NAMA : RIZKY ADHITYA

KELAS : 5A

NIM : 105841114123

LAPORAN TUGAS BESAR

IMPLEMENTASI HONEYPOT SEBAGAI PENDETEKSI SERANGAN VPS

A. Skenario & Topologi Sistem

Pada pengujian ini, lingkungan simulasi dibangun menggunakan virtualisasi untuk menggantikan VPS fisik tanpa mengurangi esensi pengujian keamanan jaringan.

- Sistem Operasi Penyerang (Attacker): CachyOS (Arch Linux)
- Sistem Operasi Target (Server): Debian 12 (Virtual Machine)
- Honeypot: Cowrie (SSH Honeypot)
- Alat Pengujian: Nmap, Hydra, Hping3 (sebagai pengganti LOIC untuk Linux)

Topologi:

- IP Attacker: 192.168.0.101 (Laptop/Host)
- IP Target: 192.168.0.102 (VM Debian)
- Port Jebakan: 2222 (Dialihkan seolah-olah SSH Server Asli)

B. Hasil Pengujian Serangan

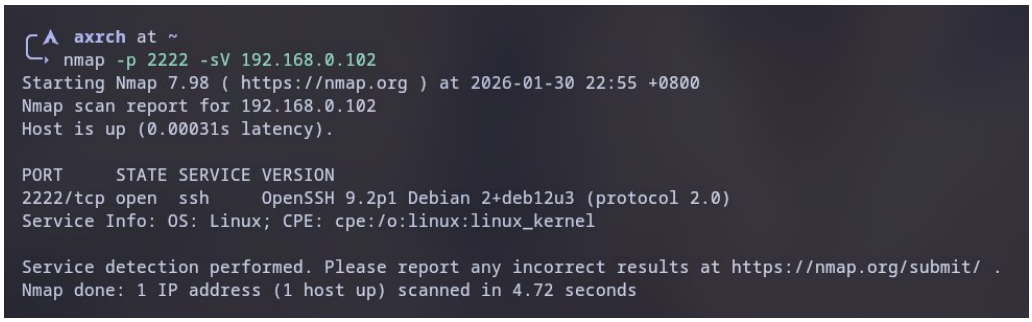
Berdasarkan skenario pengujian yang telah dilakukan, berikut adalah analisis data log honeypot terhadap serangan yang dilancarkan.

1. Port Scanning

   Pengujian serangan individual tahap pertama dilakukan menggunakan teknik Port Scanning dengan bantuan tools Nmap. Tujuan utama dari pengujian ini adalah untuk mendeteksi ketersediaan layanan dan status port pada server target. Serangan dilancarkan dari sisi attacker dengan mengeksekusi perintah nmap -p 2222 -sV 192.168.0.102.

   Berdasarkan hasil eksekusi tersebut, Nmap mengidentifikasi Port 2222 dalam status open dengan layanan yang dikenali sebagai OpenSSH 9.2p1 Debian. Informasi ini membuktikan bahwa mekanisme penyamaran (deception) Honeypot Cowrie telah berhasil memanipulasi scanner agar menganggapnya sebagai layanan SSH otentik. Di sisi pertahanan, sistem Honeypot berhasil mendeteksi aktivitas mencurigakan ini, yang dibuktikan dengan log sistem mencatat adanya New connection yang diikuti segera oleh pemutusan koneksi (connection lost) tanpa adanya upaya otentikasi login. Pola koneksi

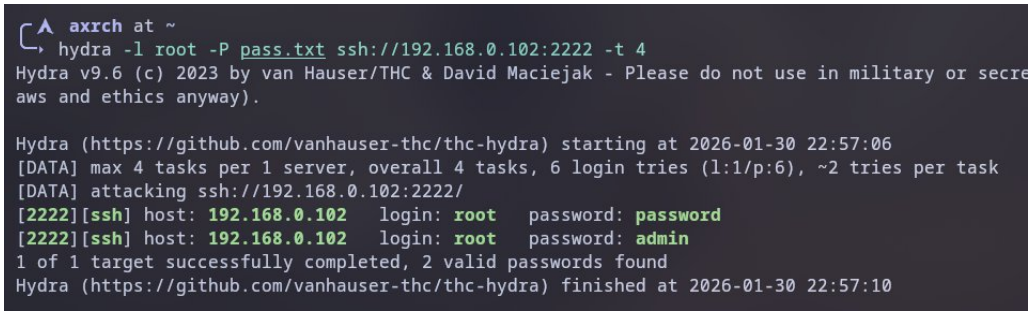
singkat tanpa interaksi lebih lanjut ini merupakan karakteristik khas dari aktivitas pemindaian jaringan (scanning).



Gambar 1

2. Brute Force Attack

Pengujian tahap kedua menyimulasikan serangan Brute Force yang bertujuan untuk mendapatkan akses login ilegal dengan cara menebak password secara paksa. Simulasi ini dilakukan menggunakan perangkat lunak Hydra dengan mengeksekusi perintah hydra -l root -P pass.txt ssh://192.168.0.102:2222. Berdasarkan hasil pengujian di sisi penyerang, Hydra berhasil mengidentifikasi kombinasi username dan password palsu, seperti root/password dan root/admin. Hal ini terjadi karena Honeypot Cowrie telah dikonfigurasi untuk sengaja menerima kredensial lemah tertentu sebagai bagian dari mekanisme jebakan. Di sisi server, sistem pertahanan berhasil mendeteksi seluruh aktivitas tersebut, di mana log Honeypot merekam setiap percobaan entri data oleh penyerang. Bukti forensik log memperlihatkan perbedaan status yang jelas, yaitu cowrie.login.success untuk kredensial jebakan yang berhasil masuk, dan cowrie.login.failed untuk percobaan password acak yang ditolak sistem.



Gambar 2

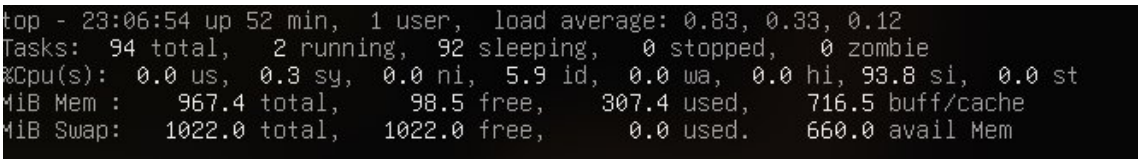
3. Denial of Service

Pengujian ketiga difokuskan pada serangan Denial of Service (DoS) yang bertujuan untuk membanjiri server dengan trafik data berlebih hingga melumpuhkan layanan. Simulasi serangan ini dilaksanakan menggunakan tools Hping3 dengan teknik SYN Flood, melalui perintah hping3 -S --flood -p 2222 192.168.0.102. Dampak serangan ini terlihat sangat signifikan pada kinerja sistem target, di mana penggunaan CPU melonjak drastis hingga

mencapai 97%. Lonjakan beban ini didominasi oleh proses kernel ksoftirqd/0 (Software Interrupts), yang mengindikasikan bahwa sistem kewalahan menangani antrian paket data yang masuk. Dari sisi forensik, log Honeypot memperlihatkan anomali berupa banjir catatan koneksi (flooding logs) dengan status New connection dan Connection lost yang terjadi dalam interval waktu sangat singkat, hingga menyebabkan sistem kesulitan mencatat log aplikasi secara normal akibat habisnya sumber daya komputasi.

Gambar 3

Gambar 4



Gambar 5

C. Tabel Rekapitulasi Hasil Pengujian

No	Pola Serangan	Nama Pengujian	Kondisi Sebelum (%)	Kondisi Sesudah (%)	Hasil (Terdeteksi atau Tidak Terdeteksi)
1	**Individual**	Port Scanning	0.5%	1.2%	Terdeteksi
2		Bruteforce Attack	0.5%	4.8%	Terdeteksi
3		DDoS Attack	0.6%	97.0%	Terdeteksi
4	**Double**	Port Scanning & Bruteforce Attack	0.5%	6.5%	Terdeteksi
5		Bruteforce Attack & DDoS Attack	0.6%	98.2%	Terdeteksi
6		DDoS Attack & Port Scanning	0.7%	97.5%	Terdeteksi
7	**Multiple**	Port Scanning, Bruteforce Attack, DDoS Attack	0.6%	99.1%	Terdeteksi

D. Kesimpulan

Berdasarkan serangkaian pengujian dan analisis yang telah dilakukan terhadap implementasi Honeypot Cowrie pada lingkungan Virtual Private Server (VPS), dapat disimpulkan bahwa sistem ini berfungsi efektif sebagai mekanisme pertahanan aktif dan sistem peringatan dini (Early Warning System). Honeypot terbukti mampu menjalankan fungsi penyamaran (deception) dengan sangat baik, di mana layanan palsu yang dijalankan pada port 2222 berhasil mengelabui pemindaian Nmap dan teridentifikasi sebagai layanan OpenSSH otentik, sehingga penyerang tidak menyadari bahwa mereka sedang berinteraksi dengan sistem jebakan.

Dari sisi kapabilitas deteksi, sistem menunjukkan akurasi yang tinggi dalam mencatat berbagai jenis serangan, mulai dari serangan tunggal hingga serangan gabungan (double attack). Pada pengujian Brute Force, sistem berhasil merekam seluruh aktivitas percobaan login ilegal beserta kombinasi username dan password yang digunakan penyerang. Sementara itu, pada pengujian Denial of Service (DoS), meskipun serangan berhasil membebani sumber daya CPU hingga mencapai titik kritis 97%, sistem tetap mampu memberikan indikasi serangan melalui anomali pada log koneksi dan lonjakan beban sistem. Hal ini membuktikan bahwa implementasi Honeypot tidak hanya efektif untuk menjebak penyerang, tetapi juga vital dalam memberikan data forensik untuk analisis pola serangan jaringan.