PRAKTIKUM IMPLEMENTASI HONEYPOT COWRIE SEBAGAI PENDETEKSI MULTIPLE ATTACK PADA JARINGAN LOKAL

NAMA TIM : **MUH REYHAN DWI WIJAYA (105841112623)**

: **FATHYA SHABIRA A.T (105841111923)**

KELOMPOK : **2**

KELAS : **5-JK-A**

---

1. IMPLEMENTASI HONEYPOT SEBAGAI PENDETEKSI SERANGAN PADA LINGKUNGAN VIRTUAL

Implementasi honeypot pada praktikum ini dilakukan dengan menggunakan **honeypot Cowrie** sebagai layanan SSH tiruan yang berfungsi untuk mendeteksi dan mencatat aktivitas serangan jaringan. Honeypot Cowrie dipilih karena mampu mensimulasikan layanan SSH secara realistis sehingga dapat menarik perhatian penyerang tanpa memberikan akses ke sistem asli.

Pada praktikum ini, honeypot diimplementasikan pada **lingkungan jaringan lokal** menggunakan **IP private**, bukan pada Virtual Private Server (VPS) publik. Meskipun dijalankan pada jaringan lokal, implementasi ini tetap mampu merepresentasikan skenario serangan nyata, seperti *port scanning*, *brute force login*, dan *Denial of Service (DoS)*.

Honeypot Cowrie dikonfigurasi untuk menerima koneksi SSH pada port tertentu dan mencatat seluruh aktivitas penyerangan ke dalam sistem log. Setiap percobaan login, baik yang gagal maupun yang berhasil secara simulasi, direkam secara detail, termasuk alamat IP penyerang, username, password yang dicoba, serta durasi koneksi.

Dengan implementasi ini, honeypot berperan sebagai **sistem umpan (decoy)** yang mengalihkan serangan dari sistem asli sekaligus menyediakan data yang dapat digunakan untuk analisis keamanan jaringan. Implementasi honeypot Cowrie pada jaringan lokal ini diharapkan dapat memberikan pemahaman yang lebih mendalam mengenai pola dan karakteristik serangan jaringan, khususnya serangan terhadap layanan SSH.

2. TUJUAN PRAKTIKUM

Praktikum ini bertujuan untuk:

1. Mengimplementasikan honeypot Cowrie sebagai layanan SSH tiruan.
2. Mendeteksi dan mencatat berbagai jenis serangan jaringan.
3. Menganalisis pola serangan multiple attack yang diarahkan ke satu target.
4. Memahami cara kerja honeypot dalam mengalihkan dan merekam aktivitas penyerang.
5. Membuktikan bahwa honeypot dapat berjalan tanpa VPS publik, cukup di jaringan lokal (IP private).

3. LINGKUNGAN IMPLEMENTASI DAN TOPOLOGI

A. Lingkungan Implementasi

Implementasi honeypot pada praktikum ini dilakukan pada **lingkungan jaringan lokal (Local Area Network/LAN)** dengan menggunakan **IP private**, tanpa melibatkan Virtual Private Server (VPS) publik. Meskipun tidak terhubung langsung ke internet, lingkungan lokal ini tetap mampu merepresentasikan skenario serangan jaringan secara realistis untuk keperluan pembelajaran dan analisis keamanan jaringan.

Honeypot yang digunakan adalah **Cowrie**, yaitu honeypot *low-interaction* yang dirancang khusus untuk mensimulasikan layanan **Secure Shell (SSH)**. Cowrie mampu meniru perilaku SSH asli sehingga dapat menarik penyerang dan mencatat seluruh aktivitas serangan, seperti *port scanning*, *brute force login*, hingga *Denial of Service (DoS)*.

Lingkungan implementasi terdiri dari dua mesin utama, yaitu mesin target dan mesin penyerang, yang berada dalam satu segmen jaringan lokal.

- **Target (Server Honeypot)**
  - OS: Ubuntu Linux
  - IP: 192.168.1.19 (IP private / lokal)
  - Honeypot: Cowrie v2.5.0
  - Layanan:
    - SSH Honeypot → port 22
    - Web Server (Apache) → port 80

- **Mesin Penyerang**
  - OS: Kali Linux
  - Tools:
    - Nmap (port scanning)
    - Nikto (web vulnerability scanning)
    - Hping3 (TCP scanning & flooding)
    - Hydra (brute force SSH)
    - LOIC (DoS attack)

Pengujian serangan dilakukan dari mesin Kali Linux menuju mesin Ubuntu yang menjalankan honeypot Cowrie. Seluruh trafik serangan diarahkan ke layanan honeypot, sehingga sistem operasi target tetap aman dan tidak benar-benar dieksploitasi.

B. Topologi Implementasi

Topologi implementasi pada praktikum ini menggunakan **topologi sederhana client–server dalam jaringan lokal**. Mesin penyerang dan mesin target terhubung ke jaringan yang sama melalui router atau switch lokal.

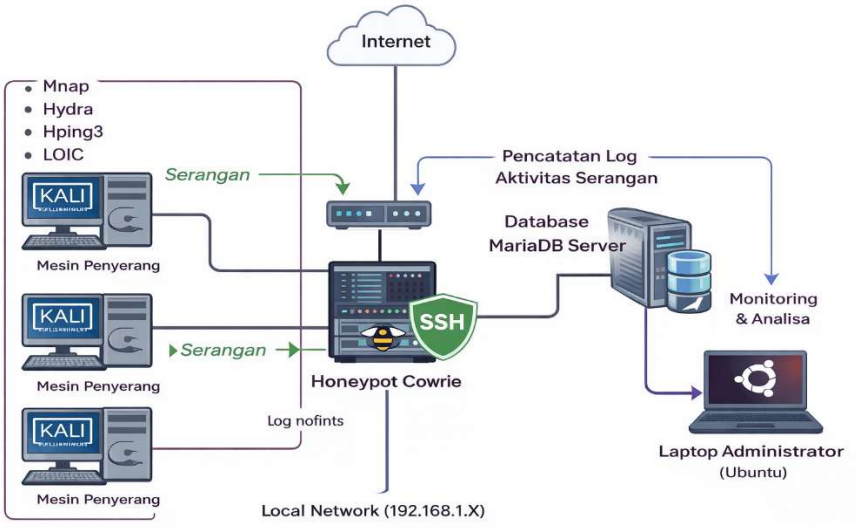
Secara konseptual, alur topologi implementasi dapat dijelaskan sebagai berikut:

- Mesin penyerang (Kali Linux) melakukan serangan jaringan seperti:
  - Port scanning
  - Brute force SSH
  - DoS attack
- Seluruh serangan diarahkan ke IP target 192.168.1.19.
- Layanan SSH pada port 2222 telah dikonfigurasi sebagai honeypot Cowrie, sehingga setiap koneksi SSH yang masuk akan ditangani oleh honeypot.
- Honeypot Cowrie mencatat seluruh aktivitas penyerang ke dalam sistem log tanpa memberikan akses ke sistem asli.
- Administrator hanya berperan sebagai pengamat dan analis hasil log serangan.

  Topologi ini memungkinkan pemisahan yang jelas antara:
  - Alur penyerangan, yaitu koneksi dari mesin penyerang ke layanan honeypot.
  - Alur analisis, yaitu proses pencatatan dan pengamatan aktivitas serangan oleh honeypot.

Dengan topologi ini, honeypot dapat berfungsi secara optimal sebagai alat pendeteksi dan pencatat serangan, meskipun diimplementasikan pada jaringan lokal berbasis IP private.

C. Topologi Sistem Honeypot Cowrie



Gambar 1 Topologi Sistem Honeypot Cowrie pada Jaringan Lokal

4. TOOLS YANG DIGUNAKAN

- **Cowrie**

  Digunakan sebagai honeypot SSH untuk mensimulasikan layanan SSH dan mencatat aktivitas serangan.

- **Nmap**

  Digunakan untuk melakukan port scanning dan mendeteksi layanan yang aktif pada target.

- **Nikto**

  Digunakan untuk melakukan scanning keamanan pada layanan web.

- **Hping3**

  Digunakan untuk menguji respon port dan melakukan scanning TCP tingkat rendah.

- **Hydra**

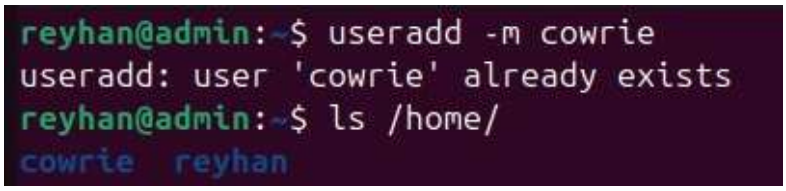
  Digunakan untuk melakukan serangan brute force terhadap layanan SSH.

- **LOIC (Low Orbit Ion Cannon)**

  Digunakan untuk mensimulasikan serangan Denial of Service (DoS).

5. INSTALASI DAN PERSIAPAN LINGKUNGAN

- **Pembuatan User Cowrie**



Gambar 2 Pembuatan dan Verifikasi User Cowrie

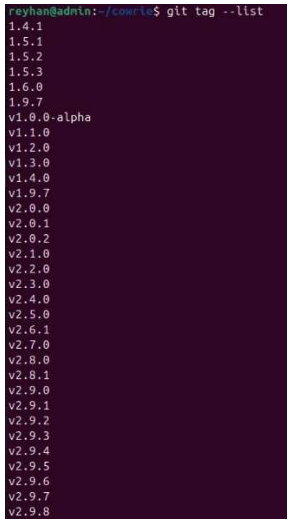
Gambar ini menunjukkan proses pembuatan user cowrie menggunakan perintah useradd -m cowrie. Sistem menampilkan pesan bahwa user cowrie sudah ada, yang menandakan user tersebut telah berhasil dibuat sebelumnya. Keberadaan user diverifikasi melalui direktori /home/.

- **Clone Repository Cowrie**

Gambar 3 Proses Cloning Repository Cowrie

Selanjutnya dilakukan proses cloning source code Cowrie dari repositori resmi GitHub menggunakan perintah git clone https://github.com/cowrie/cowrie.git. Proses cloning berjalan dengan sukses hingga mencapai 100%, menandakan seluruh file Cowrie berhasil diunduh dan siap untuk dikonfigurasi.

- **Pemilihan Versi Cowrie (Checkout v2.5.0)**



Gambar 4 Daftar Tag Versi Cowrie

Gambar ini menunjukkan daftar versi (tag) Honeypot Cowrie yang tersedia pada repository GitHub menggunakan perintah git tag --list. Daftar ini digunakan untuk memilih versi Cowrie yang stabil sebelum dilakukan proses checkout dan instalasi.

- **Proses Checkout dan Verifikasi Versi Cowrie v2.5.0**

Gambar 5 Pemilihan Versi Cowrie (Checkout Versi Stabil)

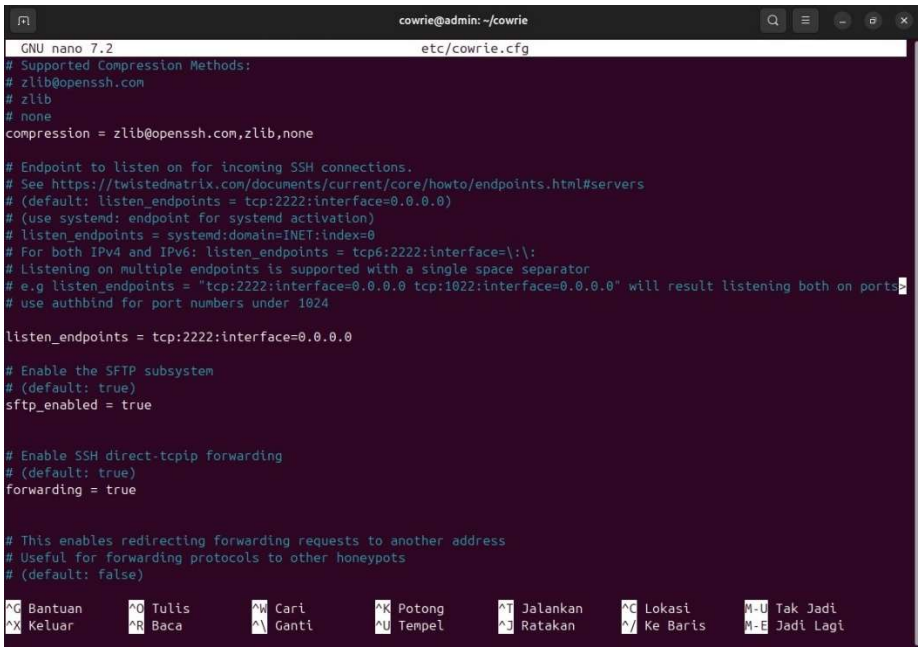
Gambar ini menunjukkan proses perpindahan repository Cowrie ke versi stabil v2.5.0 menggunakan perintah git checkout v2.5.0. Verifikasi versi dilakukan dengan perintah git branch --show-current dan git describe --tags, yang memastikan bahwa Cowrie berjalan pada versi yang sesuai untuk proses instalasi dan pengujian.

- **Peralihan User dan Aktivasi Virtual Environment Cowrie**

Gambar 6 Aktivasi Virtual Environment dan Instalasi Dependency

Gambar ini menunjukkan proses perpindahan ke user **cowrie**, masuk ke direktori Cowrie, serta aktivasi virtual environment menggunakan perintah source cowrie-env/bin/activate. Tahapan ini dilakukan sebelum proses instalasi dependency agar Cowrie berjalan pada lingkungan Python yang terisolasi.

- **Konfigurasi Port Honeypot**



Gambar 7 Konfigurasi Parameter listen_endpoints pada File cowrie.cfg

Gambar ini menunjukkan proses konfigurasi file cowrie.cfg pada honeypot Cowrie, khususnya pada parameter listen_endpoints yang digunakan untuk menentukan port layanan SSH tiruan. Konfigurasi ini bertujuan agar Cowrie dapat menerima koneksi SSH sebagai target serangan pada lingkungan pengujian.

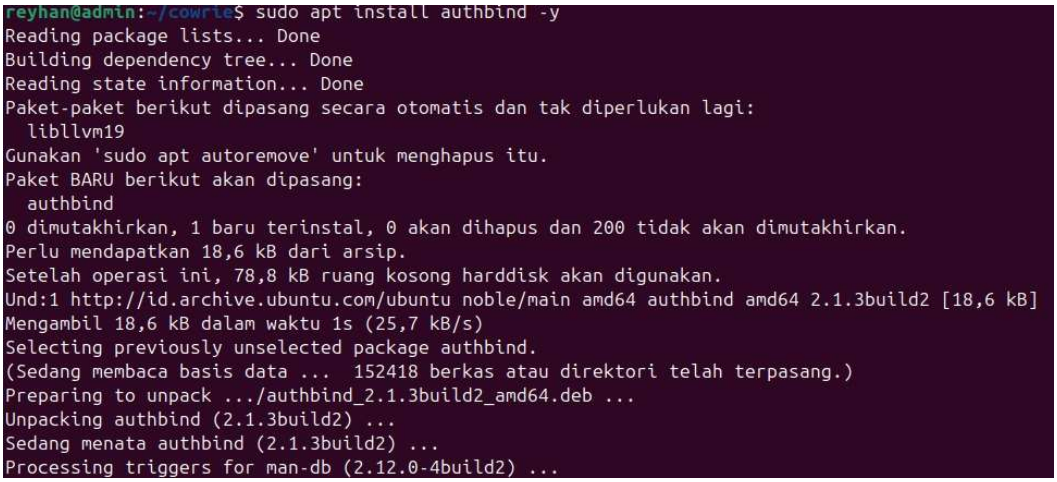
- **Instalasi Dependency Cowrie Menggunakan Requirements.txt**

Gambar 8 Instalasi Dependency Cowrie Menggunakan Requirements.txt

Gambar ini menunjukkan proses instalasi dan pengecekan dependency Cowrie menggunakan perintah pip install -r requirements.txt pada virtual environment, yang menandakan seluruh library pendukung telah terpasang dengan baik.

6. KONFIGURASI AUTHBIND

- **Instalasi Authbind**



Gambar 9 Instalasi Authbind pada Sistem

Pada tahap ini dilakukan instalasi authbind menggunakan perintah sudo apt install authbind -y. Authbind merupakan mekanisme pada sistem Linux yang memungkinkan aplikasi non-root untuk melakukan *binding* pada port tertentu, khususnya port di bawah 1024 yang secara default hanya dapat diakses oleh user root.

Penggunaan authbind pada praktikum ini bertujuan agar honeypot Cowrie tetap dijalankan menggunakan user biasa (cowrie), namun tetap dapat berfungsi sebagai layanan SSH tiruan yang berjalan pada port standar. Dengan demikian, keamanan sistem tetap terjaga tanpa harus memberikan hak akses root kepada aplikasi honeypo.

- **Pembuatan File Binding Port**

Gambar 10 Pembuatan File Authbind untuk Port 22

Setelah authbind berhasil diinstal, dilakukan pembuatan file izin binding pada direktori /etc/authbind/byport/. File ini dibuat menggunakan perintah sudo touch /etc/authbind/byport/22. File tersebut berfungsi sebagai *token* izin yang menandakan bahwa port 22 diperbolehkan untuk digunakan oleh aplikasi non-root.

Tahap ini sangat penting karena tanpa adanya file izin tersebut, aplikasi seperti Cowrie tidak akan diizinkan untuk menggunakan port SSH standar meskipun authbind telah terpasang.

- **Pengaturan Hak Akses Authbind**

```
reyhan@admin:~/cowrie$ sudo chmod 755 /etc/authbind/byport/22
```

Gambar 11 Pengaturan Hak Akses Authbind untuk Port 22

Pada tahap ini dilakukan pengaturan hak akses terhadap file /etc/authbind/byport/22 menggunakan perintah sudo chmod 755 /etc/authbind/byport/22. Pengaturan permission ini bertujuan agar user yang menjalankan honeypot memiliki izin yang cukup untuk menggunakan port tersebut. Dengan pengaturan ini, Cowrie dapat melakukan binding ke port 22 tanpa dijalankan sebagai root. Langkah ini merupakan bagian dari penerapan prinsip keamanan *least privilege*, yaitu memberikan hak akses seminimal mungkin namun tetap fungsional.

- **Menjalankan Cowrie dengan Authbind**

```
(cowrie-env) cowrie@admin:~/cowrie$ authbind --deep python3 src/cowrie/scripts/cowrie.py start
cowrie is already running (PID: 8956).
```

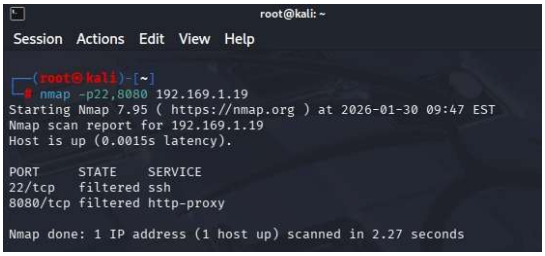
Gambar 12 Menjalankan Honeypot Cowrie Menggunakan Authbind

Setelah seluruh konfigurasi authbind selesai, honeypot Cowrie dijalankan menggunakan perintah authbind --deep python3 src/cowrie/scripts/cowrie.py start. Opsi --deep digunakan agar authbind diterapkan pada seluruh proses turunan yang dijalankan oleh Cowrie.

Output terminal menunjukkan bahwa Cowrie berhasil dijalankan dan berada dalam kondisi aktif (*running*). Dengan konfigurasi ini, Cowrie mampu menerima koneksi SSH tiruan pada port yang ditentukan dan mencatat seluruh aktivitas serangan tanpa mengganggu sistem utama.

7. PENGUJIAN SERANGAN TERHADAP HONEYPOT PADA LINGKUNGAN JARINGAN LOKAL

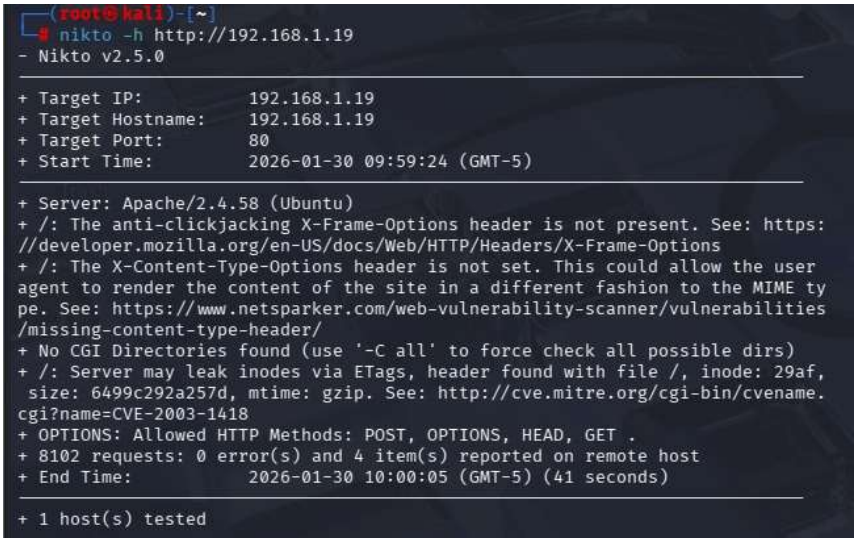
- **Pengujian Port Scanning terhadap Honeypot**
  - **Port Scanning Menggunakan Nmap**



Gambar 13 Hasil Port Scanning terhadap Honeypot Menggunakan Nmap

Serangan port scanning dilakukan menggunakan tool Nmap dari mesin penyerang (Kali Linux) dengan target IP 192.168.1.19. Hasil pemindaian menunjukkan bahwa host dalam kondisi aktif dan layanan tertentu dapat terdeteksi. Pada implementasi ini, layanan SSH yang terdeteksi diarahkan ke honeypot Cowrie, sehingga proses scanning tidak mengarah ke sistem SSH asli.

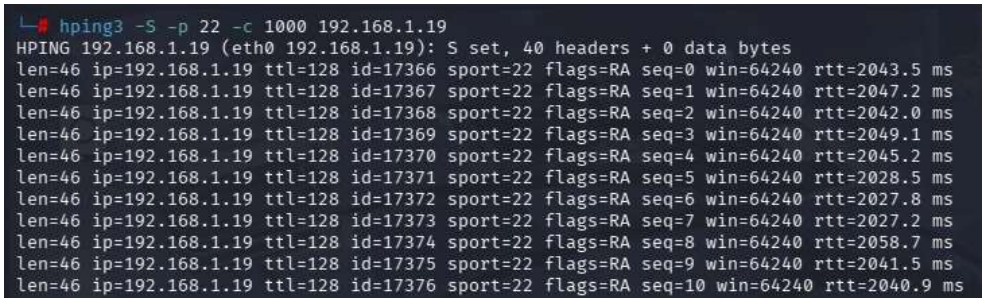
- **Port Scanning Menggunakan Nikto**



Gambar 14 Hasil Web Scanning terhadap Layanan HTTP Menggunakan Nikto

Nikto digunakan untuk melakukan pemindaian keamanan terhadap layanan web pada mesin target. Hasil scanning menunjukkan informasi versi web server serta beberapa konfigurasi keamanan yang belum aktif. Pengujian ini menunjukkan bahwa selain layanan SSH, layanan web juga dapat menjadi target awal serangan.

- **Port Scanning Menggunakan Hping3**

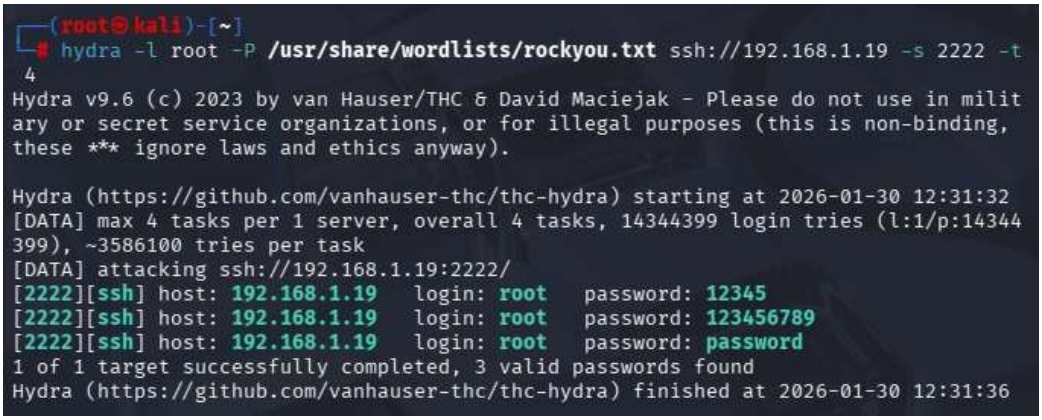


Gambar 15 Pengujian Port Scanning Menggunakan Hping3 pada Port SSH

Pengujian dilakukan dengan mengirim paket TCP SYN ke port SSH menggunakan hping3. Respon berupa SYN-ACK (SA) menandakan bahwa port

dalam kondisi terbuka. Seluruh trafik scanning ini diterima oleh honeypot Cowrie dan tidak menuju sistem asli.

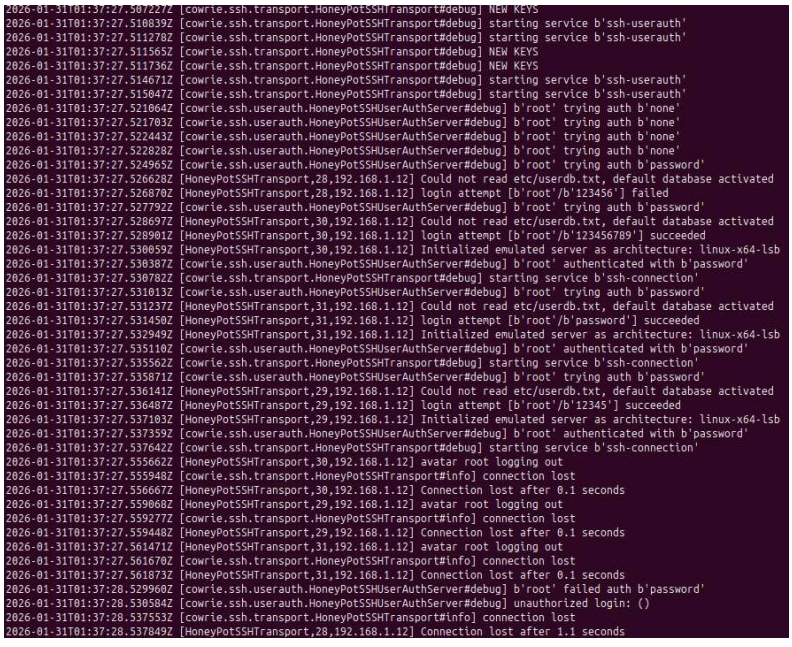
- **Pengujian Brute Force Attack terhadap Honeypot**



Gambar 16 Simulasi Serangan Brute Force SSH terhadap Honeypot Menggunakan Hydra

Serangan brute force dilakukan menggunakan tool Hydra dengan wordlist untuk mencoba berbagai kombinasi username dan password pada layanan SSH honeypot. Hasil menunjukkan bahwa beberapa kredensial berhasil "diterima" oleh honeypot Cowrie.

- **Analisis Log Serangan Honeypot Cowrie**



Gambar 17 Log Aktivitas Serangan Brute Force SSH pada Honeypot Cowrie

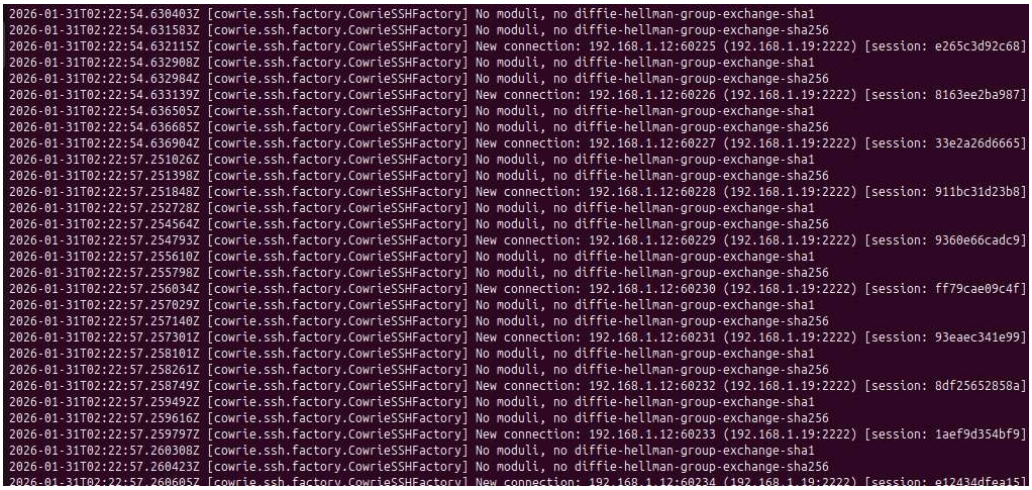
Log Cowrie mencatat secara detail aktivitas serangan, seperti:

- Percobaan login gagal dan berhasil
- Username dan password yang dicoba
- Alamat IP penyerang
- Durasi dan status koneksi
- Proses login dan logout avatar palsu

- **Pengujian DoS Attack terhadap Honeypot**

Gambar 18 Konfigurasi dan Eksekusi Serangan DoS Menggunakan LOIC terhadap Honeypot

Serangan Denial of Service (DoS) disimulasikan menggunakan tool LOIC dengan target IP honeypot dan port SSH. Serangan menghasilkan trafik dalam jumlah besar yang menyebabkan koneksi masuk secara berulang dalam waktu singkat.



Gambar 19 Log Aktivitas Koneksi Berulang pada Honeypot Cowrie saat Serangan DoS

Log Cowrie menunjukkan banyak sesi koneksi baru, *connection lost*, dan *timeout* yang merupakan ciri khas serangan DoS.

8. POLA MULTIPLE ATTACK SESUAI MODUL

- **Pola Pengujian Multiple Attack**

Tabel 1 Proses Pengujian Multiple Attack terhadap Honeypot Cowrie

No	Jenis Serangan	Tools yang Digunakan	Target	Keterangan
1	Port Scanning	Nmap	Honeypot Cowrie	Digunakan untuk mendeteksi port dan layanan aktif
2	Web Scanning	Nikto	Layanan HTTP	Digunakan untuk mengidentifikasi konfigurasi keamanan web
3	TCP Scanning	Hping3	Honeypot Cowrie	Digunakan untuk menguji respon port SSH dan HTTP
4	Brute Force SSH	Hydra	Honeypot Cowrie	Digunakan untuk mencoba berbagai kombinasi login SSH
5	DoS Attack	LOIC	Honeypot Cowrie	Digunakan untuk mensimulasikan traffic flooding

- **Hasil Pengujian Serangan**

Tabel 2 Hasil Pengujian Serangan terhadap Honeypot Cowrie

No	Jenis Serangan	Kondisi Sebelum	Kondisi Sesudah	Hasil
1	Port Scanning	Tidak terdeteksi	Terdeteksi	Honeypot berhasil mencatat aktivitas scanning
2	Web Scanning	Tidak terdeteksi	Terdeteksi	Informasi layanan web berhasil diperoleh
3	Brute Force SSH	Tidak ada login	Login palsu tercatat	Honeypot mencatat kredensial yang dicoba
4	DoS Attack	Trafik normal	Trafik meningkat	Honeypot mendeteksi koneksi berulang

9. POLA INDIVIDU, DOUBLE, MULTIPLE ATTACK

- **INDIVIDU ATTACK**

Gambar 20 Log Individu Attack pada Honeypot Cowrie

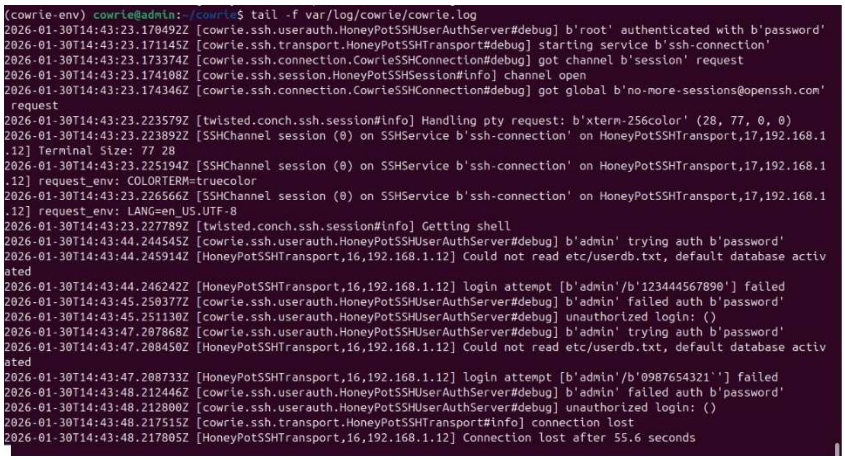
Individu attack merupakan pengujian serangan yang dilakukan satu jenis serangan saja dalam satu waktu terhadap honeypot.

Pada praktikum ini, individu attack ditunjukkan oleh:

- Percobaan login SSH dengan satu username dan satu password

- Contoh pada log Cowrie: login attempt ['root'/'123456'] failed

- **DOUBLE ATTACK**



Gambar 21 Log Double Attack pada Honeypot Cowrie

Double attack merupakan pengujian yang melibatkan dua jenis serangan secara berurutan terhadap honeypot.

Pada praktikum ini, double attack ditunjukkan oleh:

- Port scanning (Nmap / Hping3)
- Dilanjutkan dengan brute force SSH (Hydra)

Log Cowrie menunjukkan:

- Koneksi SSH masuk
- Diikuti percobaan login berulang dari IP yang sama

- **MULTIPLE ATTACK**

Gambar 22 Log Multiple Attack pada Honeypot Cowrie

Multiple attack merupakan pengujian yang melibatkan lebih dari dua jenis serangan secara bersamaan atau berurutan dalam satu skenario.

Pada praktikum ini, multiple attack ditunjukkan oleh:

- Port scanning
- Brute force SSH dengan banyak kombinasi username & password
- Koneksi berulang dalam waktu singkat (indikasi DoS ringan)

Log Cowrie menunjukkan:

- Banyak username berbeda (root, admin, doble, individu, multiple)
- Percobaan login berulang
- Connection lost dan timeout

10. KESIMPULAN

Berdasarkan hasil praktikum yang telah dilakukan, dapat disimpulkan bahwa honeypot **Cowrie** berhasil diimplementasikan dan diuji pada lingkungan **jaringan lokal menggunakan IP private**. Honeypot mampu berfungsi sebagai layanan SSH tiruan yang efektif untuk menarik, mendeteksi, dan mencatat berbagai aktivitas serangan tanpa memberikan akses ke sistem asli.

Pengujian serangan yang dilakukan meliputi **port scanning**, **web scanning**, **brute force SSH**, serta **Denial of Service (DoS)**. Seluruh serangan berhasil diarahkan ke honeypot dan terekam secara detail dalam log Cowrie, termasuk informasi alamat IP penyerang, username, password yang dicoba, status login, serta durasi koneksi.

Selain itu, pengujian **individu, double, dan multiple attack** menunjukkan bahwa honeypot Cowrie mampu mendeteksi pola serangan tunggal hingga serangan kompleks yang dilakukan secara berurutan maupun berulang. Hal ini membuktikan bahwa honeypot efektif sebagai alat monitoring dan analisis keamanan jaringan.

Dengan demikian, praktikum ini membuktikan bahwa honeypot Cowrie dapat digunakan sebagai media pembelajaran keamanan jaringan yang aman, terkontrol, dan tidak memerlukan VPS publik, namun tetap mampu merepresentasikan skenario serangan nyata.