North Star Security - Mini-Range Lab 001

Lab 001 Student Guide

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

Mini-Range Lab 001: Suspicious Login Investigation

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

Lab 001 Student Guide

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

---

7. Unknowns / limitations
8. Resume bullet or interview story note

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.

Student Worksheet: Suspicious Login Investigation

Use this worksheet before opening the answer key.

1. Alert triage

1. What alert fired?
2. Which user account is the alert focused on?
3. Which source IP is most important?
4. Which host or service is involved?
5. What time window should you review?

2. Authentication evidence

Review ‘evidence/auth.log‘.

1. What is the first suspicious event you can find?
2. Which usernames were targeted before the successful login?
3. How many failed login attempts can you identify from the primary source IP?
4. Was there a successful login? If yes, for which user and at what time?
5. What happened after the successful login?
6. Did the user attempt any privileged or administrative action?

3. VPN and user-context evidence

Review ‘evidence/vpn-log.csv‘ and ‘evidence/user-directory.csv‘.

1. Does the suspicious source IP appear in the VPN log?
2. What source IP or device is normally associated with the affected user?
3. Is the user account active?

Lab 001 Student Guide

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

---

4. Is MFA enrolled for the affected user?
5. What context makes the activity more or less suspicious?

4. Timeline

Build a timeline with at least five rows.

```
Time UTC  |  Event  |  Evidence source  |  Why it matters
```

5. Findings

Write short answers.

1. What is confirmed?
2. What is suspected?
3. What is unknown?
4. What severity would you assign and why?
5. What immediate containment or validation step should happen first?

6. Report draft

Write a short incident report using ‘incident-report-template.md‘.

Your report should answer:

- What happened?
- What evidence supports it?
- What was the impact or possible impact?
- What should happen next?
- What still needs validation?

7. Portfolio packaging

After you finish, write:

1. One resume bullet.
2. A 4-6 sentence interview story explaining how you investigated the alert.

Incident Report Template: Suspicious Login Investigation

Incident title

Suspicious SSH login for [user] from [source IP]

Executive summary

North Star Security - Mini-Range Lab 001

Lab 001 Student Guide

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

Write 3-5 sentences explaining what happened, what evidence supports the conclusion, what risk exists, and what should happen next.

Scope

Alert ID:
Affected user:
Affected asset/service:
Source IP:
Review window:
Analyst:

Timeline

```
Time UTC  |  Event  |  Evidence
```

Evidence reviewed

- Alert summary:
- Authentication logs:
- VPN logs:
- User directory context:
- Other notes:

Findings

1. Confirmed:
2. Suspected:
3. Unknown / limitation:

Impact

Explain what could happen if the activity was unauthorized. Avoid exaggerating beyond the evidence.

Recommended actions

1. Immediate containment or validation:
2. Account/security control action:
3. Log review or monitoring action:
4. Documentation/reporting action:

Final status

Open / Needs validation / Contained / Closed

Resume bullet draft

Lab 001 Student Guide

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

Investigated [event] using [evidence sources], documented [deliverable], and recommended [action/outcome].

Resume Bullet and Interview Prompts

Use this after completing the lab and report.

Resume bullet formula

Investigated [event/finding] using [evidence sources], documented [deliverable], and recommended [action/outcome].

Example resume bullet

Investigated a simulated suspicious SSH login by analyzing authentication logs, VPN records, and user context; built a timeline, separated confirmed evidence from unknowns, and produced an incident report with containment and validation recommendations.

Short LinkedIn / portfolio summary

Completed a North Star mini-range investigation focused on suspicious login activity. Reviewed SSH authentication logs, VPN records, and user-directory context to identify a successful login after repeated failures, document evidence, and write a SOC-style incident report with recommended next steps.

Interview story prompt

Use this structure:

1. What was the alert?
2. What evidence did you review?
3. What did you confirm?
4. What stayed unknown?
5. What did you recommend?
6. What did you learn about reporting and evidence?

Example interview answer

I investigated a simulated suspicious login alert where multiple failed SSH attempts were followed by a successful password login for a real user account. I reviewed the authentication log, VPN log, and user-directory context, then built a timeline showing failed attempts, successful login, session start, and a failed sudo attempt. I concluded that the activity should be treated as suspected unauthorized access, but I avoided claiming full compromise because the lab evidence did not include user validation or endpoint telemetry. My recommended next steps were to validate with the user, reset

Lab 001 Student Guide

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

credentials if unverified, review host activity, enable MFA, and search for the source IP across other logs. The main lesson was to separate confirmed evidence from assumptions and write the report so another analyst could review it.

Evidence File Index

- ‘evidence/alert-summary.json‘
- ‘evidence/auth.log‘
- ‘evidence/vpn-log.csv‘
- ‘evidence/user-directory.csv‘