North Star Security - LinkedIn Attachment Resource

Incident Report Walkthrough: SSH Brute-Force Alert

A realistic sample from alert to timeline, findings, actions, and resume bullet.

North Star Security

This is a simulated example for learning and portfolio practice. It is not from a real customer environment.

Scenario

A SOC analyst receives an alert for repeated failed SSH login attempts against a demo Linux server.

Alert name: Repeated SSH authentication failures
Severity: Medium
Affected asset: demo-linux-01
Source IP: 203.0.113.42
Target service: SSH
Status: Investigated; no successful login confirmed

Executive summary

On July 1, a security alert triggered for repeated failed SSH login attempts against demo-linux-01. Authentication logs showed multiple failed attempts against common usernames over a short period. No successful login from the source IP was confirmed in the reviewed log window. Recommended actions are to block the source IP where appropriate, confirm SSH exposure and account lockout settings, review administrative access controls, and continue monitoring for related activity.

Timeline

Time	Event	Evidence
09:12	Alert triggered for repeated SSH failures	SIEM alert SSH-FAIL-1042
09:13	Analyst reviewed authentication log sample	auth.log extract
09:17	Source IP and username pattern reviewed	failed usernames: admin, root, test
09:21	Search performed for successful logins from same source	no accepted password event found
09:28	Recommended containment and monitoring actions documented	incident notes

Evidence reviewed

- SIEM alert name and ID
- Authentication log sample for the affected asset
- Failed username list
- Source IP frequency summary
- Search for successful authentication events
- Current incident notes and assumptions

North Star Security - LinkedIn Attachment Resource

Incident Report Walkthrough: SSH Brute-Force Alert

A realistic sample from alert to timeline, findings, actions, and resume bullet.

Findings

1. The source IP generated repeated failed SSH login attempts.
2. The attempted usernames were common targets for brute-force activity.
3. No successful login from the same source IP was confirmed in the reviewed time window.
4. The activity appears consistent with opportunistic brute-force scanning.
5. The remaining unknown is whether related activity occurred before or after the reviewed window.

Impact

The reviewed evidence does not confirm account compromise. However, repeated SSH authentication attempts can indicate credential guessing activity. If weak passwords, exposed administrative services, or missing lockout controls exist, this type of activity could lead to unauthorized access.

Recommended actions

1. Block or rate-limit the source IP where appropriate.
2. Confirm SSH is only exposed where needed.
3. Enforce key-based authentication or MFA for administrative access where supported.
4. Review account lockout and password policy settings.
5. Expand the log review window and monitor for similar source IPs.
6. Document the final status and evidence location.

Final report paragraph

Repeated SSH authentication failures were observed against demo-linux-01 from source IP 203.0.113.42. Reviewed authentication logs show failed attempts against common usernames, including admin, root, and test. No successful login from that source IP was confirmed in the reviewed window. The activity is consistent with brute-force scanning and should be handled through access-control review, source blocking or rate limiting, and continued monitoring.

Resume bullet version

Investigated repeated SSH brute-force activity using SIEM alerts and authentication logs, built a timeline of failed login attempts, confirmed no successful login in the reviewed window, and documented containment and monitoring recommendations.

Interview story version

I investigated a simulated SSH brute-force alert by reviewing authentication logs,

Incident Report Walkthrough: SSH Brute-Force Alert

A realistic sample from alert to timeline, findings, actions, and resume bullet.

identifying the source IP and username pattern, checking for successful login events, and writing a short incident report. The key lesson was that the report needed to separate confirmed evidence from assumptions and end with clear next actions.

North Star standard

Do not just say "brute force happened." Show the evidence, what was confirmed, what remains unknown, and what should happen next.