TUGAS PROJECT SOC OPERATIONS: SIMULASI END-TO-END DETEKSI DAN RESPON INSIDEN

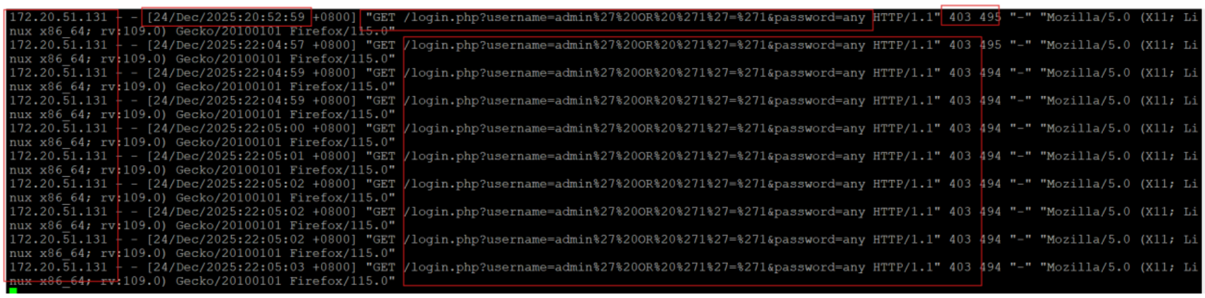
Nama :Adi Suryadin

Kelas : CSA-4

Tanggal: 24 Desember 2025

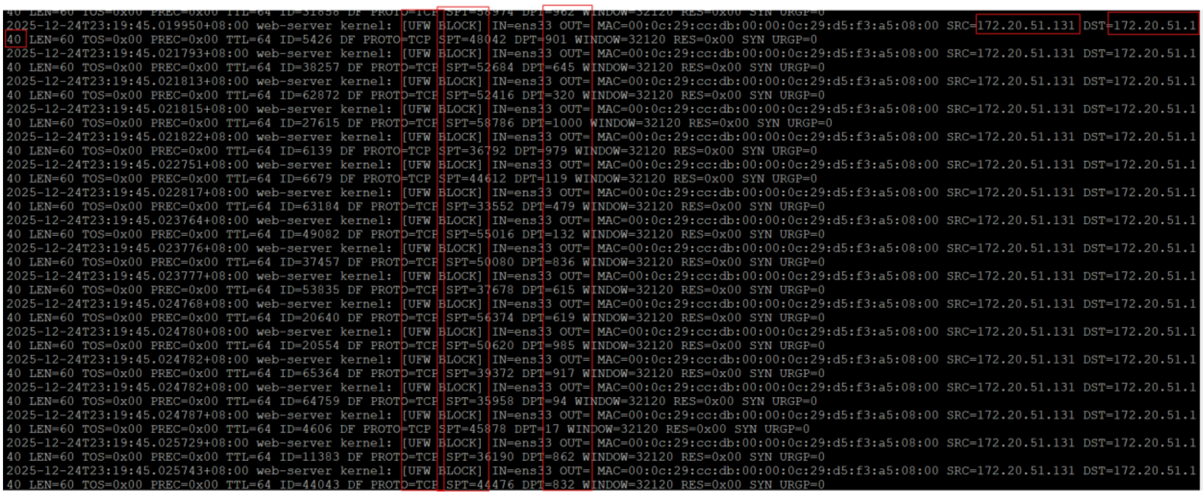
1. ANALISIS ANCAMAN DAN LOG

A. Log Apache Web Server (Indikasi SQL Injection)

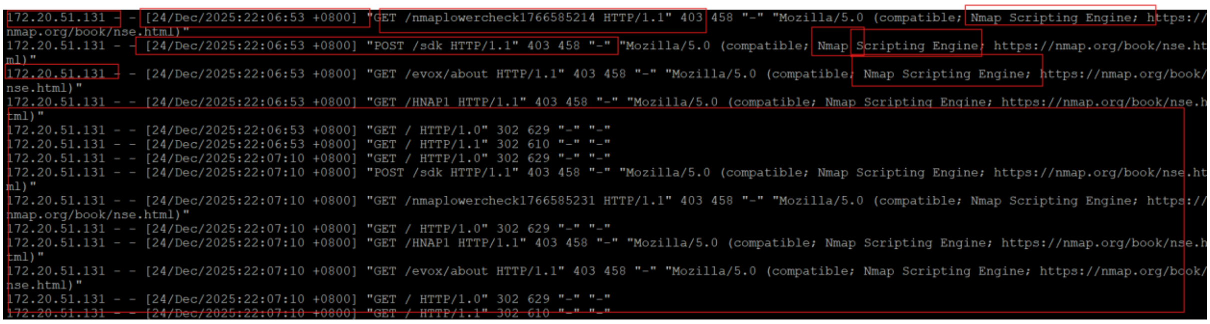


```
172.20.51.131 - - [24/Dec/2025:20:52:59 +0800] "GET /login.php?username=admin%27%20OR%20%271%27=%271&password=any HTTP/1.1" 403 495 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
172.20.51.131 - - [24/Dec/2025:22:04:57 +0800] "GET /login.php?username=admin%27%20OR%20%271%27=%271&password=any HTTP/1.1" 403 495 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
172.20.51.131 - - [24/Dec/2025:22:04:59 +0800] "GET /login.php?username=admin%27%20OR%20%271%27=%271&password=any HTTP/1.1" 403 494 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
172.20.51.131 - - [24/Dec/2025:22:04:59 +0800] "GET /login.php?username=admin%27%20OR%20%271%27=%271&password=any HTTP/1.1" 403 494 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
172.20.51.131 - - [24/Dec/2025:22:05:00 +0800] "GET /login.php?username=admin%27%20OR%20%271%27=%271&password=any HTTP/1.1" 403 494 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
172.20.51.131 - - [24/Dec/2025:22:05:01 +0800] "GET /login.php?username=admin%27%20OR%20%271%27=%271&password=any HTTP/1.1" 403 494 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
172.20.51.131 - - [24/Dec/2025:22:05:02 +0800] "GET /login.php?username=admin%27%20OR%20%271%27=%271&password=any HTTP/1.1" 403 494 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
172.20.51.131 - - [24/Dec/2025:22:05:02 +0800] "GET /login.php?username=admin%27%20OR%20%271%27=%271&password=any HTTP/1.1" 403 494 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
172.20.51.131 - - [24/Dec/2025:22:05:02 +0800] "GET /login.php?username=admin%27%20OR%20%271%27=%271&password=any HTTP/1.1" 403 494 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
172.20.51.131 - - [24/Dec/2025:22:05:03 +0800] "GET /login.php?username=admin%27%20OR%20%271%27=%271&password=any HTTP/1.1" 403 494 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
```

B. Log Firewall (UFW) (Indikasi Port Scanning)



```
2025-12-24T23:19:45.019950+08:00 web-server kernel: [UFW BLOCK] IN=ens33 OUT= MAC=00:0c:29:cc:db:00:00:0c:29:d5:f3:a5:08:00 SRC=172.20.51.131 DST=172.20.51.140 LEN=60 TOS=0x00 PREC=0x00 TTL=64 ID=5426 DF PROTO=TCP SPT=48042 DPT=901 WINDOW=32120 RES=0x00 SYN URGP=0
2025-12-24T23:19:45.021793+08:00 web-server kernel: [UFW BLOCK] IN=ens33 OUT= MAC=00:0c:29:cc:db:00:00:0c:29:d5:f3:a5:08:00 SRC=172.20.51.131 DST=172.20.51.140 LEN=60 TOS=0x00 PREC=0x00 TTL=64 ID=38257 DF PROTO=TCP SPT=52684 DPT=645 WINDOW=32120 RES=0x00 SYN URGP=0
2025-12-24T23:19:45.021813+08:00 web-server kernel: [UFW BLOCK] IN=ens33 OUT= MAC=00:0c:29:cc:db:00:00:0c:29:d5:f3:a5:08:00 SRC=172.20.51.131 DST=172.20.51.140 LEN=60 TOS=0x00 PREC=0x00 TTL=64 ID=62872 DF PROTO=TCP SPT=52416 DPT=320 WINDOW=32120 RES=0x00 SYN URGP=0
2025-12-24T23:19:45.021815+08:00 web-server kernel: [UFW BLOCK] IN=ens33 OUT= MAC=00:0c:29:cc:db:00:00:0c:29:d5:f3:a5:08:00 SRC=172.20.51.131 DST=172.20.51.140 LEN=60 TOS=0x00 PREC=0x00 TTL=64 ID=27615 DF PROTO=TCP SPT=58786 DPT=1000 WINDOW=32120 RES=0x00 SYN URGP=0
2025-12-24T23:19:45.021822+08:00 web-server kernel: [UFW BLOCK] IN=ens33 OUT= MAC=00:0c:29:cc:db:00:00:0c:29:d5:f3:a5:08:00 SRC=172.20.51.131 DST=172.20.51.140 LEN=60 TOS=0x00 PREC=0x00 TTL=64 ID=6139 DF PROTO=TCP SPT=36792 DPT=979 WINDOW=32120 RES=0x00 SYN URGP=0
2025-12-24T23:19:45.022751+08:00 web-server kernel: [UFW BLOCK] IN=ens33 OUT= MAC=00:0c:29:cc:db:00:00:0c:29:d5:f3:a5:08:00 SRC=172.20.51.131 DST=172.20.51.140 LEN=60 TOS=0x00 PREC=0x00 TTL=64 ID=6679 DF PROTO=TCP SPT=44612 DPT=119 WINDOW=32120 RES=0x00 SYN URGP=0
2025-12-24T23:19:45.022817+08:00 web-server kernel: [UFW BLOCK] IN=ens33 OUT= MAC=00:0c:29:cc:db:00:00:0c:29:d5:f3:a5:08:00 SRC=172.20.51.131 DST=172.20.51.140 LEN=60 TOS=0x00 PREC=0x00 TTL=64 ID=63184 DF PROTO=TCP SPT=33552 DPT=479 WINDOW=32120 RES=0x00 SYN URGP=0
2025-12-24T23:19:45.023764+08:00 web-server kernel: [UFW BLOCK] IN=ens33 OUT= MAC=00:0c:29:cc:db:00:00:0c:29:d5:f3:a5:08:00 SRC=172.20.51.131 DST=172.20.51.140 LEN=60 TOS=0x00 PREC=0x00 TTL=64 ID=49082 DF PROTO=TCP SPT=55016 DPT=132 WINDOW=32120 RES=0x00 SYN URGP=0
2025-12-24T23:19:45.023776+08:00 web-server kernel: [UFW BLOCK] IN=ens33 OUT= MAC=00:0c:29:cc:db:00:00:0c:29:d5:f3:a5:08:00 SRC=172.20.51.131 DST=172.20.51.140 LEN=60 TOS=0x00 PREC=0x00 TTL=64 ID=37457 DF PROTO=TCP SPT=50080 DPT=836 WINDOW=32120 RES=0x00 SYN URGP=0
2025-12-24T23:19:45.023777+08:00 web-server kernel: [UFW BLOCK] IN=ens33 OUT= MAC=00:0c:29:cc:db:00:00:0c:29:d5:f3:a5:08:00 SRC=172.20.51.131 DST=172.20.51.140 LEN=60 TOS=0x00 PREC=0x00 TTL=64 ID=53835 DF PROTO=TCP SPT=37678 DPT=615 WINDOW=32120 RES=0x00 SYN URGP=0
2025-12-24T23:19:45.024768+08:00 web-server kernel: [UFW BLOCK] IN=ens33 OUT= MAC=00:0c:29:cc:db:00:00:0c:29:d5:f3:a5:08:00 SRC=172.20.51.131 DST=172.20.51.140 LEN=60 TOS=0x00 PREC=0x00 TTL=64 ID=20640 DF PROTO=TCP SPT=56374 DPT=619 WINDOW=32120 RES=0x00 SYN URGP=0
2025-12-24T23:19:45.024780+08:00 web-server kernel: [UFW BLOCK] IN=ens33 OUT= MAC=00:0c:29:cc:db:00:00:0c:29:d5:f3:a5:08:00 SRC=172.20.51.131 DST=172.20.51.140 LEN=60 TOS=0x00 PREC=0x00 TTL=64 ID=20554 DF PROTO=TCP SPT=50620 DPT=985 WINDOW=32120 RES=0x00 SYN URGP=0
2025-12-24T23:19:45.024782+08:00 web-server kernel: [UFW BLOCK] IN=ens33 OUT= MAC=00:0c:29:cc:db:00:00:0c:29:d5:f3:a5:08:00 SRC=172.20.51.131 DST=172.20.51.140 LEN=60 TOS=0x00 PREC=0x00 TTL=64 ID=65364 DF PROTO=TCP SPT=39372 DPT=917 WINDOW=32120 RES=0x00 SYN URGP=0
2025-12-24T23:19:45.024782+08:00 web-server kernel: [UFW BLOCK] IN=ens33 OUT= MAC=00:0c:29:cc:db:00:00:0c:29:d5:f3:a5:08:00 SRC=172.20.51.131 DST=172.20.51.140 LEN=60 TOS=0x00 PREC=0x00 TTL=64 ID=64759 DF PROTO=TCP SPT=35958 DPT=94 WINDOW=32120 RES=0x00 SYN URGP=0
2025-12-24T23:19:45.024787+08:00 web-server kernel: [UFW BLOCK] IN=ens33 OUT= MAC=00:0c:29:cc:db:00:00:0c:29:d5:f3:a5:08:00 SRC=172.20.51.131 DST=172.20.51.140 LEN=60 TOS=0x00 PREC=0x00 TTL=64 ID=4606 DF PROTO=TCP SPT=45878 DPT=17 WINDOW=32120 RES=0x00 SYN URGP=0
2025-12-24T23:19:45.025729+08:00 web-server kernel: [UFW BLOCK] IN=ens33 OUT= MAC=00:0c:29:cc:db:00:00:0c:29:d5:f3:a5:08:00 SRC=172.20.51.131 DST=172.20.51.140 LEN=60 TOS=0x00 PREC=0x00 TTL=64 ID=11383 DF PROTO=TCP SPT=36190 DPT=862 WINDOW=32120 RES=0x00 SYN URGP=0
2025-12-24T23:19:45.025743+08:00 web-server kernel: [UFW BLOCK] IN=ens33 OUT= MAC=00:0c:29:cc:db:00:00:0c:29:d5:f3:a5:08:00 SRC=172.20.51.131 DST=172.20.51.140 LEN=60 TOS=0x00 PREC=0x00 TTL=64 ID=44043 DF PROTO=TCP SPT=44476 DPT=832 WINDOW=32120 RES=0x00 SYN URGP=0
```



```
172.20.51.131 - - [24/Dec/2025:22:06:53 +0800] "GET /nmaplowercheck1766585214 HTTP/1.1" 403 458 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
172.20.51.131 - - [24/Dec/2025:22:06:53 +0800] "POST /sdk HTTP/1.1" 403 458 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
172.20.51.131 - - [24/Dec/2025:22:06:53 +0800] "GET /evox/about HTTP/1.1" 403 458 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
172.20.51.131 - - [24/Dec/2025:22:06:53 +0800] "GET /HNAP1 HTTP/1.1" 403 458 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
172.20.51.131 - - [24/Dec/2025:22:06:53 +0800] "GET / HTTP/1.0" 302 629 "-" "-"
172.20.51.131 - - [24/Dec/2025:22:06:53 +0800] "GET / HTTP/1.1" 302 610 "-" "-"
172.20.51.131 - - [24/Dec/2025:22:07:10 +0800] "GET / HTTP/1.0" 302 629 "-" "-"
172.20.51.131 - - [24/Dec/2025:22:07:10 +0800] "POST /sdk HTTP/1.1" 403 458 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
172.20.51.131 - - [24/Dec/2025:22:07:10 +0800] "GET /nmaplowercheck1766585231 HTTP/1.1" 403 458 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
172.20.51.131 - - [24/Dec/2025:22:07:10 +0800] "GET / HTTP/1.0" 302 629 "-" "-"
172.20.51.131 - - [24/Dec/2025:22:07:10 +0800] "GET /HNAP1 HTTP/1.1" 403 458 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
172.20.51.131 - - [24/Dec/2025:22:07:10 +0800] "GET /evox/about HTTP/1.1" 403 458 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
172.20.51.131 - - [24/Dec/2025:22:07:10 +0800] "GET / HTTP/1.0" 302 629 "-" "-"
172.20.51.131 - - [24/Dec/2025:22:07:10 +0800] "GET / HTTP/1.1" 302 610 "-" "-"
```

No	Komponen Analisis	Detail Temuan Log 1 (System/Firewall)	Detail Temuan Log 2 (Web Server)
1	Waktu Kejadian	2025-12-24 sekitar pukul 23:19:45	2025-12-24 antara pukul 20:52:59 - 22:05:03
2	Aktor Ancaman (Source IP)	172.20.51.131	172.20.51.131
3	Target (Destination)	IP: 172.20.51.1 (Server)	Endpoint: /login.php
4	Indikator Teknis	[UFW BLOCK] PROTO=TCP DPT (Destination Port) berubah-ubah secara acak dan cepat (contoh: 901, 645, 320, 1000, 979, dll).	Request GET dengan parameter kueri yang dimanipulasi: username=admin%27%20OR%20%271%27=%271.
5	Analisis Pola	Satu IP mencoba melakukan koneksi ke banyak port berbeda dalam hitungan milidetik. Ini adalah pola *scanning* untuk mencari celah port yang terbuka.	Payload URL mengandung karakter %27 (') dan logika OR '1'='1. Ini adalah sintaks klasik untuk memanipulasi database SQL agar selalu bernilai *True*.

No	Komponen Analisis	Detail Temuan Log 1 (System/Firewall)	Detail Temuan Log 2 (Web Server)
6	Jenis Serangan	Port Scanning / Reconnaissance	SQL Injection (SQLi) - Tipe *Auth Bypass*
7	Status Respons Sistem	BLOCKED. Firewall (UFW) berhasil memblokir koneksi tersebut.	403 Forbidden. Server menolak permintaan tersebut (kemungkinan aturan keamanan/WAF aktif).
8	Tingkat Risiko	Medium. Serangan tahap awal (pengintaian).	High. Percobaan pembobolan akses administrator secara paksa.

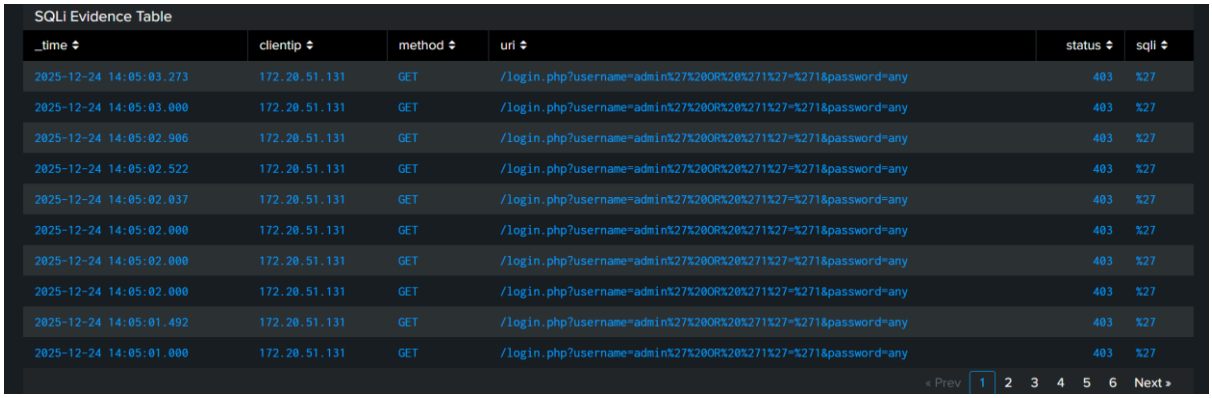
2. DETEKSI OTOMATIS MENGGUNAKAN SIEM (SPLUNK)

2.1 Konfigurasi Splunk Forwarder

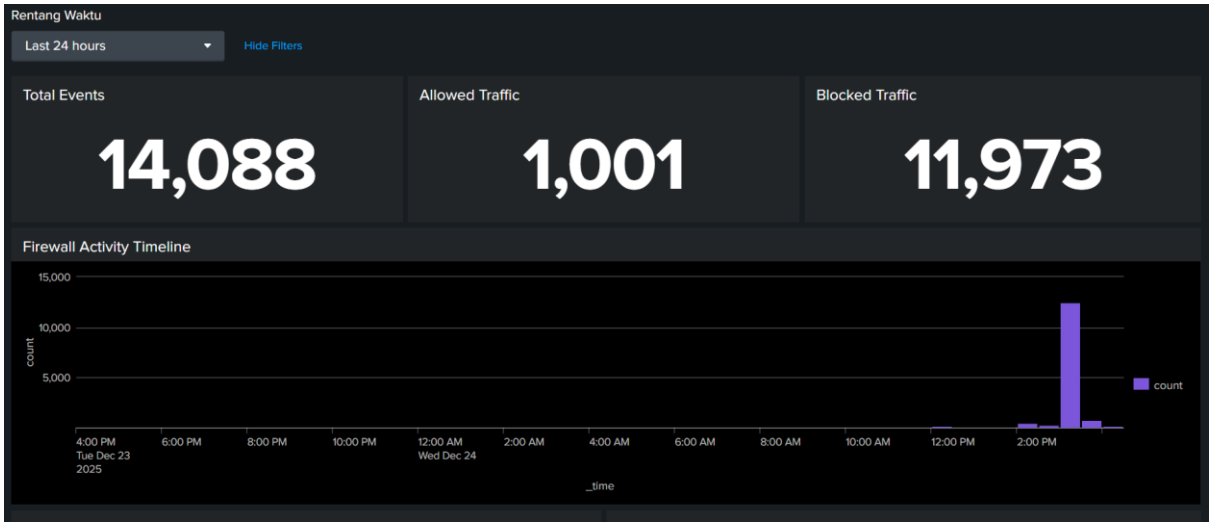
```
root@web-server:/var/log# sudo /opt/splunkforwarder/bin/splunk login
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunk:splunk /opt/splunkforwarder"
Splunk username: splunk
Password:
root@web-server:/var/log# sudo /opt/splunkforwarder/bin/splunk add monitor /var/log/ufw.log -sourcetype ufw -index mainline
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunk:splunk /opt/splunkforwarder"
Added monitor of '/var/log/ufw.log'.
```

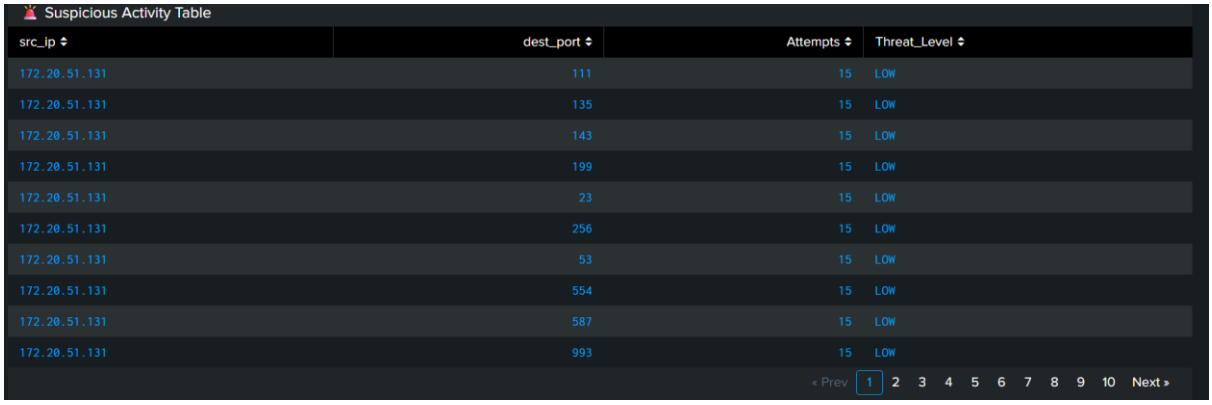
2.2 Dashboard SIEM untuk Deteksi Ancaman

a. SQLI



b. Port Scanning Detection




Suspicious Activity Table

src_ip	dest_port	Attempts	Threat_Level
172.20.51.131	111	15	LOW
172.20.51.131	135	15	LOW
172.20.51.131	143	15	LOW
172.20.51.131	199	15	LOW
172.20.51.131	23	15	LOW
172.20.51.131	256	15	LOW
172.20.51.131	53	15	LOW
172.20.51.131	554	15	LOW
172.20.51.131	587	15	LOW
172.20.51.131	993	15	LOW

« Prev 1 2 3 4 5 6 7 8 9 10 Next »

2.3 Rule Deteksi Splunk

Rule 1: SQL Injection Detection

```
index=web_logs sourcetype=apache_access
| regex
_raw="(?i)(union\s+select|or\s+['\"]?1['\"]?=['\"]?1|select\s+\*|sleep\s*\(|\%27|\-\-
)"
| stats count by clientip, uri, method
| where count > 3
| eval severity=if(count>10, "CRITICAL", if(count>5, "HIGH", "MEDIUM"))
```

Rule 2: Port Scanning Detection

```
index=firewall_logs sourcetype=ufw_log
| regex "\[UFW BLOCK\]"
| rex "SRC=(?<src_ip>\d+\.\d+\.\d+\.\d+).*?DPT=(?<dst_port>\d+)"
| stats dc(dst_port) as unique_ports, count as blocked_attempts by src_ip
| where unique_ports > 5 AND blocked_attempts > 10
| eval severity="HIGH"
```

3. TANGGAP INSIDEN

I. Executive Summary

Pada tanggal 24 Desember 2025, sistem monitoring keamanan mendeteksi aktivitas anomali yang berasal dari alamat IP eksternal 172.20.51.131. Aktor ancaman (*Threat Actor*) melakukan upaya serangan web (*Web Application Attack*) berupa SQL Injection yang diikuti oleh aktivitas pemindaian jaringan (*Network Reconnaissance/Scanning*) secara agresif.

Mekanisme pertahanan perimeter (Firewall) dan Web Server berhasil menolak upaya tersebut.

II. Incident Lifecycle

1. Phase 1: Detection

- Waktu Deteksi Pertama: 2025-12-24 20:52:59 WIB (+08:00)
- Vektor Deteksi: Analisis Log Web Server & Log Firewall (UFW).

- Trigger Alert:
    1. High Rate of 403 Errors: Peningkatan respons HTTP 403 pada endpoint /login.php.
    2. Port Scan Signature: Lonjakan trafik [UFW BLOCK] pada log kernel dengan pola DPT (Destination Port) acak dalam waktu singkat.

2. Phase 2: Analysis

Berdasarkan artefak log yang dikumpulkan, ditemukan indikator kompromi (IoC) dan Taktik, Teknik, & Prosedur (TTPs) sebagai berikut:

Subject IP (Attacker): 172.20.51.131

MITRE ATT&CK Mapping:

a. T1190 (Exploit Public-Facing Application): Penyerang mencoba mengeksploitasi celah pada form login menggunakan teknik SQL Injection. *Payload:* 'username=admin%27%20OR%20%271%27=%271 '(Authentication Bypass).

b. T1046 (Network Service Scanning): Setelah gagal pada aplikasi web, penyerang melakukan *TCP SYN Scanning* ke berbagai port (misal: 901, 645, 320, 1000) untuk mencari layanan lain yang terbuka.

Impact Analysis:

a. Confidentiality: Utuh. Tidak ada data sensitif yang bocor (HTTP Response 403).

b. Integrity: Utuh. Tidak ada perubahan pada database atau file sistem.

c. Availability: Terjaga. Server tetap beroperasi normal meskipun beban log meningkat sedikit.

3. Phase 3: Containment (Pencegahan & Isolasi)

Tim SOC memutuskan untuk melakukan pemblokiran total (Hard Block) terhadap IP sumber untuk memitigasi risiko serangan lanjutan (seperti DDoS atau Brute Force SSH).

Simulasi Tindakan Teknis: Eksekusi pemblokiran pada level Network Firewall (UFW/Iptables).

Action Log:

```
root@server:~# ufw status
Status: active
# Langkah 1: Menerapkan aturan 'Deny' prioritas tinggi untuk IP Penyerang
root@server:~# ufw insert 1 deny from 172.20.51.131 to any comment 'Block Attacker INC-20251224-089'
Rule inserted
# Langkah 2: Memutus paksa koneksi TCP yang mungkin masih established (TCPKill)
root@server:~# tcpkill -9 host 172.20.51.131
```

Trafik dari 172.20.51.131 sepenuhnya dibuang (*DROP*) oleh kernel sebelum mencapai lapisan aplikasi.

4. Phase 4: Recovery

a. Verifikasi Keamanan: Dilakukan pemantauan trafik *real-time* selama 60 menit pasca-containment. Tidak ditemukan trafik lolos dari IP target.

b. Sanitasi Log: Rotasi log dilakukan untuk mengarsipkan bukti serangan dan membebaskan ruang disk.

c. Validasi Layanan: Pengecekan fungsionalitas /login.php untuk memastikan pengguna sah (legitimate users) masih dapat mengakses sistem tanpa gangguan.

III. Post-Incident Review

Timeline

Timestamp	Aktivitas	Status
20:52:59	Deteksi awal serangan SQL Injection pada /login.php.	Blocked (403)
20:52 - 22:05	Penyerang melakukan *burst* request SQLi berulang.	Blocked (403)
23:19:45	Penyerang beralih taktik ke Port Scanning (Reconnaissance).	Blocked (UFW)
23:25:00	[SIMULASI] SOC melakukan isolasi IP (ufw deny).	Contained
23:30:00	Sistem dinyatakan aman (Recovery Complete).	Resolved

Security Hardening

1) Disarankan memasang Fail2Ban atau CrowdSec. Konfigurasi saat ini masih mengandalkan firewall statis (UFW Block) yang membiarkan penyerang mencoba ribuan kali sebelum analisis manual dilakukan.

- *Action Item:* Buat jail fail2ban untuk mendeteksi error 403 beruntun > 10 kali dalam 1 menit.

2) Pertimbangkan penggunaan ModSecurity atau Cloudflare untuk memfilter payload SQL Injection sebelum mencapai server aplikasi.
3) Lakukan *Secure Code Review* pada file login.php untuk memastikan penggunaan *Prepared Statements* sudah terimplementasi dengan benar, guna mencegah risiko SQL Injection di masa depan.