

Laporan Akhir Analisis Intelijen Ancaman Menggunakan Honeypot Cowrie

Tanggal Laporan : 25 Agustus 2025
Penerima : Aditya (Mentor)
Penyusun : Rangga – Nanda

1. Ringkasan Eksekutif

Laporan ini merinci hasil dari implementasi sistem **honeypot interaktif Cowrie v2.6.1** pada server Ubuntu 20.04. Tujuannya adalah untuk secara pasif menangkap dan menganalisis aktivitas siber guna mengumpulkan intelijen ancaman. Selama periode observasi, honeypot berhasil merekam beberapa sesi serangan yang berasal dari satu sumber (10.10.11.1).

Sistem ini berhasil mencatat seluruh siklus serangan, mulai dari fase percobaan login (brute-force), infiltrasi (login berhasil) menggunakan kredensial lemah, pengintaian sistem (reconnaissance) pasca-eksploitasi, hingga upaya pengiriman *payload* (pengunduhan file). Analisis log menunjukkan Taktik, Teknik, dan Prosedur (TTP) yang jelas dari penyerang. Proyek ini membuktikan bahwa honeypot Cowrie adalah alat yang sangat efektif untuk memahami perilaku penyerang dan mengidentifikasi potensi kerentanan.

2. Metodologi dan Lingkungan Teknis

- **Perangkat Lunak Honeypot:** Cowrie v2.6.1 pada Python 3.10.12
- **Sistem Operasi Server:** Ubuntu Server 20.04
- **Alamat IP Honeypot:** 10.10.11.131
- **Konfigurasi Jaringan:** Aturan **iptables DNAT** diterapkan untuk meneruskan koneksi dari port standar SSH (TCP/22) ke port layanan Cowrie (TCP/2222), memastikan penangkapan serangan yang realistis sambil mempertahankan alamat IP asli penyerang.
- **Sumber Serangan Teridentifikasi:**
 - ❖ **Alamat IP:** 10.10.11.1
 - ❖ **Klien SSH:** SSH-2.0-OpenSSH_for_Windows_9.5

3. Analisis Hasil dan Perilaku Penyerang

Aktivitas penyerang yang terekam dalam log dapat dianalisis dalam tiga fase utama.

3.1. Fase 1: Percobaan Login (Brute-Force)

Penyerang melakukan beberapa upaya untuk mendapatkan akses dengan menebak kombinasi *username* dan *password*. Honeypot berhasil mencatat semua upaya ini pada (Gambar 1.1).

```
2025-08-24T00:57:10.093184Z [cowrie.ssh.factory.CowrieSSHFactory] New connection: 10.10.11.1:49876 (10.10.11.128:2222) [session: 9a2b3fa82855]
2025-08-24T00:57:10.094884Z [HoneyPotSSHTransport,0,10.10.11.1] Remote SSH version: SSH-2.0-OpenSSH_for_Windows_9.5
2025-08-24T00:57:10.096400Z [HoneyPotSSHTransport,0,10.10.11.1] SSH client hash fingerprint: 701158e75b508e76f0410d5d22ef9df0
2025-08-24T00:57:10.097396Z [cowrie.ssh.transport.HoneyPotSSHTransport#debug] kex alg=b'curve25519-sha256' key alg=b'ssh-ed25519'
2025-08-24T00:57:10.097491Z [cowrie.ssh.transport.HoneyPotSSHTransport#debug] outgoing: b'aes128-ctr' b'hmac-sha2-256' b'none'
2025-08-24T00:57:10.097557Z [cowrie.ssh.transport.HoneyPotSSHTransport#debug] incoming: b'aes128-ctr' b'hmac-sha2-256' b'none'
2025-08-24T00:57:14.685342Z [cowrie.ssh.transport.HoneyPotSSHTransport#debug] NEW KEYS
2025-08-24T00:57:14.687398Z [cowrie.ssh.transport.HoneyPotSSHTransport#debug] starting service b'ssh-userauth'
2025-08-24T00:57:14.692714Z [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'admin' trying auth b'none'
2025-08-24T00:57:16.725928Z [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'admin' trying auth b'password'
2025-08-24T00:57:16.726565Z [HoneyPotSSHTransport,0,10.10.11.1] Could not read etc/userdb.txt, default database activated
2025-08-24T00:57:16.727321Z [HoneyPotSSHTransport,0,10.10.11.1] login attempt [b'admin'/b'admin'] failed
2025-08-24T00:57:17.730295Z [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'admin' failed auth b'password'
2025-08-24T00:57:17.730995Z [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] unauthorized login: ()
2025-08-24T00:57:23.926214Z [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'admin' trying auth b'password'
2025-08-24T00:57:23.926808Z [HoneyPotSSHTransport,0,10.10.11.1] Could not read etc/userdb.txt, default database activated
2025-08-24T00:57:23.927141Z [HoneyPotSSHTransport,0,10.10.11.1] login attempt [b'admin'/b'kali'] failed
2025-08-24T00:57:23.929951Z [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'admin' failed auth b'password'
2025-08-24T00:57:24.930590Z [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] unauthorized login: ()
2025-08-24T00:57:30.295393Z [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'admin' trying auth b'password'
2025-08-24T00:57:30.296045Z [HoneyPotSSHTransport,0,10.10.11.1] Could not read etc/userdb.txt, default database activated
2025-08-24T00:57:30.296385Z [HoneyPotSSHTransport,0,10.10.11.1] login attempt [b'admin'/b'wazuh'] failed
2025-08-24T00:57:31.299094Z [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'admin' failed auth b'password'
2025-08-24T00:57:31.300225Z [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] unauthorized login: ()
2025-08-24T00:57:31.309940Z [cowrie.ssh.transport.HoneyPotSSHTransport#info] connection lost
2025-08-24T00:57:31.310389Z [HoneyPotSSHTransport,0,10.10.11.1] Connection lost after 21.2 seconds
```

Gambar 1.1

```
2025-08-20T18:58:04.546201Z [twisted.scripts._twisted_unix_unixserverfactory] twisted 25.5.0 (/home/cowrie/cowrie/cowrie-em/dln/python 3.10.12) starting up.
2025-08-20T18:58:04.546301Z [twisted.scripts._twisted_unix_unixserverfactory] reactor class: Twisted.internet.epollreactor.FPollReactor.
2025-08-20T18:58:04.551807Z [-] CowrieSSHFactory starting on 2222
2025-08-20T18:58:04.552031Z [cowrie.ssh.factory.CowrieSSHFactory] starting factory <cowrie.ssh.factory.CowrieSSHFactory object at 0x7f4d16d124e0>
2025-08-20T18:58:04.613017Z [-] ready to accept ssh connections
2025-08-20T18:58:37.298064Z [cowrie.ssh.factory.CowrieSSHFactory] new connection: 10.10.11.1:60138 (10.10.11.128:2222) [session: 2b0a3c3e0d5]
2025-08-20T18:58:37.308866Z [cowrie.ssh.transport.HoneyPotSSHTransport#info] connection lost
2025-08-20T18:58:37.309054Z [HoneyPotSSHTransport,0,10.10.11.1] Connection lost after 0.6 seconds
2025-08-20T18:58:37.323411Z [cowrie.ssh.factory.CowrieSSHFactory] new connection: 10.10.11.1:60112 (10.10.11.128:2222) [session: 4453bee422f]
2025-08-20T18:58:37.332382Z [HoneyPotSSHTransport,0,10.10.11.1] Remote SSH version: SSH-2.0-nmap-SSH-client
2025-08-20T18:58:37.335180Z [cowrie.ssh.transport.HoneyPotSSHTransport#info] connection lost
2025-08-20T18:58:37.335272Z [HoneyPotSSHTransport,0,10.10.11.1] Connection lost after 0.6 seconds
2025-08-20T18:58:37.336222Z [HoneyPotSSHTransport,0,10.10.11.1] Remote SSH version: SSH-2.0-nmap-SSH-client
2025-08-20T18:58:37.339312Z [cowrie.ssh.transport.HoneyPotSSHTransport#info] connection lost
2025-08-20T18:58:37.339861Z [HoneyPotSSHTransport,0,10.10.11.1] Connection lost after 0.6 seconds
2025-08-20T18:58:37.340282Z [cowrie.ssh.factory.CowrieSSHFactory] new connection: 10.10.11.1:60130 (10.10.11.128:2222) [session: 790f6ec3c0f]
2025-08-20T18:58:37.354641Z [HoneyPotSSHTransport,0,10.10.11.1] Remote SSH version: SSH-2.0-nmap-SSH-client
2025-08-20T18:58:37.356890Z [HoneyPotSSHTransport,0,10.10.11.1] SSH client hash fingerprint: 0780c678a2297d5d62624f6d2918
2025-08-20T18:58:37.357740Z [cowrie.ssh.transport.HoneyPotSSHTransport#info] Disconnecting with error, code 3
reason: b'Can't match all kex parts'
2025-08-20T18:58:37.358367Z [cowrie.ssh.transport.HoneyPotSSHTransport#info] connection lost
2025-08-20T18:58:37.358367Z [HoneyPotSSHTransport,0,10.10.11.1] Connection lost after 0.6 seconds
2025-08-20T18:58:37.359401Z [cowrie.ssh.factory.CowrieSSHFactory] new connection: 10.10.11.1:60130 (10.10.11.128:2222) [session: 64f333ed07b]
2025-08-20T18:58:37.372362Z [HoneyPotSSHTransport,0,10.10.11.1] Remote SSH version: SSH-2.0-nmap-SSH-client
2025-08-20T18:58:37.380902Z [HoneyPotSSHTransport,0,10.10.11.1] SSH client hash fingerprint: 0780c678a2297d5d62624f6d2918
2025-08-20T18:58:37.381172Z [cowrie.ssh.transport.HoneyPotSSHTransport#debug] kex alg=b'diffie-hellman-group14-sha1' key alg=b'ssh-rsa'
2025-08-20T18:58:37.381444Z [cowrie.ssh.transport.HoneyPotSSHTransport#debug] outgoing: b'aes128-ctr' b'hmac-md5' b'none'
2025-08-20T18:58:37.381648Z [cowrie.ssh.transport.HoneyPotSSHTransport#debug] incoming: b'aes128-ctr' b'hmac-md5' b'none'
2025-08-20T18:58:37.413482Z [cowrie.ssh.transport.HoneyPotSSHTransport#info] connection lost
2025-08-20T18:58:37.413482Z [HoneyPotSSHTransport,0,10.10.11.1] Connection lost after 0.1 seconds
2025-08-20T18:58:37.435174Z [cowrie.ssh.factory.CowrieSSHFactory] new connection: 10.10.11.1:60130 (10.10.11.128:2222) [session: d2793302b7a6]
2025-08-20T18:58:37.437602Z [HoneyPotSSHTransport,0,10.10.11.1] Remote SSH version: SSH-2.0-nmap-SSH-client
2025-08-20T18:58:37.441411Z [HoneyPotSSHTransport,0,10.10.11.1] SSH client hash fingerprint: 0780c678a2297d5d62624f6d2918
2025-08-20T18:58:37.442252Z [cowrie.ssh.transport.HoneyPotSSHTransport#debug] outgoing: b'aes128-ctr' b'hmac-md5' b'none'
2025-08-20T18:58:37.442362Z [cowrie.ssh.transport.HoneyPotSSHTransport#debug] incoming: b'aes128-ctr' b'hmac-md5' b'none'
2025-08-20T18:58:37.451862Z [cowrie.ssh.transport.HoneyPotSSHTransport#info] connection lost
2025-08-20T18:58:37.451862Z [HoneyPotSSHTransport,0,10.10.11.1] Connection lost after 0.1 seconds
2025-08-20T18:58:37.518364Z [HoneyPotSSHTransport,0,10.10.11.1] Connection lost after 0.1 seconds
2025-08-20T18:58:37.518502Z [cowrie.ssh.factory.CowrieSSHFactory] new connection: 10.10.11.1:60043 (10.10.11.128:2222) [session: 7db099c0b0ec]
2025-08-20T18:58:37.517372Z [HoneyPotSSHTransport,0,10.10.11.1] Remote SSH version: SSH-2.0-nmap-SSH-client
2025-08-20T18:58:37.517482Z [HoneyPotSSHTransport,0,10.10.11.1] SSH client hash fingerprint: 0780c678a2297d5d62624f6d2918
2025-08-20T18:58:37.526802Z [cowrie.ssh.transport.HoneyPotSSHTransport#info] Disconnecting with error, code 3
reason: b'Can't match all kex parts'
2025-08-20T18:58:37.521802Z [cowrie.ssh.transport.HoneyPotSSHTransport#info] connection lost
2025-08-20T18:58:37.521802Z [HoneyPotSSHTransport,0,10.10.11.1] Connection lost after 0.6 seconds
2025-08-20T18:58:37.534417Z [cowrie.ssh.factory.CowrieSSHFactory] new connection: 10.10.11.1:60043 (10.10.11.128:2222) [session: b63555d6f1b]
2025-08-20T18:58:37.538472Z [HoneyPotSSHTransport,0,10.10.11.1] Remote SSH version: SSH-2.0-nmap-SSH-client
2025-08-20T18:58:37.540402Z [HoneyPotSSHTransport,0,10.10.11.1] SSH client hash fingerprint: 0780c678a2297d5d62624f6d2918
2025-08-20T18:58:37.541202Z [cowrie.ssh.transport.HoneyPotSSHTransport#info] Disconnecting with error, code 3
reason: b'Can't match all kex parts'
```

Gambar 1.2

Analisis Gambar 1.2: Pola ini menunjukkan penggunaan daftar kata sandi yang umum atau terkait dengan alat keamanan siber, yang mengindikasikan kemungkinan serangan otomatis. Selain itu, adanya aktivitas **Nmap** menegaskan bahwa penyerang melakukan *scanning* untuk mencari celah sebelum mencoba login.

3.2. Fase 2: Infiltrasi Berhasil

Setelah beberapa kali gagal, penyerang berhasil masuk ke sistem dengan menargetkan akun **root** menggunakan kredensial yang sangat lemah.

```

2025-08-24T01:13:33.555845Z [HoneyPotSSHTransport,2,10.10.11.1] login attempt [b'root'/b'12345'] succeeded
2025-08-24T01:13:33.558843Z [HoneyPotSSHTransport,2,10.10.11.1] Initialized emulated server as architecture: linux-x64-lsb
2025-08-24T01:13:33.565155Z [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'root' authenticated with b'password'
2025-08-24T01:13:33.565696Z [cowrie.ssh.transport.HoneyPotSSHTransport#debug] starting service b'ssh-connection'
2025-08-24T01:13:33.570742Z [cowrie.ssh.connection.CowrieSSHConnection#debug] got channel b'session' request
2025-08-24T01:13:33.571288Z [cowrie.ssh.session.HoneyPotSSHSessionInfo] channel open
2025-08-24T01:13:33.571623Z [cowrie.ssh.connection.CowrieSSHConnection#debug] got global b'no-more-sessions@openssh.com' request
2025-08-24T01:13:33.616626Z [twisted.conch.ssh.sessioninfo] Handling pty request: b'xterm-256color' (40, 84, 640, 480)
2025-08-24T01:13:33.637915Z [SSHChannel session (0) on SSHService b'ssh-connection' on HoneyPotSSHTransport,2,10.10.11.1] Terminal Size: 84 40
2025-08-24T01:13:33.639291Z [twisted.conch.ssh.sessioninfo] Getting shell
2025-08-24T01:13:38.308515Z [HoneyPotSSHTransport,2,10.10.11.1] CMD: ls
2025-08-24T01:13:38.309633Z [HoneyPotSSHTransport,2,10.10.11.1] Command found: ls
2025-08-24T01:13:40.997279Z [HoneyPotSSHTransport,2,10.10.11.1] CMD: uname -a
2025-08-24T01:13:40.998116Z [HoneyPotSSHTransport,2,10.10.11.1] Command found: uname -a
2025-08-24T01:13:57.744766Z [HoneyPotSSHTransport,2,10.10.11.1] CMD: lsb_release -a
2025-08-24T01:13:57.749390Z [HoneyPotSSHTransport,2,10.10.11.1] Can't find command lsb_release
2025-08-24T01:13:57.749653Z [HoneyPotSSHTransport,2,10.10.11.1] Command not found: lsb_release -a
2025-08-24T01:14:04.153162Z [HoneyPotSSHTransport,2,10.10.11.1] CMD: lsb_release -a
2025-08-24T01:14:04.159371Z [HoneyPotSSHTransport,2,10.10.11.1] Can't find command lsb_release
2025-08-24T01:14:04.159647Z [HoneyPotSSHTransport,2,10.10.11.1] Command not found: lsb_release -a
2025-08-24T01:14:31.483976Z [HoneyPotSSHTransport,2,10.10.11.1] CMD: lsb_release -a
2025-08-24T01:14:31.485118Z [HoneyPotSSHTransport,2,10.10.11.1] Can't find command lsb_release
2025-08-24T01:14:31.485405Z [HoneyPotSSHTransport,2,10.10.11.1] Command not found: lsb_release -a
2025-08-24T01:17:17.801139Z [HoneyPotSSHTransport,2,10.10.11.1] CMD: wget https://ash-speed.hetzner.com/100MB.bin
2025-08-24T01:17:17.802194Z [HoneyPotSSHTransport,2,10.10.11.1] Command found: wget https://ash-speed.hetzner.com/100MB.bin
2025-08-24T01:17:17.803303Z [HoneyPotSSHTransport,2,10.10.11.1] resolve_cname(ash-speed.hetzner.com)
2025-08-24T01:17:17.804536Z [HoneyPotSSHTransport,2,10.10.11.1] b'/etc/resolv.conf' changed, reparsing
2025-08-24T01:17:17.804904Z [HoneyPotSSHTransport,2,10.10.11.1] Resolver added ('127.0.0.53', 53) to server list
2025-08-24T01:17:17.808113Z [HoneyPotSSHTransport,2,10.10.11.1] DNSDatagramProtocol starting on 31065
2025-08-24T01:17:17.808505Z [HoneyPotSSHTransport,2,10.10.11.1] Starting protocol <twisted.names.dns.DNSDatagramProtocol object at 0x7f9c959886a0>
2025-08-24T01:17:17.854813Z [-] (UDP Port 31065 Closed)
2025-08-24T01:17:17.855302Z [-] Stopping protocol <twisted.names.dns.DNSDatagramProtocol object at 0x7f9c959886a0>
2025-08-24T01:17:17.874322Z [twisted.web.client.HTTP11ClientFactory#info] Starting factory <function HTTPConnectionPool._newConnection.<locals>.quiescentCallback at 0x7f9c950e97e0>, <twisted.internet.endpoints.WrapperEndpoint object at 0x7f9c95988640>)
2025-08-24T01:18:33.566046Z [-] Timeout reached in HoneyPotSSHTransport
2025-08-24T01:18:33.575270Z [HoneyPotSSHTransport,2,10.10.11.1] Closing TTY Log: var/lib/cowrie/tty/8dae68139b7736aeb7337d296f0856142f8335d2f67adc1d55b2f01640d574ba after 299.9 seconds
2025-08-24T01:18:33.583548Z [HoneyPotSSHTransport,2,10.10.11.1] avatar root logging out
2025-08-24T01:18:33.584300Z [cowrie.ssh.transport.HoneyPotSSHTransport#info] connection lost
2025-08-24T01:18:33.584921Z [HoneyPotSSHTransport,2,10.10.11.1] Connection lost after 304.1 seconds

```

Gambar 1.3

Analisis Gambar 1.3: Keberhasilan ini menyoroti risiko keamanan yang signifikan dari penggunaan kata sandi yang lemah pada akun dengan hak akses tinggi.

3.3. Fase 3: Aktivitas Pasca-Eksploitasi

Ini adalah fase paling kritis di mana intelijen mengenai niat penyerang dapat dikumpulkan pada (Gambar 1.4).

A. Pengintaian Sistem (Reconnaissance)

Setelah masuk, penyerang segera menjalankan serangkaian perintah untuk mengidentifikasi lingkungan sistem, seperti **ls**, **uname -a**, serta **lsb_release -a**. Perilaku ini umum dalam fase pengintaian.

B. Pengiriman Payload (Payload Delivery)

Tujuan akhir penyerang terungkap saat ia mencoba mengunduh file biner dari URL <https://ash-speed.hetzner.com/100MB.bin> menggunakan perintah **wget**. Untungnya, honeypot berhasil mencegahnya.

```

2025-08-24T01:17:17.801139Z [HoneyPotSSHTransport,2,10.10.11.1] CMD: wget https://ash-speed.hetzner.com/100MB.bin
2025-08-24T01:17:17.802194Z [HoneyPotSSHTransport,2,10.10.11.1] Command found: wget https://ash-speed.hetzner.com/100MB.bin
2025-08-24T01:17:17.803303Z [HoneyPotSSHTransport,2,10.10.11.1] resolve_cname(ash-speed.hetzner.com)
2025-08-24T01:17:17.804536Z [HoneyPotSSHTransport,2,10.10.11.1] b'/etc/resolv.conf' changed, reparsing
2025-08-24T01:17:17.804904Z [HoneyPotSSHTransport,2,10.10.11.1] Resolver added ('127.0.0.53', 53) to server list
2025-08-24T01:17:17.808113Z [HoneyPotSSHTransport,2,10.10.11.1] DNSDatagramProtocol starting on 31065
2025-08-24T01:17:17.808505Z [HoneyPotSSHTransport,2,10.10.11.1] Starting protocol <twisted.names.dns.DNSDatagramProtocol object at 0x7f9c959886a0>
2025-08-24T01:17:17.854813Z [-] (UDP Port 31065 Closed)
2025-08-24T01:17:17.855302Z [-] Stopping protocol <twisted.names.dns.DNSDatagramProtocol object at 0x7f9c959886a0>
2025-08-24T01:17:17.874322Z [twisted.web.client.HTTP11ClientFactory#info] Starting factory <function HTTPConnectionPool._newConnection.<locals>.quiescentCallback at 0x7f9c950e97e0>, <twisted.internet.endpoints.WrapperEndpoint object at 0x7f9c95988640>)
2025-08-24T01:18:33.566046Z [-] Timeout reached in HoneyPotSSHTransport
2025-08-24T01:18:33.575270Z [HoneyPotSSHTransport,2,10.10.11.1] Closing TTY Log: var/lib/cowrie/tty/8dae68139b7736aeb7337d296f0856142f8335d2f67adc1d55b2f01640d574ba after 299.9 seconds
2025-08-24T01:18:33.583548Z [HoneyPotSSHTransport,2,10.10.11.1] avatar root logging out
2025-08-24T01:18:33.584300Z [cowrie.ssh.transport.HoneyPotSSHTransport#info] connection lost
2025-08-24T01:18:33.584921Z [HoneyPotSSHTransport,2,10.10.11.1] Connection lost after 304.1 seconds

```

Gambar 1.4

4. Temuan Teknis dan Observasi

- **Batas Emulasi Honeypot:** Kegagalan honeypot dalam merespons perintah **lsb_release** menunjukkan bahwa penyerang yang canggih mungkin dapat mendeteksi bahwa mereka berada dalam lingkungan palsu.
- **Potensi Bug Perangkat Lunak:** Pada pukul 01:34:50Z, log mencatat **Unhandled error in Deferred** dengan `KeyError: 'S2'`. Error internal ini mengindikasikan potensi bug dalam Cowrie saat menangani sesi tertentu.

5. Kesimpulan

Proyek implementasi honeypot ini dinilai berhasil. Sistem yang dibangun mampu menarik dan menipu penyerang, merekam intelijen berharga (TTP), dan mengumpulkan artefak serangan (file). Data yang terkumpul memberikan bukti nyata tentang metode yang digunakan oleh penyerang dan menegaskan kembali pentingnya kebijakan kata sandi yang kuat serta pemantauan keamanan proaktif.