North Star Security - Mini-Range Lab 001

Student Worksheet: Suspicious Login Investigation

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

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?
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?

North Star Security - Mini-Range Lab 001

Student Worksheet: Suspicious Login Investigation

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

---

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.