Dokumen Proof of Concept (PoC)

Pemantauan Keselamatan (correlatipon tcpdump & journalctl)

1. Objektif

Membuktikan correlation antara pemerhatian tahap rangkaian menggunakan alat penangkap paket (tcpdump) dan log tahap sistem (journalctl) terhadap percubaan log masuk tanpa kebenaran (SSH Brute Force).

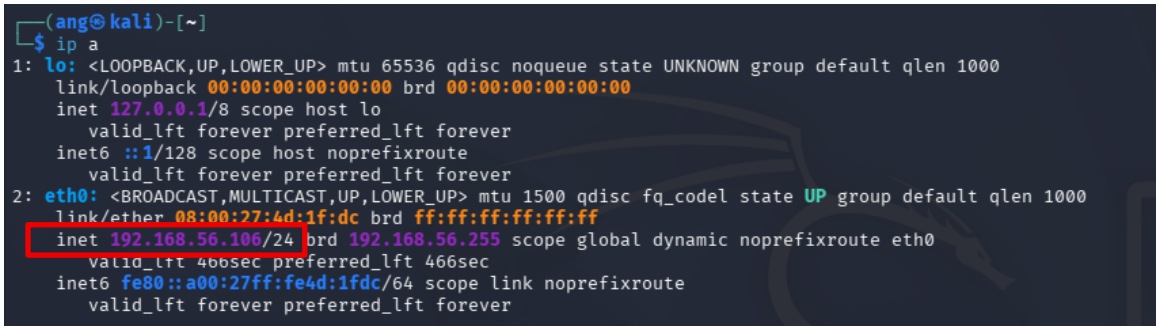
2. Keperluan Persekitaran Makmal

Mesin Sasaran (Server): Kali Linux (Menjalankan perkhidmatan SSH).
Mesin Penguji (Client): Mesin berasaskan Windows atau Linux (Bertindak sebagai pemerhati/penyerang).

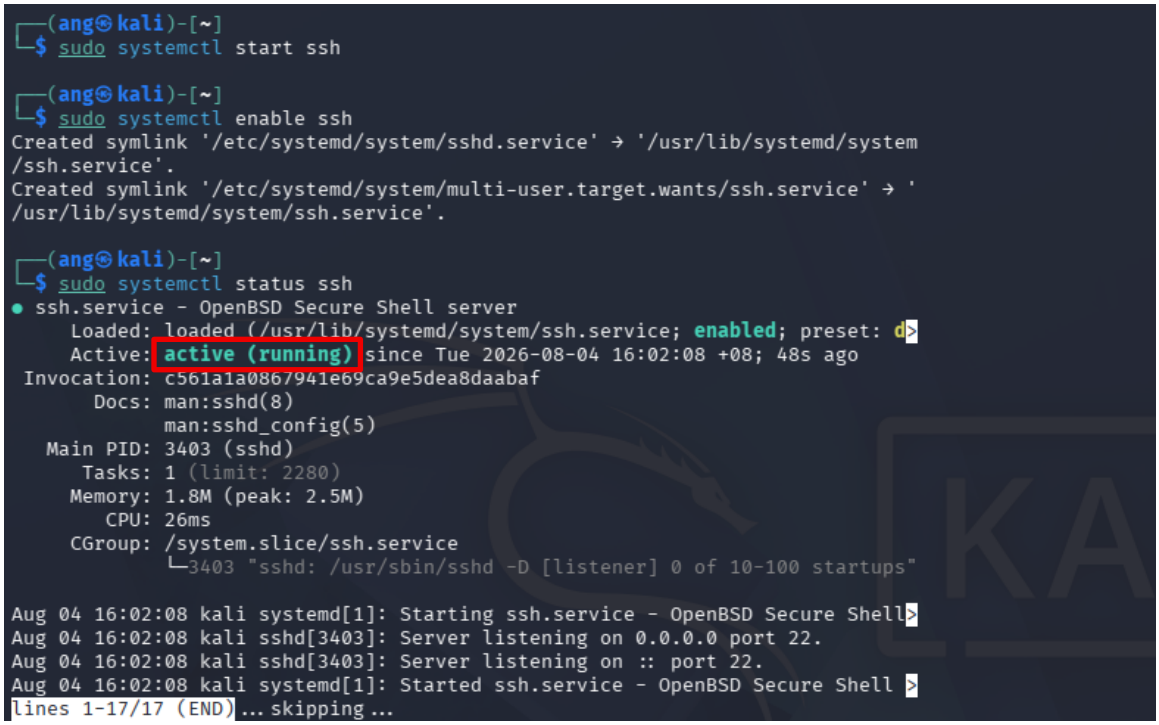
3. Langkah-Langkah Pelaksanaan (Kali Linux)

Fasa 1: Persediaan Mesin Sasaran (Server - Kali Linux)

i. Buka Terminal pada Kali Linux dan dapatkan alamat IP



ii. Aktifkan perkhidmatan SSH

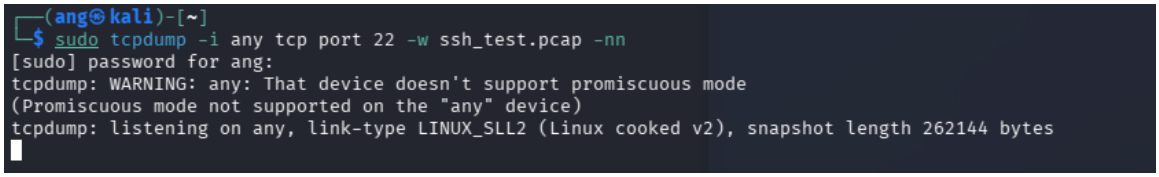


Fasa 2: Pemantauan Data Rangkaian & Log (Server)

Buka dua (2) Terminal baharu pada Kali Linux.

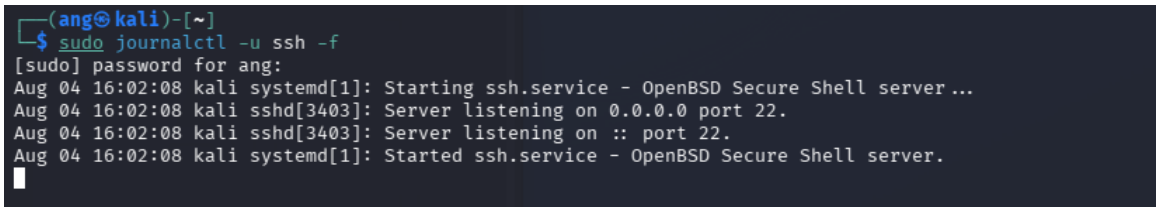
i. Terminal 1 (Tangkapan Rangkaian dengan tcpdump):

sudo tcpdump -i any tcp port 22 -w ssh_test.pcap -nn



ii. Terminal 2 (Pemantauan Log Sistem secara Real-Time dengan journalctl):

sudo journalctl -u ssh -f



Fasa 3: hantar command payload daripada pc pengujian (client) Pemantauan Data Rangkaian & Log (Server)

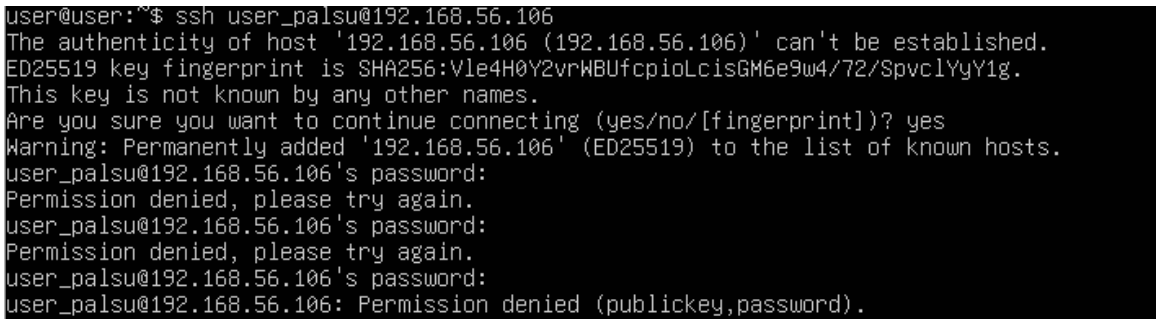
1. **Buka Command Prompt (CMD) atau Terminal pada PC Penguji (Client).**

2. **Lakukan percubaan akses SSH menggunakan akaun palsu ke IP Server (Ganti <IP_Server> dengan IP dari Fasa 1):**

   ssh user_palsu@<IP_Server>

3. ***Masukkan kata laluan yang salah (rawak) beberapa kali sehingga sambungan diputuskan dengan ralat***

   "Permission denied" (publickey, password).



Fasa 3: Hentikan pemantauan & Analisi Data Server

1. **Kembali ke Server (Kali Linux) dan tekan Ctrl + C pada Terminal 1 dan Terminal 2 untuk menghentikan pemantauan**

```
┌──(ang㉿kali)-[~]
└─$ sudo tcpdump -i any tcp port 22 -w ssh_test.pcap -nn
[sudo] password for ang:
tcpdump: WARNING: any: That device doesn't support promiscuous mode
(Promiscuous mode not supported on the "any" device)
tcpdump: listening on any, link-type LINUX_SLL2 (Linux cooked v2), snapshot length 262144 bytes
^C37 packets captured
37 packets received by filter
0 packets dropped by kernel
```

Terminal 1

```
┌──(ang㉿kali)-[~]
└─$ sudo journalctl -u ssh -f
[sudo] password for ang:
Aug 04 16:02:08 kali systemd[1]: Starting ssh.service - OpenBSD Secure Shell server...
Aug 04 16:02:08 kali sshd[3403]: Server listening on 0.0.0.0 port 22.
Aug 04 16:02:08 kali sshd[3403]: Server listening on :: port 22.
Aug 04 16:02:08 kali systemd[1]: Started ssh.service - OpenBSD Secure Shell server.
Aug 04 16:11:30 kali sshd-session[8554]: Invalid user user_palsu from 192.168.56.102 port 41840
Aug 04 16:11:35 kali sshd-session[8554]: pam_unix(sshd:auth): check pass; user unknown
Aug 04 16:11:35 kali sshd-session[8554]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid
=0 tty=ssh ruser= rhost=192.168.56.102
Aug 04 16:11:37 kali sshd-session[8554]: Failed password for invalid user user_palsu from 192.168.56.102
port 41840 ssh2
Aug 04 16:11:41 kali sshd-session[8554]: pam_unix(sshd:auth): check pass; user unknown
Aug 04 16:11:43 kali sshd-session[8554]: Failed password for invalid user user_palsu from 192.168.56.102
port 41840 ssh2
Aug 04 16:11:46 kali sshd-session[8554]: pam_unix(sshd:auth): check pass; user unknown
Aug 04 16:11:48 kali sshd-session[8554]: Failed password for invalid user user_palsu from 192.168.56.102
port 41840 ssh2
Aug 04 16:11:48 kali sshd-session[8554]: Connection closed by invalid user user_palsu 192.168.56.102 port
 41840 [preauth]
Aug 04 16:11:48 kali sshd-session[8554]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ss
h ruser= rhost=192.168.56.102
^C
```

Terminal 2

2. **Analisis Tangkapan Paket Rangkaian (tcpdump):**

tcpdump -r ssh_test.pcap -nn

```
┌──(ang㉿kali)-[~]
└─$ tcpdump -r ssh_test.pcap -nn
reading from file ssh_test.pcap, link-type LINUX_SLL2 (Linux cooked v2), snapshot length 262144
Warning: interface names might be incorrect
16:11:27.520860 eth0  In  IP 192.168.56.102.41840 > 192.168.56.106.22: Flags [S], seq 113989585, win 6424
0, options [mss 1460,sackOK,TS val 3516156838 ecr 0,nop,wscale 7], length 0
16:11:27.520896 eth0  Out IP 192.168.56.106.22 > 192.168.56.102.41840: Flags [S.], seq 2960978509, ack 11
3989586, win 65160, options [mss 1460,sackOK,TS val 3859400107 ecr 3516156838,nop,wscale 8], length 0
16:11:27.521372 eth0  In  IP 192.168.56.102.41840 > 192.168.56.106.22: Flags [.], ack 1, win 502, options
 [nop,nop,TS val 3516156839 ecr 3859400107], length 0
16:11:27.521629 eth0  In  IP 192.168.56.102.41840 > 192.168.56.106.22: Flags [P.], seq 1:44, ack 1, win 5
02, options [nop,nop,TS val 3516156839 ecr 3859400107], length 43: SSH: SSH-2.0-OpenSSH_9.6p1 Ubuntu-3ubu
ntu13.14
16:11:27.521643 eth0  Out IP 192.168.56.106.22 > 192.168.56.102.41840: Flags [.], ack 44, win 255, option
s [nop,nop,TS val 3859400108 ecr 3516156839], length 0
16:11:27.557924 eth0  Out IP 192.168.56.106.22 > 192.168.56.102.41840: Flags [P.], seq 1:34, ack 44, win
255, options [nop,nop,TS val 3859400145 ecr 3516156839], length 33: SSH: SSH-2.0-OpenSSH_10.3p1 Debian-4
16:11:27.558147 eth0  Out IP 192.168.56.106.22 > 192.168.56.102.41840: Flags [P.], seq 34:1074, ack 44, w
in 255, options [nop,nop,TS val 3859400145 ecr 3516156839], length 1040
16:11:27.558541 eth0  In  IP 192.168.56.102.41840 > 192.168.56.106.22: Flags [.], ack 34, win 502, option
s [nop,nop,TS val 3516156876 ecr 3859400145], length 0
16:11:27.558542 eth0  In  IP 192.168.56.102.41840 > 192.168.56.106.22: Flags [.], ack 1074, win 494, opti
ons [nop,nop,TS val 3516156876 ecr 3859400145], length 0
16:11:27.559686 eth0  In  IP 192.168.56.102.41840 > 192.168.56.106.22: Flags [P.], seq 44:1580, ack 1074,
 win 494, options [nop,nop,TS val 3516156877 ecr 3859400145], length 1536
16:11:27.559781 eth0  Out IP 192.168.56.106.22 > 192.168.56.102.41840: Flags [.], ack 1580, win 250, opti
ons [nop,nop,TS val 3859400146 ecr 3516156877], length 0
16:11:27.619652 eth0  In  IP 192.168.56.102.41840 > 192.168.56.106.22: Flags [P.], seq 1580:2788, ack 107
4, win 494, options [nop,nop,TS val 3516156937 ecr 3859400146], length 1208
```

3. **Analisis Log Sistem / End Device (journalctl):**

sudo journalctl -u ssh | grep "Failed password"

```
┌──(ang㉿kali)-[~]
└─$ sudo journalctl -u ssh | grep "Failed password"
Aug 04 16:11:37 kali sshd-session[8554]: Failed password for invalid user user_palsu from 192.168.56.102
port 41840 ssh2
Aug 04 16:11:43 kali sshd-session[8554]: Failed password for invalid user user_palsu from 192.168.56.102
port 41840 ssh2
Aug 04 16:11:48 kali sshd-session[8554]: Failed password for invalid user user_palsu from 192.168.56.102
port 41840 ssh2
```

4. Hasil dan Analisis PoC (Korelasi Data)

Perbandingan data dari kedua-dua pemerhatian akan menunjukkan corak dan bukti correlation seperti jadual di bawah:

Elemen Korelasi	Network Data (tcpdump)	Host Log Data (journalctl)	Analisis SOC
Cap Masa (Timestamp)	Contoh: 10:15:00.123456	Contoh: Oct 24 10:15:01	Kejadian berlaku pada waktu yang selari.
IP Sumber (Source IP)	Contoh: 192.168.56.1	Contoh: 192.168.56.1	Pengesahan identiti sumber ancaman dari IP yang sama.
Port Sumber (Source Port)	Contoh: 54210	Contoh: 54210	Mengesahkan ia adalah sesi komunikasi tunggal (session) yang tepat.
Dapatan Akhir (Outcome)	Sambungan TCP ke port 22 dibina (Flags [S], [P.]).	"Failed password for invalid user user_palsu"	Trafik berjaya melepasi rangkaian, namun ditolak pada tahap aplikasi pelayan kerana kelayakan salah.

5. **Terangkan apakah yang dimaksudkan dengan tcpdump, fungsi tcpdump dan kerja yang dilakukan oleh tcp dump**

tcpdump ialah alat (network packet analyzer) yang digunakan dalam sistem operasi Linux/Unix untuk menangkap (capture), memaparkan dan menganalisis paket data yang melalui antara muka rangkaian (network interface). Ia membantu pentadbir sistem dan penganalisis keselamatan memantau aktiviti rangkaian secara masa nyata.

Fungsi tcpdump

1. Menangkap paket data yang melalui rangkaian.
2. Memantau komunikasi antara hos (host).
3. Menganalisis trafik rangkaian untuk tujuan penyelesaian masalah (troubleshooting).
4. Mengesan aktiviti yang mencurigakan seperti serangan Brute Force, port scanning dan DDoS.
5. Menyimpan paket ke dalam fail .pcap untuk analisis lanjut menggunakan Wireshark atau tcpdump.

Kerja yang dilakukan oleh tcpdump

- Mendengar trafik pada network interface.
- Menapis paket mengikut protokol, IP atau nombor port.
- Merekod maklumat penting seperti:
    - Timestamp
    - Source IP
    - Destination IP
    - Source Port
    - Destination Port
    - TCP Flags
- Menyimpan hasil tangkapan ke dalam fail untuk analisis forensik.

6. Penerangan Terperinci Arahan (*Commands*)

i. sudo tcpdump -i any tcp port 22 -w ssh_test.pcap -nn

Komponen	Fungsi
sudo	Menjalankan arahan sebagai pentadbir (root).
tcpdump	Program untuk menangkap paket rangkaian.
-i any	Memantau semua network interface.
tcp	Menapis hanya paket TCP.
port 22	Menapis trafik yang menggunakan port SSH (22).
-w ssh_test.pcap	Menyimpan semua paket ke fail ssh_test.pcap.
-nn	Tidak menukar IP kepada hostname dan port kepada nama servis.

ii. sudo journalctl -u ssh -f

Komponen	Fungsi
sudo	Jalankan sebagai root.
journalctl	Melihat log sistem Linux.
-u ssh	Paparkan log servis SSH sahaja.
-f	Ikut log secara masa nyata (real-time).

iii. tcpdump -r ssh_test.pcap -nn

Komponen	Fungsi
tcpdump	Membaca fail packet capture.
-r	Read fail .pcap.
ssh_test.pcap	Fail yang telah dirakam.
-nn	Paparkan nombor IP dan port sebenar tanpa penukaran nama.

iv. sudo journalctl -u ssh | grep "Failed password"

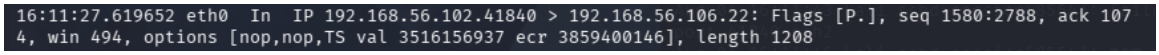
Komponen	Fungsi
journalctl	Paparkan log sistem.
-u ssh	Log servis SSH sahaja.
grep	Menapis output.
"Failed password"	Paparkan hanya percubaan login yang gagal.

7. Penjelasan Baris Hasil sudo journalctl -u ssh -f



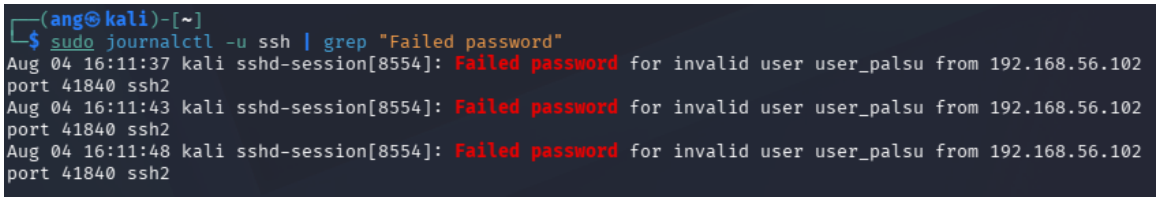
Bahagian Output	Penerangan
Aug 04 16:11:48	Tarikh dan masa kejadian berlaku, iaitu pada **4 Ogos** jam **4:11:48 petang**.
kali	Nama hos (hostname) bagi mesin pelayan yang menjalankan perkhidmatan SSH.
sshd-session[8554]	Proses sesi SSH yang mengendalikan percubaan log masuk. Nombor **8554** ialah Process ID (PID) bagi proses tersebut.
Failed password	Menunjukkan percubaan log masuk gagal kerana pengesahan kata laluan tidak berjaya.
invalid user	Nama pengguna yang dimasukkan tidak wujud dalam sistem pelayan.
user_palsu	Nama akaun yang digunakan semasa percubaan log masuk.
from 192.168.56.102	Alamat IP komputer (client) yang membuat percubaan log masuk ke pelayan.
port 41840	Nombor port sumber (source port) yang digunakan oleh komputer client untuk sambungan SSH.
ssh2	Menunjukkan sambungan menggunakan protokol **SSH versi 2**.

8. Penjelasan Baris Hasil tcpdump -r ssh_test.pcap -nn



Bahagian Output	Penerangan
16:11:27.619652	Masa paket diterima oleh pelayan dengan ketepatan sehingga mikro saat.
eth0	Nama network interface yang menerima paket.
In	Menunjukkan paket masuk ke dalam pelayan.
IP	Paket menggunakan protokol Internet Protocol (IPv4).
192.168.56.102	Alamat IP sumber, iaitu komputer client atau penyerang.
41840	Source Port yang digunakan oleh client untuk sambungan SSH.
192.168.56.106	Alamat IP destinasi, iaitu pelayan SSH.
22	Port destinasi bagi perkhidmatan SSH.
Flags [P.]	TCP Push dan Acknowledgement. Ini menunjukkan data sedang dihantar dalam sambungan yang telah berjaya diwujudkan.
seq 1580:2788	Julat nombor urutan (sequence number) bagi data yang dihantar.
ack 1074	Nombor pengakuan (acknowledgement number) untuk paket yang diterima sebelum ini.
win 494	Saiz TCP Window, iaitu jumlah data yang boleh diterima tanpa pengesahan tambahan.
options [nop, nop, TS val 3516156937 ecr 3859400146]	Maklumat tambahan TCP seperti timestamp untuk meningkatkan ketepatan dan prestasi komunikasi.
length 1208	Saiz data yang dihantar ialah 1208 bait (bytes).

9. Huraikan Kesemua Hasil Dapatan sudo journalctl -u ssh | grep "Failed password"



Perkara	Maksud
Jumlah Percubaan	**3 kali**
Masa	**16:11:37, 16:11:43, 16:11:48** (setiap ~5–6 saat)
User Sasaran	**user_palsu** *(TIDAK wujud dalam sistem)*
IP Sumber	**192.168.56.102** *(SAMA untuk semua percubaan)*
Port Sumber	**41840** *(SAMA untuk semua percubaan)*
PID	**8554** *(SAMA untuk semua percubaan)*
Status	**Kesemua 3 percubaan GAGAL**

Hasil Dapatan

- Serangan SSH Brute Force berjaya dikesan.
- Sumber serangan dikenal pasti daripada IP 192.168.56.102.
- Pengguna yang digunakan ialah user_palsu, iaitu pengguna yang tidak wujud dalam sistem.
- Kesemua 3 percubaan log masuk gagal kerana pengesahan (authentication) tidak berjaya.
- Tiada kompromi sistem berlaku kerana pelayan berjaya menolak semua percubaan log masuk.
- Data rangkaian (tcpdump) dan log sistem (journalctl) adalah sepadan, iaitu menggunakan IP sumber 192.168.56.102 dan Source Port 41840, sekali gus membuktikan korelasi antara trafik rangkaian dan log sistem.

Kesimpulan

Melalui PoC ini, telah dibuktikan bahawa pemerhatian berpusat menggunakan log berbilang dimensi amat penting di dalam sesebuah Pusat Operasi Keselamatan (SOC).

Data Rangkaian (tcpdump) membantu penganalisis mengenal pasti asal-usul ancaman dan pergerakannya melalui infrastruktur rangkaian. Manakala, **Data Log Sistem (journalctl)** membekalkan konteks terperinci pada peringkat titik akhir (endpoint) untuk mengesahkan sama ada serangan tersebut berjaya atau gagal. Correlation(gabungan) kedua-dua pemerhatian ini mengesahkan bahawa percubaan pencerobohan berjaya dihalang dan tiada kompromi sistem berlaku.