TUBES

ADVANCED NETWORK SECURITY AND PROTOCOLS

RUNAL REZKIAWAN, S.Kom.,M.T

OLEH :

MUH. TAZKIYAH ISLAM KAMALUDDIN

105841110823

IF-5C

PROGRAM STUDI INFORMATIKA

FAKULTAS TEKNIK

UNIVERSITAS MUHAMMADIYAH MAKASSAR

2025

BAB 1

PENDAHULUAN

1.1 Latar Belakang

Laporan ini disusun sebagai dokumentasi teknis komprehensif mengenai hasil implementasi, konfigurasi, dan pengujian sistem keamanan jaringan berbasis Honeypot. Di era digital saat ini, ancaman siber yang menargetkan infrastruktur server, terutama melalui protokol manajemen jarak jauh seperti SSH, terus meningkat secara signifikan baik dalam volume maupun kompleksitas. Serangan otomatis menggunakan botnet sering kali melakukan pemindaian massal untuk mencari kerentanan.

Dalam menghadapi ancaman ini, penggunaan Honeypot menjadi strategi pertahanan aktif yang krusial. Berbeda dengan firewall tradisional yang bersifat pasif (memblokir trafik), Honeypot bekerja dengan cara memancing penyerang masuk ke dalam lingkungan yang terkendali. Hal ini memungkinkan tim keamanan untuk mengecoh penyerang, memperlambat pergerakan mereka, serta mengumpulkan intelijen mendalam (Threat Intelligence) mengenai metode, alat, dan asal serangan tanpa membahayakan aset digital yang sesungguhnya.

1.2 Tujuan Pengujian

Fokus utama dari pengujian yang dilakukan oleh Kelompok 7 adalah mengevaluasi efektivitas sistem Cowrie sebagai *medium-interaction honeypot*. Pengujian ini bertujuan untuk:

1. Memvalidasi kemampuan deteksi sistem terhadap aktivitas pemindaian (*reconnaissance*).
2. Menguji ketahanan sistem dalam mencatat upaya penetrasi paksa (*brute force*).
3. Menganalisis respon sistem saat menghadapi banjir trafik (*denial of service*).
4. Menghasilkan data log yang dapat digunakan untuk analisis forensik digital

BAB 2

SPESIFIKASI TOOLS & LINGKUNGAN PENGUJIAN

2.1 Perangkat Lunak (Security Tools)

Dalam pelaksanaan pengujian ini, Kelompok 7 menggunakan berbagai perangkat lunak khusus keamanan jaringan. Setiap alat dipilih berdasarkan fungsinya dalam siklus serangan siber agar simulasi berjalan realistis.

Daftar alat di atas menunjukkan kombinasi antara perangkat pertahanan (Honeypot) dan perangkat penyerangan (Nmap, Hydra, LOIC) yang digunakan untuk menguji efektivitas sistem.

Berikut adalah rincian fungsionalitas dari setiap alat yang digunakan dalam pengujian:

Nama Alat (Tools)	**Kategori**	**Fungsi Spesifik dalam Pengujian**
Cowrie Honeypot	*Deception Tech*	Emulasi layanan SSH/Telnet yang interaktif untuk menangkap *shell interaction* penyerang.
Nmap (Network Mapper)	*Reconnaissance*	Melakukan *port discovery* dan *service fingerprinting* pada target IP.
THC-Hydra	*Exploitation*	Melakukan serangan login paralel menggunakan teknik *dictionary attack*.
LOIC (Low Orbit Ion Cannon)	*Disruption*	Menguji ambang batas (threshold) koneksi Honeypot melalui teknik *flooding*.

Nama Alat (Tools)	**Kategori**	**Fungsi Spesifik dalam Pengujian**
Tail & Grep	*Monitoring*	Melakukan inspeksi log secara *real-time* dan memfilter event spesifik berdasarkan kata kunci.

Tabel di atas mengklasifikasikan alat berdasarkan perannya dalam *Cyber Kill Chain*, mulai dari tahap pengintaian hingga gangguan layanan, guna memberikan gambaran menyeluruh tentang metodologi pengujian.

2.2 Detail Infrastruktur Teknis

Infrastruktur pengujian dirancang untuk mengisolasi aktivitas serangan sehingga tidak berdampak pada jaringan luar. Target menggunakan Kali Linux yang dikonfigurasi secara khusus untuk menjalankan Cowrie dalam lingkungan virtual Python (cowrie-env). Penggunaan cowrie-env memastikan bahwa penyerang yang berhasil masuk ke "shell palsu" tidak dapat mengeksploitasi kernel atau pustaka sistem operasi utama.

BAB 3

METODOLOGI

3.1 Tahap Persiapan: Aktivasi Sistem Monitoring

Sebelum memulai skenario serangan, tim harus memastikan bahwa sistem monitoring log telah aktif dan siap mencatat trafik. Hal ini dilakukan dengan memantau file cowrie.log secara *real-time*.

Gambar di atas memperlihatkan tampilan terminal saat tim menjalankan perintah monitoring. Terlihat bahwa sistem sudah dalam status *ready* untuk menerima koneksi.

Penjelasan dokumentasi: Perintah yang digunakan adalah tail -f ~/cowrie/var/log/cowrie/cowrie.log. Monitoring ini berfungsi untuk memverifikasi secara langsung apakah serangan yang dilancarkan dari sisi penyerang berhasil masuk ke dalam pangkalan data log Honeypot atau tidak.

3.2 Skenario 1: Port Scanning (Tahap Pengintaian)

Pada tahap awal, penyerang melakukan pemindaian port untuk mengetahui layanan apa saja yang terbuka pada alamat IP target 192.168.1.80.

Gambar di atas menunjukkan output dari perintah Nmap yang dijalankan oleh penyerang. Port 22 terlihat dalam status open (terbuka).

Penjelasan dokumentasi: Prosedur ini menggunakan perintah nmap -sV -p 22 192.168.1.80. Meskipun yang terdeteksi adalah layanan SSH, sebenarnya layanan tersebut adalah emulasi dari Cowrie. Respon Honeypot terhadap pemindaian ini membuktikan bahwa sistem berhasil memancing perhatian penyerang dengan menampilkan identitas layanan palsu.

3.3 Skenario 2: Bruteforce Attack (Tahap Penetrasi)

Setelah mengetahui adanya port SSH yang terbuka, penyerang mencoba melakukan serangan *brute force* untuk menebak kombinasi *username* dan password administratif (root).

Gambar di atas menampilkan proses berjalan dari tool Hydra yang mencoba berbagai kombinasi password dari file pass.txt.

Penjelasan dokumentasi: Perintah yang digunakan adalah hydra -l root -P pass.txt 192.168.1.80 ssh -t 4. Cowrie secara cerdas mencatat setiap upaya login yang gagal ini ke dalam log, termasuk alamat IP asal dan kredensial yang dicoba. Data ini sangat berharga bagi administrator untuk memahami pola kata sandi yang sering digunakan oleh peretas.

3.4 Skenario 3: DDoS Attack (Tahap Pelumpuhan)

Skenario terakhir melibatkan serangan *flooding* untuk menguji bagaimana Honeypot menangani volume koneksi yang sangat besar dalam waktu singkat.

Gambar di atas menunjukkan pengaturan pada alat LOIC (Low Orbit Ion Cannon) yang diarahkan ke IP target dengan metode TCP Flood.

Penjelasan dokumentasi: Pengujian ini bertujuan untuk melihat ambang batas koneksi simultan. Berdasarkan pengamatan, log Cowrie menunjukkan lonjakan drastis pada entri new connection, namun sistem host tetap stabil karena isolasi lingkungan virtual yang baik.

BAB 4

ANALISIS HASIL PENGUJIAN

Bagian ini merangkum efektivitas Honeypot dalam mendeteksi ketiga jenis serangan yang telah disimulasikan oleh Kelompok 7.

Berikut adalah tabel rekapitulasi hasil pengujian yang telah dilaksanakan:

No	Kategori Serangan	Parameter Deteksi	Kondisi Sebelum	Kondisi Sesudah	Status
1	Reconnaissance	Identitas IP & Port	0%	100%	Berhasil Terdeteksi
2	Brute Force	Akurasi Wordlist & User	0%	100%	Berhasil Terdeteksi
3	DDoS	Volume Koneksi Per Detik	0%	100%	Berhasil Terdeteksi

Tabel di atas menunjukkan bahwa tingkat deteksi sistem mencapai 100% pada semua parameter. Kondisi "0%" merujuk pada ketiadaan catatan serangan sebelum alat penyerang dijalankan, sedangkan "100%" menunjukkan keberhasilan sistem dalam menangkap seluruh aktivitas serangan ke dalam file log.

Analisis Forensik Log

Data log yang dihasilkan disimpan dalam format JSON. Melalui analisis log, Kelompok 7 menemukan beberapa parameter kunci:

- Session ID: Digunakan untuk melacak urutan tindakan yang dilakukan oleh satu penyerang tertentu.

- Input Terminal: Rekaman setiap karakter yang diketikkan penyerang jika mereka berhasil melewati tahap login palsu.
- File Download: Kemampuan Honeypot untuk menyimpan file malware yang mungkin diunggah oleh penyerang untuk analisis lebih lanjut.

BAB 5

KESIMPULAN DAN SARAN

5.1 Kesimpulan

Implementasi Honeypot Cowrie oleh Kelompok 7 dinyatakan berhasil sepenuhnya. Sistem terbukti mampu:

1. Menyamarkan diri sebagai server SSH yang rentan secara meyakinkan.
2. Mendeteksi dan mencatat aktivitas penyerang mulai dari tahap pemindaian hingga upaya pelumpuhan layanan.
3. Memberikan isolasi keamanan sehingga serangan tidak berdampak pada sistem operasi utama.

5.2 Saran Pengembangan

Untuk meningkatkan kapabilitas sistem di masa mendatang, disarankan untuk melakukan integrasi dengan sistem SIEM guna visualisasi data log yang lebih interaktif, serta menerapkan otomasi firewall yang dapat memblokir alamat IP penyerang secara otomatis setelah mereka terdeteksi melakukan serangan berbahaya pada Honeypot.