5.0 (/cowrie/cowrie-env/bin/
python3 3.11.2) starting up.
2026-01-27T15:19:00+0000 [twisted.scripts._twistd_unix.UnixAppLogger#info] reactor class: twisted.internet.epollr
eactor.EPollReactor.
2026-01-27T15:19:00+0000 [-] CowrieSSHFactory starting on 2222
2026-01-27T15:19:00+0000 [cowrie.ssh.factory.CowrieSSHFactory#info] Starting factory <cowrie.ssh.factory.CowrieSS
HFactory object at 0x7fed20e591d0>
2026-01-27T15:19:00+0000 [-] Ready to accept SSH connections
```

Setelah berhasil menginstal Docker, langkah krusial berikutnya adalah mengaktifkan layanan *Honeypot Cowrie* menggunakan perintah `sudo docker run` untuk membuat "pintu jebakan" SSH yang aktif. Dalam proses ini, sistem melakukan pemetaan port (*port mapping*) di mana port fisik 22 pada laptop target dihubungkan langsung ke port internal 2222 milik kontainer Cowrie. Begitu perintah dijalankan, terminal akan menampilkan inisialisasi mesin Cowrie, mulai dari pembacaan konfigurasi `cowrie.cfg.dist` hingga pemuatan mesin log berbasis JSON. Indikator keberhasilan dari tahap ini terlihat pada baris log terakhir yang menyatakan *"Ready to accept SSH connections"*, yang berarti SSH jebakan tersebut kini sudah aktif sepenuhnya dan siap merekam setiap interaksi ilegal dari penyerang. Dengan aktifnya Cowrie di dalam lingkungan Docker, laptop target kini memiliki pertahanan berlapis yang mampu mensimulasikan layanan SSH palsu tanpa mengekspos keamanan sistem operasi yang sebenarnya.

5. Port Scanning

a. Penyerang

```
(root@ririn)-[/home/ririn]
# nmap -Pn -sV -p 22 10.206.206.124
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-27 23:50 WITA
Nmap scan report for 10.206.206.124
Host is up (0.021s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 9.2p1 Debian 2+deb12u3 (protocol 2.0)
MAC Address: 50:BB:B5:34:BC:26 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.73 seconds

(root@ririn)-[/home/ririn]
#
```

Setelah infrastruktur pertahanan aktif, tahap selanjutnya dalam simulasi ini adalah melakukan *Port Scanning* dari sisi penyerang (`root@ririn`) sebagai bagian dari fase pengintaian aktif (*active reconnaissance*). Proses ini dilakukan menggunakan *tool* Nmap dengan perintah `nmap -Pn -sV -p 22 10.206.206.124` yang bertujuan untuk mengidentifikasi status port serta versi layanan yang berjalan pada target. Hasil

pemindaian menunjukkan bahwa port 22/tcp dalam status *open* dan berhasil mengelabui penyerang dengan menampilkan identitas layanan palsu berupa OpenSSH 9.2p1 Debian. Identitas ini sebenarnya merupakan hasil simulasi dari Honeypot Cowrie, yang dirancang untuk terlihat seperti layanan SSH asli guna memancing penyerang melakukan interaksi lebih jauh. Keberhasilan deteksi port ini menjadi jembatan bagi penyerang untuk melanjutkan ke tahap serangan berikutnya, yaitu *Bruteforce* dan *DDoS*, karena penyerang kini meyakini bahwa terdapat celah masuk yang valid pada server target.

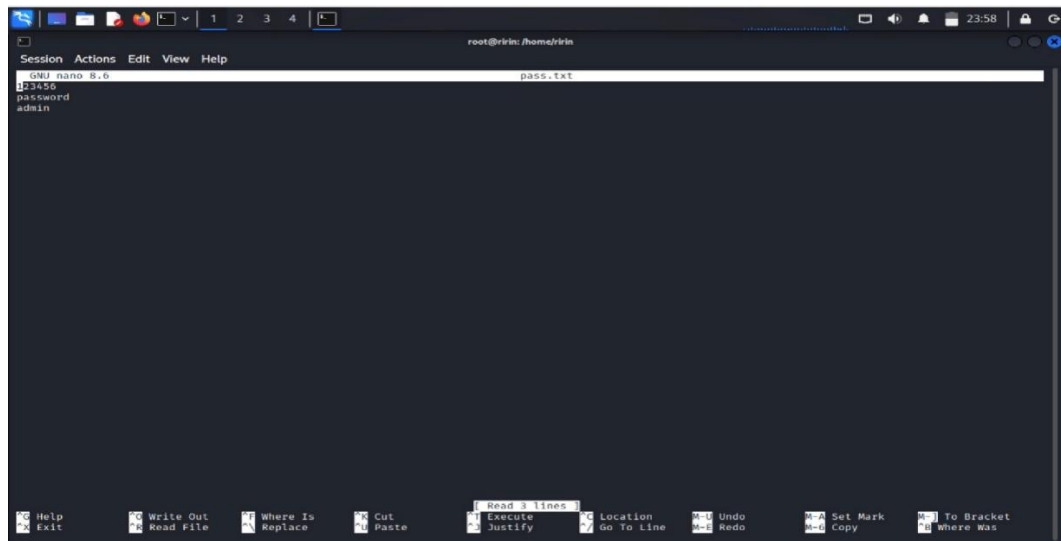
b. Target

```
(ummul@kali)-[~]
$ sudo docker run -p 22:2222 cowrie/cowrie
[sudo] password for ummul:
/cowrie/cowrie-env/lib/python3.11/site-packages/twisted/conch/ssh/transport.py:110: 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"3des-cbc": (algorithms.TripleDES, 24, modes.CBC),
/cowrie/cowrie-env/lib/python3.11/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"3des-ctr": (algorithms.TripleDES, 24, modes.CTR),
2026-01-27T15:36:25+0000 [-] Reading configuration from ['/cowrie/cowrie-git/etc/cowrie.cfg.dist']
2026-01-27T15:36:26+0000 [-] Python Version 3.11.2 (main, Apr 28 2025, 14:11:48) [GCC 12.2.0]
2026-01-27T15:36:26+0000 [-] Twisted Version 25.5.0
2026-01-27T15:36:26+0000 [-] Cowrie Version 2.9.9.dev1+g7d81de406
2026-01-27T15:36:26+0000 [-] Sensor UUID: 80ea96c2-fab7-11f0-bb6a-ee532cd24139
2026-01-27T15:36:26+0000 [-] Loaded output engine: jsonlog
2026-01-27T15:36:26+0000 [twisted.scripts._twistd_unix.UnixAppLogger#info] twistd 25.5.0 (/cowrie/cowrie-env/bin/python3 3.11.2) starting up.
2026-01-27T15:36:26+0000 [twisted.scripts._twistd_unix.UnixAppLogger#info] reactor class: twisted.internet.epollractor.EPollReactor.
2026-01-27T15:36:26+0000 [-] CowrieSSHFactory starting on 2222
2026-01-27T15:36:26+0000 [cowrie.ssh.factory.CowrieSSHFactory#info] Starting factory <cowrie.ssh.factory.CowrieSSHFactory object at 0x7f5ebd5716d0>
2026-01-27T15:36:27+0000 [-] Ready to accept SSH connections
2026-01-27T15:50:20+0000 [cowrie.ssh.factory.CowrieSSHFactory] No moduli, no diffie-hellman-group-exchange-sha1
2026-01-27T15:50:20+0000 [cowrie.ssh.factory.CowrieSSHFactory] No moduli, no diffie-hellman-group-exchange-sha256
2026-01-27T15:50:20+0000 [cowrie.ssh.factory.CowrieSSHFactory] New connection: 10.206.206.39:59612 (172.17.0.2:22) [session: d533ac968675]
2026-01-27T15:50:20+0000 [HoneyPotSSHTransport,0,10.206.206.39] Remote SSH version:
2026-01-27T15:50:20+0000 [HoneyPotSSHTransport,0,10.206.206.39] Bad protocol version identification: b''
2026-01-27T15:50:20+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#info] connection lost
2026-01-27T15:50:20+0000 [HoneyPotSSHTransport,0,10.206.206.39] Connection lost after 0.0 seconds
```

Pada sisi target (ummul@kali), aktivitas pengintaian yang dilakukan oleh penyerang melalui *port scanning* terekam secara mendetail di dalam log kontainer Cowrie. Segera setelah Nmap mengeksekusi perintah pemindaian, terminal target menampilkan baris log New connection: 10.206.206.39 yang mengonfirmasi bahwa Honeypot telah berhasil mencegah upaya koneksi dari alamat IP penyerang pada port 22. Sistem kemudian mencatat upaya identifikasi versi protokol dengan keterangan Bad protocol version identification, yang merupakan karakteristik umum dari pemindaian otomatis Nmap saat mencoba menentukan versi layanan tanpa melakukan proses *handshake* penuh. Rangkaian log ini diakhiri dengan pesan connection lost setelah Nmap selesai mengambil data yang diperlukan, membuktikan bahwa Cowrie secara *real-time* mampu mendeteksi dan mengidentifikasi setiap jejak aktivitas mencurigakan sejak fase pengintaian awal dilakukan.

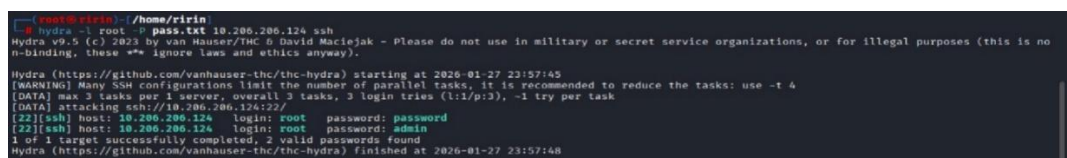
6. Bruteforce Attack

a. Membuat Password (Penyerang)



Tahapan selanjutnya dalam skenario penyerangan adalah mempersiapkan serangan *Bruteforce* SSH pada sisi penyerang (root@ririn) dengan membuat daftar kata sandi (*wordlist*) yang akan digunakan untuk menguji kredibilitas keamanan target. Proses ini dilakukan menggunakan editor teks nano untuk membuat sebuah file bernama `pass.txt`, yang di dalamnya berisi daftar kata sandi umum seperti 123456, password, dan admin. Pembuatan daftar kata sandi ini merupakan langkah krusial sebelum menjalankan *tool* Hydra, karena efektivitas serangan *Bruteforce* sangat bergantung pada kualitas dan relevansi daftar kata yang digunakan untuk menebak autentikasi pada port 22 target. Dengan tersedianya file `pass.txt` ini, penyerang telah memiliki basis data untuk melakukan percobaan login secara otomatis dan masif terhadap alamat IP target 10.206.206.124 yang sebelumnya telah teridentifikasi memiliki port SSH yang terbuka.

b. Menyerang



Setelah daftar kata sandi dipersiapkan, tahap serangan dimulai dengan mengeksekusi *Bruteforce Attack* menggunakan *tool* Hydra dari laptop penyerang (root@ririn). Penyerang menjalankan perintah `hydra -l root -P pass.txt 10.206.206.124 ssh`, yang mengarahkan serangan secara otomatis ke layanan SSH pada IP target menggunakan daftar kata sandi yang telah dibuat sebelumnya. Dalam

hitungan detik, Hydra melaporkan hasil percobaan login dan secara mengejutkan menunjukkan bahwa ditemukan dua kata sandi yang dianggap valid, yaitu password dan admin, untuk pengguna root. Hasil ini sebenarnya merupakan bagian dari keberhasilan simulasi Honeypot Cowrie, yang sengaja menerima percobaan login tersebut guna memancing penyerang masuk lebih dalam ke dalam sistem jebakan untuk memantau aktivitas mereka. Eksekusi serangan ini membuktikan bahwa kerentanan autentikasi dapat dieksploitasi dengan sangat cepat oleh penyerang jika tidak dilindungi oleh sistem keamanan yang memadai.

c. Target

```

2026-01-27T15:57:41+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#debug] incoming: b'aes256-ctr' b'hmac-sha2-256' b'none'
2026-01-27T15:57:41+0000 [HoneyPotSSHTransport,2,10.206.206.39] SSH client hassh fingerprint: 742b4fd5532ca4f243a
ae081017fe8c5
2026-01-27T15:57:41+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#debug] kex alg=b'curve25519-sha256' key alg=b
'ssh-ed25519'
2026-01-27T15:57:41+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#debug] outgoing: b'aes256-ctr' b'hmac-sha2-256' b'none'
2026-01-27T15:57:41+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#debug] incoming: b'aes256-ctr' b'hmac-sha2-256' b'none'
2026-01-27T15:57:41+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#debug] NEW KEYS
2026-01-27T15:57:41+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#debug] NEW KEYS
2026-01-27T15:57:41+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#debug] NEW KEYS
2026-01-27T15:57:41+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#debug] starting service b'ssh-userauth'
2026-01-27T15:57:41+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#debug] starting service b'ssh-userauth'
2026-01-27T15:57:41+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#debug] starting service b'ssh-userauth'
2026-01-27T15:57:41+0000 [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'root' trying auth b'none'
2026-01-27T15:57:41+0000 [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'root' trying auth b'none'
2026-01-27T15:57:41+0000 [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'root' trying auth b'none'
2026-01-27T15:57:41+0000 [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'root' trying auth b'password'
2026-01-27T15:57:41+0000 [HoneyPotSSHTransport,2,10.206.206.39] Could not read etc/userdb.txt, default database a
ctivated
2026-01-27T15:57:41+0000 [HoneyPotSSHTransport,2,10.206.206.39] login attempt [b'root'/b'123456'] failed
2026-01-27T15:57:41+0000 [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'root' trying auth b'password'
2026-01-27T15:57:41+0000 [HoneyPotSSHTransport,4,10.206.206.39] Could not read etc/userdb.txt, default database a
ctivated
2026-01-27T15:57:41+0000 [HoneyPotSSHTransport,4,10.206.206.39] login attempt [b'root'/b'admin'] succeeded
2026-01-27T15:57:41+0000 [HoneyPotSSHTransport,4,10.206.206.39] Initialized emulated server as architecture: linu
x-x64-lsb
2026-01-27T15:57:41+0000 [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'root' authenticated with b'passw
ord'
2026-01-27T15:57:41+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#debug] starting service b'ssh-connection'
2026-01-27T15:57:41+0000 [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'root' trying auth b'password'
2026-01-27T15:57:41+0000 [HoneyPotSSHTransport,3,10.206.206.39] Could not read etc/userdb.txt, default database a
ctivated
2026-01-27T15:57:41+0000 [HoneyPotSSHTransport,3,10.206.206.39] login attempt [b'root'/b'password'] succeeded
2026-01-27T15:57:41+0000 [HoneyPotSSHTransport,3,10.206.206.39] Initialized emulated server as architecture: linu
x-x64-lsb
2026-01-27T15:57:41+0000 [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'root' authenticated with b'passw
ord'
2026-01-27T15:57:41+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#debug] starting service b'ssh-connection'
2026-01-27T15:57:41+0000 [HoneyPotSSHTransport,3,10.206.206.39] avatar root logging out
2026-01-27T15:57:41+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#info] connection lost
2026-01-27T15:57:41+0000 [HoneyPotSSHTransport,3,10.206.206.39] Connection lost after 0.4 seconds
2026-01-27T15:57:41+0000 [HoneyPotSSHTransport,4,10.206.206.39] avatar root logging out
2026-01-27T15:57:41+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#info] connection lost
2026-01-27T15:57:41+0000 [HoneyPotSSHTransport,4,10.206.206.39] Connection lost after 0.4 seconds
2026-01-27T15:57:42+0000 [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'root' failed auth b'password'
2026-01-27T15:57:42+0000 [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] unauthorized login: ()
2026-01-27T15:58:12+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#info] connection lost
2026-01-27T15:58:12+0000 [HoneyPotSSHTransport,2,10.206.206.39] Connection lost after 31.4 seconds

```

Setelah penyerang meluncurkan serangan *Bruteforce* menggunakan Hydra, seluruh aktivitas tersebut terekam secara komprehensif pada log Honeypot Cowrie di sisi target (ummul@kali). Log menunjukkan bahwa sistem mendeteksi percobaan login berulang untuk pengguna root dari alamat IP penyerang 10.206.206.39. Cowrie mencatat setiap detail upaya autentikasi, mulai dari kegagalan login untuk kata sandi 123456 hingga keberhasilan login palsu menggunakan kata sandi admin dan password. Setelah penyerang berhasil "masuk", Honeypot segera menginisialisasi

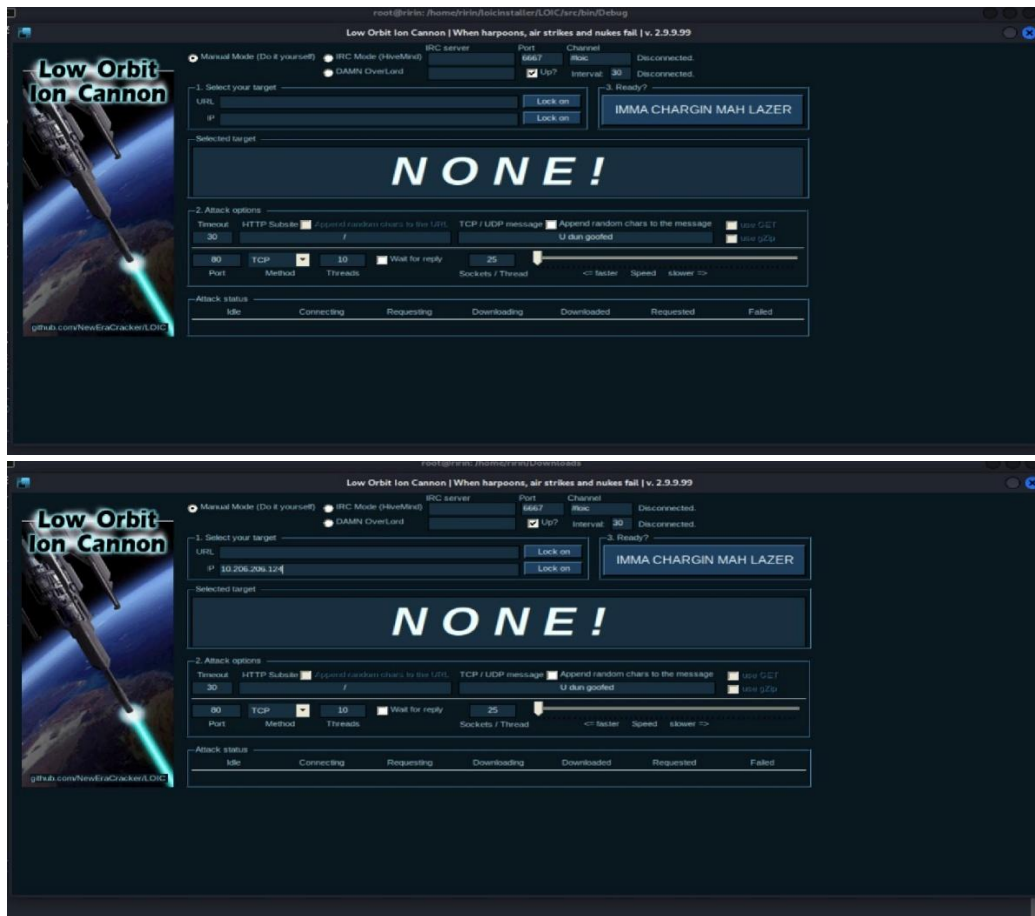
server emulasi dengan arsitektur linux-x64-lsb untuk memantau aktivitas penyerang lebih lanjut di dalam sistem jebakan tersebut. Rangkaian log ini membuktikan kemampuan Cowrie dalam membedakan serta merekam setiap kombinasi *username* dan *password* yang dicoba oleh penyerang, sekaligus memberikan gambaran nyata mengenai interaksi penyerang dengan layanan SSH yang sedang disimulasikan.

7. Ddos

a. Masuk ke LOIC (Penyerang)

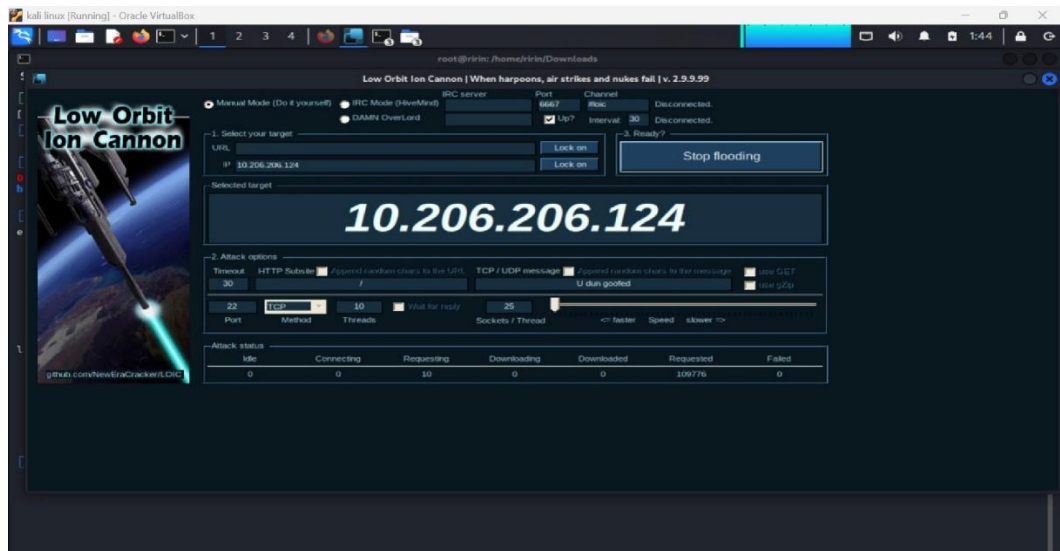
```
(root@ririn)-[ /home/.../LOIC/src/bin/Debug ]
# mono LOIC.exe
Gtk not found (missing LD_LIBRARY_PATH to libgtk-x11-2.0.so.0?), using built-in colorscheme
```

Setelah berhasil melakukan simulasi serangan *Bruteforce*, tahap berikutnya dalam skenario serangan ganda (*Double Attack*) adalah meluncurkan serangan DDoS (Distributed Denial of Service) menggunakan perangkat lunak LOIC (Low Orbit Ion Cannon) dari sisi penyerang (root@ririn). Penyerang menavigasi terminal ke direktori binari aplikasi di /home/.../LOIC/src/bin/Debug dan mengeksekusi perintah mono LOIC.exe untuk menjalankan aplikasi berbasis .



Setelah perintah mono LOIC.exe dieksekusi, jendela aplikasi Low Orbit Ion Cannon (LOIC) akan terbuka, memungkinkan penyerang untuk melakukan konfigurasi target serangan secara grafis. Pada antarmuka utama, langkah pertama

yang dilakukan adalah memasukkan alamat IP target, yaitu 10.206.206.124, ke dalam kolom "IP" yang tersedia di bagian *Select your target*. Setelah IP dimasukkan, penyerang menekan tombol "Lock on" untuk mengunci target sehingga sistem secara otomatis mengenali alamat tersebut sebagai titik akhir yang akan dibanjiri oleh paket data.



Setelah target berhasil dikunci pada alamat IP 10.206.206.124, langkah selanjutnya dalam antarmuka LOIC adalah melakukan konfigurasi parameter serangan pada bagian *Attack options*. Penyerang secara spesifik mengubah nilai "Port" menjadi 22 agar serangan banjir trafik tepat mengarah pada layanan SSH yang sedang disimulasikan oleh Honeypot. Selain itu, metode serangan ditetapkan pada protokol TCP dengan pengaturan *Threads* sebanyak 10 untuk memastikan volume paket data yang dikirimkan cukup masif untuk membebani target. Setelah seluruh parameter sesuai, penyerang menekan tombol "IMMA CHARGIN MAH LAZER", yang kemudian berubah status menjadi "Stop flooding", menandakan bahwa serangan DDoS sedang berlangsung secara aktif. Indikator keberhasilan serangan ini terlihat pada bagian *Attack status*, di mana kolom *Requested* menunjukkan angka yang terus meningkat pesat hingga mencapai lebih dari 100.000 permintaan, membuktikan adanya pengiriman paket data dalam skala besar ke arah target.

b. Target

```
x-x64-lsb
2026-01-27T15:57:41+0000 [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'root' authenticated with b'passwd'
2026-01-27T15:57:41+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#debug] starting service b'ssh-connection'
2026-01-27T15:57:41+0000 [HoneyPotSSHTransport,3,10.206.206.39] avatar root logging out
2026-01-27T15:57:41+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#info] connection lost
2026-01-27T15:57:41+0000 [HoneyPotSSHTransport,3,10.206.206.39] Connection lost after 0.4 seconds
2026-01-27T15:57:41+0000 [HoneyPotSSHTransport,4,10.206.206.39] avatar root logging out
2026-01-27T15:57:41+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#info] connection lost
2026-01-27T15:57:41+0000 [HoneyPotSSHTransport,4,10.206.206.39] Connection lost after 0.4 seconds
2026-01-27T15:57:42+0000 [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'root' failed auth b'password'
2026-01-27T15:57:42+0000 [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] unauthorized login: ()
2026-01-27T15:58:12+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#info] connection lost
2026-01-27T15:58:12+0000 [HoneyPotSSHTransport,2,10.206.206.39] Connection lost after 31.4 seconds
2026-01-27T17:43:59+0000 [cowrie.ssh.factory.CowrieSSHFactory] No moduli, no diffie-hellman-group-exchange-sha1
2026-01-27T17:43:59+0000 [cowrie.ssh.factory.CowrieSSHFactory] No moduli, no diffie-hellman-group-exchange-sha256
2026-01-27T17:43:59+0000 [cowrie.ssh.factory.CowrieSSHFactory] New connection: 10.206.206.39:41772 (172.17.0.2:22)
22) [session: eb5b0491e13]
2026-01-27T17:43:59+0000 [cowrie.ssh.factory.CowrieSSHFactory] No moduli, no diffie-hellman-group-exchange-sha1
2026-01-27T17:43:59+0000 [cowrie.ssh.factory.CowrieSSHFactory] No moduli, no diffie-hellman-group-exchange-sha256
2026-01-27T17:43:59+0000 [cowrie.ssh.factory.CowrieSSHFactory] New connection: 10.206.206.39:41784 (172.17.0.2:22)
22) [session: 55c308b47324]
2026-01-27T17:43:59+0000 [cowrie.ssh.factory.CowrieSSHFactory] No moduli, no diffie-hellman-group-exchange-sha1
2026-01-27T17:43:59+0000 [cowrie.ssh.factory.CowrieSSHFactory] No moduli, no diffie-hellman-group-exchange-sha256
2026-01-27T17:43:59+0000 [cowrie.ssh.factory.CowrieSSHFactory] New connection: 10.206.206.39:41794 (172.17.0.2:22)
22) [session: c00d7eabb9a7]
2026-01-27T17:43:59+0000 [cowrie.ssh.factory.CowrieSSHFactory] No moduli, no diffie-hellman-group-exchange-sha1
2026-01-27T17:43:59+0000 [cowrie.ssh.factory.CowrieSSHFactory] No moduli, no diffie-hellman-group-exchange-sha256
2026-01-27T17:43:59+0000 [cowrie.ssh.factory.CowrieSSHFactory] New connection: 10.206.206.39:41802 (172.17.0.2:22)
22) [session: 85bd2a2c1770]
2026-01-27T17:44:00+0000 [cowrie.ssh.factory.CowrieSSHFactory] No moduli, no diffie-hellman-group-exchange-sha1
2026-01-27T17:44:00+0000 [cowrie.ssh.factory.CowrieSSHFactory] No moduli, no diffie-hellman-group-exchange-sha256
2026-01-27T17:44:00+0000 [cowrie.ssh.factory.CowrieSSHFactory] New connection: 10.206.206.39:41806 (172.17.0.2:22)
22) [session: 3c8b1cd52ccf]
2026-01-27T17:44:00+0000 [cowrie.ssh.factory.CowrieSSHFactory] No moduli, no diffie-hellman-group-exchange-sha1
2026-01-27T17:44:00+0000 [cowrie.ssh.factory.CowrieSSHFactory] No moduli, no diffie-hellman-group-exchange-sha256
2026-01-27T17:44:00+0000 [cowrie.ssh.factory.CowrieSSHFactory] New connection: 10.206.206.39:41814 (172.17.0.2:22)
22) [session: 7e779811f924]
2026-01-27T17:44:01+0000 [cowrie.ssh.factory.CowrieSSHFactory] No moduli, no diffie-hellman-group-exchange-sha1
2026-01-27T17:44:01+0000 [cowrie.ssh.factory.CowrieSSHFactory] No moduli, no diffie-hellman-group-exchange-sha256
2026-01-27T17:44:01+0000 [cowrie.ssh.factory.CowrieSSHFactory] New connection: 10.206.206.39:41828 (172.17.0.2:22)
22) [session: 3a650affa17c]
2026-01-27T17:44:01+0000 [cowrie.ssh.factory.CowrieSSHFactory] No moduli, no diffie-hellman-group-exchange-sha1
2026-01-27T17:44:01+0000 [cowrie.ssh.factory.CowrieSSHFactory] No moduli, no diffie-hellman-group-exchange-sha256
2026-01-27T17:44:01+0000 [cowrie.ssh.factory.CowrieSSHFactory] New connection: 10.206.206.39:41842 (172.17.0.2:22)
22) [session: cee57ea5fd94]
2026-01-27T17:44:02+0000 [cowrie.ssh.factory.CowrieSSHFactory] No moduli, no diffie-hellman-group-exchange-sha1
2026-01-27T17:44:02+0000 [cowrie.ssh.factory.CowrieSSHFactory] No moduli, no diffie-hellman-group-exchange-sha256
2026-01-27T17:44:02+0000 [cowrie.ssh.factory.CowrieSSHFactory] New connection: 10.206.206.39:41858 (172.17.0.2:22)
22) [session: c64409536d0d]
2026-01-27T17:44:02+0000 [cowrie.ssh.factory.CowrieSSHFactory] No moduli, no diffie-hellman-group-exchange-sha1
2026-01-27T17:44:02+0000 [cowrie.ssh.factory.CowrieSSHFactory] No moduli, no diffie-hellman-group-exchange-sha256
22) [session: 74b58daafd26]
2026-01-27T17:45:27+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#info] connection lost
2026-01-27T17:45:27+0000 [HoneyPotSSHTransport,14,10.206.206.39] Connection lost after 84.7 seconds
2026-01-27T17:45:27+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#info] connection lost
2026-01-27T17:45:27+0000 [HoneyPotSSHTransport,5,10.206.206.39] Connection lost after 88.2 seconds
2026-01-27T17:45:27+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#info] connection lost
2026-01-27T17:45:27+0000 [HoneyPotSSHTransport,9,10.206.206.39] Connection lost after 87.2 seconds
2026-01-27T17:45:27+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#info] connection lost
2026-01-27T17:45:27+0000 [HoneyPotSSHTransport,10,10.206.206.39] Connection lost after 86.7 seconds
2026-01-27T17:45:27+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#info] connection lost
2026-01-27T17:45:27+0000 [HoneyPotSSHTransport,7,10.206.206.39] Connection lost after 88.2 seconds
2026-01-27T17:45:27+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#info] connection lost
2026-01-27T17:45:27+0000 [HoneyPotSSHTransport,13,10.206.206.39] Connection lost after 85.3 seconds
2026-01-27T17:45:27+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#info] connection lost
2026-01-27T17:45:27+0000 [HoneyPotSSHTransport,8,10.206.206.39] Connection lost after 87.8 seconds
2026-01-27T17:45:27+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#info] connection lost
2026-01-27T17:45:27+0000 [HoneyPotSSHTransport,6,10.206.206.39] Connection lost after 88.2 seconds
2026-01-27T17:45:27+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#info] connection lost
2026-01-27T17:45:27+0000 [HoneyPotSSHTransport,11,10.206.206.39] Connection lost after 86.3 seconds
2026-01-27T17:45:27+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#info] connection lost
2026-01-27T17:45:27+0000 [HoneyPotSSHTransport,12,10.206.206.39] Connection lost after 85.8 seconds
```

Setelah serangan DDoS dilancarkan menggunakan LOIC, log pada sisi target (ummul@kali) menunjukkan lonjakan aktivitas koneksi yang sangat masif dan terjadi secara simultan. Honeypot Cowrie merekam ribuan baris log baru bertuliskan New connection: 10.206.206.39 dalam interval waktu yang sangat singkat, yang mengonfirmasi bahwa target sedang dibanjiri permintaan dari alamat IP penyerang. Karena volume permintaan yang sangat tinggi dan sifat serangan TCP yang berulang, sistem mulai mencatat kegagalan protokol seperti ketiadaan modul diffie-hellman-group-exchange untuk setiap sesi baru yang dibuat. Selanjutnya, log

menunjukkan rentetan pesan connection lost yang berurutan, menandakan bahwa koneksi tersebut segera diputus setelah membebani sumber daya Honeypot. Fenomena ini membuktikan bahwa serangan DDoS berhasil menciptakan beban kerja yang signifikan pada layanan SSH palsu tersebut, sekaligus menunjukkan kemampuan Cowrie dalam mendokumentasikan setiap paket banjir data sebagai bukti forensik serangan *denial of service*.

B. DOUBLE

1. Port Scanning & Burteforce Attack

a. Cek ip (target)

```
(ummul@kali)-[~]
$ ifconfig
docker0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    inet 172.17.0.1 netmask 255.255.0.0 broadcast 172.17.255.255
    ether 02:42:93:4c:14:19 txqueuelen 0 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 7 overruns 0 carrier 0 collisions 0

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.101.196.124 netmask 255.255.255.0 broadcast 10.101.196.255
    inet6 fe80::a00:27ff:feec:98c9 prefixlen 64 scopeid 0<20<link>
    inet6 2400:9800:b01:2d2e:a00:27ff:feec:98c9 prefixlen 64 scopeid 0<0<global>
    inet6 2400:9800:b01:2d2e:ae7:1761:f301:cbc3 prefixlen 64 scopeid 0<0<global>
    ether 08:00:27:ec:98:c9 txqueuelen 1000 (Ethernet)
    RX packets 47 bytes 5927 (5.7 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 38 bytes 7210 (7.0 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Langkah awal yang paling krusial dalam prosedur pengujian ini adalah melakukan verifikasi alamat jaringan pada laptop target (ummul@kali) dengan mengeksekusi perintah ifconfig untuk memastikan target sudah terhubung secara benar ke dalam infrastruktur jaringan yang sama dengan penyerang. Berdasarkan hasil pembacaan pada antarmuka jaringan utama eth0, teridentifikasi bahwa target memiliki alamat IPv4 10.101.196.124, yang nantinya akan ditetapkan sebagai titik tuju tunggal bagi seluruh simulasi serangan.

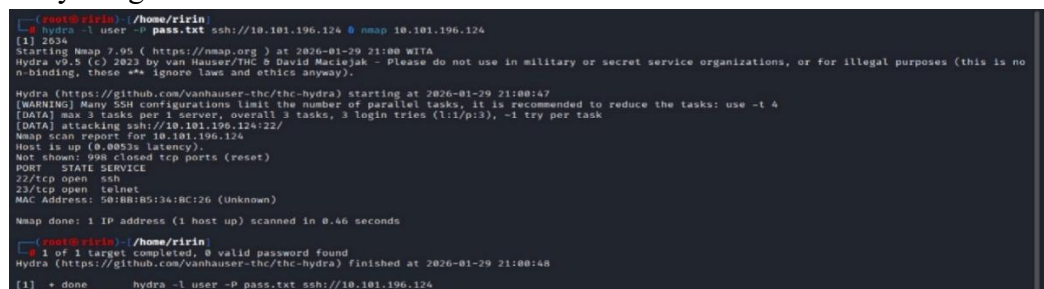
b. Nyalakan Cowrie

```
(ummul@kali)-[~]
$ sudo docker ps
CONTAINER ID   IMAGE          COMMAND                                     CREATED        STATUS        PORTS
fd4449e19102   cowrie/cowrie "/cowrie/cowrie-env/..."               44 hours ago   Up 18 seconds  2223/tcp, 0.0.0.0:22→2222/tcp, [::]:22→2222/tcp
                serene_lalande

(ummul@kali)-[~]
$ sudo docker logs -f fd4449e19102
/cowrie/cowrie-env/lib/python3.11/site-packages/twisted/conch/ssh/transport.py:110: 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"3des-cbc": (algorithms.TripleDES, 24, modes.CBC),
/cowrie/cowrie-env/lib/python3.11/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"3des-ctr": (algorithms.TripleDES, 24, modes.CTR),
2026-01-27T15:36:25+0000 [-] Reading configuration from ['/cowrie/cowrie-git/etc/cowrie.cfg.dist']
2026-01-27T15:36:26+0000 [-] Python Version 3.11.2 (main, Apr 28 2025, 14:11:48) [GCC 12.2.0]
2026-01-27T15:36:26+0000 [-] Twisted Version 25.5.0
2026-01-27T15:36:26+0000 [-] Cowrie Version 2.9.9.dev1+g7d81de406
2026-01-27T15:36:26+0000 [-] Sensor UUID: 80ea96c2-fab7-11f0-bb6a-ee532cd24139
2026-01-27T15:36:26+0000 [-] Loaded output engine: jsonlog
2026-01-27T15:36:26+0000 [twisted.scripts._twistd_unix.UnixAppLogger#info] twistd 25.5.0 (/cowrie/cowrie-env/bin/python3 3.11.2) starting up.
2026-01-27T15:36:26+0000 [twisted.scripts._twistd_unix.UnixAppLogger#info] reactor class: twisted.internet.epollr
```

Proses aktivasi pertahanan dilakukan dengan menjalankan layanan Honeypot Cowrie berbasis Docker pada perangkat target (10.101.196.124) menggunakan perintah `sudo docker run -p 22:2222 cowrie/cowrie`. Langkah ini secara strategis memetakan port fisik 22 ke dalam lingkungan emulasi port 2222, sehingga setiap upaya akses SSH dari pihak eksternal—termasuk serangan dari IP penyerang 10.101.196.39—akan langsung dialihkan ke dalam sistem jebakan tanpa membahayakan integritas sistem operasi utama. Keberhasilan inisialisasi ditandai dengan munculnya indikator status "Ready to accept SSH connections" pada log konsol.

c. Penyerang



```
root@rinu: /home/rinu
# hydra -l user -P pass.txt ssh://10.101.196.124 & nmap 10.101.196.124
[1] 2034
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-29 21:00 WITA
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is no
n-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2026-01-29 21:00:47
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 3 tasks per 1 server, overall 3 tasks, 3 login tries (l:l/p:3), -i try per task
[DATA] attacking ssh://10.101.196.124:22/
Nmap scan report for 10.101.196.124
Host is up (0.0053s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
23/tcp    open  telnet
MAC Address: 50:BB:B5:34:BC:26 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.46 seconds

root@rinu: /home/rinu
# 1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2026-01-29 21:00:48
[1] + done      hydra -l user -P pass.txt ssh://10.101.196.124
```

Gambar ini merepresentasikan pelaksanaan simulasi serangan siber (*Cyber Attack Simulation*) secara *real-time*, di mana sisi penyerang terlihat mengeksekusi perintah gabungan menggunakan Hydra untuk melakukan *Bruteforce* dan Nmap untuk pemindaian port secara simultan terhadap target. Di sisi pertahanan, infrastruktur Honeypot divalidasi melalui status aktif kontainer Docker Cowrie yang siap menjebak koneksi masuk pada port 2222, sebelum akhirnya seluruh sesi pengujian diakhiri dengan mematikan layanan secara terkontrol, sebagaimana dibuktikan oleh log sistem yang mencetak status "*Server Shut Down*".

d. Target

```
ummul@kali: ~  
Session Actions Edit View Help  
eactor.EPollReactor.  
2026-01-29T12:59:52+0000 [-] CowrieSSHFactory starting on 2222  
2026-01-29T12:59:52+0000 [cowrie.ssh.factory.CowrieSSHFactory#info] Starting factory <cowrie.ssh.factory.CowrieSSHFactory object at 0x7f9d21d74110>  
2026-01-29T12:59:52+0000 [-] Ready to accept SSH connections  
2026-01-29T13:00:41+0000 [cowrie.ssh.factory.CowrieSSHFactory] No moduli, no diffie-hellman-group-exchange-sha1  
2026-01-29T13:00:41+0000 [cowrie.ssh.factory.CowrieSSHFactory] No moduli, no diffie-hellman-group-exchange-sha256  
2026-01-29T13:00:41+0000 [cowrie.ssh.factory.CowrieSSHFactory] New connection: 10.101.196.39:54298 (172.17.0.2:2222) [session: 8ff8ff32aee4]  
2026-01-29T13:00:41+0000 [HoneyPotSSHTransport,0,10.101.196.39] Remote SSH version: SSH-2.0-libssh_0.11.3  
2026-01-29T13:00:41+0000 [HoneyPotSSHTransport,0,10.101.196.39] SSH client hassh fingerprint: 742b4fd5532ca4f243a  
ae081017fe8c5  
2026-01-29T13:00:41+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#debug] kex alg=b'curve25519-sha256' key alg=b'ssh-ed25519'  
2026-01-29T13:00:41+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#debug] outgoing: b'aes256-ctr' b'hmac-sha2-256' b'none'  
2026-01-29T13:00:41+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#debug] incoming: b'aes256-ctr' b'hmac-sha2-256' b'none'  
2026-01-29T13:00:41+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#debug] NEW KEYS  
2026-01-29T13:00:41+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#debug] starting service b'ssh-userauth'  
2026-01-29T13:00:41+0000 [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'user' trying auth b'none'  
2026-01-29T13:00:41+0000 [HoneyPotSSHTransport,0,10.101.196.39] Got remote error, code 11 reason: b'Bye Bye'  
2026-01-29T13:00:41+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#info] connection lost  
2026-01-29T13:00:41+0000 [HoneyPotSSHTransport,0,10.101.196.39] Connection lost after 0.2 seconds  
2026-01-29T13:00:41+0000 [cowrie.ssh.factory.CowrieSSHFactory] No moduli, no diffie-hellman-group-exchange-sha1  
2026-01-29T13:00:41+0000 [cowrie.ssh.factory.CowrieSSHFactory] No moduli, no diffie-hellman-group-exchange-sha256  
2026-01-29T13:00:41+0000 [cowrie.ssh.factory.CowrieSSHFactory] New connection: 10.101.196.39:54306 (172.17.0.2:2222) [session: 17d6ade81362]  
2026-01-29T13:00:41+0000 [cowrie.ssh.factory.CowrieSSHFactory] No moduli, no diffie-hellman-group-exchange-sha1  
2026-01-29T13:00:41+0000 [cowrie.ssh.factory.CowrieSSHFactory] No moduli, no diffie-hellman-group-exchange-sha256  
2026-01-29T13:00:41+0000 [cowrie.ssh.factory.CowrieSSHFactory] New connection: 10.101.196.39:54308 (172.17.0.2:2222) [session: ab8404c5afa0]  
2026-01-29T13:00:41+0000 [HoneyPotSSHTransport,1,10.101.196.39] Remote SSH version: SSH-2.0-libssh_0.11.3  
2026-01-29T13:00:41+0000 [cowrie.ssh.factory.CowrieSSHFactory] No moduli, no diffie-hellman-group-exchange-sha1  
2026-01-29T13:00:41+0000 [cowrie.ssh.factory.CowrieSSHFactory] No moduli, no diffie-hellman-group-exchange-sha256  
2026-01-29T13:00:41+0000 [cowrie.ssh.factory.CowrieSSHFactory] New connection: 10.101.196.39:54316 (172.17.0.2:2222) [session: ae57be715830]  
2026-01-29T13:00:41+0000 [HoneyPotSSHTransport,2,10.101.196.39] Remote SSH version: SSH-2.0-libssh_0.11.3  
2026-01-29T13:00:41+0000 [HoneyPotSSHTransport,3,10.101.196.39] Remote SSH version: SSH-2.0-libssh_0.11.3  
2026-01-29T13:00:41+0000 [HoneyPotSSHTransport,1,10.101.196.39] SSH client hassh fingerprint: 742b4fd5532ca4f243a  
ae081017fe8c5  
2026-01-29T13:00:41+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#debug] kex alg=b'curve25519-sha256' key alg=b'ssh-ed25519'  
2026-01-29T13:00:41+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#debug] outgoing: b'aes256-ctr' b'hmac-sha2-256' b'none'  
2026-01-29T13:00:41+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#debug] incoming: b'aes256-ctr' b'hmac-sha2-256' b'none'  
2026-01-29T13:00:41+0000 [HoneyPotSSHTransport,2,10.101.196.39] SSH client hassh fingerprint: 742b4fd5532ca4f243a  
ae081017fe8c5  
2026-01-29T13:00:41+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#debug] kex alg=b'curve25519-sha256' key alg=b'ssh-ed25519'  
2026-01-29T13:00:41+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#debug] outgoing: b'aes256-ctr' b'hmac-sha2-256' b'none'  
2026-01-29T13:00:41+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#debug] NEW KEYS  
2026-01-29T13:00:41+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#debug] NEW KEYS  
2026-01-29T13:00:41+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#debug] NEW KEYS  
2026-01-29T13:00:41+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#debug] starting service b'ssh-userauth'  
2026-01-29T13:00:41+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#debug] starting service b'ssh-userauth'  
2026-01-29T13:00:41+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#debug] starting service b'ssh-userauth'  
2026-01-29T13:00:41+0000 [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'user' trying auth b'none'  
2026-01-29T13:00:41+0000 [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'user' trying auth b'none'  
2026-01-29T13:00:41+0000 [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'user' trying auth b'none'  
2026-01-29T13:00:41+0000 [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'user' trying auth b'password'  
2026-01-29T13:00:41+0000 [HoneyPotSSHTransport,1,10.101.196.39] Could not read etc/userdb.txt, default database activated  
2026-01-29T13:00:41+0000 [HoneyPotSSHTransport,1,10.101.196.39] login attempt [b'user'/b'password'] failed  
2026-01-29T13:00:41+0000 [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'user' trying auth b'password'  
2026-01-29T13:00:41+0000 [HoneyPotSSHTransport,2,10.101.196.39] Could not read etc/userdb.txt, default database activated  
2026-01-29T13:00:41+0000 [HoneyPotSSHTransport,2,10.101.196.39] login attempt [b'user'/b'admin'] failed  
2026-01-29T13:00:41+0000 [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'user' trying auth b'password'  
2026-01-29T13:00:41+0000 [HoneyPotSSHTransport,3,10.101.196.39] Could not read etc/userdb.txt, default database activated  
2026-01-29T13:00:41+0000 [HoneyPotSSHTransport,3,10.101.196.39] login attempt [b'user'/b'123456'] failed  
2026-01-29T13:00:42+0000 [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'user' failed auth b'password'  
2026-01-29T13:00:42+0000 [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] unauthorized login: ()  
2026-01-29T13:00:42+0000 [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'user' failed auth b'password'  
2026-01-29T13:00:42+0000 [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] unauthorized login: ()  
2026-01-29T13:00:42+0000 [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'user' failed auth b'password'  
2026-01-29T13:00:42+0000 [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] unauthorized login: ()  
2026-01-29T13:00:42+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#info] connection lost  
2026-01-29T13:00:42+0000 [HoneyPotSSHTransport,3,10.101.196.39] Connection lost after 1.2 seconds  
2026-01-29T13:00:42+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#info] connection lost  
2026-01-29T13:00:42+0000 [HoneyPotSSHTransport,1,10.101.196.39] Connection lost after 1.2 seconds  
2026-01-29T13:00:42+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#info] connection lost  
2026-01-29T13:00:42+0000 [HoneyPotSSHTransport,2,10.101.196.39] Connection lost after 1.2 seconds
```

Pada sisi target (ummul@kali), HoneyPot Cowrie berhasil mendeteksi dan merekam seluruh rangkaian serangan secara *real-time*. Aktivitas dimulai dengan inisialisasi layanan yang ditandai status "Ready to accept SSH connections", yang kemudian segera diikuti oleh rentetan notifikasi "New connection" dari alamat IP

2. Bruteforce Attack dan DdoS

[illegible]

Pada sisi penyerang (root@ririn), operasi ofensif gabungan menunjukkan keberhasilan penetrasi sekaligus gangguan layanan terhadap target 10.101.196.124. Eksekusi serangan *Bruteforce* menggunakan Hydra berhasil memecahkan lapisan otentikasi SSH, di mana alat tersebut melaporkan temuan dua kredensial valid untuk pengguna root dengan kata sandi admin dan password. Secara simultan, serangan DDoS dilancarkan menggunakan aplikasi LOIC (Low Orbit Ion Cannon) yang dikonfigurasi untuk membanjiri Port 22 menggunakan metode TCP dengan kekuatan 10 *threads*, yang pada saat pemantauan tercatat telah mengirimkan lebih dari 14.000 paket permintaan (*requested*) guna melumpuhkan sumber daya jaringan target.

b. Target

```
2026-02-02T09:43:45+0000 [-] Ready to accept SSH connections
2026-02-02T09:46:00+0000 [cowrie.ssh.factory.CowrieSSHFactory] No moduli, no diffie-hellman-group-exchange-sha1
2026-02-02T09:46:00+0000 [cowrie.ssh.factory.CowrieSSHFactory] No moduli, no diffie-hellman-group-exchange-sha256
2026-02-02T09:46:00+0000 [cowrie.ssh.factory.CowrieSSHFactory] New connection: 10.101.196.39:48938 (172.17.0.2:2222) [session: 3bbcc467ef36]
2026-02-02T09:46:00+0000 [HoneyPotSSHTransport,0,10.101.196.39] Remote SSH version: SSH-2.0-libssh_0.11.3
2026-02-02T09:46:01+0000 [HoneyPotSSHTransport,0,10.101.196.39] SSH client hashsh fingerprint: 742b4fd5532ca4f243aae081017fe8c5
2026-02-02T09:46:01+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#debug] key alg=b'curve25519-sha256' key alg=b'ssh-ed25519'
2026-02-02T09:46:01+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#debug] outgoing: b'aes256-ctr' b'hmac-sha2-256' b'none'
2026-02-02T09:46:01+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#debug] incoming: b'aes256-ctr' b'hmac-sha2-256' b'none'
2026-02-02T09:46:01+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#debug] NEW KEYS
2026-02-02T09:46:01+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#debug] starting service b'ssh-userauth'
2026-02-02T09:46:01+0000 [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'root' trying auth b'none'
2026-02-02T09:46:01+0000 [HoneyPotSSHTransport,0,10.101.196.39] Got remote error, code 11 reason: b'Bye Bye'
2026-02-02T09:46:01+0000 [cowrie.ssh.factory.CowrieSSHFactory] No moduli, no diffie-hellman-group-exchange-sha1
2026-02-02T09:46:01+0000 [cowrie.ssh.factory.CowrieSSHFactory] No moduli, no diffie-hellman-group-exchange-sha256
2026-02-02T09:46:01+0000 [cowrie.ssh.factory.CowrieSSHFactory] New connection: 10.101.196.39:48944 (172.17.0.2:2222) [session: d2db4ba535dc]
2026-02-02T09:46:01+0000 [cowrie.ssh.factory.CowrieSSHFactory] No moduli, no diffie-hellman-group-exchange-sha1
2026-02-02T09:46:01+0000 [cowrie.ssh.factory.CowrieSSHFactory] No moduli, no diffie-hellman-group-exchange-sha256
2026-02-02T09:46:01+0000 [cowrie.ssh.factory.CowrieSSHFactory] New connection: 10.101.196.39:48960 (172.17.0.2:2222) [session: 67d27ca036f]
2026-02-02T09:46:01+0000 [cowrie.ssh.factory.CowrieSSHFactory] No moduli, no diffie-hellman-group-exchange-sha1
2026-02-02T09:46:01+0000 [cowrie.ssh.factory.CowrieSSHFactory] No moduli, no diffie-hellman-group-exchange-sha256
2026-02-02T09:46:01+0000 [cowrie.ssh.factory.CowrieSSHFactory] New connection: 10.101.196.39:48966 (172.17.0.2:2222) [session: cfcbfd22ba29]
2026-02-02T09:46:01+0000 [HoneyPotSSHTransport,1,10.101.196.39] Remote SSH version: SSH-2.0-libssh_0.11.3
2026-02-02T09:46:01+0000 [HoneyPotSSHTransport,2,10.101.196.39] Remote SSH version: SSH-2.0-libssh_0.11.3
2026-02-02T09:46:01+0000 [HoneyPotSSHTransport,3,10.101.196.39] Remote SSH version: SSH-2.0-libssh_0.11.3
2026-02-02T09:46:01+0000 [HoneyPotSSHTransport,2,10.101.196.39] SSH client hashsh fingerprint: 742b4fd5532ca4f243aae081017fe8c5
2026-02-02T09:46:01+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#debug] key alg=b'curve25519-sha256' key alg=b'ssh-ed25519'
2026-02-02T09:46:01+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#debug] outgoing: b'aes256-ctr' b'hmac-sha2-256' b'none'
2026-02-02T09:46:01+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#debug] incoming: b'aes256-ctr' b'hmac-sha2-256' b'none'
2026-02-02T09:46:01+0000 [HoneyPotSSHTransport,1,10.101.196.39] SSH client hashsh fingerprint: 742b4fd5532ca4f243aae081017fe8c5
2026-02-02T09:46:01+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#debug] key alg=b'curve25519-sha256' key alg=b'ssh-ed25519'
2026-02-02T09:46:01+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#debug] outgoing: b'aes256-ctr' b'hmac-sha2-256' b'none'
2026-02-02T09:46:01+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#debug] incoming: b'aes256-ctr' b'hmac-sha2-256' b'none'
2026-02-02T09:46:01+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#debug] NEW KEYS
2026-02-02T09:46:01+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#debug] starting service b'ssh-userauth'
2026-02-02T09:46:01+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#debug] starting service b'ssh-userauth'
2026-02-02T09:46:01+0000 [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'root' trying auth b'none'
2026-02-02T09:46:01+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#debug] NEW KEYS
2026-02-02T09:46:01+0000 [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'root' trying auth b'none'
2026-02-02T09:46:01+0000 [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'root' trying auth b'password'
2026-02-02T09:46:01+0000 [HoneyPotSSHTransport,2,10.101.196.39] Could not read etc/userdb.txt, default database activated
2026-02-02T09:46:01+0000 [HoneyPotSSHTransport,2,10.101.196.39] login attempt [b'root'/b'password'] succeeded
2026-02-02T09:46:01+0000 [HoneyPotSSHTransport,2,10.101.196.39] Initialized emulated server as architecture: linux-x64-lsb
2026-02-02T09:46:01+0000 [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'root' authenticated with b'password'
2026-02-02T09:46:11+0000 [cowrie.ssh.factory.CowrieSSHFactory] No moduli, no diffie-hellman-group-exchange-sha1
2026-02-02T09:46:11+0000 [cowrie.ssh.factory.CowrieSSHFactory] No moduli, no diffie-hellman-group-exchange-sha256
2026-02-02T09:46:11+0000 [cowrie.ssh.factory.CowrieSSHFactory] New connection: 10.101.196.39:56868 (172.17.0.2:2222) [session: eca38ad60cab]
2026-02-02T09:46:11+0000 [cowrie.ssh.factory.CowrieSSHFactory] No moduli, no diffie-hellman-group-exchange-sha1
2026-02-02T09:46:11+0000 [cowrie.ssh.factory.CowrieSSHFactory] No moduli, no diffie-hellman-group-exchange-sha256
2026-02-02T09:46:11+0000 [cowrie.ssh.factory.CowrieSSHFactory] New connection: 10.101.196.39:56876 (172.17.0.2:2222) [session: 7be214a8be3]
2026-02-02T09:46:12+0000 [cowrie.ssh.factory.CowrieSSHFactory] No moduli, no diffie-hellman-group-exchange-sha1
2026-02-02T09:46:12+0000 [cowrie.ssh.factory.CowrieSSHFactory] No moduli, no diffie-hellman-group-exchange-sha256
2026-02-02T09:46:12+0000 [cowrie.ssh.factory.CowrieSSHFactory] New connection: 10.101.196.39:56892 (172.17.0.2:2222) [session: cbda7a6839c5]
2026-02-02T09:46:12+0000 [cowrie.ssh.factory.CowrieSSHFactory] No moduli, no diffie-hellman-group-exchange-sha1
2026-02-02T09:46:12+0000 [cowrie.ssh.factory.CowrieSSHFactory] No moduli, no diffie-hellman-group-exchange-sha256
2026-02-02T09:46:12+0000 [cowrie.ssh.factory.CowrieSSHFactory] New connection: 10.101.196.39:56104 (172.17.0.2:2222) [session: 4fcb3a1d5927]
2026-02-02T09:46:13+0000 [cowrie.ssh.factory.CowrieSSHFactory] No moduli, no diffie-hellman-group-exchange-sha1
2026-02-02T09:46:13+0000 [cowrie.ssh.factory.CowrieSSHFactory] No moduli, no diffie-hellman-group-exchange-sha256
2026-02-02T09:46:13+0000 [cowrie.ssh.factory.CowrieSSHFactory] New connection: 10.101.196.39:56118 (172.17.0.2:2222) [session: 6662a59c4a52]
2026-02-02T09:46:13+0000 [cowrie.ssh.factory.CowrieSSHFactory] No moduli, no diffie-hellman-group-exchange-sha1
2026-02-02T09:46:13+0000 [cowrie.ssh.factory.CowrieSSHFactory] No moduli, no diffie-hellman-group-exchange-sha256
2026-02-02T09:46:13+0000 [cowrie.ssh.factory.CowrieSSHFactory] New connection: 10.101.196.39:56134 (172.17.0.2:2222) [session: e7d7cd00c1c4]
2026-02-02T09:46:14+0000 [cowrie.ssh.factory.CowrieSSHFactory] No moduli, no diffie-hellman-group-exchange-sha1
2026-02-02T09:46:14+0000 [cowrie.ssh.factory.CowrieSSHFactory] No moduli, no diffie-hellman-group-exchange-sha256
2026-02-02T09:46:14+0000 [cowrie.ssh.factory.CowrieSSHFactory] New connection: 10.101.196.39:56138 (172.17.0.2:2222) [session: 5fad18ea5ef8]
2026-02-02T09:46:14+0000 [cowrie.ssh.factory.CowrieSSHFactory] No moduli, no diffie-hellman-group-exchange-sha1
2026-02-02T09:46:14+0000 [cowrie.ssh.factory.CowrieSSHFactory] No moduli, no diffie-hellman-group-exchange-sha256
2026-02-02T09:46:14+0000 [cowrie.ssh.factory.CowrieSSHFactory] New connection: 10.101.196.39:56146 (172.17.0.2:2222) [session: 70b71684ff33]
2026-02-02T09:46:15+0000 [cowrie.ssh.factory.CowrieSSHFactory] No moduli, no diffie-hellman-group-exchange-sha1
2026-02-02T09:46:15+0000 [cowrie.ssh.factory.CowrieSSHFactory] No moduli, no diffie-hellman-group-exchange-sha256
2026-02-02T09:46:15+0000 [cowrie.ssh.factory.CowrieSSHFactory] New connection: 10.101.196.39:56158 (172.17.0.2:2222) [session: dc9d032e3dfa]
2026-02-02T09:46:15+0000 [cowrie.ssh.factory.CowrieSSHFactory] No moduli, no diffie-hellman-group-exchange-sha1
2026-02-02T09:46:15+0000 [cowrie.ssh.factory.CowrieSSHFactory] No moduli, no diffie-hellman-group-exchange-sha256
2026-02-02T09:46:15+0000 [cowrie.ssh.factory.CowrieSSHFactory] New connection: 10.101.196.39:56168 (172.17.0.2:2222) [session: f2532774052d]
2026-02-02T09:46:16+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#info] connection lost
2026-02-02T09:46:16+0000 [HoneyPotSSHTransport,11,10.101.196.39] Connection lost after 1.4 seconds
2026-02-02T09:46:16+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#info] connection lost
2026-02-02T09:46:16+0000 [HoneyPotSSHTransport,6,10.101.196.39] Connection lost after 4.2 seconds
2026-02-02T09:46:16+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#info] connection lost
2026-02-02T09:46:16+0000 [HoneyPotSSHTransport,12,10.101.196.39] Connection lost after 1.2 seconds
2026-02-02T09:46:16+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#info] connection lost
2026-02-02T09:46:16+0000 [HoneyPotSSHTransport,10,10.101.196.39] Connection lost after 1.7 seconds
2026-02-02T09:46:16+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#info] connection lost
2026-02-02T09:46:16+0000 [HoneyPotSSHTransport,13,10.101.196.39] Connection lost after 0.7 seconds
2026-02-02T09:46:16+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#info] connection lost
2026-02-02T09:46:16+0000 [HoneyPotSSHTransport,9,10.101.196.39] Connection lost after 2.7 seconds
2026-02-02T09:46:16+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#info] connection lost
2026-02-02T09:46:16+0000 [HoneyPotSSHTransport,8,10.101.196.39] Connection lost after 3.3 seconds
2026-02-02T09:46:16+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#info] connection lost
2026-02-02T09:46:16+0000 [HoneyPotSSHTransport,7,10.101.196.39] Connection lost after 3.7 seconds
2026-02-02T09:46:16+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#info] connection lost
2026-02-02T09:46:16+0000 [HoneyPotSSHTransport,5,10.101.196.39] Connection lost after 4.8 seconds
2026-02-02T09:46:16+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#info] connection lost
```

Di sisi target (10.101.196.124), log sistem Honeypot Cowrie secara akurat merekam dampak dari serangan ganda yang terjadi. Log memperlihatkan bahwa sistem emulasi berhasil "ditembus" oleh serangan *Bruteforce*, yang ditandai dengan pesan "login attempt [b'root'/b'password'] succeeded" dan diikuti oleh inisialisasi server palsu (*emulated server*). Namun, pada saat yang hampir bersamaan, log aktivitas juga dipenuhi oleh ribuan baris "New connection" dari IP penyerang 10.101.196.39 yang segera disusul dengan pesan "connection lost" dalam interval waktu milidetik. Fenomena banjir trafik

ini mengonfirmasi bahwa serangan DDoS sedang berlangsung secara masif, namun Cowrie tetap mampu memilah aktivitas tersebut dan mendokumentasikan intrusi login ilegal di tengah kekacauan trafik jaringan yang terjadi.

3. Ddos dan Port Scanning

a. Penyerang



```
(root@ririn)-[/home/ririn]
# nmap 10.101.196.124
Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-02 17:50 WITA
Nmap scan report for 10.101.196.124
Host is up (0.012s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
23/tcp    open  telnet
MAC Address: 50:BB:B5:34:BC:26 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 4.84 seconds
```

Pada sisi penyerang (root@ririn), strategi ofensif dimulai dengan tahap pengumpulan informasi (*reconnaissance*) menggunakan Nmap, yang secara efektif memetakan topologi target 10.101.196.124 dan mengungkapkan bahwa layanan kritis pada Port 22 (SSH) dan Port 23 (Telnet) berada dalam status terbuka (*open*). Berbekal temuan celah keamanan tersebut, penyerang segera meluncurkan serangan DDoS menggunakan alat LOIC (Low Orbit Ion Cannon) untuk membanjiri trafik pada Port 22. Melalui metode serangan *TCP Flooding* yang dijalankan dengan intensitas 10 *threads*, *dashboard* penyerangan mencatat pengiriman lebih dari 14.000 paket permintaan (*requested*) dalam waktu singkat, yang bertujuan untuk menghabiskan sumber daya koneksi target yang baru saja teridentifikasi tersebut.

b. Target

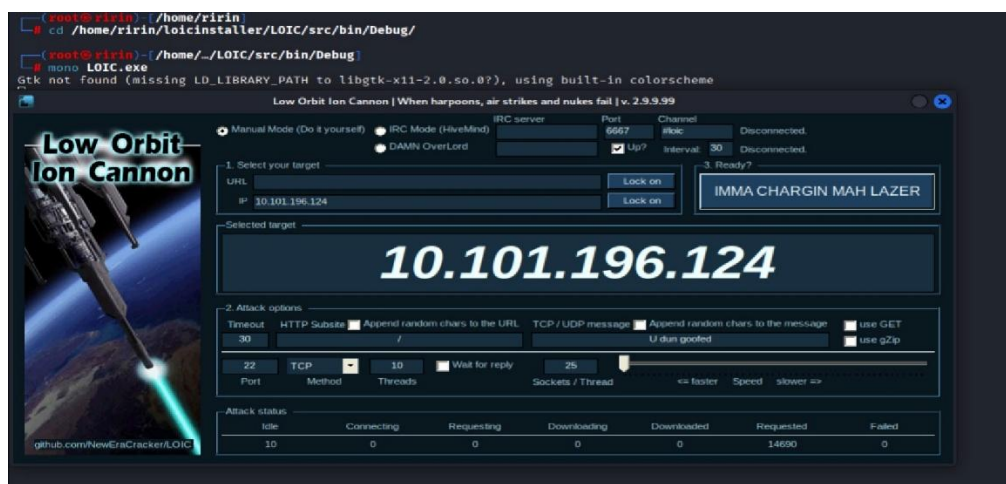
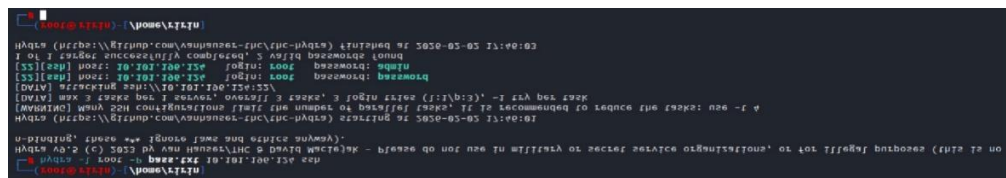
2026-02-02T09:50:32+0000	[cowrie.ssh.factory.CowrieSSHFactory]	No moduli, no diffie-hellman-group-exchange-sha256
2026-02-02T09:50:32+0000	[cowrie.ssh.factory.CowrieSSHFactory]	New connection: 10.101.196.39:49234 (172.17.0.2:2222) [session: ed81710c1fbd]
2026-02-02T09:50:32+0000	[cowrie.ssh.factory.CowrieSSHFactory]	No moduli, no diffie-hellman-group-exchange-sha1
2026-02-02T09:50:32+0000	[cowrie.ssh.factory.CowrieSSHFactory]	No moduli, no diffie-hellman-group-exchange-sha256
2026-02-02T09:50:32+0000	[cowrie.ssh.factory.CowrieSSHFactory]	New connection: 10.101.196.39:49244 (172.17.0.2:2222) [session: 600ea891c470]
2026-02-02T09:50:33+0000	[cowrie.ssh.factory.CowrieSSHFactory]	No moduli, no diffie-hellman-group-exchange-sha1
2026-02-02T09:50:33+0000	[cowrie.ssh.factory.CowrieSSHFactory]	No moduli, no diffie-hellman-group-exchange-sha256
2026-02-02T09:50:33+0000	[cowrie.ssh.factory.CowrieSSHFactory]	New connection: 10.101.196.39:49254 (172.17.0.2:2222) [session: bd0495173f91]
2026-02-02T09:50:33+0000	[cowrie.ssh.factory.CowrieSSHFactory]	No moduli, no diffie-hellman-group-exchange-sha1
2026-02-02T09:50:33+0000	[cowrie.ssh.factory.CowrieSSHFactory]	No moduli, no diffie-hellman-group-exchange-sha256
2026-02-02T09:50:34+0000	[cowrie.ssh.factory.CowrieSSHFactory]	No moduli, no diffie-hellman-group-exchange-sha1
2026-02-02T09:50:34+0000	[cowrie.ssh.factory.CowrieSSHFactory]	No moduli, no diffie-hellman-group-exchange-sha256
2026-02-02T09:50:34+0000	[cowrie.ssh.factory.CowrieSSHFactory]	New connection: 10.101.196.39:49262 (172.17.0.2:2222) [session: d6ed64c0ee95]
2026-02-02T09:50:34+0000	[cowrie.ssh.factory.CowrieSSHFactory]	No moduli, no diffie-hellman-group-exchange-sha1
2026-02-02T09:50:34+0000	[cowrie.ssh.factory.CowrieSSHFactory]	No moduli, no diffie-hellman-group-exchange-sha256
2026-02-02T09:50:34+0000	[cowrie.ssh.factory.CowrieSSHFactory]	New connection: 10.101.196.39:49270 (172.17.0.2:2222) [session: 187389b8f2e4]
2026-02-02T09:50:35+0000	[cowrie.ssh.factory.CowrieSSHFactory]	No moduli, no diffie-hellman-group-exchange-sha1
2026-02-02T09:50:35+0000	[cowrie.ssh.factory.CowrieSSHFactory]	New connection: 10.101.196.39:49286 (172.17.0.2:2222) [session: 59efbf4afad4]
2026-02-02T09:50:35+0000	[cowrie.ssh.factory.CowrieSSHFactory]	No moduli, no diffie-hellman-group-exchange-sha1
2026-02-02T09:50:35+0000	[cowrie.ssh.factory.CowrieSSHFactory]	No moduli, no diffie-hellman-group-exchange-sha256
2026-02-02T09:50:36+0000	[cowrie.ssh.factory.CowrieSSHFactory]	New connection: 10.101.196.39:49302 (172.17.0.2:2222) [session: 99fd79502494]
2026-02-02T09:50:36+0000	[cowrie.ssh.factory.CowrieSSHFactory]	No moduli, no diffie-hellman-group-exchange-sha1
2026-02-02T09:50:36+0000	[cowrie.ssh.factory.CowrieSSHFactory]	No moduli, no diffie-hellman-group-exchange-sha256
2026-02-02T09:50:36+0000	[cowrie.ssh.factory.CowrieSSHFactory]	New connection: 10.101.196.39:49318 (172.17.0.2:2222) [session: 421dd9caa344]
2026-02-02T09:50:36+0000	[cowrie.ssh.factory.CowrieSSHFactory]	No moduli, no diffie-hellman-group-exchange-sha1
2026-02-02T09:50:36+0000	[cowrie.ssh.factory.CowrieSSHFactory]	No moduli, no diffie-hellman-group-exchange-sha256
2026-02-02T09:50:36+0000	[cowrie.ssh.factory.CowrieSSHFactory]	New connection: 10.101.196.39:49328 (172.17.0.2:2222) [session: aadc78921749]
2026-02-02T09:50:47+0000	[cowrie.ssh.transport.HoneyPotSSHTransportInfo]	connection lost
2026-02-02T09:50:47+0000	[HoneyPotSSHTransport,17,10.101.196.39]	Connection lost after 13.9 seconds
2026-02-02T09:50:47+0000	[cowrie.ssh.transport.HoneyPotSSHTransportInfo]	connection lost
2026-02-02T09:50:47+0000	[HoneyPotSSHTransport,16,10.101.196.39]	Connection lost after 14.4 seconds
2026-02-02T09:50:47+0000	[cowrie.ssh.transport.HoneyPotSSHTransportInfo]	connection lost
2026-02-02T09:50:47+0000	[HoneyPotSSHTransport,18,10.101.196.39]	Connection lost after 13.4 seconds
2026-02-02T09:50:47+0000	[cowrie.ssh.transport.HoneyPotSSHTransportInfo]	connection lost
2026-02-02T09:50:47+0000	[HoneyPotSSHTransport,21,10.101.196.39]	Connection lost after 11.9 seconds
2026-02-02T09:50:47+0000	[cowrie.ssh.transport.HoneyPotSSHTransportInfo]	connection lost
2026-02-02T09:50:47+0000	[HoneyPotSSHTransport,23,10.101.196.39]	Connection lost after 10.9 seconds
2026-02-02T09:50:47+0000	[cowrie.ssh.transport.HoneyPotSSHTransportInfo]	connection lost
2026-02-02T09:50:47+0000	[HoneyPotSSHTransport,22,10.101.196.39]	Connection lost after 11.4 seconds
2026-02-02T09:50:47+0000	[cowrie.ssh.transport.HoneyPotSSHTransportInfo]	connection lost
2026-02-02T09:50:47+0000	[HoneyPotSSHTransport,19,10.101.196.39]	Connection lost after 12.9 seconds
2026-02-02T09:50:47+0000	[cowrie.ssh.transport.HoneyPotSSHTransportInfo]	connection lost
2026-02-02T09:50:47+0000	[HoneyPotSSHTransport,14,10.101.196.39]	Connection lost after 15.4 seconds
2026-02-02T09:50:47+0000	[cowrie.ssh.transport.HoneyPotSSHTransportInfo]	connection lost
2026-02-02T09:50:47+0000	[HoneyPotSSHTransport,15,10.101.196.39]	Connection lost after 14.9 seconds
2026-02-02T09:50:47+0000	[cowrie.ssh.transport.HoneyPotSSHTransportInfo]	connection lost
Session Actions Edit View Help		
2026-02-02T09:53:35+0000	[cowrie.ssh.factory.CowrieSSHFactory]	New connection: 10.101.196.39:48148 (172.17.0.2:2222) [session: 32d787fb1414]
2026-02-02T09:53:35+0000	[HoneyPotSSHTransport,24,10.101.196.39]	Remote SSH version: SSH-2.0-libssh_0.11.3
2026-02-02T09:53:35+0000	[HoneyPotSSHTransport,24,10.101.196.39]	SSH client hash fingerprint: 742b4fd5532ca4f243aae081017fe8c5
2026-02-02T09:53:35+0000	[cowrie.ssh.transport.HoneyPotSSHTransportDebug]	key alg=b'curve25519-sha256' key alg=b'ssh-ed25519'
2026-02-02T09:53:35+0000	[cowrie.ssh.transport.HoneyPotSSHTransportDebug]	outgoing: b'aes256-ctr' b'hmac-sha2-256' b'none'
2026-02-02T09:53:35+0000	[cowrie.ssh.transport.HoneyPotSSHTransportDebug]	incoming: b'aes256-ctr' b'hmac-sha2-256' b'none'
2026-02-02T09:53:36+0000	[cowrie.ssh.transport.HoneyPotSSHTransportDebug]	NEW KEYS
2026-02-02T09:53:36+0000	[cowrie.ssh.transport.HoneyPotSSHTransportDebug]	starting service b'ssh-userauth'
2026-02-02T09:53:36+0000	[cowrie.ssh.userauth.HoneyPotSSHUserAuthServerDebug]	b'root' trying auth b'none'
2026-02-02T09:53:36+0000	[HoneyPotSSHTransport,24,10.101.196.39]	Got remote error, code 11 reason: b'Bye Bye'
2026-02-02T09:53:36+0000	[cowrie.ssh.transport.HoneyPotSSHTransportInfo]	connection lost
2026-02-02T09:53:36+0000	[HoneyPotSSHTransport,24,10.101.196.39]	Connection lost after 0.4 seconds
2026-02-02T09:53:36+0000	[cowrie.ssh.factory.CowrieSSHFactory]	No moduli, no diffie-hellman-group-exchange-sha1
2026-02-02T09:53:36+0000	[cowrie.ssh.factory.CowrieSSHFactory]	No moduli, no diffie-hellman-group-exchange-sha256
2026-02-02T09:53:36+0000	[cowrie.ssh.factory.CowrieSSHFactory]	New connection: 10.101.196.39:48160 (172.17.0.2:2222) [session: 07719ccf1f0c]
2026-02-02T09:53:36+0000	[cowrie.ssh.factory.CowrieSSHFactory]	No moduli, no diffie-hellman-group-exchange-sha1
2026-02-02T09:53:36+0000	[cowrie.ssh.factory.CowrieSSHFactory]	No moduli, no diffie-hellman-group-exchange-sha256
2026-02-02T09:53:36+0000	[cowrie.ssh.factory.CowrieSSHFactory]	New connection: 10.101.196.39:48176 (172.17.0.2:2222) [session: 44f04e2e592b]
2026-02-02T09:53:36+0000	[cowrie.ssh.factory.CowrieSSHFactory]	No moduli, no diffie-hellman-group-exchange-sha1
2026-02-02T09:53:36+0000	[cowrie.ssh.factory.CowrieSSHFactory]	No moduli, no diffie-hellman-group-exchange-sha256
2026-02-02T09:53:36+0000	[cowrie.ssh.factory.CowrieSSHFactory]	New connection: 10.101.196.39:48184 (172.17.0.2:2222) [session: 4ddf98091e59]
2026-02-02T09:53:36+0000	[HoneyPotSSHTransport,25,10.101.196.39]	Remote SSH version: SSH-2.0-libssh_0.11.3
2026-02-02T09:53:36+0000	[HoneyPotSSHTransport,26,10.101.196.39]	Remote SSH version: SSH-2.0-libssh_0.11.3
2026-02-02T09:53:36+0000	[HoneyPotSSHTransport,27,10.101.196.39]	Remote SSH version: SSH-2.0-libssh_0.11.3
2026-02-02T09:53:36+0000	[HoneyPotSSHTransport,26,10.101.196.39]	SSH client hash fingerprint: 742b4fd5532ca4f243aae081017fe8c5
2026-02-02T09:53:36+0000	[cowrie.ssh.transport.HoneyPotSSHTransportDebug]	key alg=b'curve25519-sha256' key alg=b'ssh-ed25519'
2026-02-02T09:53:36+0000	[cowrie.ssh.transport.HoneyPotSSHTransportDebug]	outgoing: b'aes256-ctr' b'hmac-sha2-256' b'none'
2026-02-02T09:53:36+0000	[cowrie.ssh.transport.HoneyPotSSHTransportDebug]	incoming: b'aes256-ctr' b'hmac-sha2-256' b'none'
2026-02-02T09:53:36+0000	[HoneyPotSSHTransport,27,10.101.196.39]	SSH client hash fingerprint: 742b4fd5532ca4f243aae081017fe8c5
2026-02-02T09:53:36+0000	[cowrie.ssh.transport.HoneyPotSSHTransportDebug]	key alg=b'curve25519-sha256' key alg=b'ssh-ed25519'
2026-02-02T09:53:36+0000	[cowrie.ssh.transport.HoneyPotSSHTransportDebug]	outgoing: b'aes256-ctr' b'hmac-sha2-256' b'none'
2026-02-02T09:53:36+0000	[cowrie.ssh.transport.HoneyPotSSHTransportDebug]	incoming: b'aes256-ctr' b'hmac-sha2-256' b'none'
2026-02-02T09:53:36+0000	[HoneyPotSSHTransport,25,10.101.196.39]	SSH client hash fingerprint: 742b4fd5532ca4f243aae081017fe8c5
2026-02-02T09:53:36+0000	[cowrie.ssh.transport.HoneyPotSSHTransportDebug]	key alg=b'curve25519-sha256' key alg=b'ssh-ed25519'
2026-02-02T09:53:36+0000	[cowrie.ssh.transport.HoneyPotSSHTransportDebug]	outgoing: b'aes256-ctr' b'hmac-sha2-256' b'none'
2026-02-02T09:53:36+0000	[cowrie.ssh.transport.HoneyPotSSHTransportDebug]	incoming: b'aes256-ctr' b'hmac-sha2-256' b'none'
2026-02-02T09:53:36+0000	[cowrie.ssh.transport.HoneyPotSSHTransportDebug]	NEW KEYS
2026-02-02T09:53:36+0000	[cowrie.ssh.transport.HoneyPotSSHTransportDebug]	starting service b'ssh-userauth'
2026-02-02T09:53:36+0000	[cowrie.ssh.transport.HoneyPotSSHTransportDebug]	starting service b'ssh-userauth'
2026-02-02T09:53:36+0000	[cowrie.ssh.userauth.HoneyPotSSHUserAuthServerDebug]	b'root' trying auth b'none'
2026-02-02T09:53:36+0000	[cowrie.ssh.transport.HoneyPotSSHTransportDebug]	starting service b'ssh-userauth'
2026-02-02T09:53:36+0000	[cowrie.ssh.userauth.HoneyPotSSHUserAuthServerDebug]	b'root' trying auth b'none'
2026-02-02T09:53:36+0000	[cowrie.ssh.userauth.HoneyPotSSHUserAuthServerDebug]	b'root' trying auth b'password'
2026-02-02T09:53:36+0000	[HoneyPotSSHTransport,27,10.101.196.39]	Could not read etc/userdb.txt, default database activated
2026-02-02T09:53:36+0000	[HoneyPotSSHTransport,27,10.101.196.39]	Login attempt [b'root' b'admin'] succeeded
2026-02-02T09:53:36+0000	[HoneyPotSSHTransport,27,10.101.196.39]	Initialized emulated server as architecture: linux-x64-lsb
2026-02-02T09:53:36+0000	[cowrie.ssh.userauth.HoneyPotSSHUserAuthServerDebug]	b'root' authenticated with b'password'
2026-02-02T09:53:36+0000	[cowrie.ssh.transport.HoneyPotSSHTransportDebug]	starting service b'ssh-connection'
2026-02-02T09:53:36+0000	[cowrie.ssh.userauth.HoneyPotSSHUserAuthServerDebug]	b'root' trying auth b'none'
2026-02-02T09:53:36+0000	[cowrie.ssh.userauth.HoneyPotSSHUserAuthServerDebug]	b'root' trying auth b'password'
2026-02-02T09:53:36+0000	[HoneyPotSSHTransport,26,10.101.196.39]	Could not read etc/userdb.txt, default database activated

Di sisi target, mekanisme pemantauan HoneyPot Cowrie berhasil mengidentifikasi anomali lalu lintas jaringan yang signifikan sebagai respons terhadap aktivitas *Port Scanning* dan *DDoS* dari alamat IP 10.101.196.39. Indikasi awal pemindaian terekam saat sistem mendeteksi upaya identifikasi layanan melalui pertukaran *fingerprint* klien SSH (SSH-2.0-libssh), yang menandakan bahwa *port* sedang dipetakan oleh alat pemindai. Eskalasi serangan kemudian divisualisasi secara dramatis melalui ribuan baris log yang menampilkan siklus cepat antara status "New connection" dan "connection

C. MULTIPLE

```
(root@ririn)-[/home/ririn]
# nmap 10.101.196.124
Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-02 17:50 WITA
Nmap scan report for 10.101.196.124
Host is up (0.012s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
23/tcp    open  telnet
MAC Address: 50:BB:B5:34:BC:26 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 4.84 seconds
```



Pada sisi penyerang (root@ririn), skenario serangan gabungan dieksekusi secara sistematis dimulai dengan tahap *reconnaissance* menggunakan Nmap, yang berhasil mengungkap celah keamanan berupa status *open* pada layanan kritis Port 22 (SSH) dan Port 23 (Telnet) di target 10.101.196.124. Temuan ini langsung dieksploitasi melalui serangan *Bruteforce* menggunakan Hydra, yang secara efektif menembus otentikasi sistem dan mendapatkan dua kredensial valid untuk pengguna root (admin dan password). Operasi ofensif diakhiri dengan serangan destruktif DDoS menggunakan LOIC (Low Orbit Ion Cannon), yang membanjiri Port 22 melalui metode *TCP Flooding* dengan kekuatan 10 *threads*, mengirimkan lebih dari 14.000 paket permintaan untuk melumpuhkan ketersediaan layanan target.

b. Target

[illegible]

```

2026-02-02T09:43:45+0000 [-] Ready to accept SSH connections
2026-02-02T09:46:00+0000 [cwire.ssh.factory.CWireSSHFactory] No moduli, no diffie-hellman-group-exchange-sha1
2026-02-02T09:46:00+0000 [cwire.ssh.factory.CWireSSHFactory] No moduli, no diffie-hellman-group-exchange-sha256
2026-02-02T09:46:00+0000 [cwire.ssh.factory.CWireSSHFactory] New connection: 10.101.196.39:48938 (172.17.0.2:2222) [session: 3bbc4a67ef36]
2026-02-02T09:46:01+0000 [cwire.ssh.transport.HoneyPotSSHTransport#0,10.101.196.39] Remote SSH version: SSH-2.0-1ibss0.11.3
2026-02-02T09:46:01+0000 [cwire.ssh.transport.HoneyPotSSHTransport#0,10.101.196.39] SSH client hash fingerprint: 74264d5532cafa243aa0e0b107f8eb5
2026-02-02T09:46:01+0000 [cwire.ssh.transport.HoneyPotSSHTransport#debug] kex alg=b'curve25519-sha256' key alg=b'ssh-ed25519'
2026-02-02T09:46:01+0000 [cwire.ssh.transport.HoneyPotSSHTransport#debug] outgoing: b'aes256-ctr' b'hmac-sha2-256' b'none'
2026-02-02T09:46:01+0000 [cwire.ssh.transport.HoneyPotSSHTransport#debug] incoming: b'aes256-ctr' b'hmac-sha2-256' b'none'
2026-02-02T09:46:01+0000 [cwire.ssh.transport.HoneyPotSSHTransport#debug] NEW KEYS
2026-02-02T09:46:01+0000 [cwire.ssh.transport.HoneyPotSSHTransport#debug] Starting service b'ssh-userauth'
2026-02-02T09:46:01+0000 [cwire.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'root' trying auth b'none'
2026-02-02T09:46:01+0000 [cwire.ssh.userauth.HoneyPotSSHUserAuthServer#debug] Got remote error, code 11 reason: b'Bye Bye'
2026-02-02T09:46:01+0000 [cwire.ssh.transport.HoneyPotSSHTransport#info] connection lost
2026-02-02T09:46:01+0000 [cwire.ssh.transport.HoneyPotSSHTransport#0,10.101.196.39] Connection lost after 0.2 seconds
2026-02-02T09:46:01+0000 [cwire.ssh.factory.CWireSSHFactory] No moduli, no diffie-hellman-group-exchange-sha1
2026-02-02T09:46:01+0000 [cwire.ssh.factory.CWireSSHFactory] No moduli, no diffie-hellman-group-exchange-sha256
2026-02-02T09:46:01+0000 [cwire.ssh.factory.CWireSSHFactory] New connection: 10.101.196.39:48944 (172.17.0.2:2222) [session: d2db4ba535dc]
2026-02-02T09:46:01+0000 [cwire.ssh.factory.CWireSSHFactory] No moduli, no diffie-hellman-group-exchange-sha1
2026-02-02T09:46:01+0000 [cwire.ssh.factory.CWireSSHFactory] No moduli, no diffie-hellman-group-exchange-sha256
2026-02-02T09:46:01+0000 [cwire.ssh.factory.CWireSSHFactory] New connection: 10.101.196.39:48960 (172.17.0.2:2222) [session: 67d27ca036f]
2026-02-02T09:46:01+0000 [cwire.ssh.factory.CWireSSHFactory] No moduli, no diffie-hellman-group-exchange-sha1
2026-02-02T09:46:01+0000 [cwire.ssh.factory.CWireSSHFactory] No moduli, no diffie-hellman-group-exchange-sha256
2026-02-02T09:46:01+0000 [cwire.ssh.factory.CWireSSHFactory] New connection: 10.101.196.39:48966 (172.17.0.2:2222) [session: cfcfb22b429]
2026-02-02T09:46:01+0000 [cwire.ssh.transport.HoneyPotSSHTransport#1,10.101.196.39] Remote SSH version: SSH-2.0-1ibss0.11.3
2026-02-02T09:46:01+0000 [cwire.ssh.transport.HoneyPotSSHTransport#1,10.101.196.39] Remote SSH version: SSH-2.0-1ibss0.11.3
2026-02-02T09:46:01+0000 [cwire.ssh.transport.HoneyPotSSHTransport#1,10.101.196.39] SSH client hash fingerprint: 74264d5532cafa243aa0e0b107f8eb5
2026-02-02T09:46:01+0000 [cwire.ssh.transport.HoneyPotSSHTransport#debug] kex alg=b'curve25519-sha256' key alg=b'ssh-ed25519'
2026-02-02T09:46:01+0000 [cwire.ssh.transport.HoneyPotSSHTransport#debug] outgoing: b'aes256-ctr' b'hmac-sha2-256' b'none'
2026-02-02T09:46:01+0000 [cwire.ssh.transport.HoneyPotSSHTransport#debug] incoming: b'aes256-ctr' b'hmac-sha2-256' b'none'
2026-02-02T09:46:01+0000 [cwire.ssh.transport.HoneyPotSSHTransport#1,10.101.196.39] SSH client hash fingerprint: 74264d5532cafa243aa0e0b107f8eb5
2026-02-02T09:46:01+0000 [cwire.ssh.transport.HoneyPotSSHTransport#debug] kex alg=b'curve25519-sha256' key alg=b'ssh-ed25519'
2026-02-02T09:46:01+0000 [cwire.ssh.transport.HoneyPotSSHTransport#debug] outgoing: b'aes256-ctr' b'hmac-sha2-256' b'none'
2026-02-02T09:46:01+0000 [cwire.ssh.transport.HoneyPotSSHTransport#debug] incoming: b'aes256-ctr' b'hmac-sha2-256' b'none'
2026-02-02T09:46:01+0000 [cwire.ssh.transport.HoneyPotSSHTransport#1,10.101.196.39] SSH client hash fingerprint: 74264d5532cafa243aa0e0b107f8eb5
2026-02-02T09:46:01+0000 [cwire.ssh.transport.HoneyPotSSHTransport#debug] kex alg=b'curve25519-sha256' key alg=b'ssh-ed25519'
2026-02-02T09:46:01+0000 [cwire.ssh.transport.HoneyPotSSHTransport#debug] outgoing: b'aes256-ctr' b'hmac-sha2-256' b'none'
2026-02-02T09:46:01+0000 [cwire.ssh.transport.HoneyPotSSHTransport#debug] incoming: b'aes256-ctr' b'hmac-sha2-256' b'none'
2026-02-02T09:46:01+0000 [cwire.ssh.transport.HoneyPotSSHTransport#debug] NEW KEYS
2026-02-02T09:46:01+0000 [cwire.ssh.transport.HoneyPotSSHTransport#debug] Starting service b'ssh-userauth'
2026-02-02T09:46:01+0000 [cwire.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'root' trying auth b'none'
2026-02-02T09:46:01+0000 [cwire.ssh.userauth.HoneyPotSSHUserAuthServer#debug] NEW KEYS
2026-02-02T09:46:01+0000 [cwire.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'root' trying auth b'none'
2026-02-02T09:46:01+0000 [cwire.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'root' trying auth b'password'
2026-02-02T09:46:01+0000 [cwire.ssh.userauth.HoneyPotSSHUserAuthServer#debug] Could not read etc/ssh/ssh_config, default database activated
2026-02-02T09:46:01+0000 [cwire.ssh.userauth.HoneyPotSSHUserAuthServer#debug] login attempted (b'root' b'password') succeeded
2026-02-02T09:46:01+0000 [cwire.ssh.transport.HoneyPotSSHTransport#2,10.101.196.39] Initialized emulated server as architecture: linux-x86_64-1sb

```

```

2026-02-02T09:50:32:0000 [cowrie.ssh.factory.CowrieSSHFactory] No moduli, no diffie-hellman-group-exchange-sha256
2026-02-02T09:50:32:0000 [cowrie.ssh.factory.CowrieSSHFactory] New connection: 10.101.196.39:49234 (172.17.0.2:22222) [session: ed81710c1fbd]
2026-02-02T09:50:32:0000 [cowrie.ssh.factory.CowrieSSHFactory] No moduli, no diffie-hellman-group-exchange-sha1
2026-02-02T09:50:32:0000 [cowrie.ssh.factory.CowrieSSHFactory] No moduli, no diffie-hellman-group-exchange-sha256
2026-02-02T09:50:32:0000 [cowrie.ssh.factory.CowrieSSHFactory] New connection: 10.101.196.39:49244 (172.17.0.2:22222) [session: 600ea91c470]
2026-02-02T09:50:33:0000 [cowrie.ssh.factory.CowrieSSHFactory] No moduli, no diffie-hellman-group-exchange-sha1
2026-02-02T09:50:33:0000 [cowrie.ssh.factory.CowrieSSHFactory] No moduli, no diffie-hellman-group-exchange-sha256
2026-02-02T09:50:33:0000 [cowrie.ssh.factory.CowrieSSHFactory] New connection: 10.101.196.39:49254 (172.17.0.2:22222) [session: bd0495173f91]
2026-02-02T09:50:33:0000 [cowrie.ssh.factory.CowrieSSHFactory] No moduli, no diffie-hellman-group-exchange-sha1
2026-02-02T09:50:33:0000 [cowrie.ssh.factory.CowrieSSHFactory] No moduli, no diffie-hellman-group-exchange-sha256
2026-02-02T09:50:34:0000 [cowrie.ssh.factory.CowrieSSHFactory] New connection: 10.101.196.39:49262 (172.17.0.2:22222) [session: d6ed64c0ee95]
2026-02-02T09:50:34:0000 [cowrie.ssh.factory.CowrieSSHFactory] No moduli, no diffie-hellman-group-exchange-sha1
2026-02-02T09:50:34:0000 [cowrie.ssh.factory.CowrieSSHFactory] New connection: 10.101.196.39:49270 (172.17.0.2:22222) [session: 187389b8f2e4]
2026-02-02T09:50:35:0000 [cowrie.ssh.factory.CowrieSSHFactory] No moduli, no diffie-hellman-group-exchange-sha1
2026-02-02T09:50:35:0000 [cowrie.ssh.factory.CowrieSSHFactory] New connection: 10.101.196.39:49286 (172.17.0.2:22222) [session: 59efbfa4fad4]
2026-02-02T09:50:35:0000 [cowrie.ssh.factory.CowrieSSHFactory] No moduli, no diffie-hellman-group-exchange-sha1
2026-02-02T09:50:35:0000 [cowrie.ssh.factory.CowrieSSHFactory] No moduli, no diffie-hellman-group-exchange-sha256
2026-02-02T09:50:36:0000 [cowrie.ssh.factory.CowrieSSHFactory] New connection: 10.101.196.39:49302 (172.17.0.2:22222) [session: 99fd79502494]
2026-02-02T09:50:36:0000 [cowrie.ssh.factory.CowrieSSHFactory] No moduli, no diffie-hellman-group-exchange-sha1
2026-02-02T09:50:36:0000 [cowrie.ssh.factory.CowrieSSHFactory] No moduli, no diffie-hellman-group-exchange-sha256
2026-02-02T09:50:36:0000 [cowrie.ssh.factory.CowrieSSHFactory] New connection: 10.101.196.39:49318 (172.17.0.2:22222) [session: 421dd9caa344]
2026-02-02T09:50:36:0000 [cowrie.ssh.factory.CowrieSSHFactory] No moduli, no diffie-hellman-group-exchange-sha1
2026-02-02T09:50:36:0000 [cowrie.ssh.factory.CowrieSSHFactory] No moduli, no diffie-hellman-group-exchange-sha256
2026-02-02T09:50:36:0000 [cowrie.ssh.factory.CowrieSSHFactory] New connection: 10.101.196.39:49328 (172.17.0.2:22222) [session: aadc78921749]
2026-02-02T09:50:47:0000 [cowrie.ssh.transport.HoneyPotSSHTransport#info] connection lost
2026-02-02T09:50:47:0000 [HoneyPotSSHTransport,17,10.101.196.39] Connection lost after 13.9 seconds
2026-02-02T09:50:47:0000 [cowrie.ssh.transport.HoneyPotSSHTransport#info] connection lost
2026-02-02T09:50:47:0000 [HoneyPotSSHTransport,16,10.101.196.39] Connection lost after 14.4 seconds
2026-02-02T09:50:47:0000 [cowrie.ssh.transport.HoneyPotSSHTransport#info] connection lost
2026-02-02T09:50:47:0000 [HoneyPotSSHTransport,18,10.101.196.39] Connection lost after 13.4 seconds
2026-02-02T09:50:47:0000 [cowrie.ssh.transport.HoneyPotSSHTransport#info] connection lost
2026-02-02T09:50:47:0000 [HoneyPotSSHTransport,21,10.101.196.39] Connection lost after 11.9 seconds
2026-02-02T09:50:47:0000 [cowrie.ssh.transport.HoneyPotSSHTransport#info] connection lost
2026-02-02T09:50:47:0000 [HoneyPotSSHTransport,23,10.101.196.39] Connection lost after 10.9 seconds
2026-02-02T09:50:47:0000 [cowrie.ssh.transport.HoneyPotSSHTransport#info] connection lost
2026-02-02T09:50:47:0000 [HoneyPotSSHTransport,22,10.101.196.39] Connection lost after 11.4 seconds
2026-02-02T09:50:47:0000 [cowrie.ssh.transport.HoneyPotSSHTransport#info] connection lost
2026-02-02T09:50:47:0000 [HoneyPotSSHTransport,19,10.101.196.39] Connection lost after 12.9 seconds
2026-02-02T09:50:47:0000 [cowrie.ssh.transport.HoneyPotSSHTransport#info] connection lost
2026-02-02T09:50:47:0000 [HoneyPotSSHTransport,14,10.101.196.39] Connection lost after 15.4 seconds
2026-02-02T09:50:47:0000 [cowrie.ssh.transport.HoneyPotSSHTransport#info] connection lost
2026-02-02T09:50:47:0000 [HoneyPotSSHTransport,15,10.101.196.39] Connection lost after 14.9 seconds
2026-02-02T09:50:47:0000 [cowrie.ssh.transport.HoneyPotSSHTransport#info] connection lost

```

Di sisi target, sistem Honeypot Cowrie merekam eskalasi ancaman yang bermula dari deteksi *Port Scanning*, di mana log mencatat pertukaran identitas versi SSH (SSH-2.0-libssh) dari IP penyerang 10.101.196.39 sebagai upaya awal pemetaan layanan. Aktivitas ini segera disusul oleh keberhasilan penetrasi *Bruteforce*, yang dibuktikan dengan log kritis "login attempt [b'root'/b'password'] succeeded" dan inisialisasi server emulasi, menandakan penyerang telah masuk ke dalam perangkat honeypot. Namun, stabilitas koneksi segera terganggu oleh serangan DDoS, yang membanjiri log sistem dengan ribuan siklus "New connection" dan "Connection lost" dalam hitungan milidetik, menciptakan kebisingan trafik (*traffic noise*) yang ekstrem namun gagal menutupi jejak intrusi ilegal yang sebelumnya telah diamankan oleh sistem.

8. Hasil Penyerangan

No	Pola Serangan	Nama Pengujian	Kondisi Sebelum (%)	Kondisi Sesudah (%)	Hasil (Terdeteksi atau Tidak Terdeteksi)
1	Individual	Port Scanning	0%	100%	Terdeteksi
2		Bruteforce Attack	0%	100%	Terdeteksi
3		DdoS Attack	0%	100%	Terdeteksi
4	Double	Port Scanning & Burteforce Attack	0%	100%	Terdeteksi
5		Bruteforce Attack & DDoS Attack	0%	100%	Terdeteksi

6		DDoS Attack & Port Scanning	0%	100%	Terdeteksi
7	Multiple	Port Scanning, Bruteforce Attack, DDoS Attack	0%	100%	Terdeteksi

9. Kesimpulan

Berdasarkan seluruh rangkaian pengujian yang telah dilakukan dapat disimpulkan bahwa implementasi *Honeypot* Cowrie berbasis Docker terbukti sangat efektif sebagai mekanisme pertahanan aktif dan sistem peringatan dini. Melalui simulasi serangan bertingkat yang mencakup *Port Scanning*, *Bruteforce*, dan *DDoS*—baik dalam skenario serangan tunggal, ganda (*Double Attack*), maupun gabungan (*Multiple Attack*)—sistem mampu mencapai tingkat keberhasilan deteksi sebesar 100% dengan tetap menjaga stabilitas layanan utama melalui isolasi jaringan pada port 2222. Kemampuan Cowrie dalam memilah trafik anomali di tengah banjir serangan DDoS, serta keakuratannya dalam merekam jejak forensik digital seperti alamat IP penyerang, *fingerprint* alat serangan, dan kredensial ilegal, menegaskan bahwa sistem ini tidak hanya berfungsi sebagai alat deteksi, tetapi juga sebagai instrumen intelijen ancaman yang andal untuk meningkatkan postur keamanan server VPS secara keseluruhan.