Security Log Analysis Report

Name: Pratham Hemraj Thakur

Date: 21 August 2025

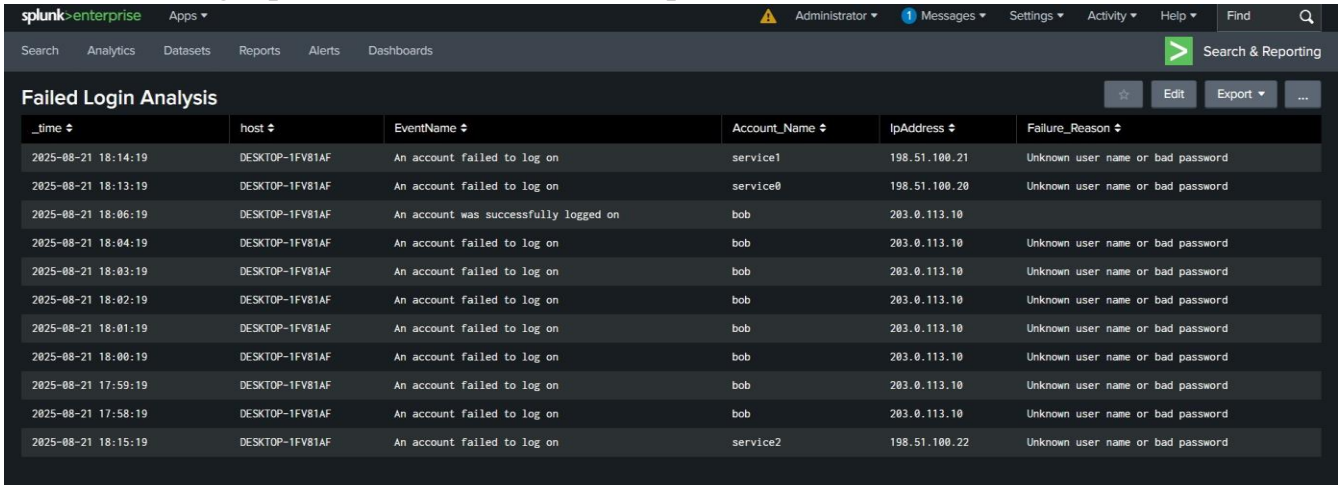
Incident Title: Multiple Security Alerts Detected Through Splunk SIEM

Summary: During routine log monitoring using Splunk SIEM, multiple suspicious activities were detected across network traffic, firewall logs, and malware alerts.

Findings & Evidences:

1. Failed Login Attempts

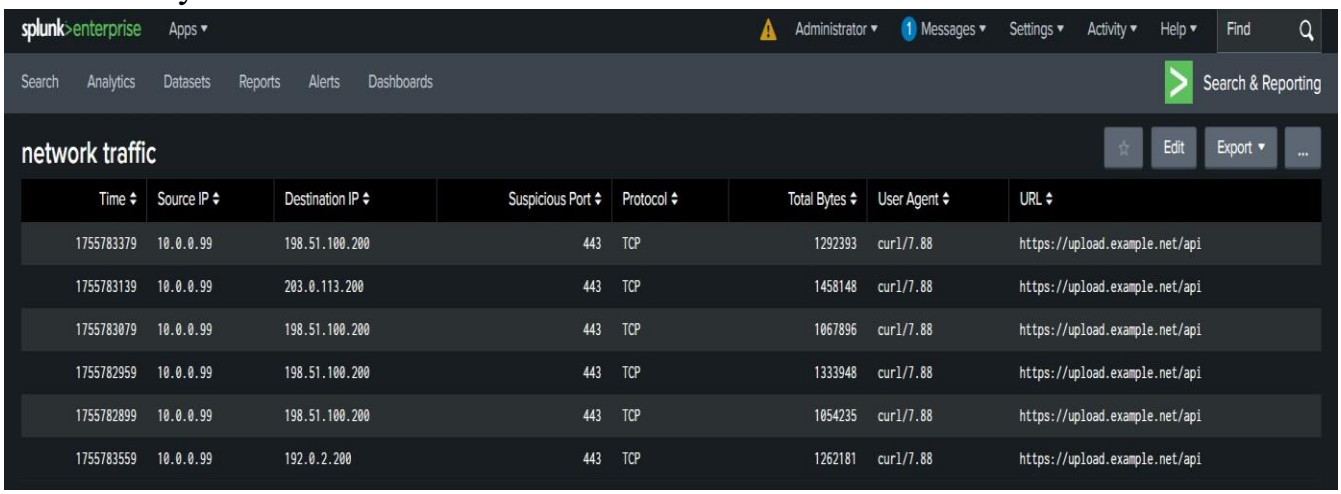
The analysis of authentication logs shows multiple failed login attempts. These attempts were primarily caused by incorrect usernames or passwords. One successful login event was also observed among the failed attempts, indicating a potential brute-force attempt.



_time	host	EventName	Account_Name	IpAddress	Failure_Reason
2025-08-21 18:14:19	DESKTOP-1FV81AF	An account failed to log on	service1	198.51.100.21	Unknown user name or bad password
2025-08-21 18:13:19	DESKTOP-1FV81AF	An account failed to log on	service0	198.51.100.20	Unknown user name or bad password
2025-08-21 18:06:19	DESKTOP-1FV81AF	An account was successfully logged on	bob	203.0.113.10	
2025-08-21 18:04:19	DESKTOP-1FV81AF	An account failed to log on	bob	203.0.113.10	Unknown user name or bad password
2025-08-21 18:03:19	DESKTOP-1FV81AF	An account failed to log on	bob	203.0.113.10	Unknown user name or bad password
2025-08-21 18:02:19	DESKTOP-1FV81AF	An account failed to log on	bob	203.0.113.10	Unknown user name or bad password
2025-08-21 18:01:19	DESKTOP-1FV81AF	An account failed to log on	bob	203.0.113.10	Unknown user name or bad password
2025-08-21 18:00:19	DESKTOP-1FV81AF	An account failed to log on	bob	203.0.113.10	Unknown user name or bad password
2025-08-21 17:59:19	DESKTOP-1FV81AF	An account failed to log on	bob	203.0.113.10	Unknown user name or bad password
2025-08-21 17:58:19	DESKTOP-1FV81AF	An account failed to log on	bob	203.0.113.10	Unknown user name or bad password
2025-08-21 18:15:19	DESKTOP-1FV81AF	An account failed to log on	service2	198.51.100.22	Unknown user name or bad password

2. Network Traffic Analysis

Suspicious outbound network traffic was detected originating from internal IP address 10.0.0.99. The traffic is directed towards multiple external IP addresses over port 443 (HTTPS). The user agent string 'curl/7.88' was identified, and repeated connections were observed to the suspicious URL: https://upload.example.net/api. This may indicate potential data exfiltration activity.



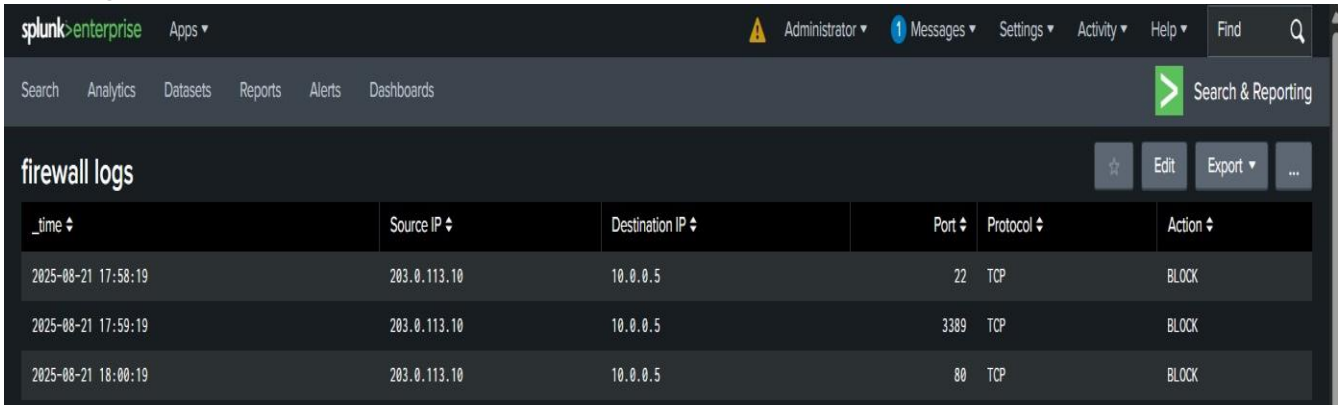
Time	Source IP	Destination IP	Suspicious Port	Protocol	Total Bytes	User Agent	URL
1755783379	10.0.0.99	198.51.100.200	443	TCP	1292393	curl/7.88	https://upload.example.net/api
1755783139	10.0.0.99	203.0.113.200	443	TCP	1458148	curl/7.88	https://upload.example.net/api
1755783079	10.0.0.99	198.51.100.200	443	TCP	1067896	curl/7.88	https://upload.example.net/api
1755782959	10.0.0.99	198.51.100.200	443	TCP	1333948	curl/7.88	https://upload.example.net/api
1755782899	10.0.0.99	198.51.100.200	443	TCP	1054235	curl/7.88	https://upload.example.net/api
1755783559	10.0.0.99	192.0.2.200	443	TCP	1262181	curl/7.88	https://upload.example.net/api

3. Firewall Logs Analysis

The firewall logs reveal multiple blocked connection attempts from the external source IP 203.0.113.10 to the internal system 10.0.0.5. The blocked ports are:

- Port 22 (SSH)
- Port 3389 (RDP)
- Port 80 (HTTP)

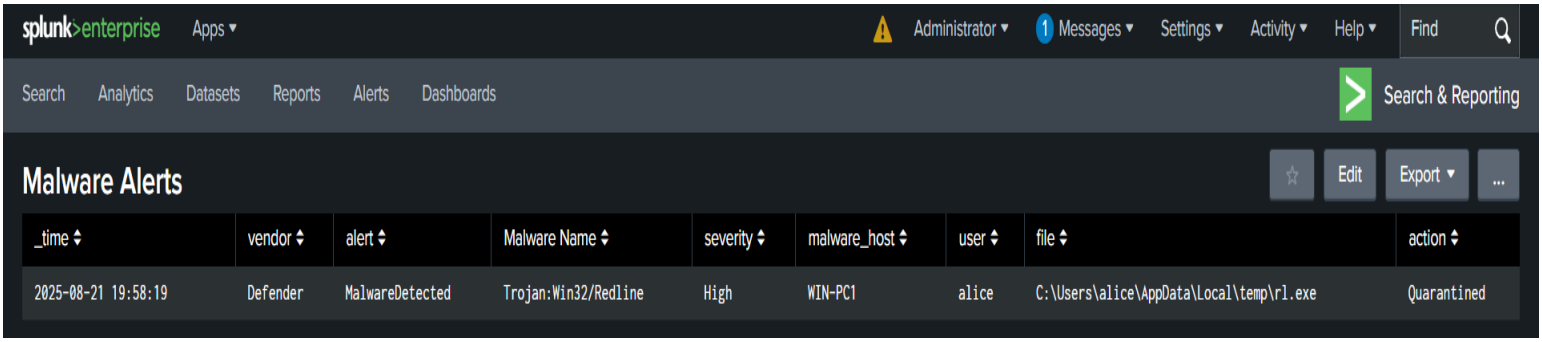
These attempts indicate possible reconnaissance or exploitation attempts against critical services.



_time	Source IP	Destination IP	Port	Protocol	Action
2025-08-21 17:58:19	203.0.113.10	10.0.0.5	22	TCP	BLOCK
2025-08-21 17:59:19	203.0.113.10	10.0.0.5	3389	TCP	BLOCK
2025-08-21 18:00:19	203.0.113.10	10.0.0.5	80	TCP	BLOCK

4. Malware Alerts :

At *2025-08-21 19:58:19*, the Defender security solution detected and quarantined **Trojan:Win32/Redline** on host **WIN-PC1** (user: *alice*). This malware is known for credential theft and data exfiltration. The quick quarantine action prevented further execution, reducing the potential impact on system integrity and data security.



_time	vendor	alert	Malware Name	severity	malware_host	user	file	action
2025-08-21 19:58:19	Defender	MalwareDetected	Trojan:Win32/Redline	High	WIN-PC1	alice	C:\Users\alice\AppData\Local\temp\rl.exe	Quarantined

Impact & Risk Assessment

- **Failed Login Attempts**: **High risk** of unauthorized access; may lead to account compromise.
- **Network Traffic**: Possible data exfiltration or malicious communication; **medium–high risk.**
- **Firewall Logs**: Repeated blocked port scans show probing activity; **medium risk.**
- **Malware Analysis**: Active malware detections (Trojan, Worm, PUA) pose **high risk** to system security and data integrity.

Recommendations / Remediation

- **Failed Login Attempts**: Enforce strong password policy, enable account lockout, and review suspicious login sources.
- **Network Traffic**: Block suspicious IPs, monitor outbound traffic, and inspect for possible C2 communication.
- **Firewall Logs**: Harden firewall rules, monitor scanning attempts, and geo-block unnecessary regions.

- **Malware Analysis:** Isolate infected host, update antivirus signatures, perform full system scan, and apply security patches.

Conclusion:

Splunk monitoring identified multiple security incidents requiring immediate mitigation
steps.

Prepared by : Pratham Hemraj Thakur