LAPORAN ADVANCE NETWORK SECURITY AND PROTOCOLS

Implementasi Honeypot Cowrie untuk Deteksi Pola Penyerangan Double Attack

DISUSUN OLEH

KELOMPOK 3

NAMA	NIM
NUR ALIYAH AMALIANI	105841106923
SUKMA WARDIA NINGSIH	105841112723

PROGRAM STUDI INFORMATIKA

FAKULTAS TEKNIK

UNIVERSITAS MUHAMMADIYAH MAKASSAR

2026

1. Pendahuluan

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

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

2. Lingkungan dan topologi pengujian

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

a. Mesin penyerang (attacker)

   Sistem Operasi : Kali linux

   Digunakan untuk melakukan simulasi serangan

b. Mesin Target

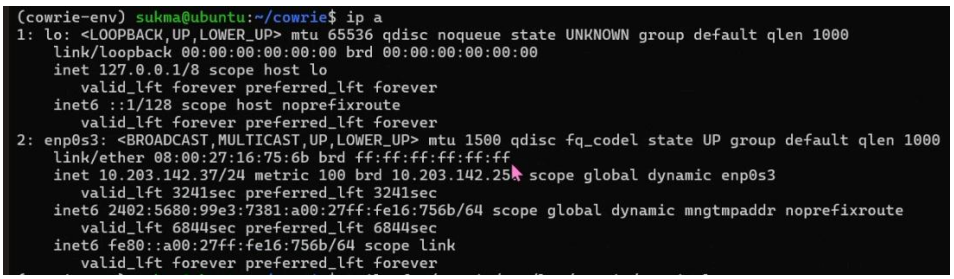
   Sistem Operasi : Ubuntu Server

   Digunakan sebagai server yang menjalankan honeypot Cowrie.

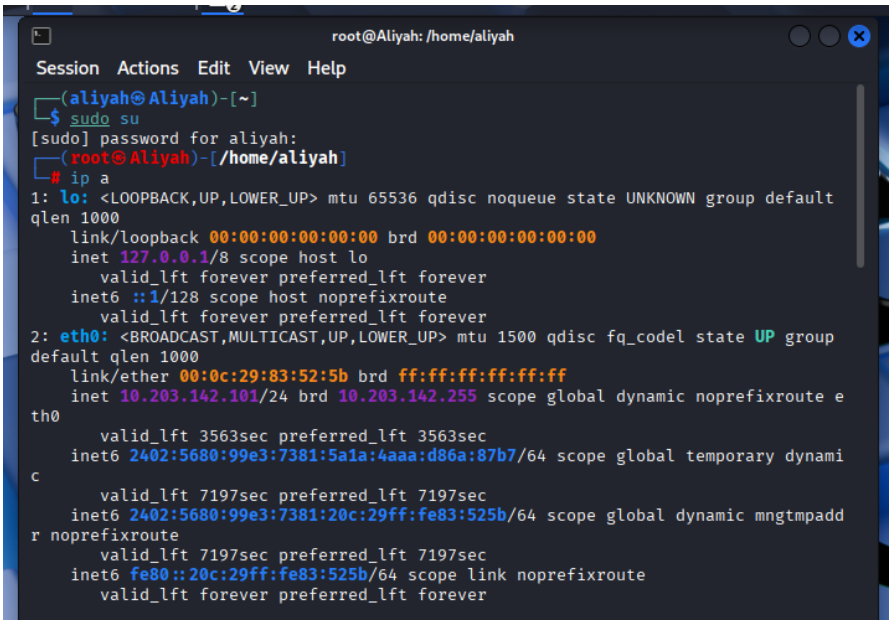
Kedua mesin dikonfigurasi berada dalam satu jaringan agar dapat saling berkomunikasi secara langsung. Konfigurasi jaringan dilakukan dengan menyamakan mode network adapter pada kedua mesin Virtual.

3. Konfigurasi Jaringan Awal

a. Pengecekan IP Address pada Ubuntu Server



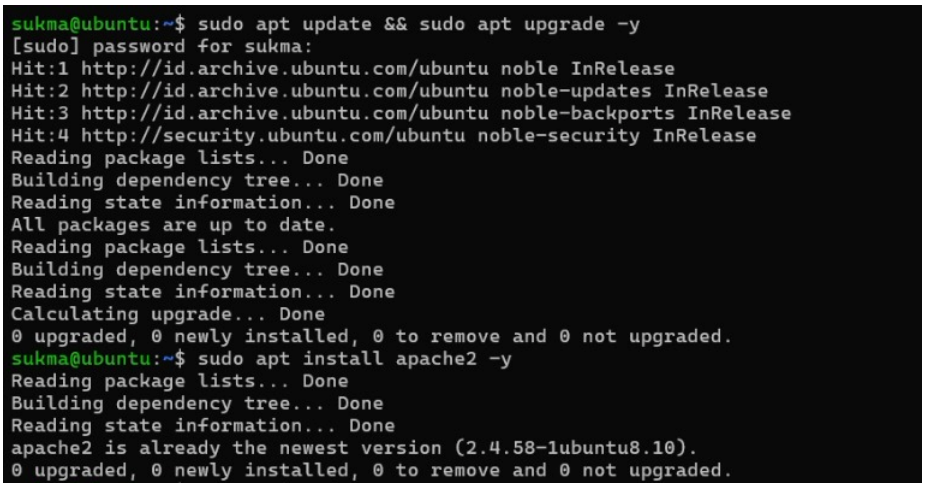
b. Pengecekan IP Address pada Kali Linux

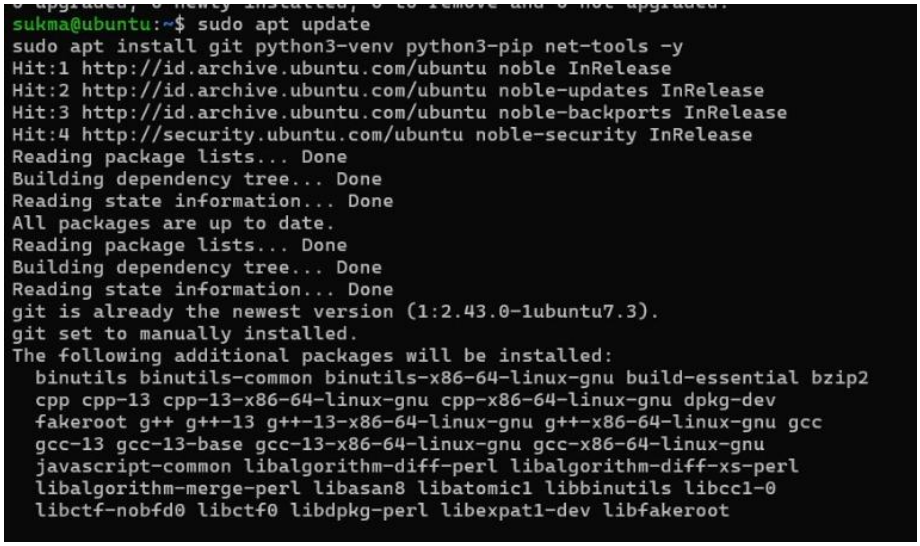


Langkah ini bertujuan untuk memastikan bahwa kedua mesin berada dalam satu subnet jaringan. Apabila mesin tidak berada dalam satu subnet, proses pengujian seperti port scanning dan serangan jaringan tidak dapat dilakukan

4. Persiapan Awal Ubuntu Server

4.1 Update Sistem



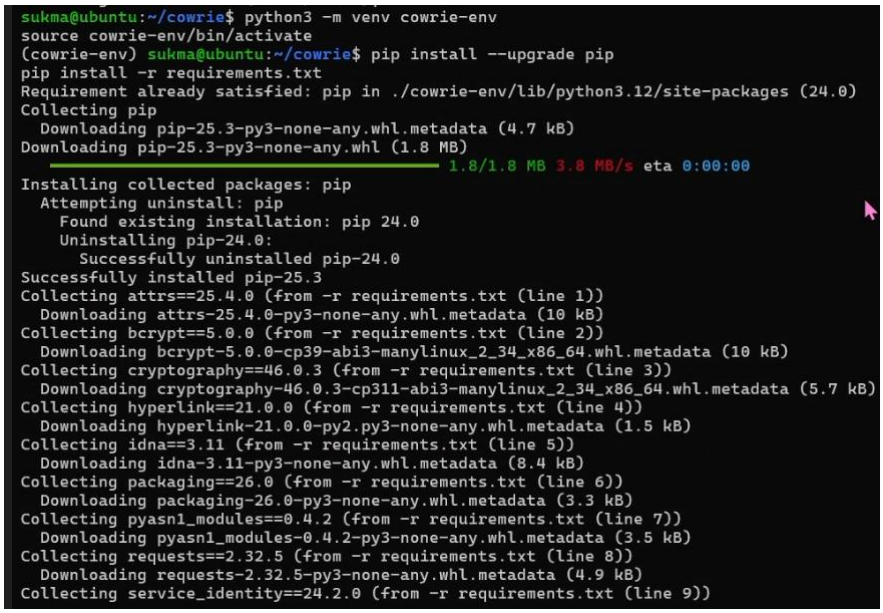


Update dilakukan untuk memastikan sistem berada pada kondisi terbaru dan menghindari konflik dependensi. Selanjutnya dilakukan instalasi beberapa paket pendukung seperti git, python3-venc, python3-pip, dan net-tools. Paket git digunakan untuk mengunduh source code honeypot Cowrie dari repositori resmi,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

4.2 Instalasi Honeypot Cowrie

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

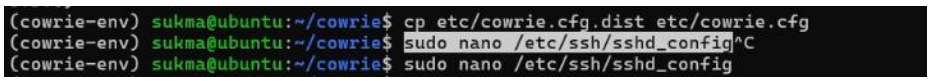
4.3 Instalasi Dependensi Python



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

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

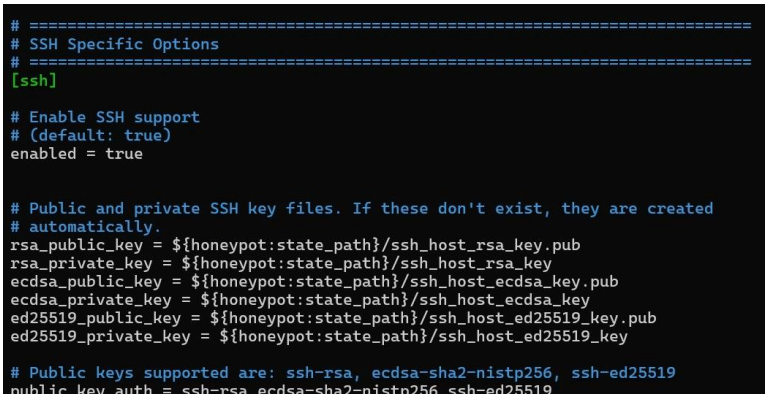
4.4 Konfigurasi Awal Cowrie



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

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

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



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

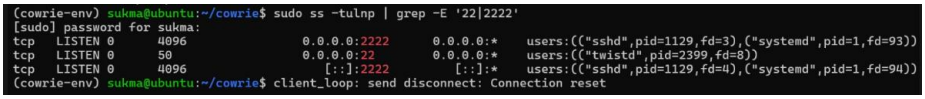
4.5 Pengamanan SSH Asli Ubuntu Server

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

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

setelah keluar retart SSH dengan perintah berikut:

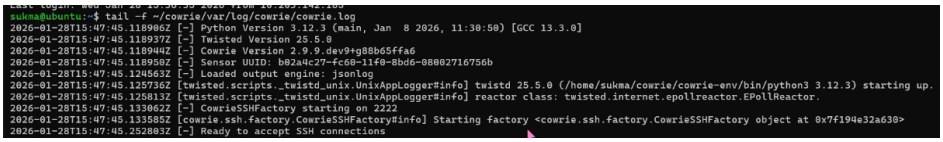
4.6 Verifikasi Port Aktif



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

4.7 Menjalankan Honeypot Cowrie

Cowrie dijalankan oleh user cowrie dalam mode foreground



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

5. Simulasi Serangan dari Kali linux

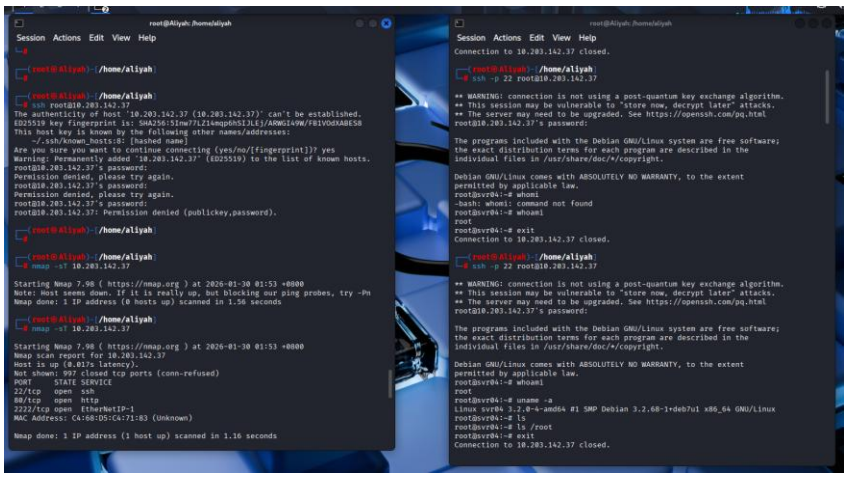
Sebelum melakukan seranga pastikan terlebih dahulu bahwa tools yang digunakan sudah tersedia.

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

Setelah itu kita masuk ke simulasi serangan double.

5.1 Simulasi Serangan Port Scanning Dan Brute Force

a. Kali linux (Attacker)

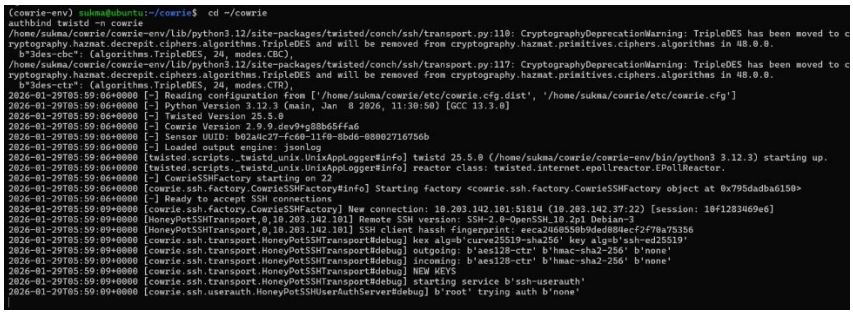


Pada tahap ini, penyerang menggunakan Kali Linux untuk melakukan port scanning dan brute force attack terhadap server target. Pemindaian port dengan Nmap menunjukkan bahwa layanan

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

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

b. Ubuntu Server (Target)



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

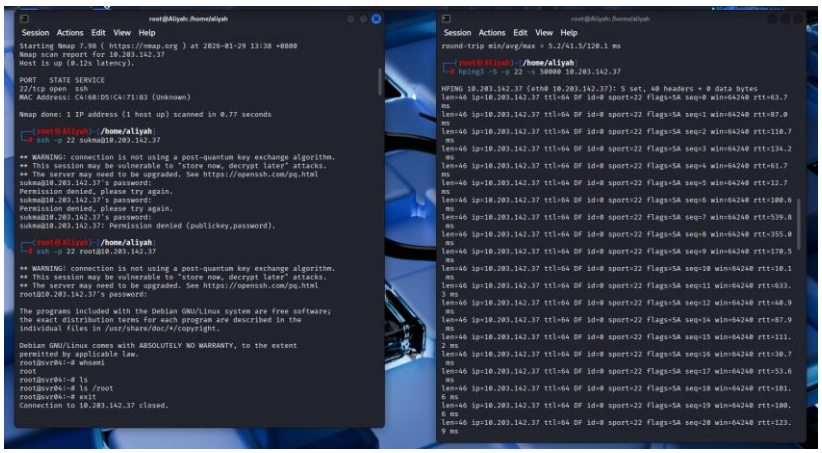
Setelah autentikasi diterima oleh sistem palsu, aktivitas penyerang seperti identifikasi pengguna, pengecekan sistem operasi,

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

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

5.2 Simulasi Serangan Brute Force Dan Ddos

a. Kali linux (Attacker)



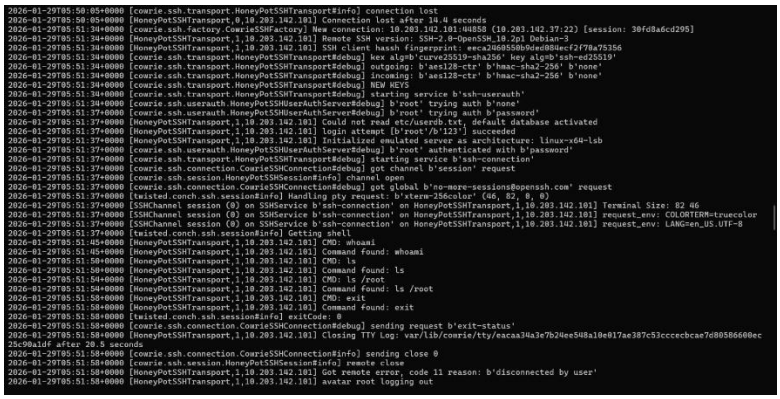
Pada tahap ini, penyerang melakukan dua jenis serangan secara berurutan, yaitu brute force SSH dan DDoS (SYN flood) terhadap server target. Serangan brute force dilakukan dengan mencoba beberapa kombinasi kata sandi pada akun root untuk menguji kerentanan autentikasi layanan SSH.

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

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

b. Ubuntu server (Target)

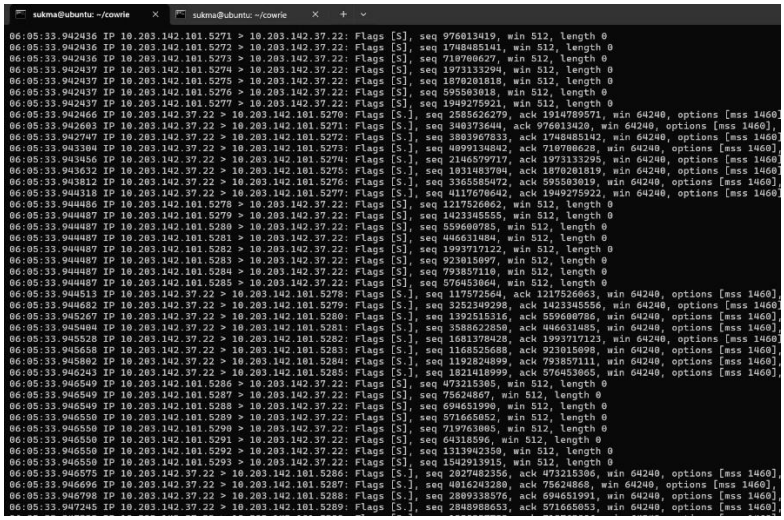
- **Brute force**



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

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

- **DDos**



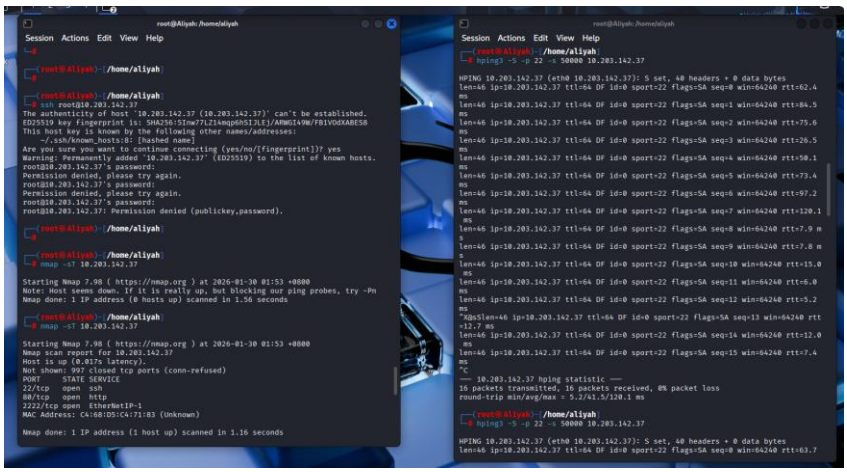
Pada tahap ini, Ubuntu Server menerima serangan DDoS berupa pengiriman paket SYN secara masif ke port SSH. Hal ini

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

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

5.3 Simulasi Serangan Port Scanning Dan Ddos

a. Kali linux (Attacker)



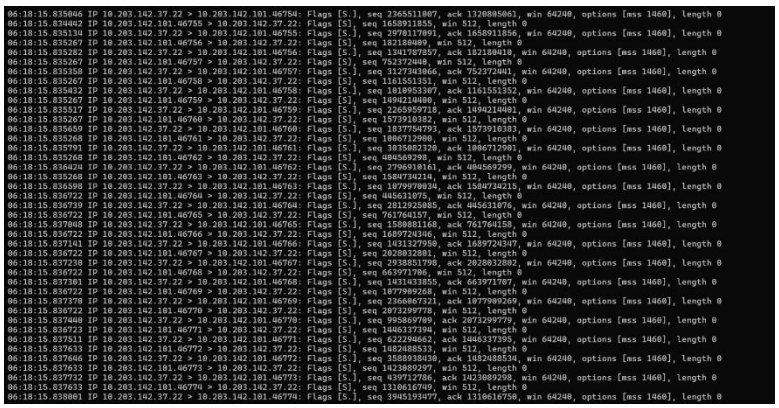
Pada tahap ini, penyerang melakukan kombinasi serangan port scanning dan DDoS terhadap server target. Serangan diawali dengan port scanning menggunakan nmap untuk mengidentifikasi port yang terbuka dan layanan yang aktif pada target. Hasil pemindaian menunjukkan bahwa layanan SSH pada port 22 dalam keadaan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

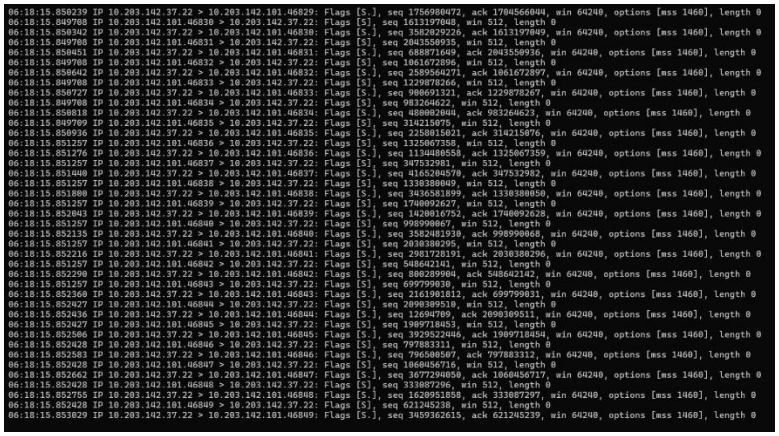
Setelah port target berhasil diidentifikasi, penyerang melanjutkan dengan serangan DDoS menggunakan teknik SYN flood. Serangan ini dilakukan dengan mengirimkan paket SYN

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

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

b. Ubuntu Server (Target)





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

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

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

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

Format Hasil Pengujian

Hasil Pengujian Penyerangan

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