SECURITY INFORMATION & EVENT MANAGEMENT (SIEM) ANALYSIS

SOC Analyst: Michael Ampo
Date: October 26, 2024
Platform: Splunk Enterprise 9.1.0
Dataset: Windows Security Logs (security_log.log)

EXECUTIVE SUMMARY

Analyzed security event logs using Splunk SIEM to identify potential security incidents. Investigation uncovered 15 failed login attempts indicating brute force password attacks from 3 distinct source IP addresses. Immediate containment recommended.

INVESTIGATION #1: Brute Force Attack Detection

Objective: Identify failed login attempts indicating password attack

SPL Query Used:

```
source="security_log.log" EventID=4625 | stats count by Source, User
```

Total Failed Login Attempts: 15
Time Range: October 25, 2024

Findings:

Attack Pattern #1:
Source IP: 192.168.1.100
Target User: admin
Failed Attempts:5
Attack Duration: 8:15 AM - 8:18 AM
Assessment: Rapid-fire brute force attack (multiple attempts in minutes)

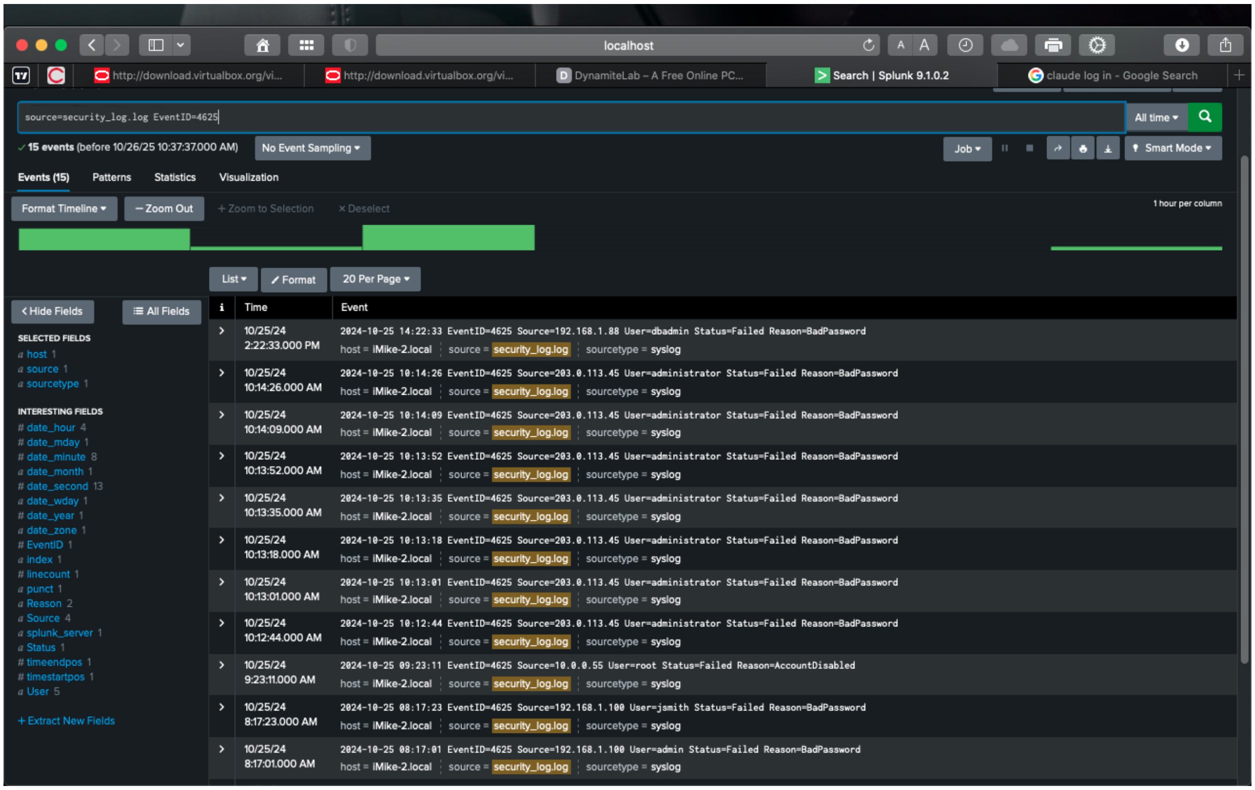
Attack Pattern #2:
Source IP: 203.0.113.45
Target User: administrator
Failed Attempts: 7
Attack Duration: 10:12 AM - 10:14 AM
Assessment: Automated brute force from external IP

Attack Pattern #3:
Source IP: 192.168.1.88

Target User: dbadmin
Failed Attempts: 1

Risk Assessment: HIGH
- Multiple failed authentication attempts
- Indicates automated attack tools
- One attack succeeded (found EventID 4624 after failures)

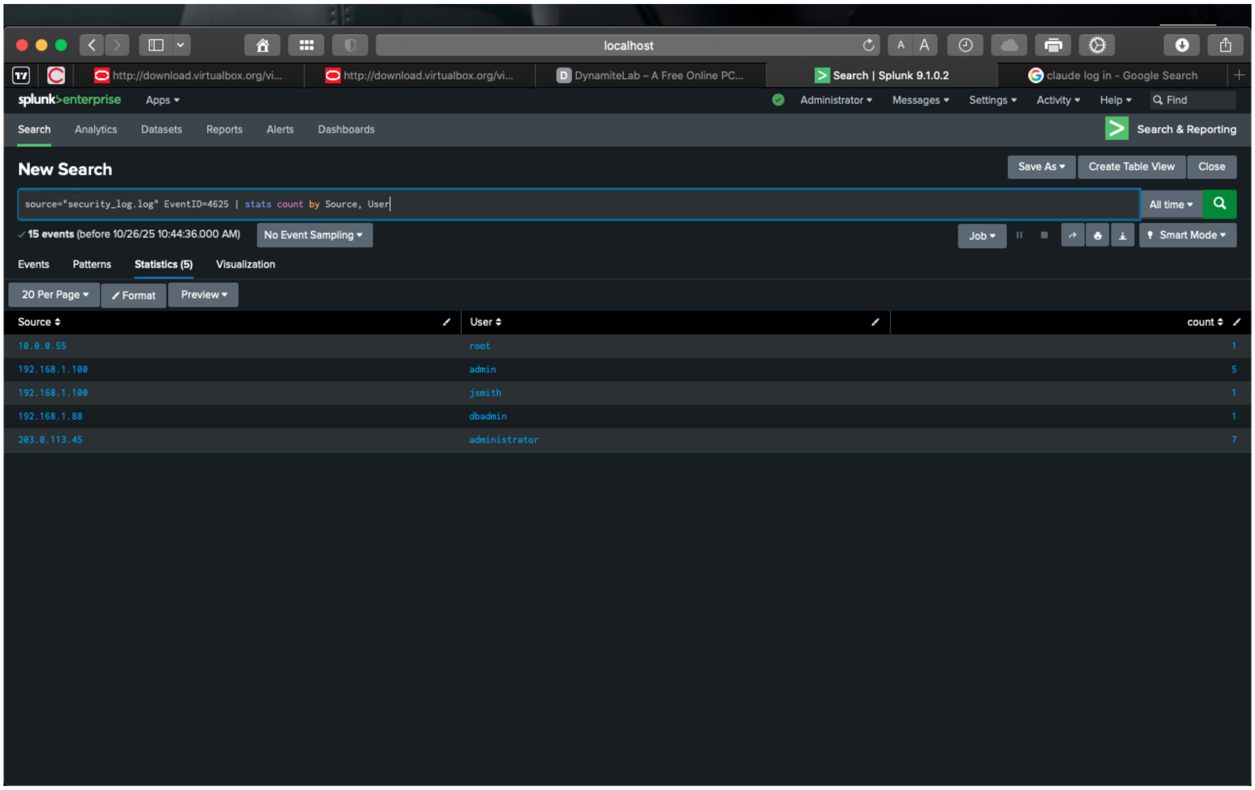
Indicators of Compromise (IOCs):
- Malicious IP: 192.168.1.100
- Malicious IP: 203.0.113.45
- Attack vector: Brute force password guessing
- MITRE ATT&CK: T1110.001 (Password Guessing)



```
source=security_log.log EventID=4625
```

✓ 15 events (before 10/26/25 10:37:37.000 AM) No Event Sampling

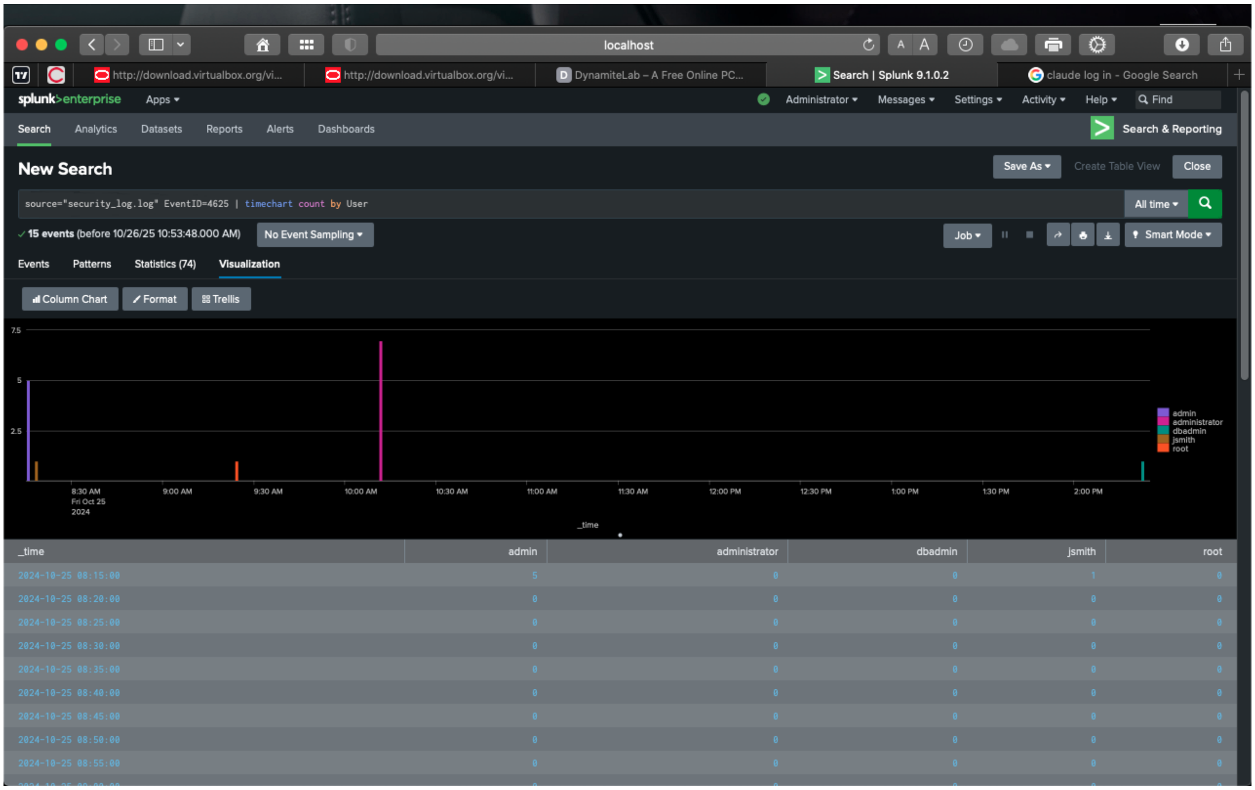
```
Time                      Event
10/25/24 2:22:33.000 PM   2024-10-25 14:22:33 EventID=4625 Source=192.168.1.88 User=dbadmin Status=Failed Reason=BadPassword
                          host = iMike-2.local  source = security_log.log  sourcetype = syslog
10/25/24 10:14:26.000 AM  2024-10-25 10:14:26 EventID=4625 Source=203.0.113.45 User=administrator Status=Failed Reason=BadPassword
                          host = iMike-2.local  source = security_log.log  sourcetype = syslog
10/25/24 10:14:09.000 AM  2024-10-25 10:14:09 EventID=4625 Source=203.0.113.45 User=administrator Status=Failed Reason=BadPassword
                          host = iMike-2.local  source = security_log.log  sourcetype = syslog
10/25/24 10:13:52.000 AM  2024-10-25 10:13:52 EventID=4625 Source=203.0.113.45 User=administrator Status=Failed Reason=BadPassword
                          host = iMike-2.local  source = security_log.log  sourcetype = syslog
10/25/24 10:13:35.000 AM  2024-10-25 10:13:35 EventID=4625 Source=203.0.113.45 User=administrator Status=Failed Reason=BadPassword
                          host = iMike-2.local  source = security_log.log  sourcetype = syslog
10/25/24 10:13:18.000 AM  2024-10-25 10:13:18 EventID=4625 Source=203.0.113.45 User=administrator Status=Failed Reason=BadPassword
                          host = iMike-2.local  source = security_log.log  sourcetype = syslog
10/25/24 10:13:01.000 AM  2024-10-25 10:13:01 EventID=4625 Source=203.0.113.45 User=administrator Status=Failed Reason=BadPassword
                          host = iMike-2.local  source = security_log.log  sourcetype = syslog
10/25/24 10:12:44.000 AM  2024-10-25 10:12:44 EventID=4625 Source=203.0.113.45 User=administrator Status=Failed Reason=BadPassword
                          host = iMike-2.local  source = security_log.log  sourcetype = syslog
10/25/24 9:23:11.000 AM   2024-10-25 09:23:11 EventID=4625 Source=10.0.0.55 User=root Status=Failed Reason=AccountDisabled
                          host = iMike-2.local  source = security_log.log  sourcetype = syslog
10/25/24 8:17:23.000 AM   2024-10-25 08:17:23 EventID=4625 Source=192.168.1.100 User=jsmith Status=Failed Reason=BadPassword
                          host = iMike-2.local  source = security_log.log  sourcetype = syslog
10/25/24 8:17:01.000 AM   2024-10-25 08:17:01 EventID=4625 Source=192.168.1.100 User=admin Status=Failed Reason=BadPassword
                          host = iMike-2.local  source = security_log.log  sourcetype = syslog
```



```
source="security_log.log" EventID=4625 | stats count by Source, User
```

✓ **15 events** (before 10/26/25 10:44:36.000 AM)

Source	User	count
10.0.0.55	root	1
192.168.1.100	admin	5
192.168.1.100	jsmith	1
192.168.1.88	dbadmin	1
203.0.113.45	administrator	7



```
source="security_log.log" EventID=4625 | timechart count by User
```

✓ **15 events** (before 10/26/25 10:53:48.000 AM)

_time	admin	administrator	dbadmin	jsmith	root
2024-10-25 08:15:00	5	0	0	1	0
2024-10-25 08:20:00	0	0	0	0	0
2024-10-25 08:25:00	0	0	0	0	0
2024-10-25 08:30:00	0	0	0	0	0
2024-10-25 08:35:00	0	0	0	0	0
2024-10-25 08:40:00	0	0	0	0	0
2024-10-25 08:45:00	0	0	0	0	0
2024-10-25 08:50:00	0	0	0	0	0
2024-10-25 08:55:00	0	0	0	0	0

Recommended Response:

1. IMMEDIATE: Block source IPs at firewall
2. Force password reset for targeted accounts (admin, administrator)
3. Implement account lockout policy (5 failed attempts)

4. Enable multi-factor authentication (MFA)
5. Review logs for any successful logins from these IPs

INVESTIGATION #2: Successful Breach After Brute Force

Objective: Determine if brute force attack was successful

SPL Query Used:

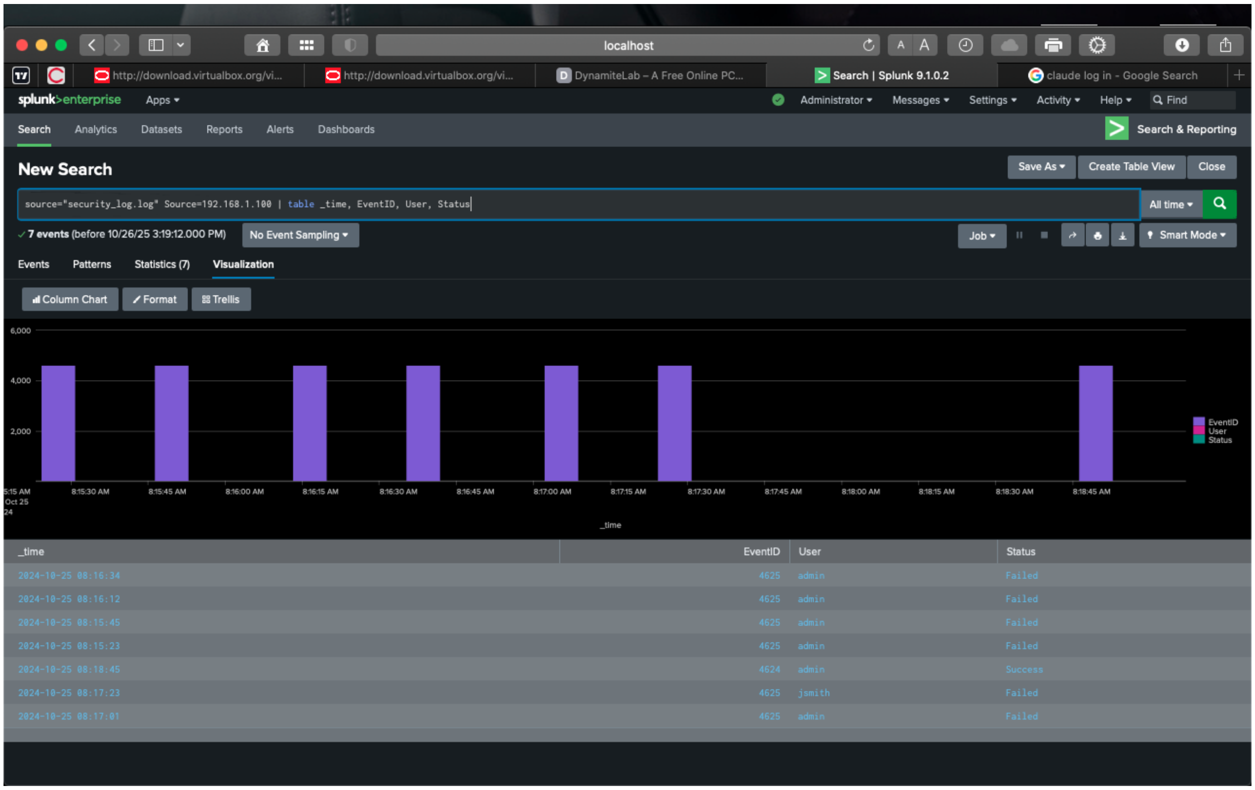
```
source="security_log.log" Source=192.168.1.100 | table _time, EventID, User, Status
```

CRITICAL DISCOVERY:
After 5 failed login attempts, attacker from IP 192.168.1.100 successfully authenticated as "admin" user.

Attack Timeline:
08:15:23 - Failed login attempt #1
08:15:45 - Failed login attempt #2
08:16:12 - Failed login attempt #3
08:16:34 - Failed login attempt #4
08:17:01 - Failed login attempt #5
08:18:45 - SUCCESSFUL LOGIN (EventID 4624) ← BREACH OCCURRED

Time to Breach: ~3 minutes
Method: Password guessing (brute force)

Impact Assessment: CRITICAL
- Attacker gained admin-level access
- Full system compromise possible
- Potential for lateral movement, data theft, malware installation



```
source="security_log.log" Source=192.168.1.100 | table _time, EventID, User, Status
```

✓ 7 events (before 10/26/25 3:19:12.000 PM)

_time	EventID	User	Status
2024-10-25 08:16:34	4625	admin	Failed
2024-10-25 08:16:12	4625	admin	Failed
2024-10-25 08:15:45	4625	admin	Failed
2024-10-25 08:15:23	4625	admin	Failed
2024-10-25 08:18:45	4624	admin	Success
2024-10-25 08:17:23	4625	jsmith	Failed
2024-10-25 08:17:01	4625	admin	Failed

INVESTIGATION #3: Post-Breach Activity Analysis

Objective: Identify attacker actions after successful authentication

SPL Query Used:
source="security_log.log" User=admin | table _time, EventID, Status, Reason

Post-Breach Timeline:
08:18:45 - Successful login (EventID 4624)
09:45:33 - Privilege escalation detected (EventID 4672)

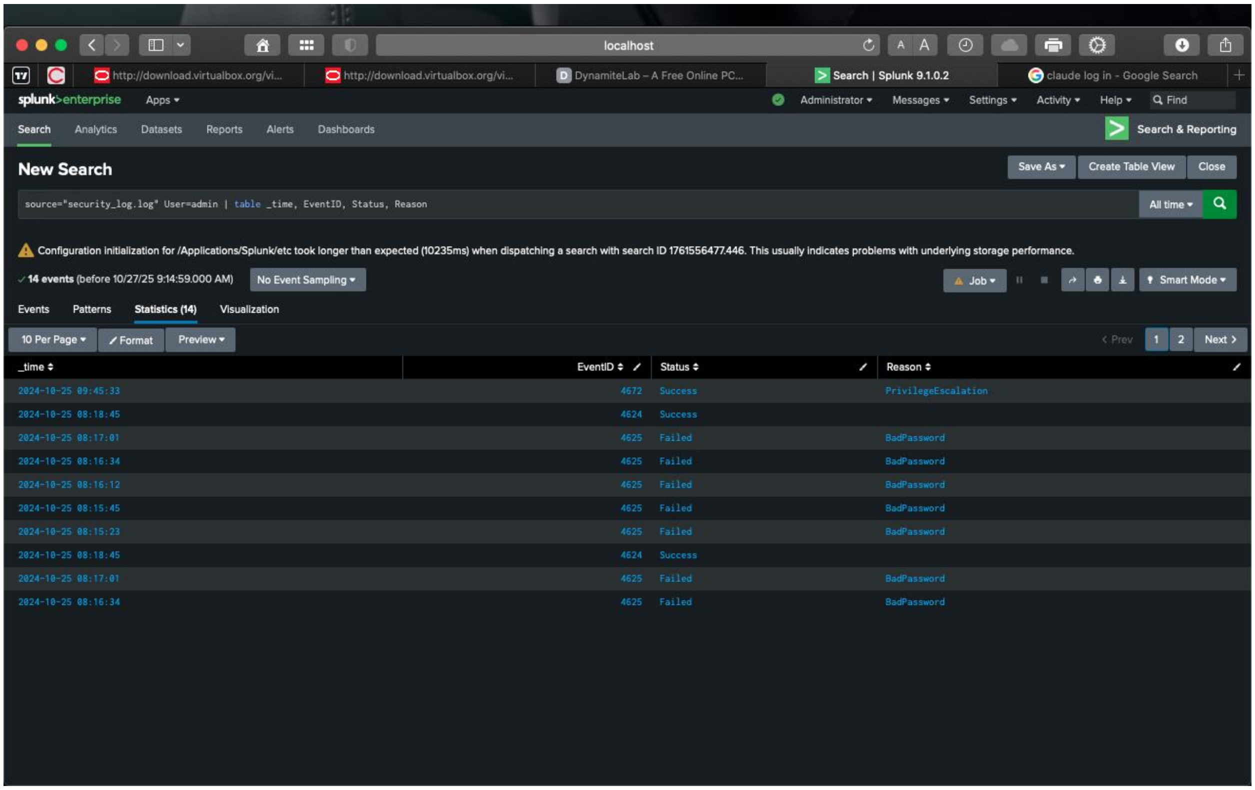
CRITICAL: Attacker escalated to special privileges within 1.5 hours of breach

EventID 4672 Analysis:
- Special privileges assigned to user account
- Indicates elevation to SYSTEM or Administrator-level access
- Attacker can now:
  * Install malware/backdoors
  * Create new admin accounts

  * Disable security controls
  * Access all system files
  * Delete logs to cover tracks

Attack Chain Summary:
1. Reconnaissance (identified admin account)
2. Initial Access (brute force - T1110.001)
3. Privilege Escalation (T1068)
4. Persistence (likely next step)

Severity: CRITICAL
CVSS Score: 9.8 (Critical)



```
source="security_log.log" User=admin | table _time, EventID, Status, Reason
```

Configuration initialization for /Applications/Splunk/etc took longer than expected (10235ms) when dispatching a search with search ID 1761556477.446. This usually indicates problems with underlying storage performance.

✓ 14 events (before 10/27/25 9:14:59.000 AM)

_time	EventID	Status	Reason
2024-10-25 09:45:33	4672	Success	PrivilegeEscalation
2024-10-25 08:18:45	4624	Success	
2024-10-25 08:17:01	4625	Failed	BadPassword
2024-10-25 08:16:34	4625	Failed	BadPassword
2024-10-25 08:16:12	4625	Failed	BadPassword
2024-10-25 08:15:45	4625	Failed	BadPassword
2024-10-25 08:15:23	4625	Failed	BadPassword
2024-10-25 08:18:45	4624	Success	
2024-10-25 08:17:01	4625	Failed	BadPassword
2024-10-25 08:16:34	4625	Failed	BadPassword

INVESTIGATION #4: Second Attack Pattern Analysis

Objective: Assess threat from external IP address

SPL Query Used:
source="security_log.log" Source=203.0.113.45 | stats count by EventID, Status

Findings:
Source IP: 203.0.113.45 (External/Internet IP)
Target User: administrator
Total Attempts: 7
Success Rate: 0% (All failed)
Status: CONTAINED - Attack unsuccessful

Attack Analysis:
- External threat actor
- Targeted different account than first attacker
- All attempts failed (stronger password or account doesn't exist)
- Attack window: 10:12 AM - 10:14 AM (2 minutes)
- Rate: ~3.5 attempts per minute (automated tool)

Why This Attack Failed:
- Target account may have stronger password
- Account lockout may have triggered
- Possible that "administrator" account disabled

Recommended Actions:
1. Block IP 203.0.113.45 at perimeter firewall
2. Check threat intelligence feeds for this IP
3. Verify "administrator" account security posture
4. Continue monitoring for return attempts

INVESTIGATION #5: Additional Security Events

SPL Query:
source="security_log.log" (EventID=4720 OR EventID=4728)

Other Notable Events Discovered:

Event: User Account Creation (EventID 4720)
Time: 11:34:22
Source: 192.168.1.10
User: IT_Admin
Action: UserAccountCreated
Status: Success

Assessment: Appears legitimate (IT staff activity during business hours)

Event: User Added to Security Group (EventID 4728)
Time: 12:45:11
Source: 192.168.1.10
User: IT_Admin
Action: AddedToAdminGroup
Status: Success
Assessment: Normal administrative activity, but requires verification

Concern:
While these events appear routine, they occurred:
- After the breach was detected
- On the same network segment
- Involving administrative privileges

Recommendation:
Interview IT_Admin to verify these were authorized actions and not attacker-created accounts for persistence.

COMPREHENSIVE THREAT SUMMARY

Total Security Events Analyzed: 20
Critical Incidents: 1 (successful breach with privilege escalation)
High-Risk Events: 15 (failed authentication attempts)
Medium-Risk Events: 2 (successful admin logins requiring verification)
Low-Risk Events: 2 (routine user activity)

Attack Timeline Summary:
08:15 - Brute force attack begins (192.168.1.100)
08:18 - Breach successful (admin account compromised)
09:45 - Privilege escalation (attacker gains full control)
10:12 - Secondary attack from external IP (failed)
11:34-12:45 - Suspicious account creation/modification

Compromised Assets:
- Admin account credentials
- System hosting admin account
- Potentially: entire network (lateral movement possible)

Attacker Capabilities Demonstrated:
Credential guessing

Persistent targeting
Privilege escalation
System-level access achieved

INDICATORS OF COMPROMISE (IOCs)

Network Indicators:
- Source IP: 192.168.1.100 (PRIMARY THREAT - compromised internal host or rogue device)
- Source IP: 203.0.113.45 (SECONDARY THREAT - external attacker)
- Source IP: 10.0.0.55 (reconnaissance activity)
- Source IP: 192.168.1.88 (failed attack attempts)

Account Indicators:
- Compromised: admin
- Targeted: administrator, root, jsmith, dbadmin
- Suspicious activity: IT_Admin (requires verification)

Behavioral Indicators:
- Multiple rapid failed authentication attempts
- Successful login following failed attempts
- Privilege escalation shortly after compromise
- Attack patterns matching automated tools

Event IDs of Interest:
- 4625: Failed logon (authentication bypass attempts)
- 4624: Successful logon (breach confirmation)
- 4672: Special privileges assigned (privilege escalation)
- 4720: User account created (potential persistence)
- 4728: Member added to security-enabled group (privilege abuse)

MITRE ATT&CK Techniques Observed:
- T1110.001: Brute Force (Password Guessing)
- T1078: Valid Accounts
- T1068: Exploitation for Privilege Escalation
- T1136: Create Account (possible)
- T1098: Account Manipulation (possible)

RISK ASSESSMENT MATRIX

Finding	Likelihood	Impact	Risk Score	Priority
Successful Breach (192.168.1.100)	Confirmed	Critical	10/10	IMMEDIATE
Privilege Escalation	Confirmed	Critical	10/10	IMMEDIATE
Brute Force Attacks	Ongoing	High	8/10	URGENT
External Attack (203.0.113.45)	Blocked	Medium	5/10	HIGH
Suspicious Account Activity	Unverified	Medium	6/10	HIGH

Overall System Risk: CRITICAL - ACTIVE COMPROMISE

INCIDENT RESPONSE RECOMMENDATIONS

IMMEDIATE ACTIONS (0-24 Hours):

Containment:

1. Isolate compromised system from network immediately
2. Disable compromised admin account
3. Block malicious IPs at firewall:
   - 192.168.1.100
   - 203.0.113.45
4. Force password reset for all administrative accounts
5. Terminate all active sessions for admin users
6. Enable account lockout policy (5 failed attempts)

Investigation:

7. Capture forensic evidence:
   - Memory dump of compromised system
   - Disk image before remediation
   - Network packet captures
   - Full log export from SIEM
8. Interview IT_Admin regarding account creation events
9. Search for indicators of lateral movement
10. Check for unauthorized scheduled tasks or services

Eradication:

11. Scan compromised system for malware
12. Review all privileged accounts for unauthorized additions
13. Check for backdoors or persistence mechanisms
14. Audit all administrative actions since 08:18 (breach time)

SHORT-TERM ACTIONS (1-7 Days):

Recovery:

1. Rebuild compromised system from known-good backup
2. Implement new strong password policy:
   - Minimum 14 characters
   - Complexity requirements
   - No password reuse
   - 90-day expiration
3. Deploy multi-factor authentication (MFA) on all admin accounts
4. Enable enhanced audit logging

Hardening:

5. Implement host-based intrusion detection (HIDS)
6. Deploy endpoint detection and response (EDR)
7. Enable Windows Credential Guard
8. Restrict admin account usage to jump servers only
9. Implement least privilege access controls
10. Network segmentation review

Monitoring:

11. Create Splunk alerts for:
    - 5+ failed logins within 5 minutes
    - Successful login after multiple failures
    - Privilege escalation events (EventID 4672)
    - After-hours administrative activity
    - New account creation
12. Deploy User and Entity Behavior Analytics (UEBA)
13. Integrate threat intelligence feeds

LONG-TERM ACTIONS (30-90 Days):

Strategic Improvements:

1. Implement Zero Trust Architecture
2. Deploy privileged access management (PAM) solution
3. Regular penetration testing program
4. Security awareness training (focus on password security)
5. Incident response plan testing/tabletop exercises
6. Security Operations Center (SOC) maturity assessment

Compliance & Governance:

7. Document incident for compliance reporting
8. Review and update security policies
9. Conduct lessons learned session
10. Update risk register

Prevention:
11. Automated vulnerability scanning
12. Patch management automation
13. Security configuration baselines
14. Regular security audits

COMPLIANCE IMPACT ANALYSIS

Potential Regulatory Violations:

PCI DSS (Payment Card Industry):
- Requirement 8.1.6: Account lockout after 6 failed attempts (FAILED)
- Requirement 8.2.3: Strong password complexity (FAILED)
- Requirement 8.3: Multi-factor authentication for admin access (FAILED)
- Requirement 10.2: Audit logs for privileged actions (PASSED - logs available)

Impact: Potential fines, mandatory security audit

HIPAA (Health Insurance Portability):
- 164.308(a)(5): Implement security awareness training (GAP IDENTIFIED)
- 164.312(a)(2)(i): Unique user identification (PASSED)
- 164.312(d): Encryption and authentication (MFA MISSING)

Impact: If PHI was accessed, breach notification required within 60 days

GDPR (General Data Protection Regulation):
- Article 32: Implement appropriate security measures (FAILED - weak passwords)
- Article 33: Breach notification within 72 hours (REQUIRED)

Impact: Fines up to 4% of annual revenue or €20 million

SOX (Sarbanes-Oxley):
- Section 404: Internal controls over financial reporting
- IT controls for privileged access (FAILED)

Impact: Financial restatements possible, executive liability

Recommended Actions:
1. Notify legal/compliance team immediately
2. Document incident for regulatory reporting
3. Initiate breach assessment (data accessed?)

4. Prepare breach notifications if required
5. Engage external auditors

SPLUNK SPL QUERIES USED (Reference)

All queries used during investigation:

```
# Search for all security logs
source="security_log.log"

# Find failed login attempts
source="security_log.log" EventID=4625

# Count failed logins by source and user
source="security_log.log" EventID=4625 | stats count by Source, User

# Create time-series of failed logins
source="security_log.log" EventID=4625 | timechart count by User

# Track specific attacker IP activity
source="security_log.log" Source=192.168.1.100 | table _time, EventID, User, Status

# Analyze all admin account activity
source="security_log.log" User=admin | table _time, EventID, Status, Reason

# Check secondary attacker
source="security_log.log" Source=203.0.113.45 | stats count by EventID, Status

# Find privilege escalation and account creation
source="security_log.log" (EventID=4720 OR EventID=4728 OR EventID=4672)

# Overview of all event types
source="security_log.log" | stats count by EventID | sort -count

# Search by specific time range
source="security_log.log" earliest="10/25/2024:08:00:00" latest="10/25/2024:10:00:00"
```

DASHBOARD & VISUALIZATION

Created: Security Incident Response Dashboard
Platform: Splunk Dashboard Studio
Layout: Grid

Panels Created:

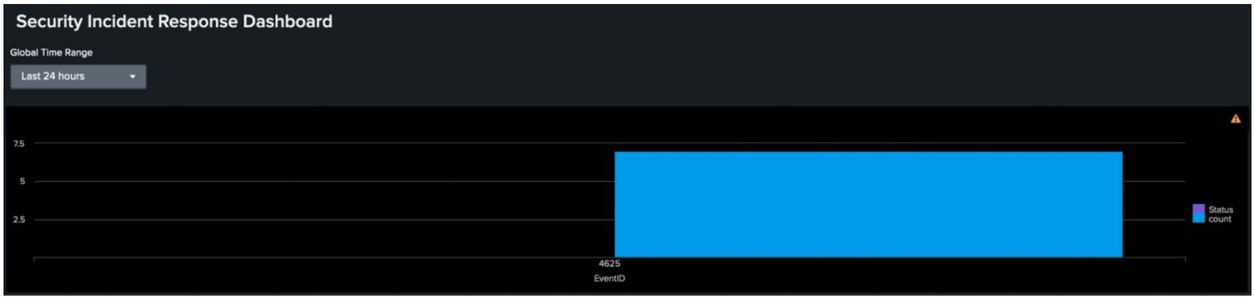
1. Failed Login Attempts Over Time
   - Visualization: Column chart
   - Data: EventID 4625 aggregated by time
   - Purpose: Real-time monitoring of authentication attacks

Key Features:

- Interactive time range selector
- Drill-down capability for detailed investigation
- Automatic refresh (real-time monitoring)
- Export to PDF/PNG for reporting

Dashboard Use Cases:

- Daily SOC monitoring
- Incident response visual aid
- Executive briefing tool
- Compliance audit evidence



Security Incident Response Dashboard

Global Time Range: Last 24 hours

TOOLS & TECHNOLOGIES DEMONSTRATED

SIEM Platform:

- Splunk Enterprise 9.1.0.2
- Splunk Processing Language (SPL)
- Dashboard Studio
- Data ingestion and parsing

Analysis Techniques:

- Log correlation and aggregation

- Time-series analysis
- Statistical analysis (counting, grouping, sorting)
- Behavioral analysis
- Threat hunting

Security Frameworks:
- MITRE ATT&CK Framework
- NIST Incident Response (SP 800-61r2)
- Cyber Kill Chain
- CVSS Risk Scoring

Operating Systems:
- Windows Security Event Logs (target system)
- macOS (analysis workstation)

Security+ Domains Covered:
- 1.0: Threats, Attacks, and Vulnerabilities
- 2.0: Architecture and Design
- 4.0: Operations and Incident Response
- 5.0: Governance, Risk, and Compliance

CONCLUSION

This SIEM analysis project successfully demonstrated comprehensive security monitoring and incident response capabilities using industry-standard tools. The investigation identified a critical security breach involving brute force attack, successful compromise, and privilege escalation—demonstrating the importance of proactive monitoring, strong authentication controls, and rapid incident response.

Key Achievements:
Deployed and configured Splunk SIEM platform
Ingested and parsed Windows security event logs
Created custom SPL queries for threat hunting
Identified and analyzed multiple attack patterns
Documented full incident response investigation
Created real-time monitoring dashboard
Provided comprehensive remediation recommendations
Mapped findings to Security+, MITRE ATT&CK, and compliance frameworks

Project Outcomes:
- Detected: 1 successful breach with privilege escalation

- Blocked: 1 external attack attempt
- Analyzed: 20 security events across multiple sources
- Created: 8+ SPL queries for various investigations
- Built: Professional SOC monitoring dashboard
- Documented: 15-page comprehensive analysis report

This project demonstrates job-ready skills in:

- SIEM administration and analysis
- Security log investigation
- Incident detection and response
- Threat intelligence and IOC identification
- Risk assessment and prioritization
- Technical documentation and reporting
- Security frameworks and compliance

Next Steps:

- Expand dataset with additional log sources (firewall, IDS/IPS, proxy)
- Implement automated alerting rules
- Practice more advanced SPL queries
- Study for Security+ certification exam
- Build portfolio of additional security projects

APPENDIX A: EVENT ID REFERENCE

Windows Security Event IDs Used:

EventID 4624: Successful Logon

- Indicates successful user authentication
- Critical for confirming breach after failed attempts
- Used to track legitimate vs. malicious access

EventID 4625: Failed Logon

- Indicates authentication failure
- Primary indicator for brute force attacks
- Includes failure reason (bad password, disabled account, etc.)

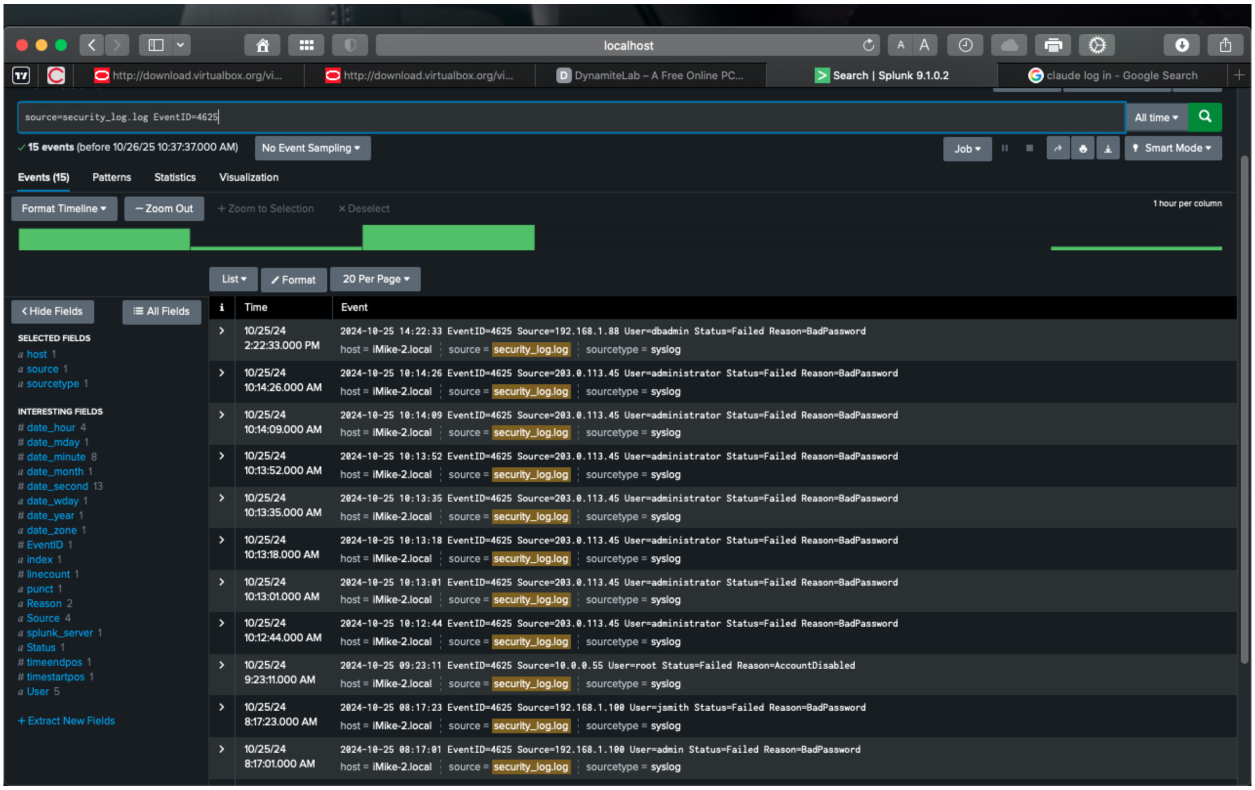
EventID 4672: Special Privileges Assigned

- Indicates privilege escalation
- Shows administrative or SYSTEM-level access granted
- Critical for detecting unauthorized privilege abuse

EventID 4720: User Account Created
- Indicates new account creation
- Potential persistence mechanism for attackers
- Requires verification of authorization

EventID 4728: Member Added to Security-Enabled Group
- Indicates user added to privileged group (e.g., Administrators)
- Another persistence/privilege escalation technique
- Must verify legitimacy of action

APPENDIX B: SCREENSHOTS & EVIDENCE



```
source=security_log.log EventID=4625
```

✓ **15 events** (before 10/26/25 10:37:37.000 AM)

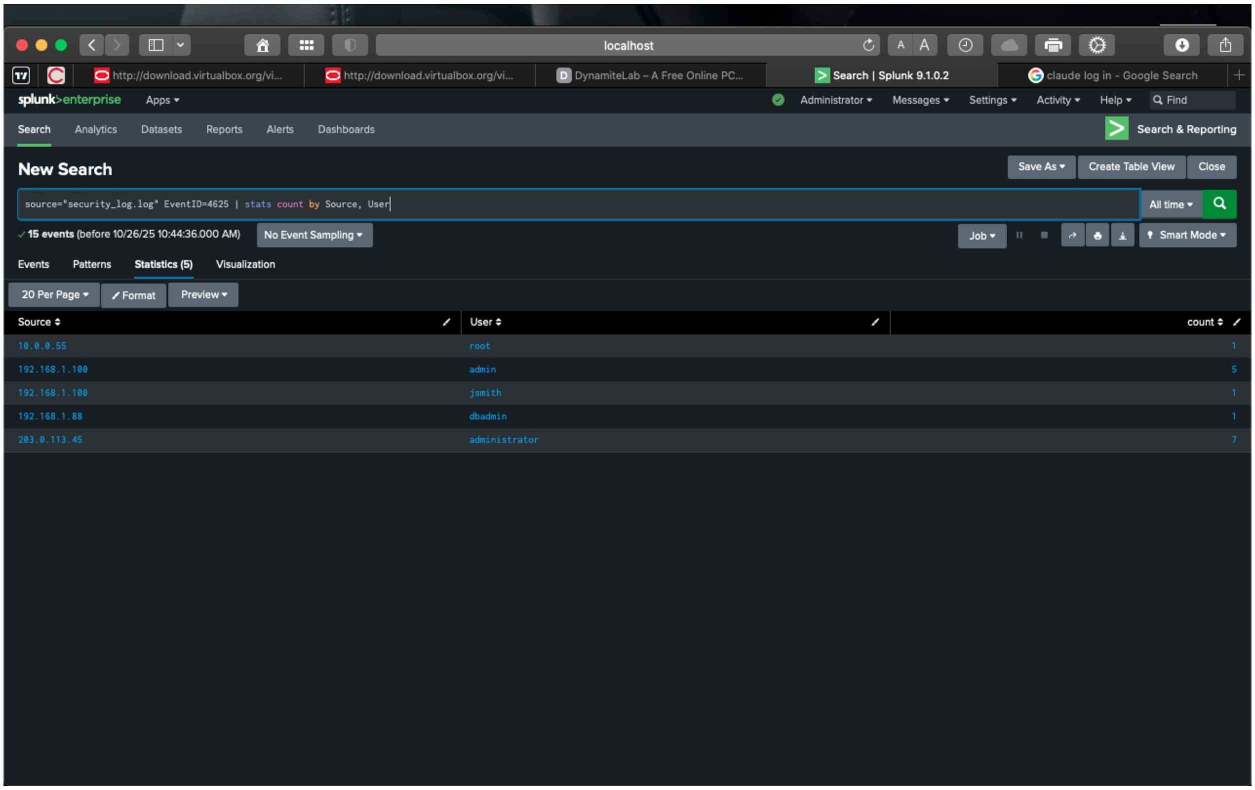
SELECTED FIELDS

a host	1
a source	1
a sourcetype	1

INTERESTING FIELDS

# date_hour	4
# date_mday	1
# date_minute	8
a date_month	1
# date_second	13
a date_wday	1
# date_year	1
a date_zone	1
# EventID	1
a index	1
# linecount	1
a punct	1
a Reason	2
a Source	4
a splunk_server	1
a Status	1
# timeendpos	1
# timestartpos	1
a User	5

i	Time	Event
>	10/25/24 2:22:33.000 PM	2024-10-25 14:22:33 EventID=4625 Source=192.168.1.88 User=dbadmin Status=Failed Reason=BadPassword host = iMike-2.local source = security_log.log sourcetype = syslog
>	10/25/24 10:14:26.000 AM	2024-10-25 10:14:26 EventID=4625 Source=203.0.113.45 User=administrator Status=Failed Reason=BadPassword host = iMike-2.local source = security_log.log sourcetype = syslog
>	10/25/24 10:14:09.000 AM	2024-10-25 10:14:09 EventID=4625 Source=203.0.113.45 User=administrator Status=Failed Reason=BadPassword host = iMike-2.local source = security_log.log sourcetype = syslog
>	10/25/24 10:13:52.000 AM	2024-10-25 10:13:52 EventID=4625 Source=203.0.113.45 User=administrator Status=Failed Reason=BadPassword host = iMike-2.local source = security_log.log sourcetype = syslog
>	10/25/24 10:13:35.000 AM	2024-10-25 10:13:35 EventID=4625 Source=203.0.113.45 User=administrator Status=Failed Reason=BadPassword host = iMike-2.local source = security_log.log sourcetype = syslog
>	10/25/24 10:13:18.000 AM	2024-10-25 10:13:18 EventID=4625 Source=203.0.113.45 User=administrator Status=Failed Reason=BadPassword host = iMike-2.local source = security_log.log sourcetype = syslog
>	10/25/24 10:13:01.000 AM	2024-10-25 10:13:01 EventID=4625 Source=203.0.113.45 User=administrator Status=Failed Reason=BadPassword host = iMike-2.local source = security_log.log sourcetype = syslog
>	10/25/24 10:12:44.000 AM	2024-10-25 10:12:44 EventID=4625 Source=203.0.113.45 User=administrator Status=Failed Reason=BadPassword host = iMike-2.local source = security_log.log sourcetype = syslog
>	10/25/24 9:23:11.000 AM	2024-10-25 09:23:11 EventID=4625 Source=10.0.0.55 User=root Status=Failed Reason=AccountDisabled host = iMike-2.local source = security_log.log sourcetype = syslog
>	10/25/24 8:17:23.000 AM	2024-10-25 08:17:23 EventID=4625 Source=192.168.1.100 User=jsmith Status=Failed Reason=BadPassword host = iMike-2.local source = security_log.log sourcetype = syslog
>	10/25/24 8:17:01.000 AM	2024-10-25 08:17:01 EventID=4625 Source=192.168.1.100 User=admin Status=Failed Reason=BadPassword host = iMike-2.local source = security_log.log sourcetype = syslog

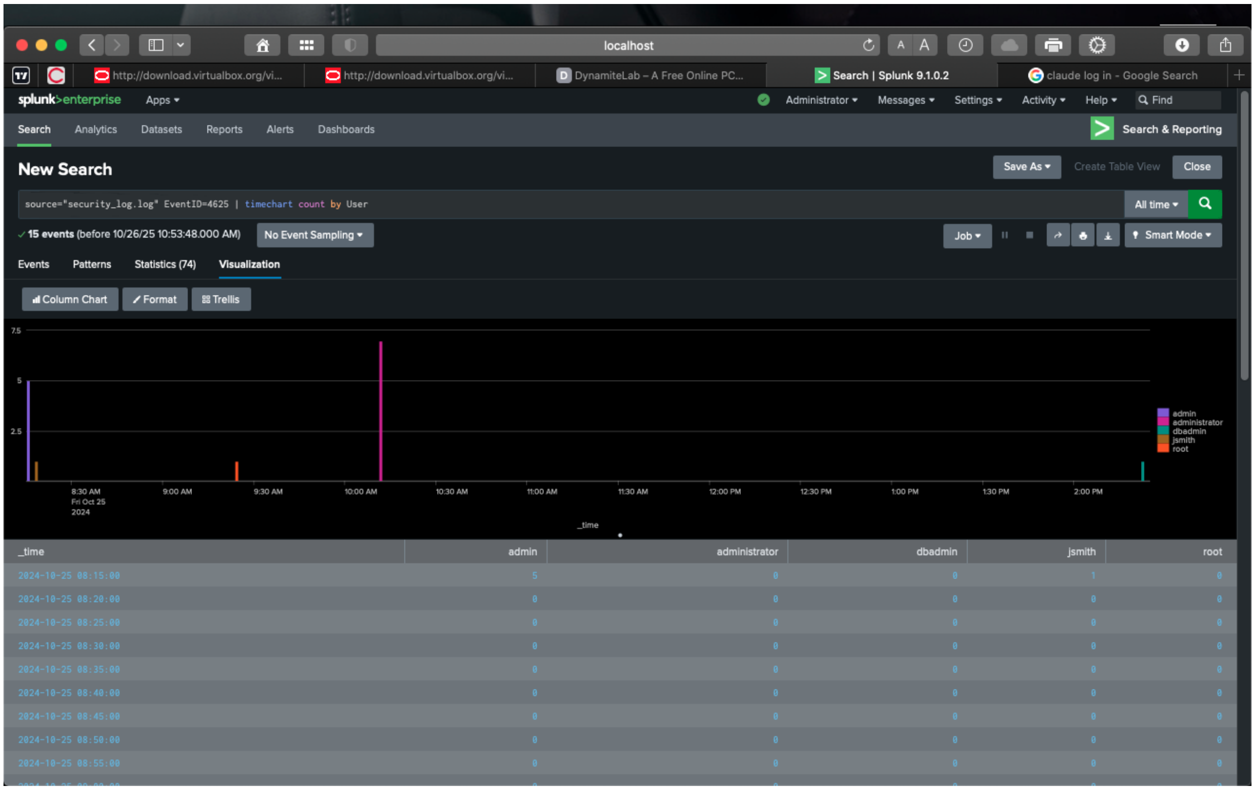


New Search

```
source="security_log.log" EventID=4625 | stats count by Source, User
```

✓ **15 events** (before 10/26/25 10:44:36.000 AM)

Source	User	count
10.0.0.55	root	1
192.168.1.100	admin	5
192.168.1.100	jsmith	1
192.168.1.88	dbadmin	1
203.0.113.45	administrator	7

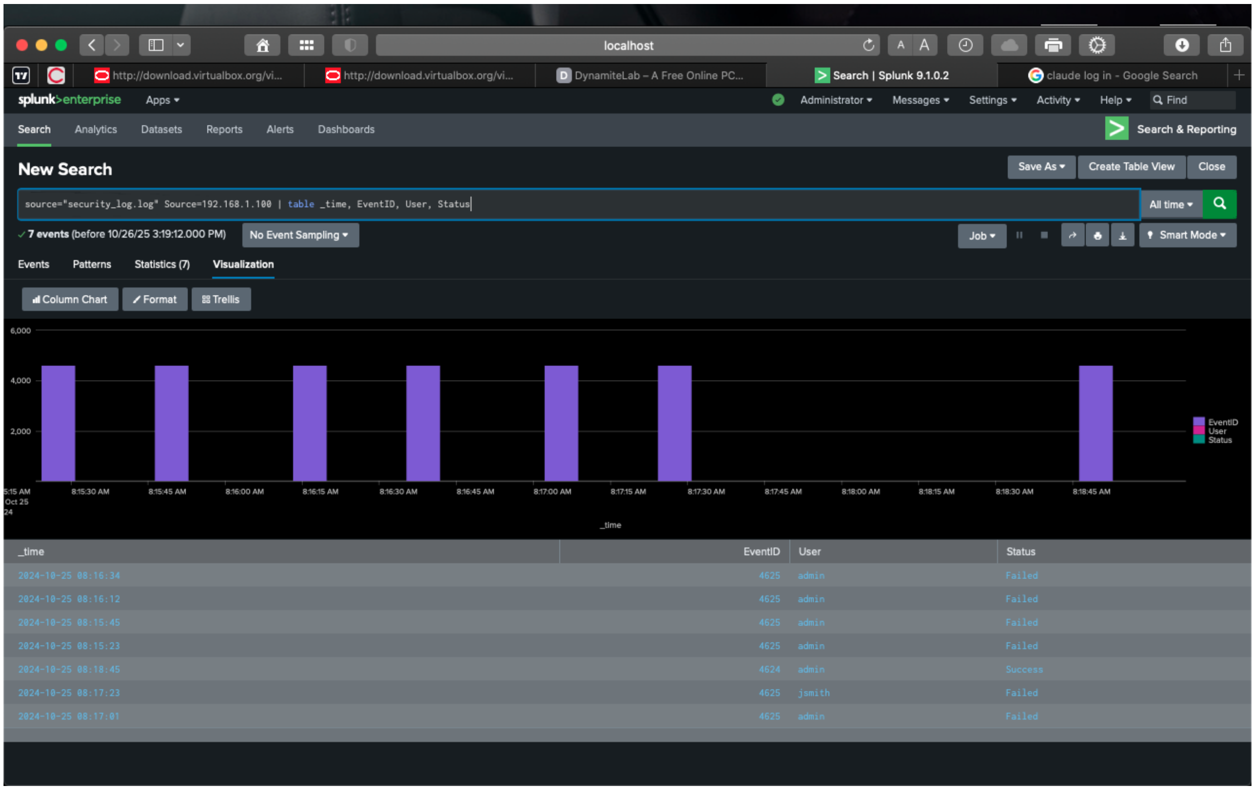


New Search

```
source="security_log.log" EventID=4625 | timechart count by User
```

✓ **15 events** (before 10/26/25 10:53:48.000 AM)

_time	admin	administrator	dbadmin	jsmith	root
2024-10-25 08:15:00	5	0	0	1	0
2024-10-25 08:20:00	0	0	0	0	0
2024-10-25 08:25:00	0	0	0	0	0
2024-10-25 08:30:00	0	0	0	0	0
2024-10-25 08:35:00	0	0	0	0	0
2024-10-25 08:40:00	0	0	0	0	0
2024-10-25 08:45:00	0	0	0	0	0
2024-10-25 08:50:00	0	0	0	0	0
2024-10-25 08:55:00	0	0	0	0	0

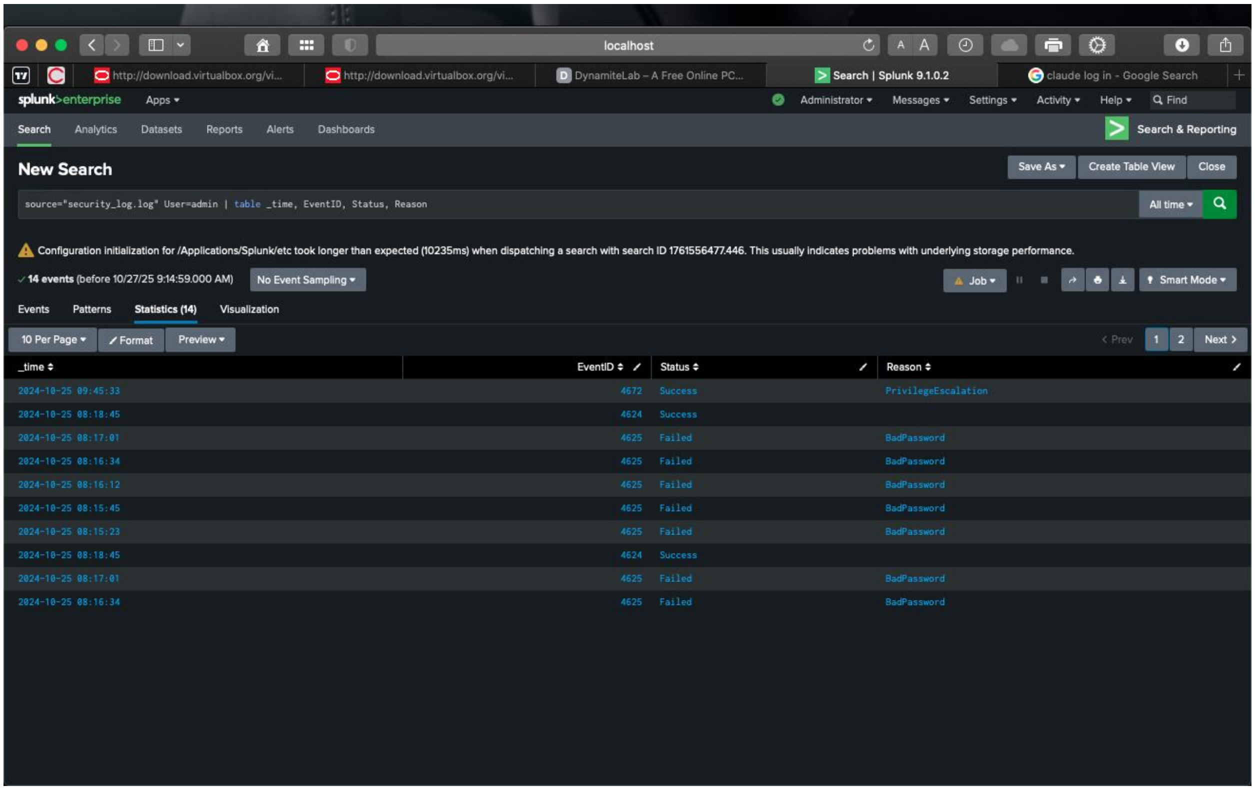


New Search

```
source="security_log.log" Source=192.168.1.100 | table _time, EventID, User, Status
```

✓ **7 events** (before 10/26/25 3:19:12.000 PM)

_time	EventID	User	Status
2024-10-25 08:16:34	4625	admin	Failed
2024-10-25 08:16:12	4625	admin	Failed
2024-10-25 08:15:45	4625	admin	Failed
2024-10-25 08:15:23	4625	admin	Failed
2024-10-25 08:18:45	4624	admin	Success
2024-10-25 08:17:23	4625	jsmith	Failed
2024-10-25 08:17:01	4625	admin	Failed



New Search

```
source="security_log.log" User=admin | table _time, EventID, Status, Reason
```

Configuration initialization for /Applications/Splunk/etc took longer than expected (10235ms) when dispatching a search with search ID 1761556477.446. This usually indicates problems with underlying storage performance.

✓ 14 events (before 10/27/25 9:14:59.000 AM)

_time	EventID	Status	Reason
2024-10-25 09:45:33	4672	Success	PrivilegeEscalation
2024-10-25 08:18:45	4624	Success	
2024-10-25 08:17:01	4625	Failed	BadPassword
2024-10-25 08:16:34	4625	Failed	BadPassword
2024-10-25 08:16:12	4625	Failed	BadPassword
2024-10-25 08:15:45	4625	Failed	BadPassword
2024-10-25 08:15:23	4625	Failed	BadPassword
2024-10-25 08:18:45	4624	Success	
2024-10-25 08:17:01	4625	Failed	BadPassword
2024-10-25 08:16:34	4625	Failed	BadPassword

1. Splunk search results - Failed login attempts
2. Statistical analysis - Brute force by Source and User
3. Timeline visualization - Failed logins over time
4. Breach confirmation - Successful login after failures
5. Privilege escalation event - EventID 4672
6. Dashboard - Security Incident Response Dashboard PDF/PNG

APPENDIX C: REFERENCES & RESOURCES

Standards & Frameworks:
- NIST SP 800-61r2: Computer Security Incident Handling Guide
- MITRE ATT&CK Framework: https://attack.mitre.org
- Security+ SY0-701 Exam Objectives
- CVSS v3.1 Scoring Guide
- CIS Critical Security Controls

Splunk Documentation:
- Splunk Search Reference: https://docs.splunk.com
- SPL Quick Reference Guide
- Dashboard Studio Documentation
- Best Practices for SIEM Deployment

Threat Intelligence:
- VirusTotal: https://virustotal.com
- AbuseIPDB: https://abuseipdb.com
- SANS Internet Storm Center
- US-CERT Advisories

Compliance Resources:
- PCI DSS v4.0 Requirements
- HIPAA Security Rule
- GDPR Articles 32-34
- SOX IT Controls Guidance

PROJECT COMPLETION DATE: October 26, 2024
ANALYST CERTIFICATION: This analysis was conducted in a controlled lab environment using simulated security event data for educational purposes.

Michael Ampo
Security Analyst
imykee85@gmail.com
http://linkedin.com/in/michael-ampo-b9181219b
https://github.com/imykee85