North Star Security - Mini-Range Lab 001

Sample Final Report: Suspicious Login Investigation

A free SOC-style investigation lab for practicing alert triage, log review, evidence notes, and incident reporting.

Incident title

Suspicious SSH login for ‘asmith‘ from ‘203.0.113.77‘

Executive summary

On 2026-06-18, SSH authentication logs for ‘demo-linux-01‘ showed multiple failed login attempts from ‘203.0.113.77‘, followed by a successful password login for the active user account ‘asmith‘ at 08:17:18 UTC. The same session then attempted to run ‘sudo‘, which failed because the user was not in sudoers. The provided VPN logs show normal ‘asmith‘ VPN activity from ‘198.51.100.23‘, but no matching VPN event from ‘203.0.113.77‘. This activity should be treated as suspected unauthorized access until the user confirms the login and additional host/session evidence is reviewed.

Scope

Alert ID: NSS-LAB-001
Affected user: asmith
Affected asset/service: demo-linux-01 / SSH
Source IP: 203.0.113.77
Review window: 2026-06-18 07:30:00Z to 2026-06-18 09:30:00Z

Timeline

```
Time UTC  |  Event  |  Evidence
07:43:18  |  Normal VPN login for ‘asmith‘ from ‘198.51.100.23‘  |  ‘vpn-log.csv‘
08:12:04  |  Failed SSH login for invalid user ‘admin‘ from ‘203.0.113.77‘  |  ‘auth.log‘
08:13:47  |  Failed SSH login for ‘asmith‘ from ‘203.0.113.77‘  |  ‘auth.log‘
08:17:18  |  Successful password login for ‘asmith‘ from ‘203.0.113.77‘  |  ‘auth.log‘
08:19:43  |  Failed sudo attempt by ‘asmith‘  |  ‘auth.log‘
08:21:09  |  SSH session disconnected  |  ‘auth.log‘
```

Evidence reviewed

- SIEM alert metadata in ‘alert-summary.json‘
- SSH authentication events in ‘auth.log‘
- VPN authentication events in ‘vpn-log.csv‘
- User context in ‘user-directory.csv‘

Findings

1. ‘203.0.113.77‘ generated repeated failed SSH login attempts against invalid and valid usernames.
2. A successful password login for ‘asmith‘ occurred from the same source IP after the failed attempts.

Sample Final Report: Suspicious Login Investigation

A free SOC-style investigation lab for practicing alert triage, log review, evidence notes, and incident reporting.

3. The session attempted a privileged command through ‘sudo‘, but the attempt failed.
4. ‘asmith‘ is an active user and is not enrolled in MFA according to the provided directory data.
5. The suspicious source IP does not appear in the provided VPN log as a successful VPN session.

Impact

The evidence does not prove data theft, malware execution, or lateral movement. However, the successful login after repeated failures may indicate valid credentials were used by an unauthorized party. If unauthorized, the account could have been used to access files, run commands, stage tools, or attempt further access.

Recommended actions

1. Contact Alice Smith to validate whether the SSH login from ‘203.0.113.77‘ was expected.
2. If not immediately verified, reset the user’s password and revoke active sessions.
3. Enable MFA for ‘asmith‘ and prioritize MFA for remote access.
4. Review command history, process logs, file access, and EDR/host telemetry around 08:17-08:21 UTC.
5. Search for ‘203.0.113.77‘ and related usernames across other authentication logs.
6. Block or rate-limit the source IP where appropriate.
7. Keep the incident open until user validation and expanded evidence review are complete.

Unknowns / limitations

- The provided evidence does not include endpoint telemetry, shell history, file access logs, or user interview results.
- The source IP may require additional enrichment or validation.
- The review window may not include all related activity.

Final status

Needs validation. Treat as suspected unauthorized access pending user confirmation and expanded host review.