🛡 SOC ANALYST LAB REPORT

Network Traffic Analysis & Threat Hunting Investigation

MD TAMEEM | SOC Analyst Project | 22 February 2026

---

1. Executive Summary

This report documents a complete SOC Analyst investigation performed in a simulated lab environment. The objective was to replicate real-world Tier-1 SOC responsibilities including network traffic capture and analysis, authentication log investigation, SIEM query development, and threat intelligence validation.

The investigation identified multiple failed logon attempts (Event ID 4625) followed by a successful logon (Event ID 4624) with elevated privileges (Event ID 4672), consistent with a brute force attack pattern. Network-level reconnaissance via SYN scanning was also captured and analyzed in Wireshark.

2. Tools & Technologies

The following tools were employed across all investigation scenarios:

- Wireshark — Packet capture and network traffic analysis
- Nmap — Network reconnaissance / port scanning simulation
- Splunk Enterprise — SIEM log ingestion, querying and correlation
- Windows Event Viewer — Windows Security log review (Event IDs 4625, 4624, 4672)
- VirusTotal — IP/domain threat intelligence lookup
- AbuseIPDB — IP abuse history and reputation scoring
- MITRE ATT&CK Framework — Tactic and technique mapping

3. Scenario 1 — Network Reconnaissance Detection

3.1 Activity Performed

Simulated port scanning was conducted using Nmap against localhost. The goal was to generate detectable SYN packets that could be captured and analyzed in Wireshark, simulating a real attacker performing network discovery.

3.2 Command Used

```
nmap -sS localhost
```

3.3 Detection Method

Wireshark was configured to capture live traffic on the active network interface. The following display filter was applied to isolate SYN-only packets (no ACK), which are characteristic of a TCP SYN stealth scan:

```
tcp.flags.syn == 1 && tcp.flags.ack == 0
```

3.4 MITRE ATT&CK Mapping

Technique: T1046 — Network Service Discovery. This technique involves adversaries attempting to discover services running on remote hosts that can be exploited for later stages of an attack.

3.5 SYN Scan Evidence (Wireshark)

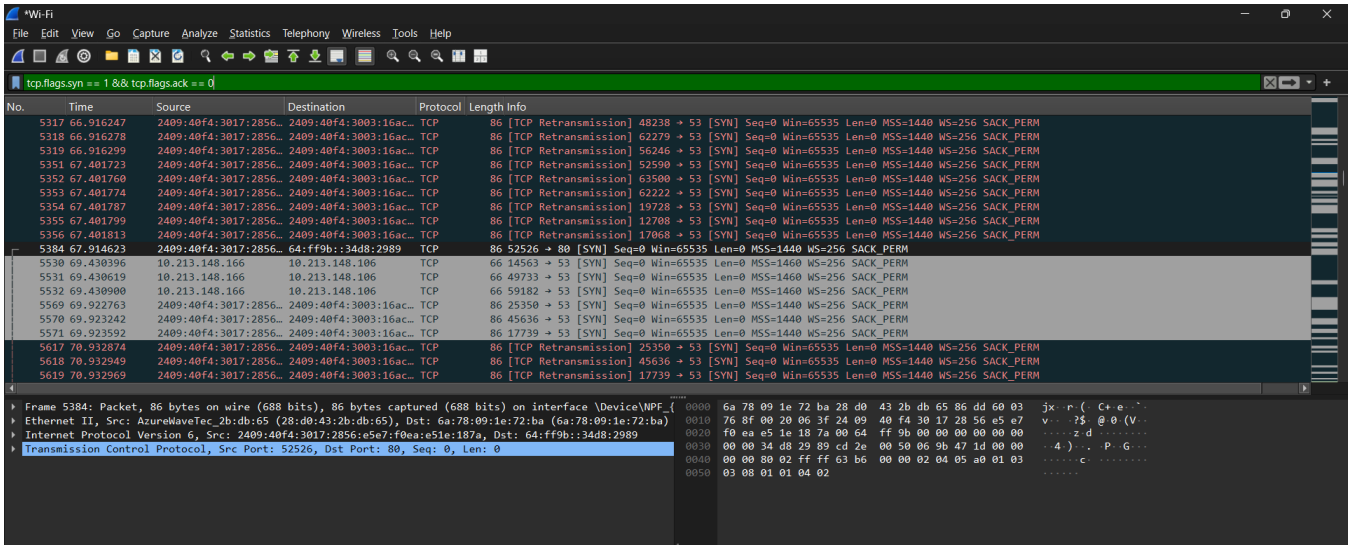


Figure: Wireshark — SYN Scan packets (tcp.flags.syn==1 && tcp.flags.ack==0)

3.6 HTTP Traffic Analysis

HTTP traffic was also captured and filtered. A GET request to /alertmessage/v1/product/sync was observed, returning HTTP 403 Forbidden. This is consistent with automated sync requests from system software.

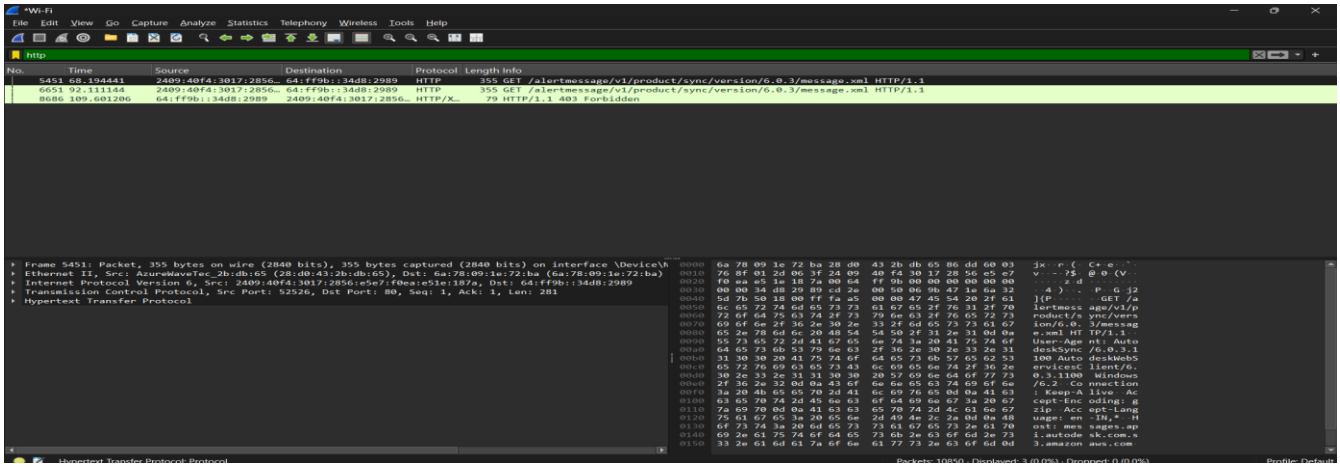


Figure: Wireshark — HTTP Traffic (GET requests and 403 Forbidden response)

3.7 DNS Traffic Analysis

DNS queries were captured showing standard resolution activity for ssl.gstatic.com and beacons.gcp.gvt2.com — Google's infrastructure domains. All DNS responses returned valid A/AAAA records.

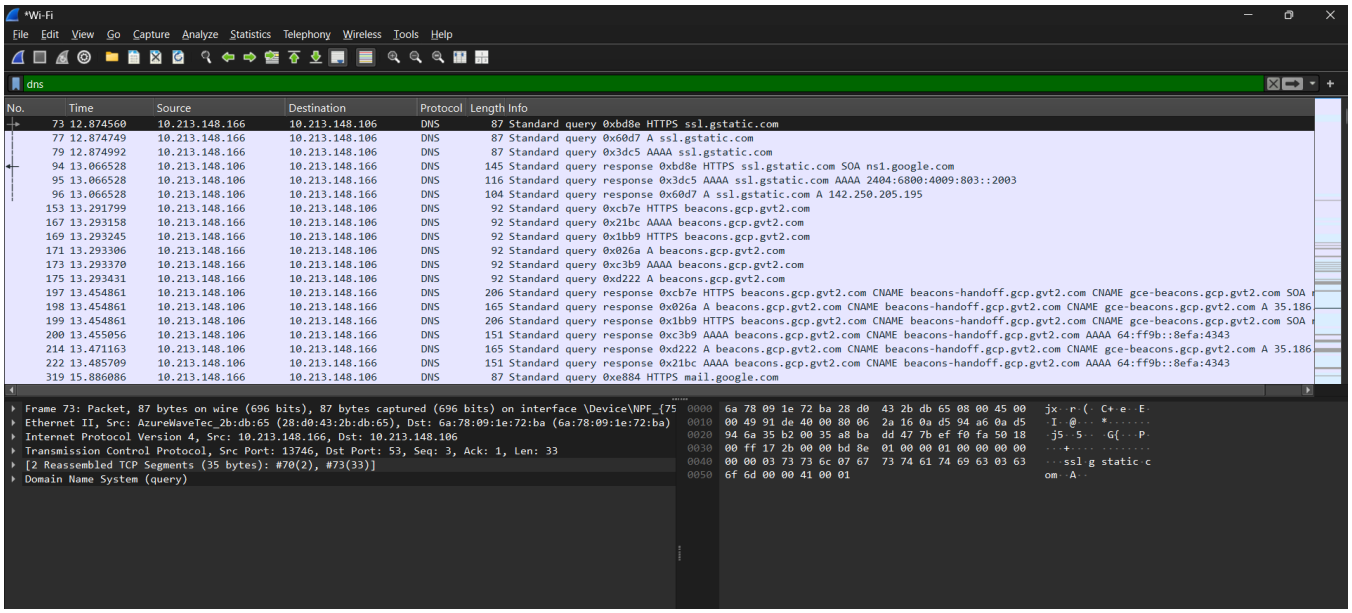


Figure: Wireshark — DNS Traffic (Google infrastructure queries)

3.8 ICMP / Ping Detection

ICMP Echo request/reply pairs were observed between 10.213.148.166 and 8.8.8.8 (Google DNS). This confirms outbound connectivity and rules out network isolation as a factor in the investigation.

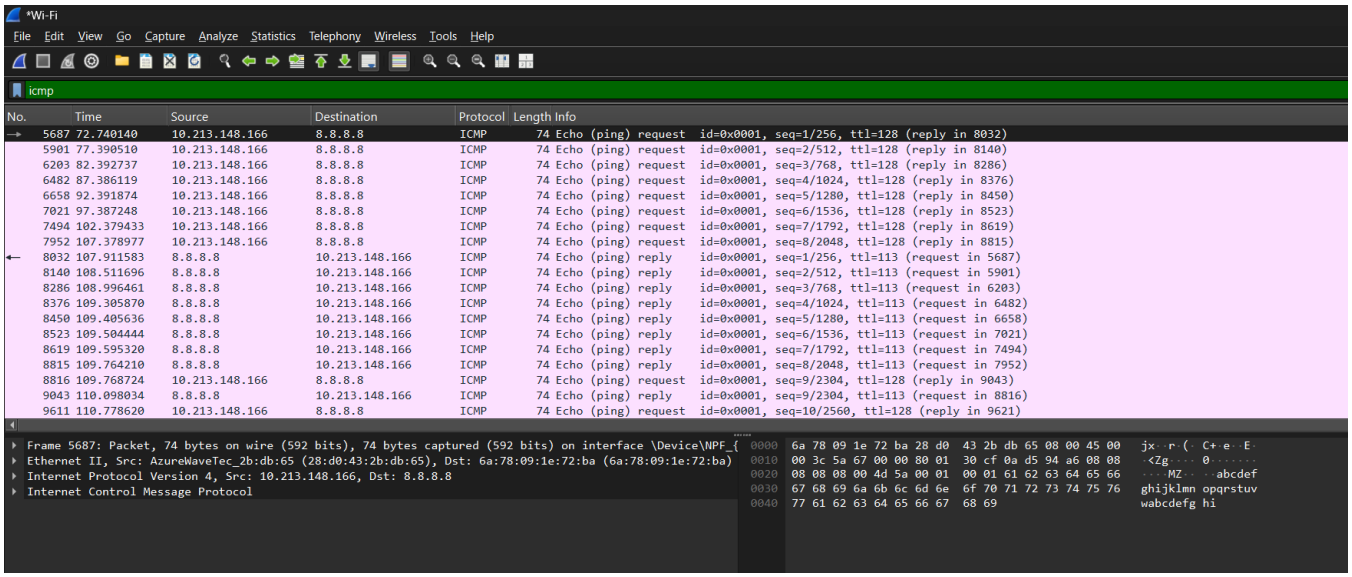


Figure: Wireshark — ICMP Ping requests to 8.8.8.8

4. Scenario 2 — Brute Force Login Detection

4.1 Activity Performed

Multiple failed login attempts were deliberately generated against the Windows account using incorrect credentials, simulating a brute force attack. Windows Security Event logging was enabled to capture authentication events.

4.2 Key Windows Event IDs

- **Event ID 4625** — An account failed to logon
- **Event ID 4624** — An account was successfully logged on
- **Event ID 4672** — Special privileges assigned to new logon
- **Event ID 1102** — The audit log was cleared (anti-forensics indicator)

4.3 MITRE ATT&CK Mapping

Technique: T1110 — Brute Force. Sub-technique: T1110.001 — Password Guessing. The pattern of repeated 4625 events followed by a 4624 event is a classic indicator of a successful brute force attack.

4.4 Successful Logon Evidence (Event ID 4624)

Event Viewer filtered to Event ID 4624 shows 5 successful logon events. The detail pane confirms Account Name: SAAD$, Logon Type 5 (Service logon), Computer: SAAD. A privileged elevated token was also recorded.

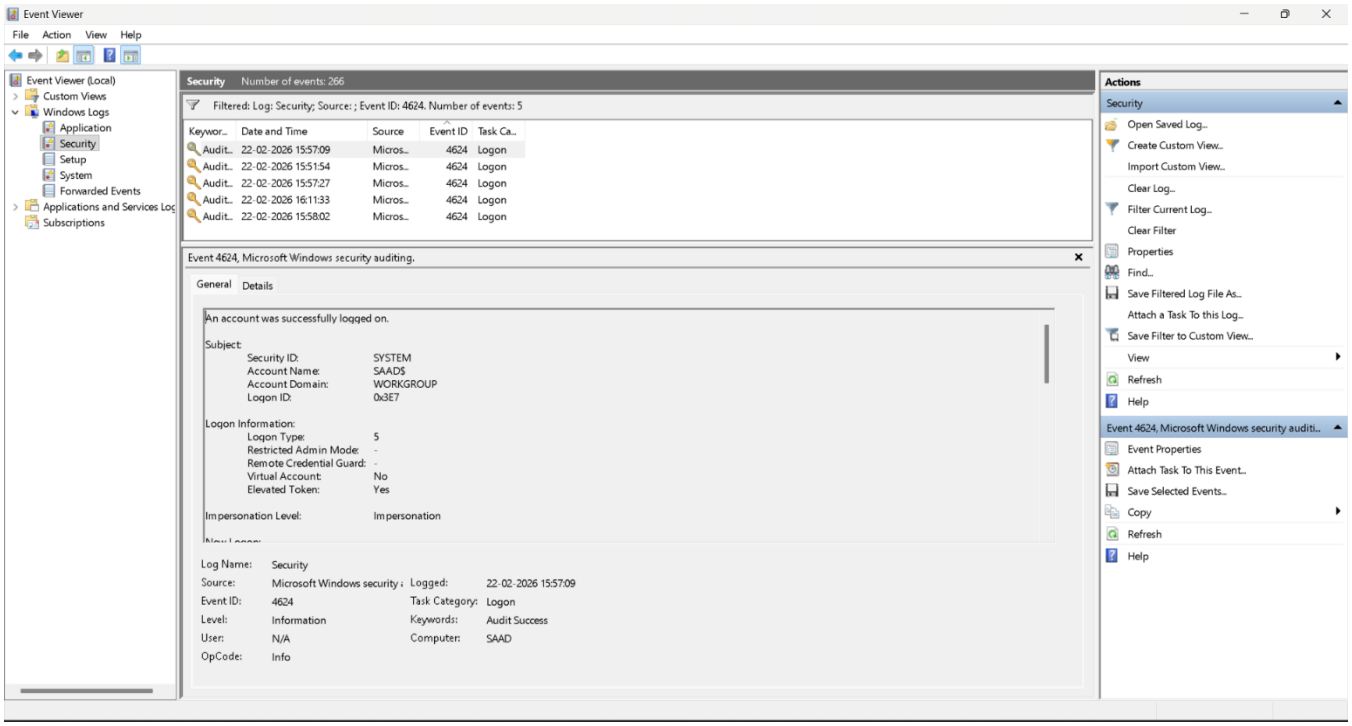


Figure: Windows Event Viewer — Event ID 4624 Successful Logon Details

4.5 Failed Login Detection in Splunk

The .evtx log file was ingested into Splunk and the following SPL query was used to detect all failed logon attempts:

```
index=main EventCode=4625
```

Result: 207 events returned, all sourced from WinEventLog:Security. Account names 'mdsaa' and 'fakeuser' appear repeatedly — a clear indicator of credential stuffing or brute force.

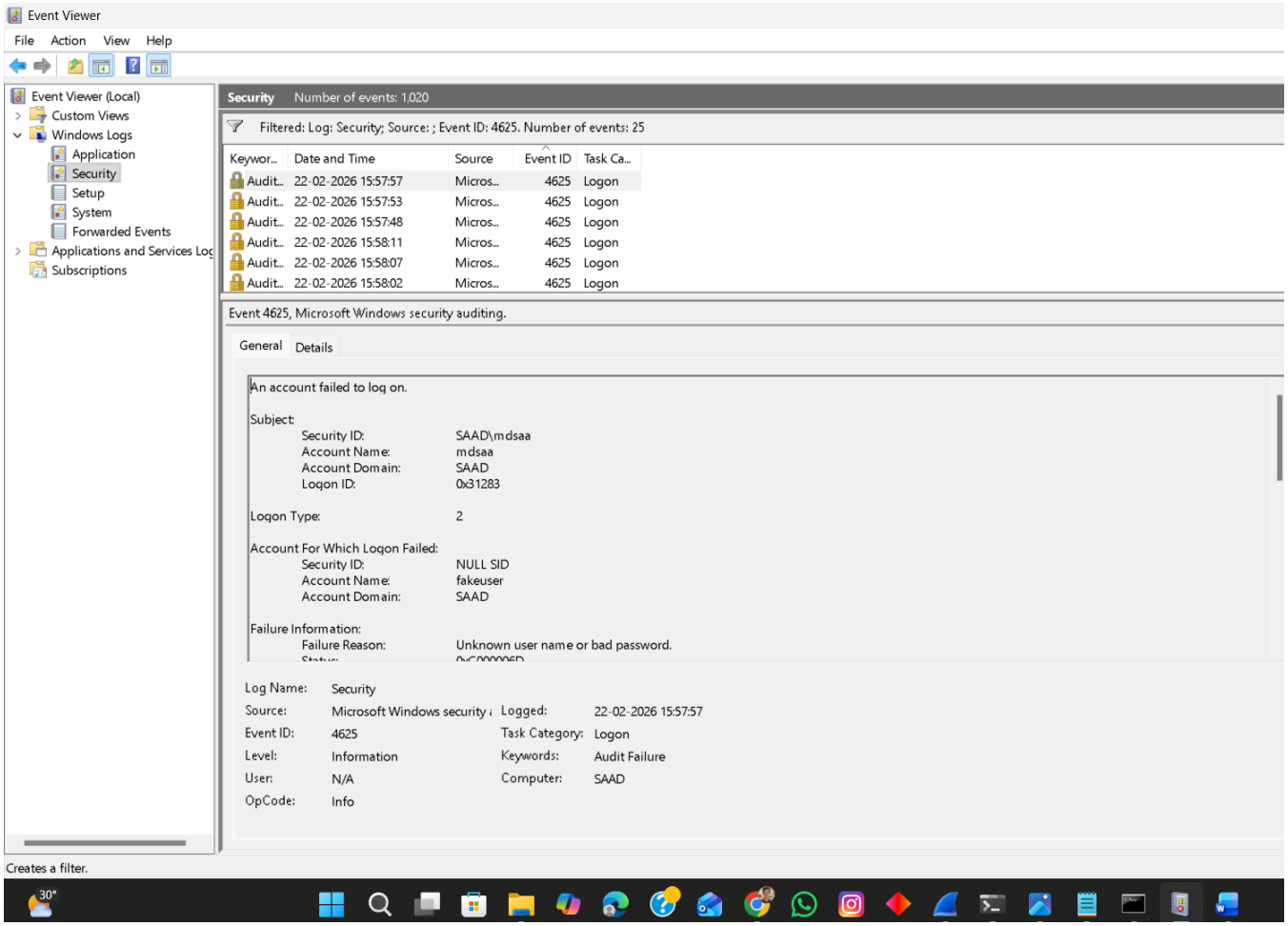


Figure: Splunk — EventCode=4625 (207 Failed Logon Events)

5. SIEM Investigation — Splunk

5.1 Log Source

Windows Security Log file: SOC-Bruteforce-Lab.evtx was ingested into Splunk Enterprise. Sourcetype: WinEventLog:Security. Host: SAAD.

5.2 Correlation Query — Success & Failure Timeline

The following SPL query was used to correlate both failed and successful logins in chronological order:

```
index=main (EventCode=4624 OR EventCode=4625)
| table _time EventCode Account_Name Logon_Type
```

This query returned 9,390 events. Results show 4625 events for accounts 'mdsaa' and 'fakeuser' (Logon Type 2) followed by 4624 events for 'SAAD$/SYSTEM' (Logon Type 5), confirming the attack sequence.

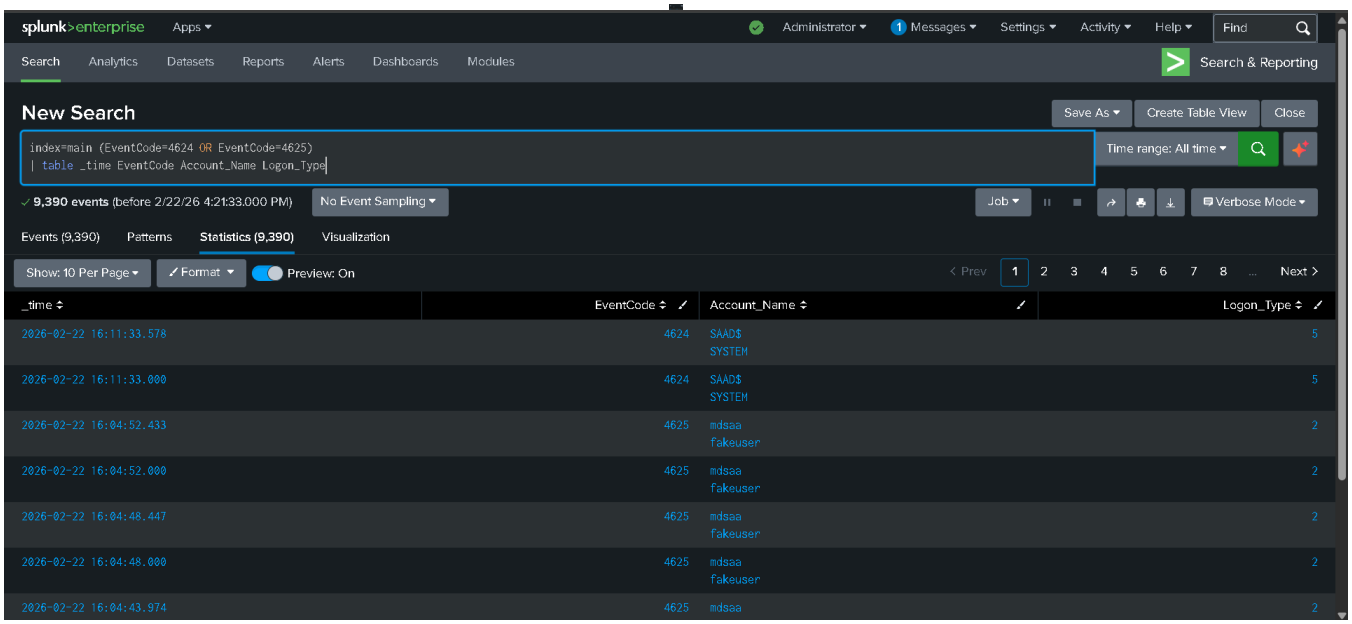


Figure: Splunk — Correlated Success & Failure Events Table

5.3 Splunk Event Table with Network Source

An extended query including Source_Network_Address was run. Failed logins (4625) originate from ::1 (localhost IPv6), while successful logins show no external source — indicating local or service-based logon.

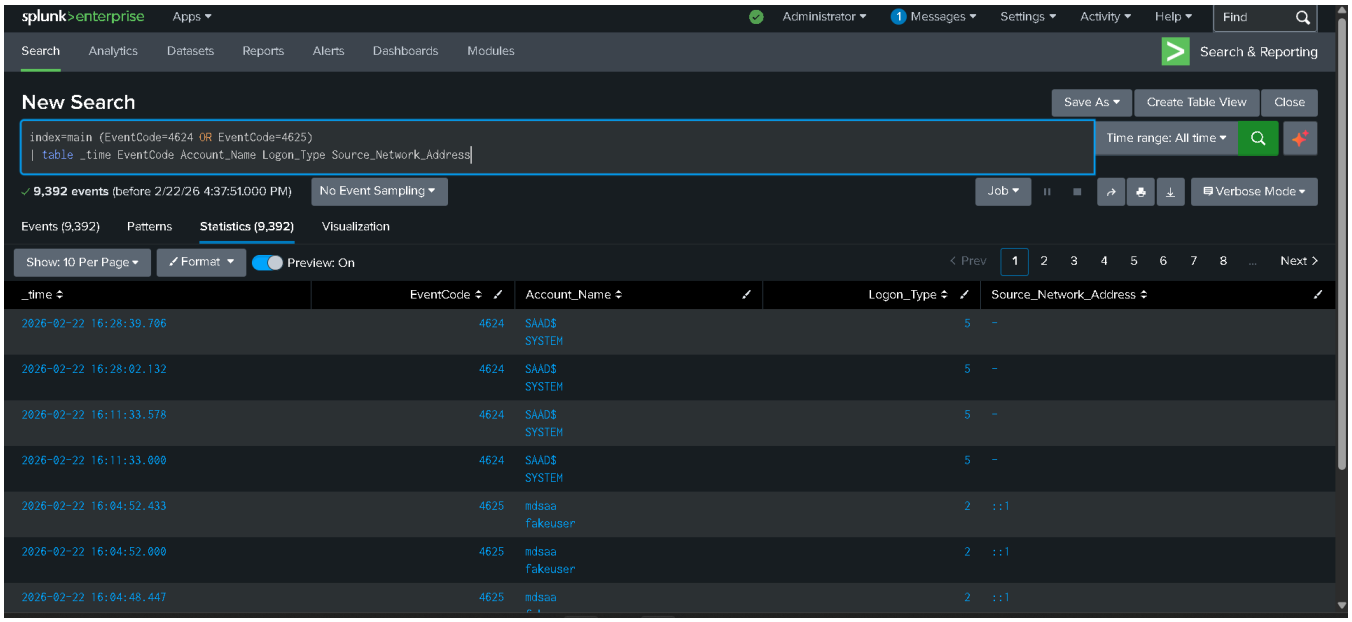


Figure: Splunk — Event Table with Account, Logon Type and Source Network

5.4 Timechart — Event Volume by Month

A timechart query was used to visualize the distribution of login events over time:

```
index=main (EventCode=4624 OR EventCode=4625) | timechart count by EventCode
```

Results show a dramatic spike in February 2026: 6,647 successful logons (4624) and 135 failed logons (4625). January 2026 recorded 2,538 successful logons and 39 failures. Earlier months (Oct-Dec 2025) had minimal activity.

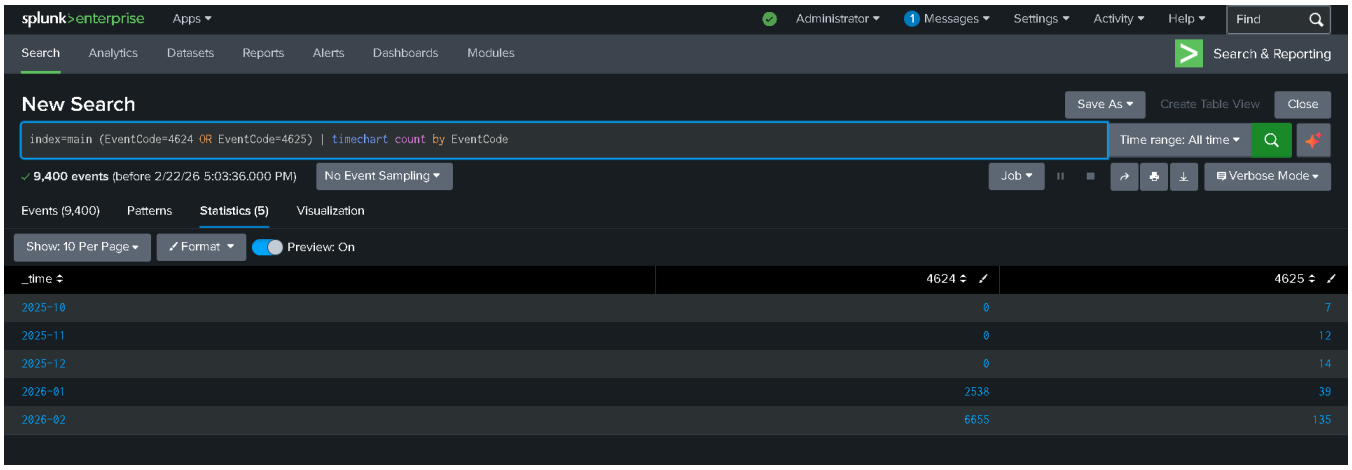
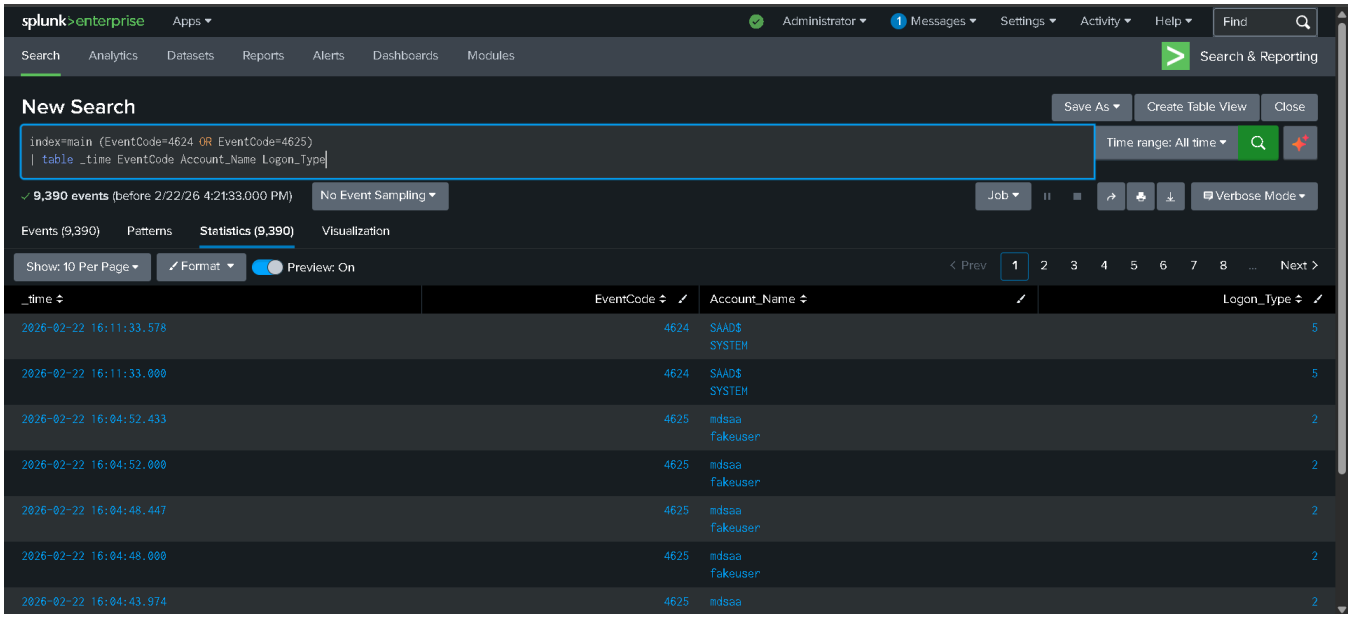


Figure: Splunk — Event volume

5.5 Additional Correlation View



6. Scenario 3 — IOC Validation & Threat Intelligence

6.1 Methodology

IPv6 addresses extracted from Wireshark packet capture were submitted to threat intelligence platforms to determine whether any observed IPs were associated with known malicious activity.

IPs investigated: 2409:40f4:3017:2856:e5e7:f0ea:e51e:187a (Reliance Jio, India)

6.2 IOC Validation Results

IOC / IP Address	VirusTotal	Talos	AbuseIPDB	Verdict
2409:40f4:3017:2856:...	0 / 93 detections	Neutral	Not in DB	✅ Clean
2409:40f4:3001:b4e2:...	0 / 93 detections	Neutral	Not in DB	✅ Clean

6.3 VirusTotal Analysis

IP address 2409:40f4:3017:2856:e5e7:f0ea:e51e:187a was analyzed on VirusTotal. Score: 0/93 security vendors flagged the IP as malicious. The IP belongs to Reliance Jio Infocomm Limited (AS55836), India. Last analyzed 4 minutes prior — verdict: Clean.

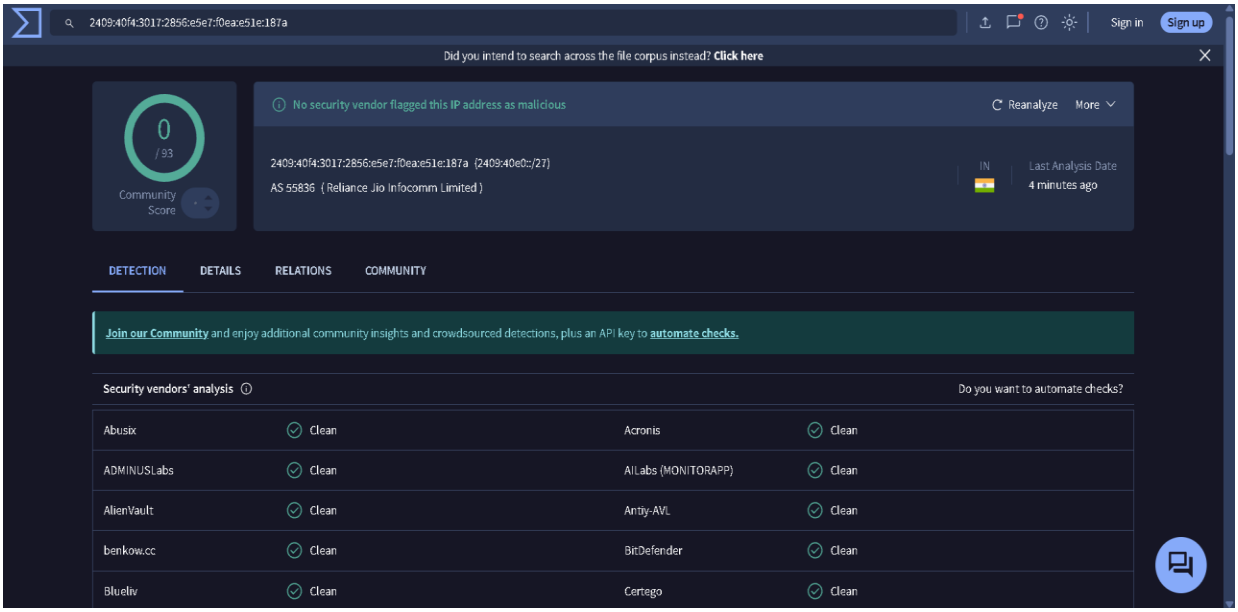


Figure: VirusTotal — IP Analysis (0/93 detections — Clean)

6.4 AbuseIPDB Analysis

The same IP address was checked against AbuseIPDB. Result: IP not found in AbuseIPDB database. ISP: Reliance Jio Infocomm Limited. Usage Type: Mobile ISP. Location: Coimbatore, Tamil Nadu, India. No abuse reports recorded — verdict: Clean.

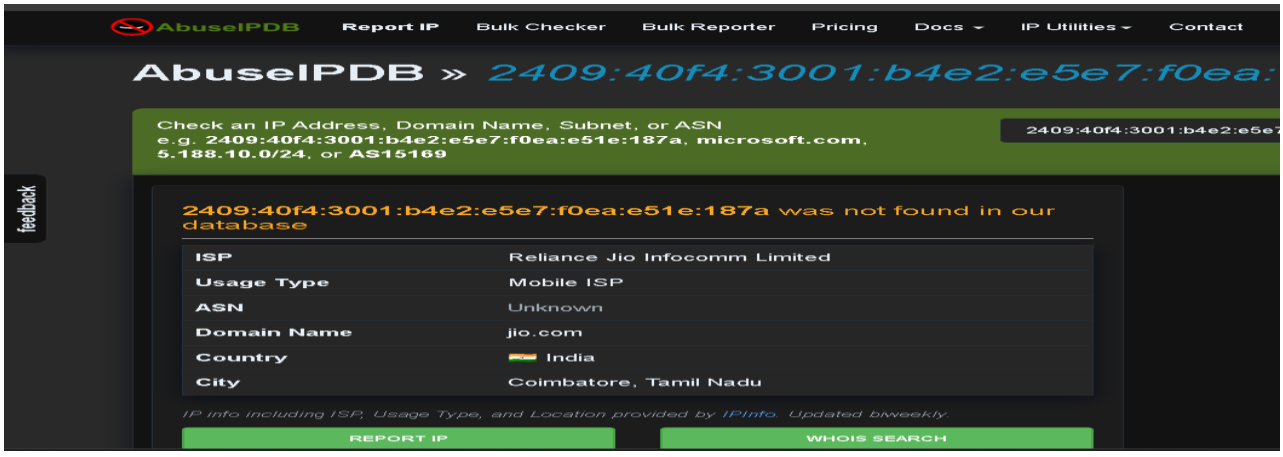


Figure: AbuseIPDB — IP Reputation Check (Not in database — Clean)

7. Risk Assessment

Risk Category	Level	Indicator	Priority
Authentication	MEDIUM-HIGH	Repeated 4625 + 4624	Immediate
Network Recon	MEDIUM	SYN scan detected	High
IOC / Threat Intel	LOW	IPs clean, Jio ISP	Monitor
Privileged Access	HIGH	4672 logged	Immediate

Overall Risk Rating: MEDIUM. The brute force pattern (repeated 4625 + successful 4624 + privileged 4672) is the primary concern. Network IOCs were clean. Immediate action on account lockout policies is recommended.

8. Recommendations

1. **Implement Account Lockout Policy:** Configure Windows Group Policy to lock accounts after 5 failed attempts within 30 minutes.
2. **Enable SIEM Alerting:** Create Splunk alerts triggered when EventCode=4625 count exceeds threshold (e.g., 10 events in 5 minutes) per account.
3. **Monitor Privileged Account Activity:** Create dedicated dashboards for Event ID 4672 (Special Privileges) and 4768 (Kerberos ticket requests).
4. **Network Segmentation:** Isolate critical systems to prevent lateral movement following any successful brute force compromise.
5. **Continuous IOC Monitoring:** Integrate AbuseIPDB and VirusTotal APIs into SIEM pipeline for automated IOC enrichment.
6. **Log Retention Policy:** Ensure Security Event logs are retained for minimum 90 days and backed up to SIEM immediately to prevent log clearing (Event ID 1102) from destroying evidence.

9. Conclusion

This SOC Analyst lab successfully demonstrated the complete Tier-1 investigation workflow from packet capture to SIEM analysis and threat intelligence validation. Key skills exercised include:

- Wireshark packet capture: SYN scan detection, HTTP, DNS and ICMP traffic analysis
- Windows Security Event log analysis: Event IDs 4625, 4624, 4672
- Splunk SIEM log ingestion, SPL query development and event correlation
- Threat intelligence validation using VirusTotal and AbuseIPDB

- MITRE ATT&CK Framework mapping (T1046 — Network Service Discovery, T1110 — Brute Force)

The project simulates real-world Tier-1 SOC analyst responsibilities and validates practical competency in blue team security operations. The identified brute force pattern would escalate to Tier-2 for further investigation of the source, scope, and potential data exposure.