

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:

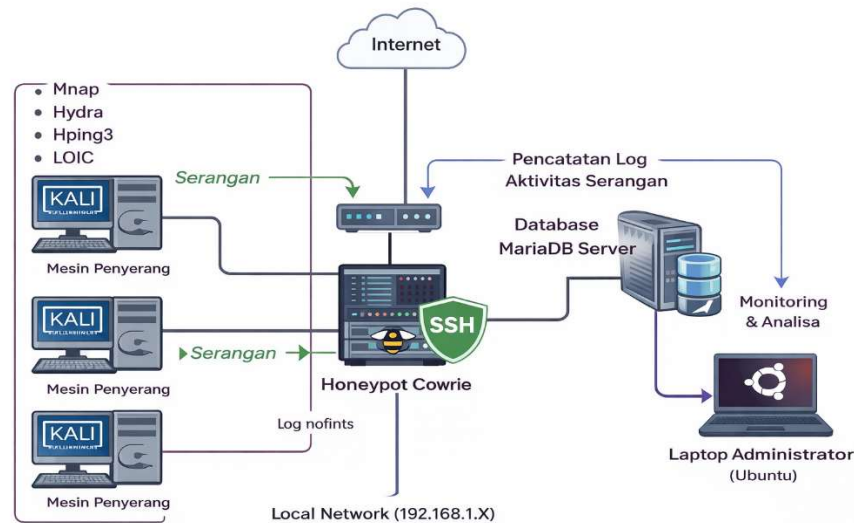
- Mesin penyerang (Kali Linux) melakukan serangan jaringan seperti:
 - Port scanning
 - Brute force SSH
 - DoS attack
- Seluruh serangan diarahkan ke IP target 192.168.1.19.
- Layanan SSH pada port 2222 telah dikonfigurasi sebagai honeypot Cowrie, sehingga setiap koneksi SSH yang masuk akan ditangani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

```
reyhan@admin:~$ useradd -m cowrie
useradd: user 'cowrie' already exists
reyhan@admin:~$ ls /home/
cowrie  reyhan
```

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

```
reyhan@admin:~$ git clone https://github.com/cowrie/cowrie.git
Kloning ke 'cowrie'...
remote: Enumerating objects: 20802, done.
remote: Counting objects: 100% (65/65), done.
remote: Compressing objects: 100% (49/49), done.
remote: Total 20802 (delta 40), reused 18 (delta 16), pack-reused 20737 (from 2)
Menerima objek: 100% (20802/20802), 11.02 mebibita | 3.07 mebibita/detik, selesai.
Menyusun delta: 100% (14538/14538), selesai.
```

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)

```
reyhan@admin:~/cowrie$ git tag --l
1.4.1
1.5.1
1.5.2
1.5.3
1.6.0
1.9.7
v1.0.0-alpha
v1.1.0
v1.2.0
v1.3.0
v1.4.0
v1.9.7
v2.0.0
v2.0.1
v2.0.2
v2.1.0
v2.2.0
v2.3.0
v2.4.0
v2.5.0
v2.6.1
v2.7.0
v2.8.0
v2.8.1
v2.9.0
v2.9.1
v2.9.2
v2.9.3
v2.9.4
v2.9.5
v2.9.6
v2.9.7
v2.9.8
```

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**

```
reyhan@admin:~/cowrie$ git checkout v2.5.0
Catatan: berganti ke 'v2.5.0'.

Anda berada dalam keadaan 'HEAD terpisah'. Anda dapat melihat-lihat, membuat
perubahan eksperimental and komit, dan Anda dapat membuang komit apa saja yang
Anda buat di dalam keadaan ini tanpa mempengaruhi cabang apapun dengan bergantinkembali ke sebuah cabang.

Jika Anda ingin membuat cabang baru untuk menyimpan komit yang Anda buat, Anda
dapat melakukannya (sekarang atau nanti) dengan:

    git switch -c <nama cabang baru>

Atau batalkan operasi ini dengan:

    git switch -

Matikan saran ini dengan menyetel variabel konfigurasi advice.detachedHead ke false

HEAD sekarang berada di 00011683 Release 2.5.0 (#1808)
reyhan@admin:~/cowrie$ git branch --show-current
reyhan@admin:~/cowrie$ git describe --tags
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.

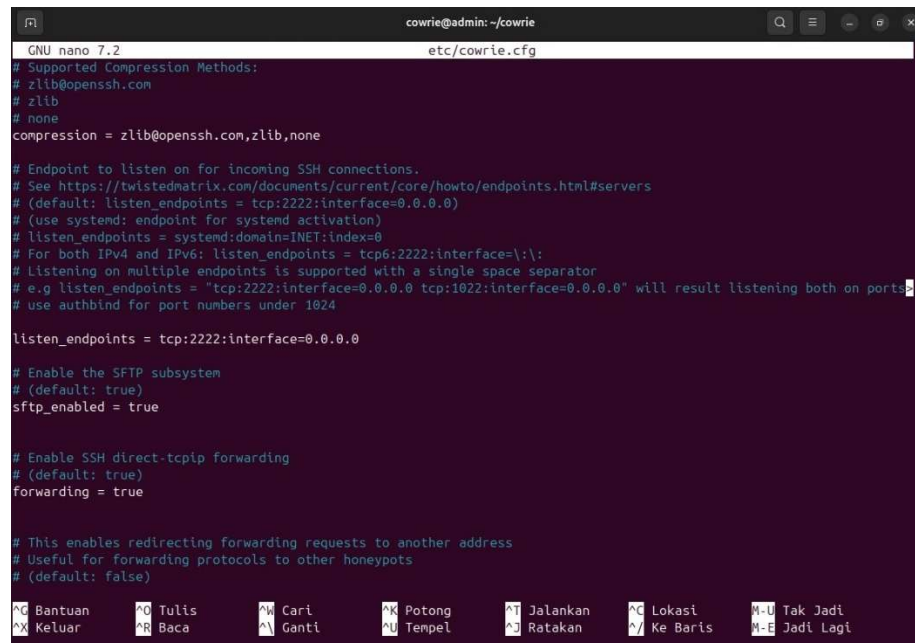
- **Peralihan User dan Aktivasi Virtual Environment Cowrie**

```
reyhan@admin:~/cowrie$ su - cowrie
Kata Sandi:
cowrie@admin:~$ cd cowrie
cowrie@admin:~/cowrie$ source cowrie-env/bin/activate
(cowrie-env) cowrie@admin:~/cowrie$ pip install --upgrade pip
Requirement already satisfied: pip in ./cowrie-env/lib/python3.12/site-packages (25.3)
```

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**



```
GNU nano 7.2 etc/cowrie.cfg
# Supported Compression Methods:
# zlib@openssh.com
# zlib
# none
compression = zlib@openssh.com,zlib,none

# Endpoint to listen on for incoming SSH connections.
# See https://twistedmatrix.com/documents/current/core/howto/endpoints.html#servers
# (default: listen_endpoints = tcp:2222:interface=0.0.0.0)
# (use systemd: endpoint for systemd activation)
# listen_endpoints = systemd:domain=INET:index=0
# For both IPv4 and IPv6: listen_endpoints = tcp6:2222:interface=:::
# Listening on multiple endpoints is supported with a single space separator
# e.g listen_endpoints = 'tcp:2222:interface=0.0.0.0 tcp:1022:interface=0.0.0.0' will result listening both on ports
# use authbind for port numbers under 1024

listen_endpoints = tcp:2222:interface=0.0.0.0

# Enable the SFTP subsystem
# (default: true)
sftp_enabled = true

# Enable SSH direct-tcpip forwarding
# (default: true)
forwarding = true

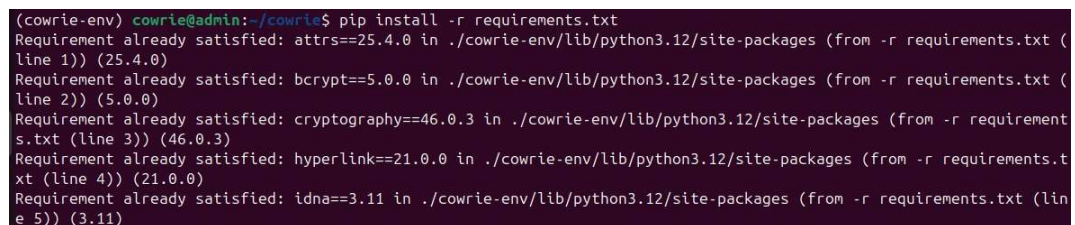
# This enables redirecting forwarding requests to another address
# Useful for forwarding protocols to other honeypots
# (default: false)

^C Bantuan ^O Tulis ^M Cari ^K Potong ^T Jalankan ^C Lokasi ^M-U Tak Jadi
^X Keluar ^R Baca ^N Ganti ^U Tempel ^D Ratakan ^V Ke Barts ^M-E Jadi Lagi
```

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**



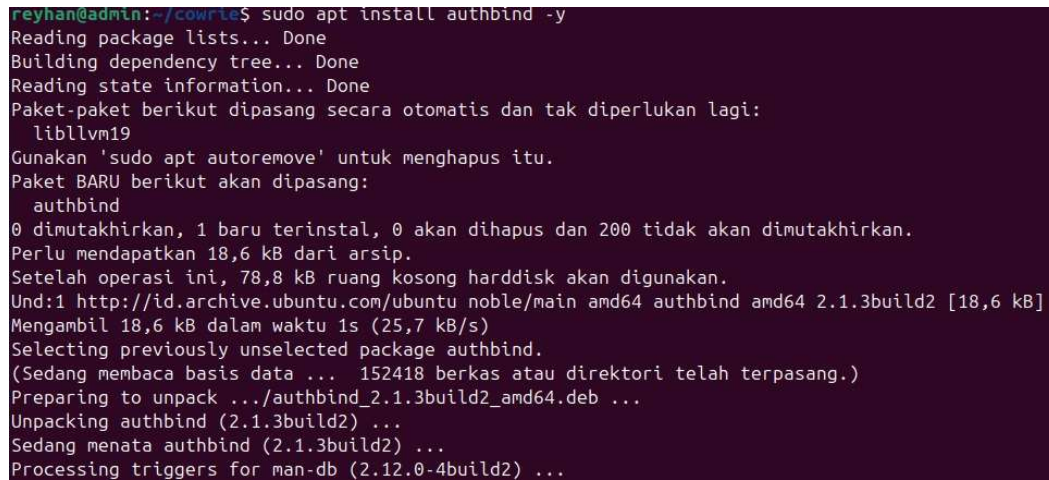
```
(cowrie-env) cowrie@admin:~/cowrie$ pip install -r requirements.txt
Requirement already satisfied: attrs==25.4.0 in ./cowrie-env/lib/python3.12/site-packages (from -r requirements.txt (line 1)) (25.4.0)
Requirement already satisfied: bcrypt==5.0.0 in ./cowrie-env/lib/python3.12/site-packages (from -r requirements.txt (line 2)) (5.0.0)
Requirement already satisfied: cryptography==46.0.3 in ./cowrie-env/lib/python3.12/site-packages (from -r requirements.txt (line 3)) (46.0.3)
Requirement already satisfied: hyperlink==21.0.0 in ./cowrie-env/lib/python3.12/site-packages (from -r requirements.txt (line 4)) (21.0.0)
Requirement already satisfied: idna==3.11 in ./cowrie-env/lib/python3.12/site-packages (from -r requirements.txt (line 5)) (3.11)
```

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




```
reyhan@admin:~/cowrie$ sudo apt install authbind -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Paket-paket berikut dipasang secara otomatis dan tak diperlukan lagi:
  libllvm19
Gunakan 'sudo apt autoremove' untuk menghapus itu.
Paket BARU berikut akan dipasang:
  authbind
0 dimutakhirkan, 1 baru terinstal, 0 akan dihapus dan 200 tidak akan dimutakhirkan.
Perlu mendapatkan 18,6 kB dari arsip.
Setelah operasi ini, 78,8 kB ruang kosong harddisk akan digunakan.
Und:1 http://id.archive.ubuntu.com/ubuntu noble/main amd64 authbind amd64 2.1.3build2 [18,6 kB]
Mengambil 18,6 kB dalam waktu 1s (25,7 kB/s)
Selecting previously unselected package authbind.
(Sedang membaca basis data ... 152418 berkas atau direktori telah terpasang.)
Preparing to unpack .../authbind_2.1.3build2_amd64.deb ...
Unpacking authbind (2.1.3build2) ...
Sedang menata authbind (2.1.3build2) ...
Processing triggers for man-db (2.12.0-4build2) ...
```

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 honeypot.

- Pembuatan File Binding Port



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

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

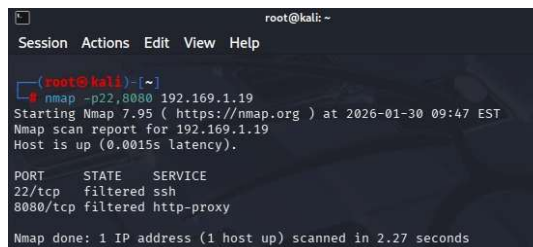
Setelah seluruh konfigurasi authbind selesai, honeypot Cowrie dijalankan menggunakan perintah `authbind --deep python3 src/cowrie/scripts/cowrie.py start`. Opsi `--deep` digunakan agar authbind diterapkan pada seluruh proses turunan yang dijalankan oleh Cowrie.

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**



```
root@kali: ~
Session Actions Edit View Help

(root@kali) ~
$ nmap -p22,8080 192.169.1.19
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-30 09:47 EST
Nmap scan report for 192.169.1.19
Host is up (0.0015s latency).

PORT      STATE SERVICE
22/tcp    filtered ssh
8080/tcp   filtered http-proxy

Nmap done: 1 IP address (1 host up) scanned in 2.27 seconds
```

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

```
(root@kali)~# nikto -h http://192.168.1.19
- Nikto v2.5.0

+ Target IP: 192.168.1.19
+ Target Hostname: 192.168.1.19
+ Target Port: 80
+ Start Time: 2026-01-30 09:59:24 (GMT-5)

+ Server: Apache/2.4.58 (Ubuntu)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /: Server may leak inodes via ETags, header found with file /, inode: 29af, size: 6499c292a257d, mtime: gzip. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ OPTIONS: Allowed HTTP Methods: POST, OPTIONS, HEAD, GET .
+ 8102 requests: 0 error(s) and 4 item(s) reported on remote host
+ End Time: 2026-01-30 10:00:05 (GMT-5) (41 seconds)

+ 1 host(s) tested
```

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

```
hping3 -S -p 22 -c 1000 192.168.1.19
HPING 192.168.1.19 (eth0 192.168.1.19): S set, 40 headers + 0 data bytes
len=46 ip=192.168.1.19 ttl=128 id=17366 sport=22 flags=RA seq=0 win=64240 rtt=2043.5 ms
len=46 ip=192.168.1.19 ttl=128 id=17367 sport=22 flags=RA seq=1 win=64240 rtt=2047.2 ms
len=46 ip=192.168.1.19 ttl=128 id=17368 sport=22 flags=RA seq=2 win=64240 rtt=2042.0 ms
len=46 ip=192.168.1.19 ttl=128 id=17369 sport=22 flags=RA seq=3 win=64240 rtt=2049.1 ms
len=46 ip=192.168.1.19 ttl=128 id=17370 sport=22 flags=RA seq=4 win=64240 rtt=2045.2 ms
len=46 ip=192.168.1.19 ttl=128 id=17371 sport=22 flags=RA seq=5 win=64240 rtt=2028.5 ms
len=46 ip=192.168.1.19 ttl=128 id=17372 sport=22 flags=RA seq=6 win=64240 rtt=2027.8 ms
len=46 ip=192.168.1.19 ttl=128 id=17373 sport=22 flags=RA seq=7 win=64240 rtt=2027.2 ms
len=46 ip=192.168.1.19 ttl=128 id=17374 sport=22 flags=RA seq=8 win=64240 rtt=2058.7 ms
len=46 ip=192.168.1.19 ttl=128 id=17375 sport=22 flags=RA seq=9 win=64240 rtt=2041.5 ms
len=46 ip=192.168.1.19 ttl=128 id=17376 sport=22 flags=RA seq=10 win=64240 rtt=2040.9 ms
```

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**

```
(root@kali)-[~]
└─$ hydra -l root -P /usr/share/wordlists/rockyou.txt ssh://192.168.1.19 -s 2222 -t 4
Hydra v9.6 (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 2026-01-30 12:31:32
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344399 login tries (l:1/p:14344399), ~3586100 tries per task
[DATA] attacking ssh://192.168.1.19:2222/
[2222][ssh] host: 192.168.1.19 login: root password: 12345
[2222][ssh] host: 192.168.1.19 login: root password: 123456789
[2222][ssh] host: 192.168.1.19 login: root password: password
1 of 1 target successfully completed, 3 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2026-01-30 12:31:36
```

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**

```
2026-01-31T01:37:27.50222Z [cowrie.ssh.transport.HoneyPotSSHTransport#debug] NEW KEYS
2026-01-31T01:37:27.510839Z [cowrie.ssh.transport.HoneyPotSSHTransport#debug] starting service b'ssh-userauth'
2026-01-31T01:37:27.511278Z [cowrie.ssh.transport.HoneyPotSSHTransport#debug] starting service b'ssh-userauth'
2026-01-31T01:37:27.511565Z [cowrie.ssh.transport.HoneyPotSSHTransport#debug] NEW KEYS
2026-01-31T01:37:27.511736Z [cowrie.ssh.transport.HoneyPotSSHTransport#debug] NEW KEYS
2026-01-31T01:37:27.514671Z [cowrie.ssh.transport.HoneyPotSSHTransport#debug] starting service b'ssh-userauth'
2026-01-31T01:37:27.515047Z [cowrie.ssh.transport.HoneyPotSSHTransport#debug] starting service b'ssh-userauth'
2026-01-31T01:37:27.521064Z [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'root' trying auth b'none'
2026-01-31T01:37:27.521703Z [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'root' trying auth b'none'
2026-01-31T01:37:27.522443Z [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'root' trying auth b'none'
2026-01-31T01:37:27.522828Z [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'root' trying auth b'none'
2026-01-31T01:37:27.524965Z [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'root' trying auth b'password'
2026-01-31T01:37:27.526628Z [HoneyPotSSHTransport,28,192.168.1.12] Could not read etc/userdb.txt, default database activated
2026-01-31T01:37:27.526870Z [HoneyPotSSHTransport,28,192.168.1.12] login attempt [b'root'/b'123456'] failed
2026-01-31T01:37:27.527792Z [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'root' trying auth b'password'
2026-01-31T01:37:27.528697Z [HoneyPotSSHTransport,30,192.168.1.12] Could not read etc/userdb.txt, default database activated
2026-01-31T01:37:27.528991Z [HoneyPotSSHTransport,30,192.168.1.12] login attempt [b'root'/b'123456789'] succeeded
2026-01-31T01:37:27.530059Z [HoneyPotSSHTransport,30,192.168.1.12] Initialized emulated server as architecture: linux-x64-lsb
2026-01-31T01:37:27.530387Z [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'root' authenticated with b'password'
2026-01-31T01:37:27.530782Z [cowrie.ssh.transport.HoneyPotSSHTransport#debug] starting service b'ssh-connection'
2026-01-31T01:37:27.531013Z [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'root' trying auth b'password'
2026-01-31T01:37:27.531237Z [HoneyPotSSHTransport,31,192.168.1.12] Could not read etc/userdb.txt, default database activated
2026-01-31T01:37:27.531450Z [HoneyPotSSHTransport,31,192.168.1.12] login attempt [b'root'/b'password'] succeeded
2026-01-31T01:37:27.532949Z [HoneyPotSSHTransport,31,192.168.1.12] Initialized emulated server as architecture: linux-x64-lsb
2026-01-31T01:37:27.535110Z [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'root' authenticated with b'password'
2026-01-31T01:37:27.535562Z [cowrie.ssh.transport.HoneyPotSSHTransport#debug] starting service b'ssh-connection'
2026-01-31T01:37:27.535871Z [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'root' trying auth b'password'
2026-01-31T01:37:27.536407Z [HoneyPotSSHTransport,29,192.168.1.12] Could not read etc/userdb.txt, default database activated
2026-01-31T01:37:27.537103Z [HoneyPotSSHTransport,29,192.168.1.12] login attempt [b'root'/b'12345'] succeeded
2026-01-31T01:37:27.537359Z [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'root' authenticated with b'password'
2026-01-31T01:37:27.537642Z [cowrie.ssh.transport.HoneyPotSSHTransport#debug] starting service b'ssh-connection'
2026-01-31T01:37:27.555662Z [HoneyPotSSHTransport,30,192.168.1.12] avatar root logging out
2026-01-31T01:37:27.555948Z [cowrie.ssh.transport.HoneyPotSSHTransport#info] connection lost
2026-01-31T01:37:27.556667Z [HoneyPotSSHTransport,30,192.168.1.12] Connection lost after 0.1 seconds
2026-01-31T01:37:27.559060Z [HoneyPotSSHTransport,29,192.168.1.12] avatar root logging out
2026-01-31T01:37:27.559277Z [cowrie.ssh.transport.HoneyPotSSHTransport#info] connection lost
2026-01-31T01:37:27.559448Z [HoneyPotSSHTransport,29,192.168.1.12] Connection lost after 0.1 seconds
2026-01-31T01:37:27.561471Z [HoneyPotSSHTransport,31,192.168.1.12] avatar root logging out
2026-01-31T01:37:27.561670Z [cowrie.ssh.transport.HoneyPotSSHTransport#info] connection lost
2026-01-31T01:37:27.561873Z [HoneyPotSSHTransport,31,192.168.1.12] Connection lost after 0.1 seconds
2026-01-31T01:37:28.529908Z [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'root' failed auth b'password'
2026-01-31T01:37:28.530504Z [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] unauthorized login: ()
2026-01-31T01:37:28.537553Z [cowrie.ssh.transport.HoneyPotSSHTransport#info] connection lost
2026-01-31T01:37:28.537849Z [HoneyPotSSHTransport,28,192.168.1.12] Connection lost after 1.1 seconds
```

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.

```
2026-01-31T02:22:54.630403Z [cowrie.ssh.factory.CowrieSSHFactory] No moduli, no diffie-hellman-group-exchange-sha1
2026-01-31T02:22:54.631583Z [cowrie.ssh.factory.CowrieSSHFactory] No moduli, no diffie-hellman-group-exchange-sha256
2026-01-31T02:22:54.632115Z [cowrie.ssh.factory.CowrieSSHFactory] New connection: 192.168.1.12:60225 (192.168.1.19:2222) [session: e265c3d92c68]
2026-01-31T02:22:54.632908Z [cowrie.ssh.factory.CowrieSSHFactory] No moduli, no diffie-hellman-group-exchange-sha1
2026-01-31T02:22:54.632984Z [cowrie.ssh.factory.CowrieSSHFactory] No moduli, no diffie-hellman-group-exchange-sha256
2026-01-31T02:22:54.633139Z [cowrie.ssh.factory.CowrieSSHFactory] New connection: 192.168.1.12:60226 (192.168.1.19:2222) [session: 8163ee2ba987]
2026-01-31T02:22:54.636505Z [cowrie.ssh.factory.CowrieSSHFactory] No moduli, no diffie-hellman-group-exchange-sha1
2026-01-31T02:22:54.636685Z [cowrie.ssh.factory.CowrieSSHFactory] No moduli, no diffie-hellman-group-exchange-sha256
2026-01-31T02:22:54.636904Z [cowrie.ssh.factory.CowrieSSHFactory] New connection: 192.168.1.12:60227 (192.168.1.19:2222) [session: 33e2a26d6665]
2026-01-31T02:22:57.251026Z [cowrie.ssh.factory.CowrieSSHFactory] No moduli, no diffie-hellman-group-exchange-sha1
2026-01-31T02:22:57.251398Z [cowrie.ssh.factory.CowrieSSHFactory] No moduli, no diffie-hellman-group-exchange-sha256
2026-01-31T02:22:57.251848Z [cowrie.ssh.factory.CowrieSSHFactory] New connection: 192.168.1.12:60228 (192.168.1.19:2222) [session: 911bc31d23b8]
2026-01-31T02:22:57.252728Z [cowrie.ssh.factory.CowrieSSHFactory] No moduli, no diffie-hellman-group-exchange-sha1
2026-01-31T02:22:57.254564Z [cowrie.ssh.factory.CowrieSSHFactory] No moduli, no diffie-hellman-group-exchange-sha256
2026-01-31T02:22:57.254793Z [cowrie.ssh.factory.CowrieSSHFactory] New connection: 192.168.1.12:60229 (192.168.1.19:2222) [session: 9360e66cad9]
2026-01-31T02:22:57.255610Z [cowrie.ssh.factory.CowrieSSHFactory] No moduli, no diffie-hellman-group-exchange-sha1
2026-01-31T02:22:57.255798Z [cowrie.ssh.factory.CowrieSSHFactory] No moduli, no diffie-hellman-group-exchange-sha256
2026-01-31T02:22:57.256034Z [cowrie.ssh.factory.CowrieSSHFactory] New connection: 192.168.1.12:60230 (192.168.1.19:2222) [session: ff79cae09c4f]
2026-01-31T02:22:57.257029Z [cowrie.ssh.factory.CowrieSSHFactory] No moduli, no diffie-hellman-group-exchange-sha1
2026-01-31T02:22:57.257140Z [cowrie.ssh.factory.CowrieSSHFactory] No moduli, no diffie-hellman-group-exchange-sha256
2026-01-31T02:22:57.257301Z [cowrie.ssh.factory.CowrieSSHFactory] New connection: 192.168.1.12:60231 (192.168.1.19:2222) [session: 93eae341e99]
2026-01-31T02:22:57.258101Z [cowrie.ssh.factory.CowrieSSHFactory] No moduli, no diffie-hellman-group-exchange-sha1
2026-01-31T02:22:57.258261Z [cowrie.ssh.factory.CowrieSSHFactory] No moduli, no diffie-hellman-group-exchange-sha256
2026-01-31T02:22:57.258749Z [cowrie.ssh.factory.CowrieSSHFactory] New connection: 192.168.1.12:60232 (192.168.1.19:2222) [session: 8df25652858a]
2026-01-31T02:22:57.259492Z [cowrie.ssh.factory.CowrieSSHFactory] No moduli, no diffie-hellman-group-exchange-sha1
2026-01-31T02:22:57.259616Z [cowrie.ssh.factory.CowrieSSHFactory] No moduli, no diffie-hellman-group-exchange-sha256
2026-01-31T02:22:57.259797Z [cowrie.ssh.factory.CowrieSSHFactory] New connection: 192.168.1.12:60233 (192.168.1.19:2222) [session: 1aef9d354bf9]
2026-01-31T02:22:57.260308Z [cowrie.ssh.factory.CowrieSSHFactory] No moduli, no diffie-hellman-group-exchange-sha1
2026-01-31T02:22:57.260423Z [cowrie.ssh.factory.CowrieSSHFactory] No moduli, no diffie-hellman-group-exchange-sha256
2026-01-31T02:22:57.260605Z [cowrie.ssh.factory.CowrieSSHFactory] New connection: 192.168.1.12:60234 (192.168.1.19:2222) [session: e17434feaf15]
```

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

```
(cowrie-env) cowrie@admin: /cowrie$ tail -f var/log/cowrie/cowrie.log
2026-01-30T14:29:02.929365Z [cowrie.ssh.userauth.HoneyPotSSHUserAuthService#debug] b'root' authenticated with b'password'
2026-01-30T14:29:02.929555Z [cowrie.ssh.transport.HoneyPotSSHTransport#debug] starting service b'ssh-connection'
2026-01-30T14:29:02.937286Z [cowrie.ssh.connection.CowrieSSHConnection#debug] got channel b'session' request
2026-01-30T14:29:02.938046Z [cowrie.ssh.session.HoneyPotSSHSession#info] channel open
2026-01-30T14:29:02.938211Z [cowrie.ssh.connection.CowrieSSHConnection#debug] got global b'no-more-sessions@openssh.com' request
2026-01-30T14:29:03.123961Z [twisted.conch.ssh.session#info] Handling pty request: b'xterm-256color' (45, 140, 0, 0)
2026-01-30T14:29:03.124289Z [SSHChannel session (0) on SSHService b'ssh-connection' on HoneyPotSSHTransport,7,192.168.1.16] Terminal Size: 140 45
2026-01-30T14:29:03.128199Z [SSHChannel session (0) on SSHService b'ssh-connection' on HoneyPotSSHTransport,7,192.168.1.16] request_env: COLORTERM=truecolor
2026-01-30T14:29:03.129440Z [SSHChannel session (0) on SSHService b'ssh-connection' on HoneyPotSSHTransport,7,192.168.1.16] request_env: LANG=en_US.UTF-8
2026-01-30T14:29:03.131042Z [twisted.conch.ssh.session#info] Getting shell
```

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**

```
(cowrie-env) cowrie@admin:~$ tail -f var/log/cowrie/cowrie.log
2026-01-30T14:43:23.170492Z [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'root' authenticated with b'password'
2026-01-30T14:43:23.171145Z [cowrie.ssh.transport.HoneyPotSSHTransport#debug] starting service b'ssh-connection'
2026-01-30T14:43:23.173374Z [cowrie.ssh.connection.CowrieSSHConnection#debug] got channel b'session' request
2026-01-30T14:43:23.174108Z [cowrie.ssh.session.HoneyPotSSHSession#info] channel open
2026-01-30T14:43:23.174346Z [cowrie.ssh.connection.CowrieSSHConnection#debug] got global b'no-more-sessions@openssh.com' request
2026-01-30T14:43:23.223579Z [twisted.conch.ssh.session#info] Handling pty request: b'xterm-256color' (28, 77, 0, 0)
2026-01-30T14:43:23.223892Z [SSHChannel session (0) on SSHService b'ssh-connection' on HoneyPotSSHTransport,17,192.168.1.12] Terminal Size: 77 28
2026-01-30T14:43:23.225194Z [SSHChannel session (0) on SSHService b'ssh-connection' on HoneyPotSSHTransport,17,192.168.1.12] request_env: COLORTERM=truecolor
2026-01-30T14:43:23.226566Z [SSHChannel session (0) on SSHService b'ssh-connection' on HoneyPotSSHTransport,17,192.168.1.12] request_env: LANG=en_US.UTF-8
2026-01-30T14:43:23.227789Z [twisted.conch.ssh.session#info] Getting shell
2026-01-30T14:43:44.244545Z [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'admin' trying auth b'password'
2026-01-30T14:43:44.245914Z [HoneyPotSSHTransport,16,192.168.1.12] Could not read etc/userdb.txt, default database activated
2026-01-30T14:43:44.246242Z [HoneyPotSSHTransport,16,192.168.1.12] login attempt [b'admin'/'b'123444567890'] failed
2026-01-30T14:43:45.250377Z [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'admin' failed auth b'password'
2026-01-30T14:43:45.251130Z [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] unauthorized login: ()
2026-01-30T14:43:47.207868Z [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'admin' trying auth b'password'
2026-01-30T14:43:47.208450Z [HoneyPotSSHTransport,16,192.168.1.12] Could not read etc/userdb.txt, default database activated
2026-01-30T14:43:47.208733Z [HoneyPotSSHTransport,16,192.168.1.12] login attempt [b'admin'/'b'0907654321'] failed
2026-01-30T14:43:48.212446Z [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'admin' failed auth b'password'
2026-01-30T14:43:48.212800Z [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] unauthorized login: ()
2026-01-30T14:43:48.217515Z [cowrie.ssh.transport.HoneyPotSSHTransport#info] connection lost
2026-01-30T14:43:48.217805Z [HoneyPotSSHTransport,16,192.168.1.12] Connection lost after 55.6 seconds
```

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**

```
(cowrie-env) cowrie@admin:~$ tail -f var/log/cowrie/cowrie.log
2026-01-30T14:51:10.119520Z [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'doble' trying auth b'password'
2026-01-30T14:51:10.119967Z [HoneyPotSSHTransport,20,192.168.1.12] Could not read etc/userdb.txt, default database activated
2026-01-30T14:51:10.120187Z [HoneyPotSSHTransport,20,192.168.1.12] login attempt [b'doble'/'b'3333333'] failed
2026-01-30T14:51:11.123705Z [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'doble' failed auth b'password'
2026-01-30T14:51:11.124056Z [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] unauthorized login: ()
2026-01-30T14:51:16.504636Z [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'individu' trying auth b'password'
2026-01-30T14:51:16.505637Z [HoneyPotSSHTransport,19,192.168.1.12] Could not read etc/userdb.txt, default database activated
2026-01-30T14:51:16.505875Z [HoneyPotSSHTransport,19,192.168.1.12] login attempt [b'individu'/'b'0123456789'] failed
2026-01-30T14:51:17.509885Z [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'individu' failed auth b'password'
2026-01-30T14:51:17.510242Z [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] unauthorized login: ()
2026-01-30T14:51:40.635250Z [.] Timeout reached in HoneyPotSSHTransport
2026-01-30T14:51:40.637153Z [cowrie.ssh.transport.HoneyPotSSHTransport#info] connection lost
2026-01-30T14:51:40.637328Z [HoneyPotSSHTransport,19,192.168.1.12] Connection lost after 120.0 seconds
2026-01-30T14:51:43.151305Z [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'multiple' trying auth b'password'
2026-01-30T14:51:43.151904Z [HoneyPotSSHTransport,21,192.168.1.12] Could not read etc/userdb.txt, default database activated
2026-01-30T14:51:43.152765Z [HoneyPotSSHTransport,21,192.168.1.12] login attempt [b'multiple'/'b'00000'] failed
2026-01-30T14:51:44.156517Z [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'multiple' failed auth b'password'
2026-01-30T14:51:44.157792Z [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] unauthorized login: ()
2026-01-30T14:51:44.165996Z [cowrie.ssh.transport.HoneyPotSSHTransport#info] connection lost
2026-01-30T14:51:44.166480Z [HoneyPotSSHTransport,21,192.168.1.12] Connection lost after 91.2 seconds
```

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.