Incident Response Report

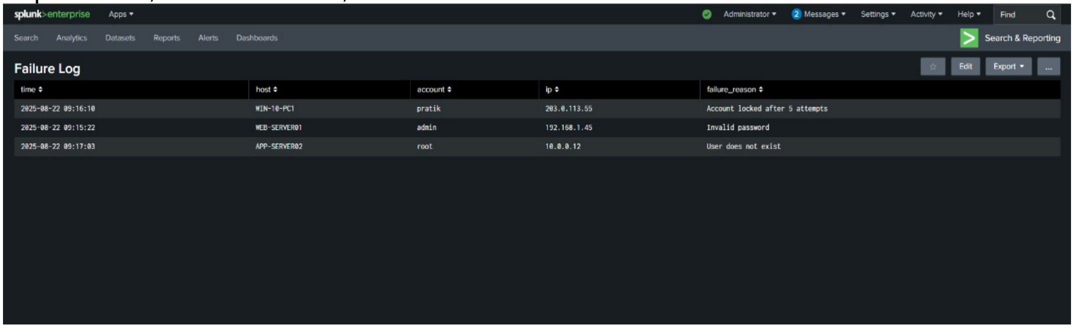
Name: **Pratik Baburao Mane**
Date: **22 August 2025**

Incident Title: Multiple Security Alerts Detected Through Splunk SIEM

Summary:
During routine log monitoring using Splunk SIEM, multiple suspicious activities were detected across failed login attempts, firewall logs, and malware alerts. This report documents the findings and provides recommendations for remediation.

Findings & Evidence:

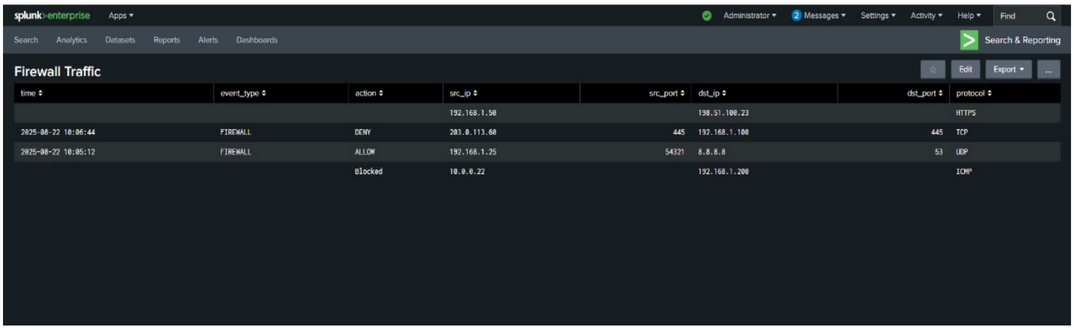
1. **Failed Login Attempts:** Multiple failed login attempts were observed with reasons such as invalid password, account locked, and user not found.



Failure Log

time	host	account	ip	failure_reason
2025-08-22 09:16:10	WIN-10-PC1	pratik	203.0.113.55	Account locked after 5 attempts
2025-08-22 09:15:22	WEB-SERVER01	admin	192.168.1.45	Invalid password
2025-08-22 09:17:03	APP-SERVER02	root	10.0.0.12	User does not exist

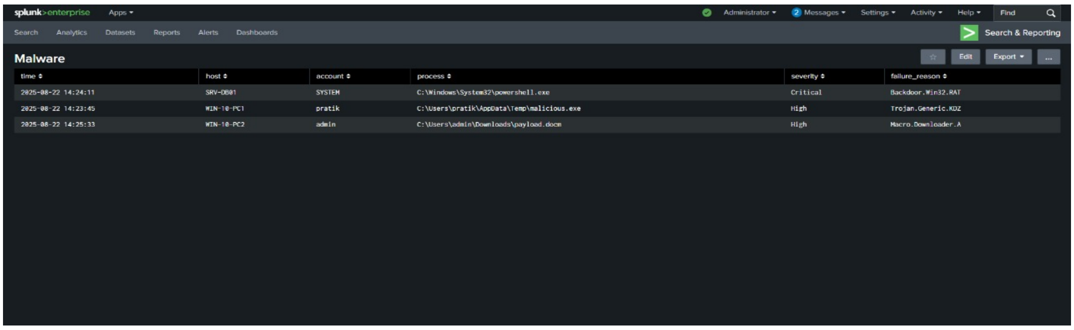
2. **Firewall Logs:** Firewall traffic showed both allowed and denied connections. Suspicious blocked connections were detected on SMB and ICMP traffic.



Firewall Traffic

time	event_type	action	src_ip	src_port	dst_ip	dst_port	protocol
			192.168.1.50		198.51.100.23		HTTPS
2025-08-22 10:06:44	FIREWALL	DENY	203.0.113.60	445	192.168.1.100	445	TCP
2025-08-22 10:05:12	FIREWALL	ALLOW	192.168.1.25	54321	8.8.8.8	53	UDP
		Blocked	10.0.0.22		192.168.1.200		ICMP

3. **Malware Alerts:** High-severity malware alerts were triggered from multiple hosts, including a Trojan, backdoor, and macro downloader.



Malware

time	host	account	process	severity	failure_reason
2025-08-22 14:24:11	SRV-DB01	SYSTEM	C:\Windows\System32\powershell.exe	Critical	Backdoor.Win32.RAT
2025-08-22 14:23:45	WIN-10-PC1	pratik	C:\Users\pratik\AppData\Temp\malicious.exe	High	Trojan.Generic.KDZ
2025-08-22 14:25:33	WIN-10-PC2	admin	C:\Users\admin\Downloads\payload.docm	High	Macro.Downloader.A

Impact & Risk Assessment:

- Failed Login Attempts: Medium risk of brute-force attacks.
- Firewall Blocked Traffic: High risk of external intrusion attempts.
- Malware Infection: Critical risk to host integrity and data security.

Recommendations / Remediation:

• Block suspicious IP addresses.
• Conduct malware removal and system patching.
• Reset compromised accounts, enforce MFA.
• Monitor RDP/SSH/SMB ports closely.
• Update antivirus signatures and Splunk detection rules.

Conclusion:

Splunk monitoring identified multiple high-risk security incidents. Immediate remediation is required to mitigate threats and secure the infrastructure.

Prepared by: **Pratik Baburao Mane**