LAPORAN TUGAS BESAR

IMPLEMENTASI HONEYPOT SEBAGAI PENDETEKSI SERANGAN VPS

FIRROFIQIL A'LA KADRAM **105841115023**

HERMI NUR SAFITRI **105841116223**

PROGRAM STUDI INFORMATIKA

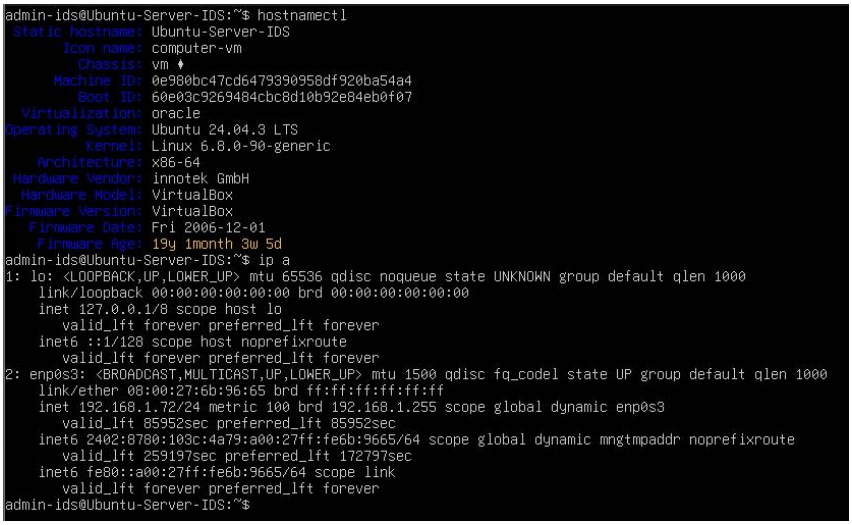
FAKULTAS TEKNIK

UNIVERSITAS MUHAMMADIYAH MAKASSAR

2026

A. Persiapan dan Konfigurasi

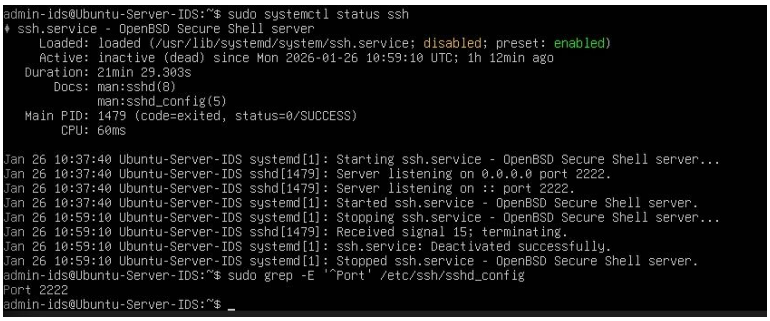
1. Informasi VPS



Langkah pertama dalam proyek ini adalah mendata spesifikasi Virtual Private Server (VPS) yang digunakan sebagai tempat berjalannya Honeypot. Data ini mencakup informasi penting seperti jenis sistem operasi, kekuatan prosesor (CPU), kapasitas RAM, serta alamat IP publik server.

Tujuannya adalah untuk mengetahui kondisi normal server sebelum diberikan serangan. Dengan mencatat spesifikasi ini, kita bisa memantau apakah server tetap stabil atau mengalami gangguan performa saat nantinya dibanjiri serangan seperti DDoS atau Brute Force. Singkatnya, dokumentasi ini menjadi acuan untuk memastikan bahwa Honeypot Cowrie dapat bekerja dengan lancar tanpa membuat server asli menjadi *hang* atau *down*."

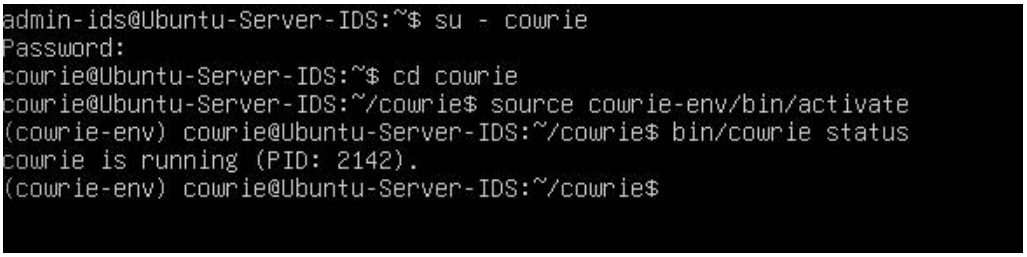
2. Status Layanan SSH Server Asli



Langkah selanjutnya adalah mengamankan pintu masuk utama server. Secara standar, pintu masuk (SSH) server berada pada port 22. Namun, agar tidak mudah ditebak oleh penyerang, kita memindahkan pintu asli tersebut ke port 2222 . Dengan cara ini, hanya administrator resmi yang tahu pintu aslinya, sementara orang asing akan tetap mengincar pintu lama yang sudah kita siapkan sebagai jebakan.

3. Status Honeypot Cowrie Aktif (Server Jebakan)

a. Status Layanan Cowrie

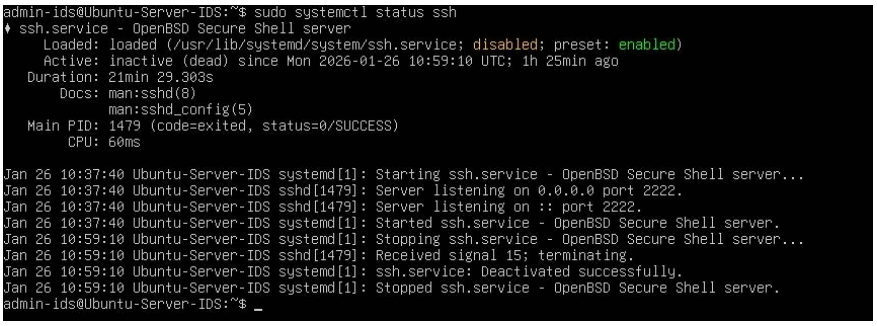


Maksud gambar diatas memastikan bahwa 'pintu jebakan' pada port 22 sudah benar-benar dijaga oleh Cowrie. Jadi, ketika ada penyerang yang mencoba masuk lewat jalur standar, mereka tidak akan sadar bahwa mereka sedang masuk ke dalam lingkungan tiruan yang sudah kita siapkan. Dokumentasi ini sangat penting untuk membuktikan bahwa server kita sudah dalam kondisi siap tempur sebelum pengujian serangan dimulai.

b. Verifikasi Port Honeypot

Perintah sudo ss -tlnp | grep :22. Di situ muncul hasil bahwa port 22 sedang digunakan oleh program bernama "twistd". Ini adalah bukti final bahwa port 22 sudah dijaga oleh Cowrie (mesin di balik Cowrie disebut twistd). Jadi sekarang, port 22 sudah resmi menjadi "pintu palsu" yang siap menjebak penyerang

c. Konfirmasi SSH Asli Tidak Aktif



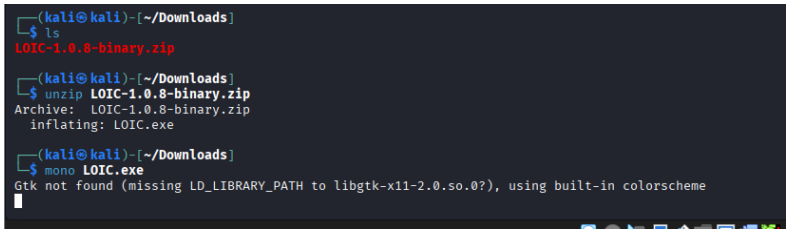
Memastikan bahwa port 22 (jalur yang paling sering diincar penyerang) telah berhasil diambil alih oleh layanan Cowrie. Terlihat pada gambar bahwa program 'twistd' yang merupakan mesin dari Cowrie sudah dalam status *LISTEN* di port 22. Dengan adanya bukti ini, dapat dipastikan bahwa strategi 'pintu jebakan' telah berhasil diimplementasikan, dan setiap upaya akses ilegal melalui port tersebut akan langsung terjebak masuk ke dalam Honeypot.

4. Tools yang digunakan
    - Tools Pertahanan: Cowrie Honeypot dan Ubuntu Server (IDS Host)
    - Tools Penyerangan: Nmap, Hydra, dan LOIC

Tahap awal dilakukan dengan memindahkan layanan SSH asli ke port 2222 agar jalur masuk admin tersembunyi dari pemindaian publik. Selanjutnya, layanan Honeypot Cowrie diaktifkan sebagai sistem jebakan, yang ditunjukkan dengan status *running* pada PID 2142. Verifikasi jaringan melalui perintah ss membuktikan bahwa port 22 kini telah sepenuhnya dikuasai oleh layanan Cowrie (*twistd*) untuk

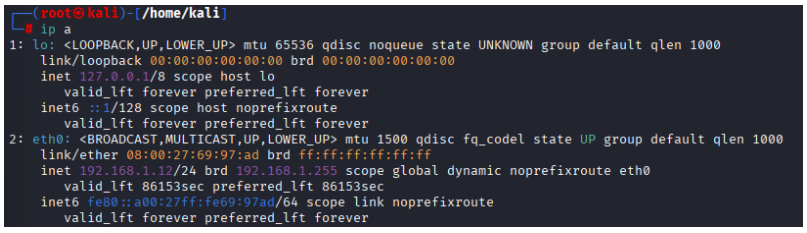
memancing penyerang. Hasilnya, sistem berhasil mendeteksi aktivitas dari IP penyerang 192.168.1.166 dan merekam setiap perintah yang mereka jalankan secara detail di dalam file log.

- Install Loic di https://sourceforge.net/projects/loic/



Skenario serangan SSH Brute Force dan TCP Flood (DoS) yang terkoordinasi terhadap target dengan IP 192.168.1.11. Serangan dimulai dengan pemindaian port menggunakan Nmap yang menemukan layanan SSH (22) dan FTP (21) aktif, diikuti penggunaan alat Hydra yang berhasil menebak kata sandi akun *root* ("password" dan "admin") dalam waktu singkat. Secara bersamaan, alat LOIC membanjiri target dengan ratusan ribu permintaan koneksi sampah mencapai 119.438 permintaan—untuk melumpuhkan sumber daya server. Seluruh aktivitas ini terekam pada log Cowrie, yang memperlihatkan banjir koneksi dari IP penyerang 192.168.1.12 dan keberhasilan login ilegal yang menyebabkan sistem mengalami ketidakstabilan atau *timeout*.

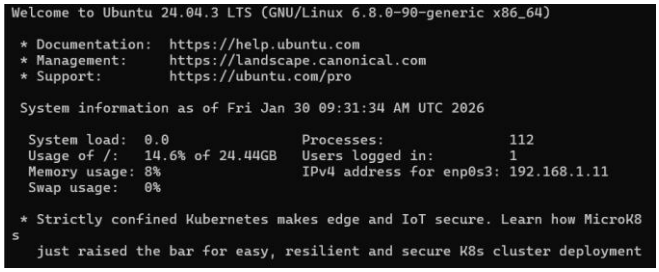
- Ip kali



Penyerang menggunakan interface jaringan eth0 dengan alamat IPv4 192.168.1.12 dan subnet mask /24. Langkah ini sangat krusial dalam skenario serangan tersebut karena penyerang perlu memastikan bahwa mereka berada

dalam satu segmen jaringan yang sama dengan target (192.168.1.11) agar alat seperti Nmap, Hydra, dan LOIC dapat menjangkau sasaran secara efektif.

- Ip ubuntu

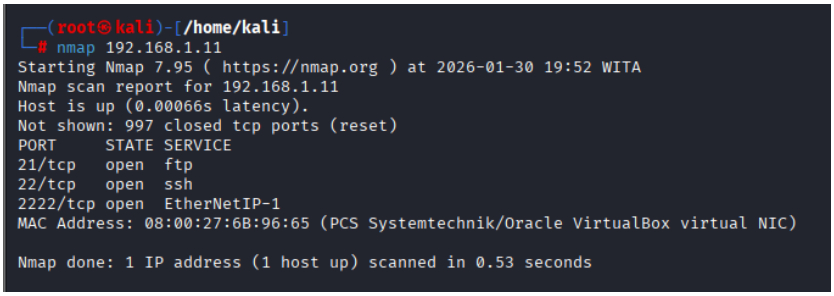


Menampilkan informasi sistem dari terminal Ubuntu 24.04.3 LTS yang bertindak sebagai target dalam skenario ini. Pada baris informasi jaringan, terlihat dengan jelas bahwa alamat IPv4 untuk interface enp0s3 adalah 192.168.1.11.

B. Pengujian Penyerangan

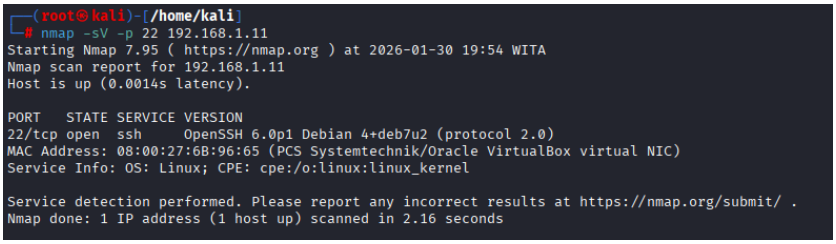
1. Pola Individual

- **Port Scanning**

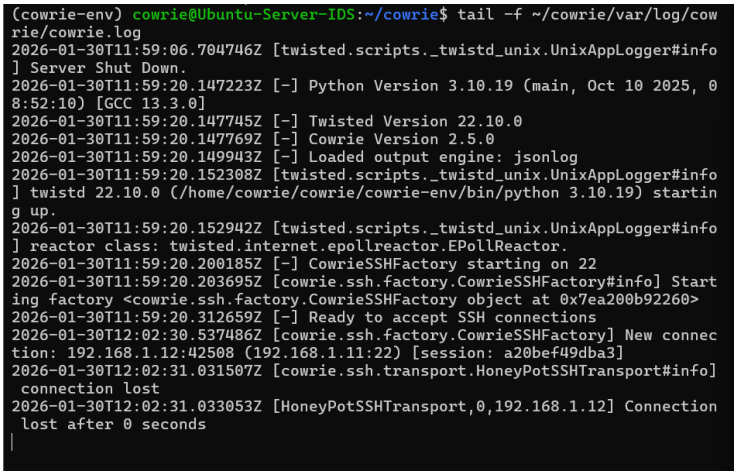


Penyerangan diatas menunjukkan hasil pemindaian jaringan menggunakan perintah Nmap terhadap alamat IP 192.168.1.11 yang dijalankan pada sistem Kali Linux dengan hak akses root. Pemindaian berhasil dilakukan, ditandai dengan status host yang aktif (host is up) dan waktu respons yang sangat rendah, menandakan perangkat berada dalam satu jaringan lokal. Dari hasil pemindaian, diketahui bahwa terdapat 997 port TCP dalam keadaan tertutup (closed) dengan alasan *reset*, sementara tiga port terdeteksi terbuka, yaitu port

21/tcp yang menjalankan layanan FTP, port 22/tcp yang menjalankan layanan SSH, dan port 2222/tcp yang teridentifikasi sebagai layanan EtherNet/IP-1

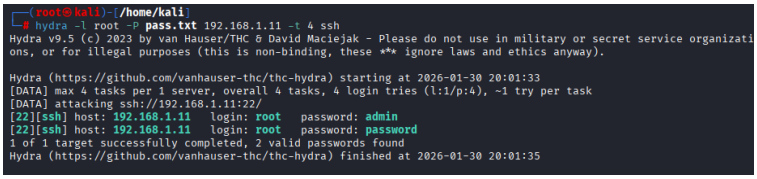


Hasil pemindaian Nmap tersebut menunjukkan bahwa host 192.168.1.11 dalam keadaan aktif dan memiliki port 22/tcp terbuka yang menjalankan layanan SSH. Layanan SSH yang digunakan adalah OpenSSH versi 6.0p1 dengan protokol 2.0 pada sistem operasi Linux.



Log diatas menunjukkan aktivitas Cowrie SSH Honeypot yang sedang berjalan di server Ubuntu. Awalnya sistem melakukan proses inisialisasi, mulai dari pemuatan Python versi 3.10.19, Twisted, hingga Cowrie versi 2.5.0, lalu layanan honeypot berhasil dijalankan pada port 22 dan siap menerima koneksi SSH. Setelah itu, tercatat adanya percobaan koneksi SSH dari alamat IP 192.168.1.12 ke server 192.168.1.11, yang menandakan adanya aktivitas akses dari host lain di jaringan. Cowrie menerima koneksi tersebut dan mencatatnya sebagai session SSH, namun koneksi tersebut kemudian terputus (connection lost) dan berakhir tanpa aktivitas lanjutan.

- **Brute Force**

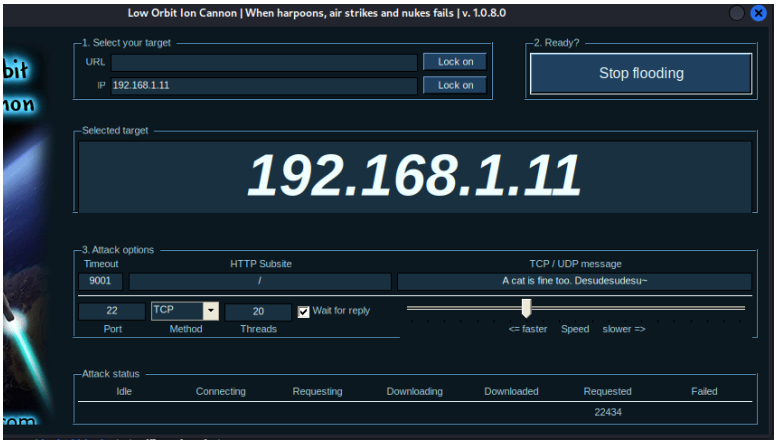


Serangan brute force pada layanan SSH di host 192.168.1.11. Hydra dijalankan dengan daftar username dan password dari file pass.txt, lalu menargetkan port SSH (22). Selama proses berjalan, Hydra mencoba beberapa kombinasi kredensial secara otomatis dan mencatat setiap percobaan login. Dari hasil pemindaian terlihat bahwa Hydra berhasil menemukan kredensial yang valid, yaitu username: root dengan password: password, yang ditandai dengan status *login successful*.

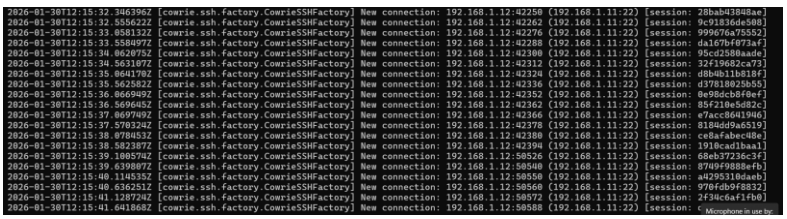
Log diatas merupakan catatan aktivitas detail dari Cowrie SSH Honeypot yang merekam serangkaian percobaan login SSH ke server 192.168.1.11 yang berasal dari IP 192.168.1.12. Awalnya terlihat proses negosiasi koneksi SSH, termasuk pertukaran versi protokol dan algoritma kriptografi (*key exchange*), yang menandakan klien berhasil terhubung ke layanan SSH palsu milik honeypot. Selanjutnya, penyerang mencoba berbagai kombinasi username dan password, dimulai dari percobaan gagal seperti root dengan password yang salah, hingga akhirnya mencoba username root dengan password “password”. Pada bagian akhir log tercatat bahwa login berhasil (login attempt succeeded), sehingga Cowrie menganggap penyerang telah masuk ke sistem palsu dan

kemudian mengaktifkan lingkungan shell tiruan untuk memantau aktivitas lanjutan.

- **Denial of Service Attack**



Serangan TCP Flood menggunakan alat bernama LOIC. Di balik layar, komputer pengirim sedang membombardir alamat IP target (192.168.1.11) dengan ribuan permintaan koneksi secara simultan melalui Port 22. Dalam kondisi ini, perangkat target dipaksa untuk mengalokasikan sumber daya CPU dan memori yang sangat besar hanya untuk merespons paket data "sampah" tersebut. Akibatnya, antrean koneksi pada target akan menjadi penuh, menyebabkan sistem menjadi sangat lambat atau bahkan mengalami *crash* total karena kehabisan sumber daya. Selain melumpuhkan kinerja perangkat, serangan ini menyebabkan kondisi yang disebut dengan Denial of Service, di mana pengguna yang sah tidak akan bisa mengakses layanan pada perangkat tersebut karena jalur komunikasinya sudah tersumbat oleh banjir data.

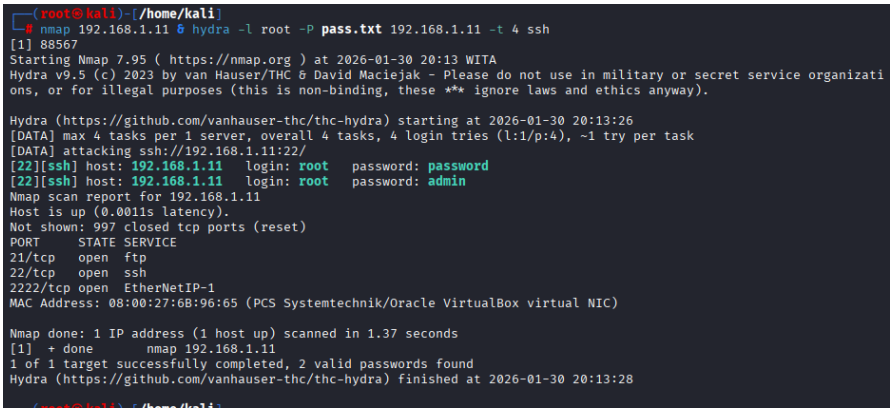


Log aktivitas server yang mencatat serangan secara *real-time*, di mana terlihat alamat IP 192.168.1.12 terus-menerus mencoba membuka koneksi baru ke

target 192.168.1.11 pada port SSH (22). Setiap baris log merekam upaya koneksi yang terjadi dalam selang waktu milidetik, yang membuktikan adanya pengiriman data otomatis secara masif untuk memenuhi antrean sesi pada server. Aktivitas ini merupakan bukti teknis dari serangan Connection Flooding yang bertujuan menghabiskan sumber daya sistem hingga server tidak lagi mampu melayani pengguna lain yang sah.

2. Pola Double

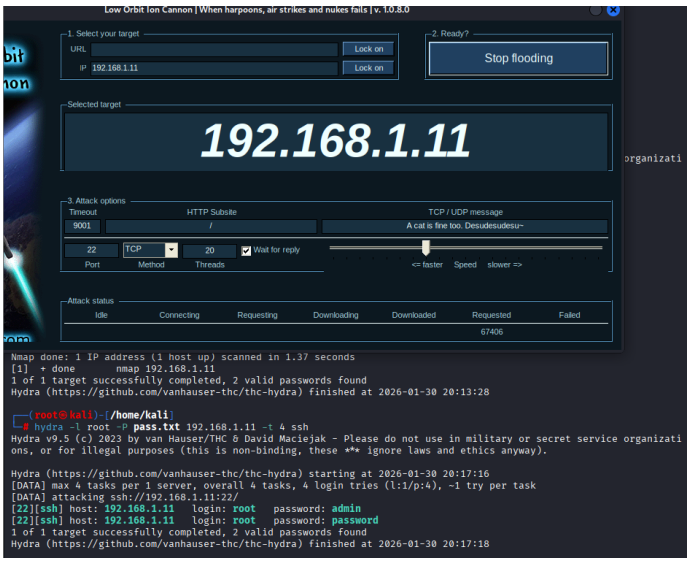
- DOUBLE 1 *(Port Scanning & Burteforce Attack)*



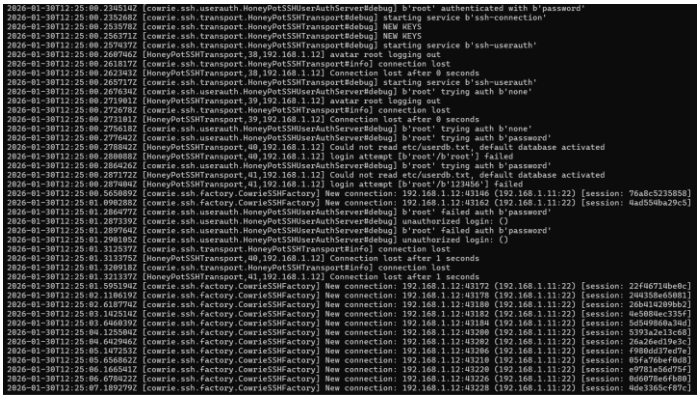
Pemindaian jaringan menggunakan Nmap untuk menemukan port terbuka, diikuti dengan serangan Brute Force menggunakan alat bernama Hydra untuk menebak kata sandi akun *root* pada layanan SSH di IP 192.168.1.11. Pola serangan yang terjadi adalah upaya eksploitasi kredensial, di mana penyerang mencoba berbagai kombinasi kata sandi dari sebuah daftar (pass.txt) hingga berhasil menemukan dua kata sandi yang valid, yaitu "password" dan "admin". Dampaknya terlihat pada log server Cowrie, yang mencatat banjirnya koneksi baru dalam waktu yang sangat singkat (beberapa kali per detik), yang menandakan bahwa sistem sedang dipaksa memproses ribuan percobaan login otomatis secara agresif hingga pertahanannya tertembus.

Log tersebut menunjukkan aktivitas serangan Brute Force SSH yang terekam secara mendalam oleh sistem *honeypot* Cowrie, di mana setiap barisnya mencatat setiap detil interaksi antara penyerang (IP 192.168.1.12) dan target (192.168.1.11). Terlihat pola serangan yang sangat cepat dan otomatis, dimulai dari pertukaran kunci enkripsi (*kex*), identifikasi sidik jari klien (*hassh fingerprint*), hingga percobaan autentikasi berulang kali dalam hitungan milidetik. Log ini mengonfirmasi keberhasilan serangan dengan munculnya pesan login attempt [b'root'/b'password'] succeeded dan login attempt [b'root'/b'admin'] succeeded, yang berarti alat penyerang telah berhasil menemukan kredensial yang tepat dan mendapatkan akses masuk ke sistem sebelum akhirnya koneksi tersebut terputus atau dikeluarkan (*logging out*).

- DOUBLE 2 *(DDoS Attack & Port Scanning)*

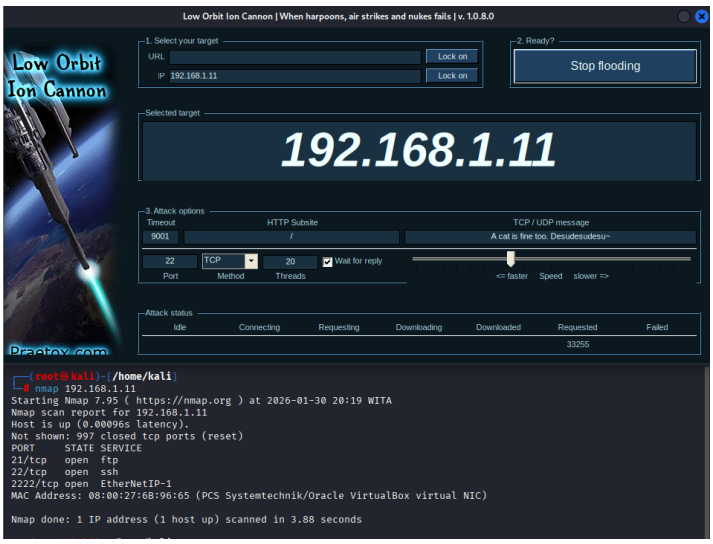


Menggabungkan dua metode utama yaitu Brute Force Attack dan Denial of Service (DoS). Serangan dimulai dengan tahap pengintaian menggunakan alat Nmap untuk memetakan port yang terbuka pada target dengan IP 192.168.1.11, di mana ditemukan port layanan SSH (22) dan FTP (21) sedang aktif. Penyerang kemudian meluncurkan serangan Brute Force menggunakan alat Hydra untuk mencoba menebak kata sandi akun *root* secara otomatis, yang terbukti berhasil dengan ditemukannya kredensial valid seperti "password" dan "admin". Selain mencoba menembus akses, penyerang juga menjalankan alat Low Orbit Ion Cannon (LOIC) untuk melakukan serangan TCP Flood (DoS) dengan mengirimkan puluhan ribu permintaan koneksi secara masif (terlihat mencapai 67.406 *requested*) guna melumpuhkan sumber daya server target.

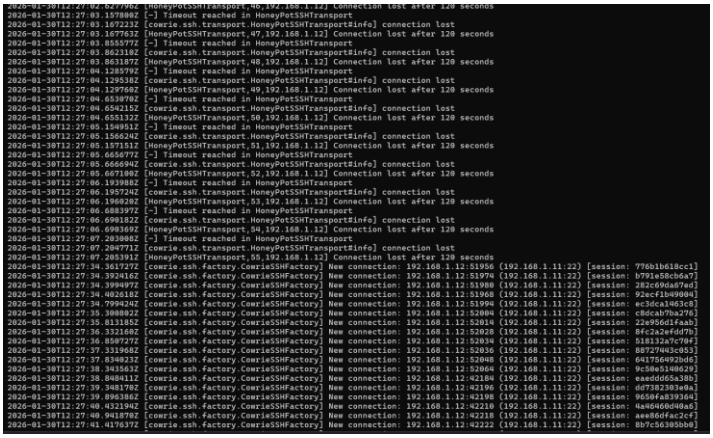


Log ini mencatat aktivitas Brute Force SSH yang sangat agresif dari alamat IP penyerang 192.168.1.12 terhadap target 192.168.1.11 pada port 22. Dalam log tersebut, terlihat setiap tahapan serangan mulai dari pembukaan koneksi baru (*New connection*), pertukaran kunci enkripsi (*kex*), hingga identifikasi sidik jari klien (*hassh fingerprint*) yang terjadi dalam hitungan milidetik. Puncak dari log ini adalah keberhasilan penyerang dalam menemukan kredensial yang tepat, ditandai dengan pesan login attempt [b'root'/b'password'] succeeded dan login attempt [b'root'/b'admin'] succeeded. Setelah berhasil masuk, log juga mencatat upaya otomatisasi lainnya seperti kegagalan login dengan kata sandi lain dan pemutusan koneksi secara cepat (*connection lost*), yang menunjukkan bahwa sistem sedang dibombardir oleh alat otomatis (seperti Hydra yang terlihat pada gambar sebelumnya) untuk memetakan kelemahan sistem.

- DOUBLE 3 *(Bruteforce Attack & DDoS Attack)*

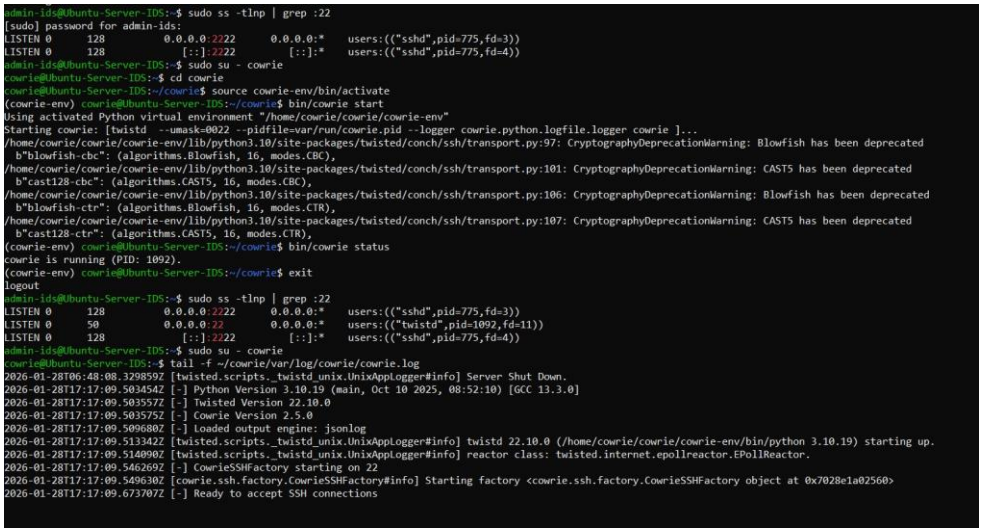


Serangan ini dimulai dengan tahap *reconnaissance* menggunakan alat Nmap untuk memindai port yang terbuka pada target IP 192.168.1.11, di mana ditemukan bahwa port 22 (SSH) dan 21 (FTP) dalam keadaan aktif. Penyerang kemudian meluncurkan Brute Force Attack menggunakan alat Hydra untuk menebak kata sandi akun *root* secara otomatis, yang berhasil menemukan dua kredensial valid yaitu "password" dan "admin" hanya dalam waktu singkat. Bersamaan dengan upaya pembobolan tersebut, penyerang juga menjalankan alat Low Orbit Ion Cannon (LOIC) untuk melakukan TCP Flood dengan mengirimkan puluhan ribu permintaan koneksi (mencapai lebih dari 67.000 permintaan) guna membanjiri sumber daya server target. Seluruh aktivitas ini terekam secara rinci pada log Cowrie Honeypot, yang memperlihatkan banjirnya koneksi baru dari IP penyerang 192.168.1.12 serta pesan login attempt succeeded yang menandakan bahwa sistem telah berhasil ditembus secara ilegal.

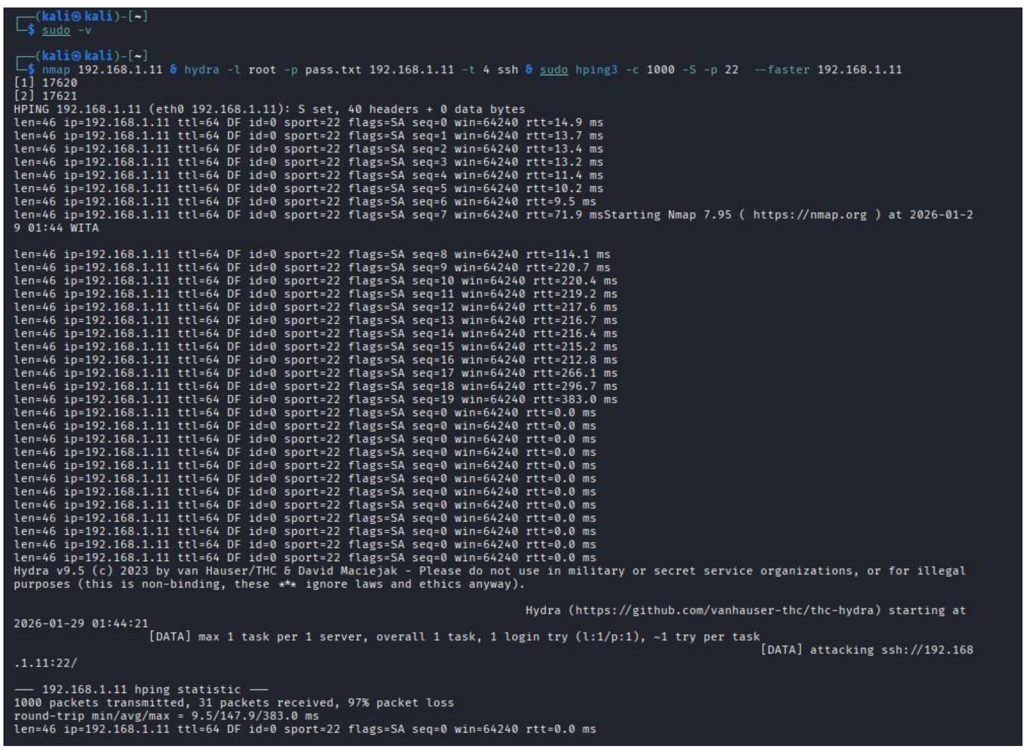


Log tersebut mendokumentasikan serangan SSH Brute Force dan TCP Flood yang dilakukan secara masif dan otomatis terhadap IP target 192.168.1.11. Baris log menunjukkan banjir koneksi baru (*New connection*) dari IP penyerang 192.168.1.12 yang terjadi setiap milidetik untuk melumpuhkan sumber daya server melalui alat LOIC. Secara bersamaan, terekam upaya penebakan kata sandi otomatis menggunakan alat Hydra yang akhirnya berhasil menembus keamanan sistem, ditandai dengan pesan login attempt [b'root'/b'password'] succeeded. Rentetan pesan connection lost dan timeout di akhir log memperjelas bahwa server mengalami gangguan stabilitas atau kehabisan sesi akibat volume serangan yang sangat tinggi.

3. Multiple



Perintah ss -tlnp | grep 22 digunakan untuk memastikan bahwa port 22 (SSH) sedang aktif. Setelah itu, pengguna berpindah ke akun *courie*, mengaktifkan virtual environment, lalu menjalankan perintah bin/courie start untuk menyalakan layanan Cowrie. Di layar terlihat proses Cowrie berhasil berjalan (PID aktif) disertai beberapa pesan peringatan kriptografi. Selanjutnya dilakukan pengecekan ulang port 22 yang menunjukkan adanya proses sshd dan twisted (Cowrie) yang sedang mendengarkan koneksi. Bagian akhir menampilkan isi file log cowrie.log yang menunjukkan bahwa Cowrie berhasil start, memuat konfigurasi, dan siap menerima koneksi SSH

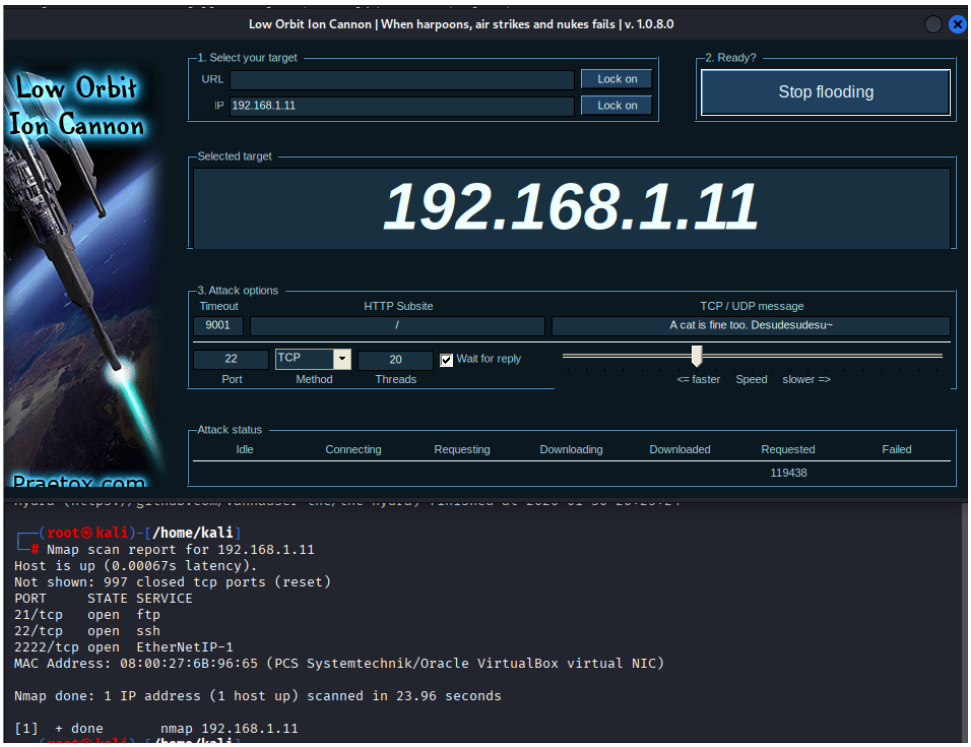


```
┌──(kali㉿kali)-[~]
└─$ sudo -v

┌──(kali㉿kali)-[~]
└─$ nmap 192.168.1.11 & hydra -l root -p pass.txt 192.168.1.11 -t 4 ssh & sudo hping3 -c 1000 -S -p 22  --faster 192.168.1.11
[1] 17620
[2] 17621
HPING 192.168.1.11 (eth0 192.168.1.11): S set, 40 headers + 0 data bytes
len=46 ip=192.168.1.11 ttl=64 DF id=0 sport=22 flags=SA seq=0 win=64240 rtt=14.9 ms
len=46 ip=192.168.1.11 ttl=64 DF id=0 sport=22 flags=SA seq=1 win=64240 rtt=13.7 ms
len=46 ip=192.168.1.11 ttl=64 DF id=0 sport=22 flags=SA seq=2 win=64240 rtt=13.4 ms
len=46 ip=192.168.1.11 ttl=64 DF id=0 sport=22 flags=SA seq=3 win=64240 rtt=13.2 ms
len=46 ip=192.168.1.11 ttl=64 DF id=0 sport=22 flags=SA seq=4 win=64240 rtt=11.4 ms
len=46 ip=192.168.1.11 ttl=64 DF id=0 sport=22 flags=SA seq=5 win=64240 rtt=10.2 ms
len=46 ip=192.168.1.11 ttl=64 DF id=0 sport=22 flags=SA seq=6 win=64240 rtt=9.5 ms
len=46 ip=192.168.1.11 ttl=64 DF id=0 sport=22 flags=SA seq=7 win=64240 rtt=71.9 msStarting Nmap 7.95 ( https://nmap.org ) at 2026-01-2
9 01:44 WITA

len=46 ip=192.168.1.11 ttl=64 DF id=0 sport=22 flags=SA seq=8 win=64240 rtt=114.1 ms
len=46 ip=192.168.1.11 ttl=64 DF id=0 sport=22 flags=SA seq=9 win=64240 rtt=220.7 ms
len=46 ip=192.168.1.11 ttl=64 DF id=0 sport=22 flags=SA seq=10 win=64240 rtt=220.4 ms
len=46 ip=192.168.1.11 ttl=64 DF id=0 sport=22 flags=SA seq=11 win=64240 rtt=219.2 ms
len=46 ip=192.168.1.11 ttl=64 DF id=0 sport=22 flags=SA seq=12 win=64240 rtt=217.6 ms
len=46 ip=192.168.1.11 ttl=64 DF id=0 sport=22 flags=SA seq=13 win=64240 rtt=216.7 ms
len=46 ip=192.168.1.11 ttl=64 DF id=0 sport=22 flags=SA seq=14 win=64240 rtt=216.4 ms
len=46 ip=192.168.1.11 ttl=64 DF id=0 sport=22 flags=SA seq=15 win=64240 rtt=215.2 ms
len=46 ip=192.168.1.11 ttl=64 DF id=0 sport=22 flags=SA seq=16 win=64240 rtt=212.8 ms
len=46 ip=192.168.1.11 ttl=64 DF id=0 sport=22 flags=SA seq=17 win=64240 rtt=266.1 ms
len=46 ip=192.168.1.11 ttl=64 DF id=0 sport=22 flags=SA seq=18 win=64240 rtt=296.7 ms
len=46 ip=192.168.1.11 ttl=64 DF id=0 sport=22 flags=SA seq=19 win=64240 rtt=383.0 ms
len=46 ip=192.168.1.11 ttl=64 DF id=0 sport=22 flags=SA seq=0 win=64240 rtt=0.0 ms
len=46 ip=192.168.1.11 ttl=64 DF id=0 sport=22 flags=SA seq=0 win=64240 rtt=0.0 ms
len=46 ip=192.168.1.11 ttl=64 DF id=0 sport=22 flags=SA seq=0 win=64240 rtt=0.0 ms
len=46 ip=192.168.1.11 ttl=64 DF id=0 sport=22 flags=SA seq=0 win=64240 rtt=0.0 ms
len=46 ip=192.168.1.11 ttl=64 DF id=0 sport=22 flags=SA seq=0 win=64240 rtt=0.0 ms
len=46 ip=192.168.1.11 ttl=64 DF id=0 sport=22 flags=SA seq=0 win=64240 rtt=0.0 ms
len=46 ip=192.168.1.11 ttl=64 DF id=0 sport=22 flags=SA seq=0 win=64240 rtt=0.0 ms
len=46 ip=192.168.1.11 ttl=64 DF id=0 sport=22 flags=SA seq=0 win=64240 rtt=0.0 ms
len=46 ip=192.168.1.11 ttl=64 DF id=0 sport=22 flags=SA seq=0 win=64240 rtt=0.0 ms
len=46 ip=192.168.1.11 ttl=64 DF id=0 sport=22 flags=SA seq=0 win=64240 rtt=0.0 ms
len=46 ip=192.168.1.11 ttl=64 DF id=0 sport=22 flags=SA seq=0 win=64240 rtt=0.0 ms
len=46 ip=192.168.1.11 ttl=64 DF id=0 sport=22 flags=SA seq=0 win=64240 rtt=0.0 ms
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 non-binding, these *** ignore laws and ethics anyway).

                                                                   Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at
2026-01-29 01:44:21
                   [DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try per task
                                                                                              [DATA] attacking ssh://192.168
.1.11:22/

--- 192.168.1.11 hping statistic ---
1000 packets transmitted, 31 packets received, 97% packet loss
round-trip min/avg/max = 9.5/147.9/383.0 ms
len=46 ip=192.168.1.11 ttl=64 DF id=0 sport=22 flags=SA seq=0 win=64240 rtt=0.0 ms
```

Proses penyerangan ini merupakan pengujian keamanan menggunakan skenario Multiple Attack, di mana penyerang mengeksekusi tiga jenis kode penyerangan berbeda secara simultan terhadap Target IP 192.168.1.11 untuk memberikan tekanan maksimal pada sistem. Serangan pertama dimulai dengan Nmap 7.95 yang melakukan pemindaian jaringan (*scanning*) untuk

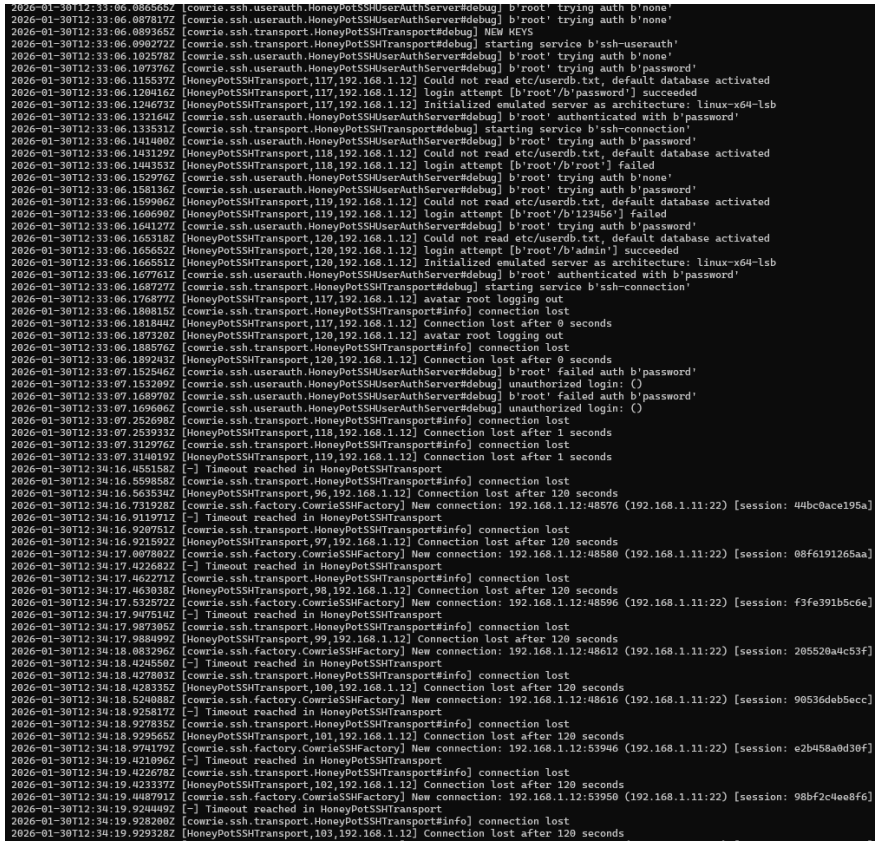
mengidentifikasi layanan yang berjalan. Secara bersamaan, penyerang menjalankan Hydra v9.5 untuk melakukan serangan Brute Force terhadap protokol SSH di port 22, menggunakan daftar kata sandi dari file pass.txt dengan target akun 'root'.

Sebagai pelengkap serangan tersebut, dijalankan pula serangan Denial of Service (DoS) menggunakan hping3 dengan metode SYN Flood. Kode penyerangan ini mengirimkan paket data dalam jumlah besar (1000 paket) dengan kecepatan tinggi (faster) untuk membanjiri sumber daya jaringan target. Efektivitas dari serangan ganda ini terlihat sangat jelas pada statistik akhir, di mana terjadi 97% packet loss (hanya 31 paket yang berhasil diterima kembali dari 1000 yang dikirim), yang menandakan bahwa sistem target telah mengalami degradasi layanan atau kelumpuhan jaringan akibat beban serangan simultan tersebut.



Serangan dimulai dengan pemindaian jaringan menggunakan Nmap untuk mengidentifikasi port yang terbuka pada target IP 192.168.1.11, di mana

ditemukan layanan SSH (port 22) dan FTP (port 21) sedang aktif. Setelah "pintu" ditemukan, penyerang meluncurkan alat Hydra untuk melakukan serangan Brute Force, yaitu mencoba menebak kata sandi akun *root* secara otomatis hingga berhasil menemukan kredensial valid berupa "password" dan "admin". Sambil mencoba masuk, penyerang juga mengoperasikan alat Low Orbit Ion Cannon (LOIC) untuk melakukan TCP Flood, mengirimkan ratusan ribu permintaan koneksi sampah (terlihat mencapai 119.438 *requested*) guna membanjiri dan melumpuhkan sumber daya server target



Log tersebut mendokumentasikan serangan SSH Brute Force dan TCP Flood yang dijalankan secara agresif oleh penyerang dengan IP 192.168.1.12 terhadap target 192.168.1.11. Di dalam log, terlihat rentetan baris New connection yang muncul dalam hitungan milidetik, menunjukkan upaya alat LOIC untuk membanjiri sumber daya server hingga mencapai ratusan ribu permintaan koneksi. Secara

bersamaan, sistem merekam detil upaya masuk otomatis menggunakan alat Hydra yang akhirnya berhasil menembus keamanan dengan kredensial root dan kata sandi password atau admin, sebagaimana dikonfirmasi oleh pesan login attempt succeeded. Banyaknya pesan connection lost dan timeout di akhir log menjadi bukti teknis bahwa server mengalami gangguan stabilitas yang parah akibat volume trafik sampah yang sangat tinggi, sehingga tidak mampu lagi melayani koneksi dengan normal.

Hasil Pengujian 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