🚨 SOC Escalation Report (L1 → L2)

Incident Type: SSH Brute Force → Account Compromise → Privilege Escalation
Severity: Critical
Affected Host: tryhackme-2404
Source IP: 10.10.242.248
Log Source: linux-alert (linux_secure)

Executive Summary

SOC monitoring identified high-volume SSH authentication failures from 10.10.242.248 targeting host tryhackme-2404. Investigation confirms a successful brute-force attack against user **john.smith**, followed by sudo-based privilege escalation and root-level activity indicating persistence.

Key Findings

- **Enumeration:** Multiple Invalid user attempts observed
- **Brute Force:** 500+ failed login attempts against john.smith
- **Compromise:** Successful SSH login (Accepted password) detected
- **Privilege Escalation:** sudo activity executed by compromised account
- **Persistence:** Root-level user creation activity identified

---

Impact Assessment

- Confirmed unauthorized access
- Administrative privileges obtained
- Persistence mechanism established
- High risk of further compromise or lateral movement

MITRE ATT&CK Mapping

- T1110 – Brute Force
- T1078 – Valid Accounts
- T1548.003 – Abuse Elevation Control Mechanism (sudo)
- T1136 – Create Account