Created by Deepak Pawar (Researcher & SOC Analyst)

SOC Incident Report

Incident Type: SSH Brute Force Attack
Environment: Windows 10 + Ubuntu + Splunk SIEM Lab

Summary:
Multiple failed login attempts were detected targeting SSH services. The alert was triggered based on threshold-based detection rules in Splunk.

Investigation:
The analyst pivoted using src_ip and user fields, correlated events across time, and confirmed repeated authentication failures from a single source.

Containment:
Fail2Ban automatically blocked the attacker IP after exceeding retry thresholds.

Lessons Learned:
Proper threshold tuning and automated response significantly reduce incident response time.