Mini-Range Lab 001: Suspicious Login Investigation

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

North Star Security

This is a simulated SOC-style investigation for learning and portfolio practice. It is not from a real customer environment.

Scenario

You are a junior SOC analyst reviewing an authentication alert for the demo environment. The SIEM generated an alert after multiple failed SSH login attempts were followed by a successful login for a real user account.

Alert ID: NSS-LAB-001
Alert name: Multiple SSH failures followed by success
Severity: Medium
Primary user: asmith
Primary source IP: 203.0.113.77
Primary asset: demo-linux-01
Review window: 2026-06-18 07:30:00Z to 2026-06-18 09:30:00Z

Your objective

Determine what happened, what evidence supports your conclusion, what remains unknown, and what should happen next.

You are not expected to perform live response or access real systems. Work only from the provided evidence files.

Evidence files

- ‘evidence/alert-summary.json‘ - SIEM alert metadata
- ‘evidence/auth.log‘ - Linux SSH authentication events
- ‘evidence/vpn-log.csv‘ - VPN authentication history for the same review window
- ‘evidence/user-directory.csv‘ - user/account context

Deliverables

Complete the worksheet and produce a short incident report that includes:

1. Executive summary
2. Timeline
3. Evidence reviewed
4. Findings
5. Impact
6. Recommended actions
7. Unknowns / limitations
8. Resume bullet or interview story note

Mini-Range Lab 001: Suspicious Login Investigation

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

Rules for the lab

- Separate confirmed evidence from assumptions.
- Do not claim data theft, malware, or full compromise unless the evidence proves it.
- Be honest about gaps.
- Write like someone else needs to review your work later.

Estimated time

45-75 minutes.