Incident Response Report

Incident Name: SSH Brute Force Leading to Successful Authentication

Severity: CRITICAL

Executive Summary

This incident involved multiple failed SSH authentication attempts from a single source IP, followed by a successful login using valid credentials. Automated detection and response mechanisms identified the threat, correlated attack behavior, and applied firewall containment to prevent further access.

Timeline of Events

- Repeated SSH authentication failures detected via journalctl
- Successful SSH login observed from the same IP address
- Privilege escalation activity identified using sudo logs
- Potential payload download activity detected (curl/wget)
- Attacker IP blocked automatically via UFW firewall rules

Detection & Analysis

Detection was performed using Bash-based correlation scripts analyzing Linux authentication logs. Threshold-based logic identified brute-force behavior, while follow-on correlation confirmed credential compromise and post-authentication activity.

Response Actions

- Automated firewall rule deployed to block attacker IP
- Incident logged and preserved for investigation
- Continuous monitoring enforced via scheduled cron execution

Impact Assessment

The incident represented a high-risk compromise scenario involving credential abuse. Automated containment limited exposure and prevented lateral movement or persistence.

MITRE ATT&CK; Mapping

- T1110: Brute Force
- T1078: Valid Accounts
- T1548: Privilege Escalation
- T1105: Ingress Tool Transfer

Lessons Learned

Early detection and correlation significantly reduced attacker dwell time. Lightweight SIEM-style tooling proved effective in low-resource environments, demonstrating the value of log-centric detection engineering.

Prepared By

Jarvis
SOC / Blue Team / Linux Security