

Answer Key: Suspicious Login Investigation

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

Use this after completing the worksheet.

Short conclusion

The evidence supports a suspicious SSH login for 'asmith' from '203.0.113.77' after multiple failed attempts against several usernames. A successful password login occurred after the failed attempts, followed by a failed sudo attempt. This should be treated as suspected unauthorized access until the user validates the activity and additional endpoint/session evidence is reviewed.

Key evidence

Finding | Evidence | Notes

Multiple failed SSH attempts occurred from one source | 'auth.log' entries from '203.0.113.77' between 08:12 and 08:17 UTC | Includes invalid users and real user 'asmith'
A successful login occurred | 'Accepted password for asmith from 203.0.113.77' at 08:17:18 UTC | The successful event follows several failed attempts
Post-login activity happened | Session opened, then sudo attempt rejected | Shows the session did more than authenticate
The source is not visible in VPN logs | 'vpn-log.csv' has normal 'asmith' VPN activity from '198.51.100.23', not '203.0.113.77' | This increases suspicion but does not prove compromise by itself
MFA is not enrolled for the affected user | 'user-directory.csv' lists 'asmith' with 'mfa_enrolled=no' | Control gap that should be remediated

Expected timeline

Time UTC | Event | Evidence source | Why it matters

07:43:18 | Normal VPN login for 'asmith' from '198.51.100.23' | 'vpn-log.csv' | Establishes normal context
08:12:04 | Failed SSH login for invalid user 'admin' from '203.0.113.77' | 'auth.log' | Start of suspicious source activity
08:13:47 | Failed SSH login for 'asmith' from '203.0.113.77' | 'auth.log' | Real user targeted
08:17:18 | Successful password login for 'asmith' from '203.0.113.77' | 'auth.log' | Primary concerning event
08:19:43 | Failed sudo attempt by 'asmith' | 'auth.log' | Indicates possible attempt to elevate privileges
08:21:09 | Session disconnect from '203.0.113.77' | 'auth.log' | Ends visible session in provided log window

Confirmed

- SSH authentication failures occurred from '203.0.113.77'.
- The real user account 'asmith' was targeted.
- A successful password login for 'asmith' occurred from '203.0.113.77'.
- A session opened after the successful login.
- A sudo attempt failed because 'asmith' was not in sudoers.
- The suspicious source IP does not appear as a successful VPN source in the provided VPN logs.

Answer Key: Suspicious Login Investigation

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

- 'asmith' is active and not enrolled in MFA in the provided directory data.

Suspected

- The 'asmith' account may have been accessed by an unauthorized party.
- The source IP activity looks consistent with credential guessing followed by a valid password.
- The sudo attempt may indicate post-login exploration or attempted privilege escalation.

Unknowns / limitations

- Whether Alice Smith recognizes the login.
- Whether the source IP belongs to a known remote workspace, proxy, or travel location.
- Whether any files were accessed, changed, copied, or deleted.
- Whether there were related events before or after the provided review window.
- Whether other systems saw activity from the same source IP.

Recommended actions

1. Validate with the user whether the login was expected.
2. Temporarily disable or reset credentials for 'asmith' if activity is not immediately verified.
3. Revoke active sessions where possible.
4. Enforce MFA for the affected user and prioritize MFA for all remote/admin access.
5. Review host activity around the session time for commands, file access, persistence, or lateral movement.
6. Search for '203.0.113.77' across other logs.
7. Block or rate-limit the source IP if appropriate.
8. Keep the incident open until user validation and expanded log review are complete.

Severity guidance

Medium is reasonable based on the alert because there is a successful login after suspicious failures. Escalate to High if the user denies the activity, additional suspicious commands are found, sensitive data was accessed, or lateral movement is identified.

North Star standard

A strong answer does not just say "compromised." It says what is confirmed, what is suspected, what is unknown, and what should happen next.