PORTFOLIO CASE STUDY

Detecting SSH Brute-Force Activity Through Linux Authentication Logs

Cybersecurity / SOC Analyst Practical Project

PROJECT OVERVIEW

I conducted a controlled security investigation in a Linux lab environment to simulate suspicious SSH authentication activity. The objective was to practice a SOC workflow: collect authentication evidence, identify an attack pattern, correlate events, build a timeline, assess risk, and recommend defensive controls.

Environment	Linux VM — controlled lab
Host IP	10.145.62.207
Service	OpenSSH / SSH — Port 22
Log Source	/var/log/auth.log
Target Account	analyst
Observed Source	127.0.0.1 (localhost)

THE CHALLENGE

Determine whether repeated SSH authentication failures followed by a successful login represent suspicious password-guessing behavior.

MY APPROACH

1. Verified the SSH service was active.
2. Monitored /var/log/auth.log.
3. Generated controlled failed SSH login attempts.
4. Performed a successful SSH authentication in the same lab.
5. Correlated events chronologically.
6. Identified investigation artifacts and assessed risk.
7. Proposed defensive controls.

KEY EVIDENCE

The logs showed repeated failed authentication attempts for the analyst account, followed by an accepted password and an opened SSH session.

```
Sep 05 15:11:46 — Failed password for analyst from 127.0.0.1
Sep 05 15:12:16 — Repeated failed password events
Sep 05 15:12:18 — PAM reports additional authentication failures
Sep 05 15:14:00 — Accepted password for analyst from 127.0.0.1
Sep 05 15:14:00 — SSH session opened for analyst
```

INCIDENT TIMELINE

Time	Observed activity	SOC interpretation
15:11:46	Failed SSH login	Authentication failure
15:12:16	Repeated failures	Password-guessing pattern
15:12:18	Additional PAM failures	Suspicious authentication burst
15:14:00	Password accepted	Potential successful credential guessing
15:14:00	Session opened	Authenticated access established

FINDINGS

The correlation of multiple failed SSH authentication attempts with a subsequent successful authentication is consistent with a common brute-force/password-guessing detection pattern. In a real SOC environment, this

would warrant validation of the account owner, source legitimacy, account privilege, and post-login activity.

Risk Assessment: High investigation priority

INVESTIGATION ARTIFACTS / IoCs

- Source observed: 127.0.0.1 (localhost; lab-only)
- Host IP: 10.145.62.207
- Target account: analyst
- Service: SSH / OpenSSH, port 22
- Log source: /var/log/auth.log
- Pattern: repeated failures → successful authentication → session opened

RECOMMENDED DEFENSIVE ACTIONS

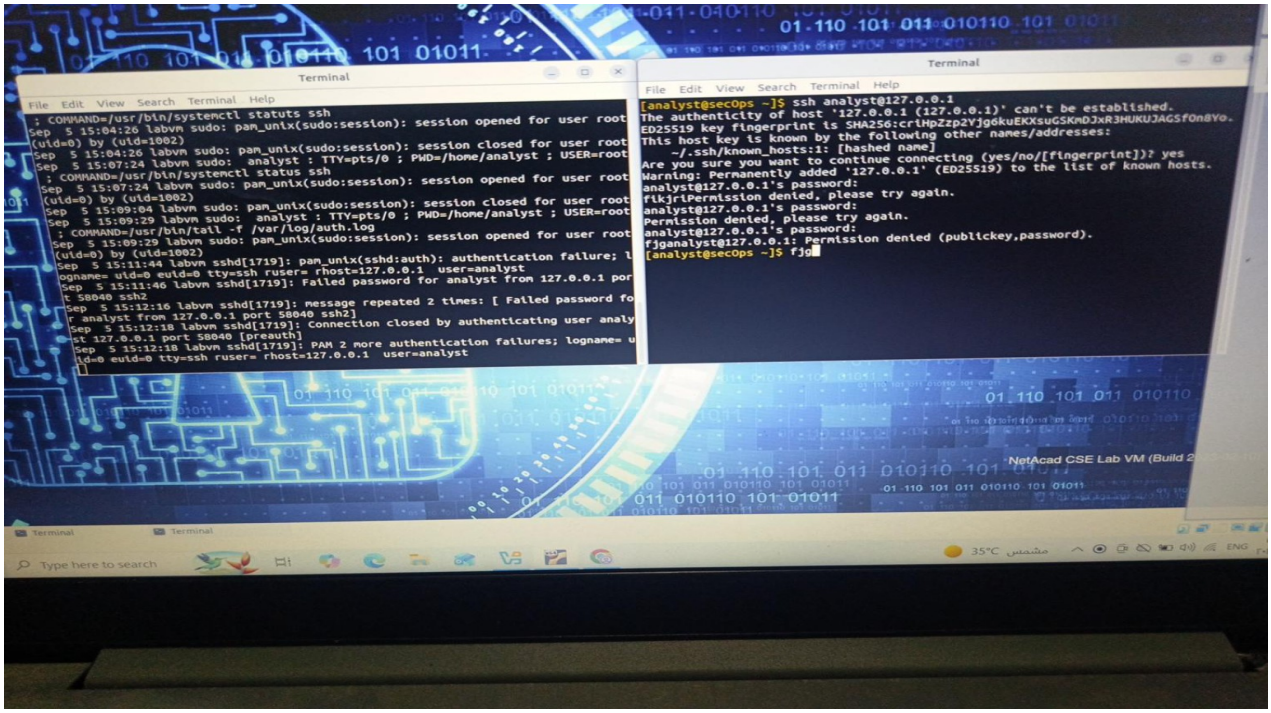
- Validate the successful login with the account owner.
- If unauthorized, terminate sessions and reset credentials.
- Review shell history, sudo activity, and surrounding authentication events.
- Prefer SSH keys and disable password authentication where appropriate.
- Enable MFA/2FA where supported.
- Deploy Fail2ban or equivalent rate limiting.
- Restrict SSH exposure with firewall rules or allowlists where feasible.
- Centralize authentication logs in a SIEM and alert on repeated failures followed by success.

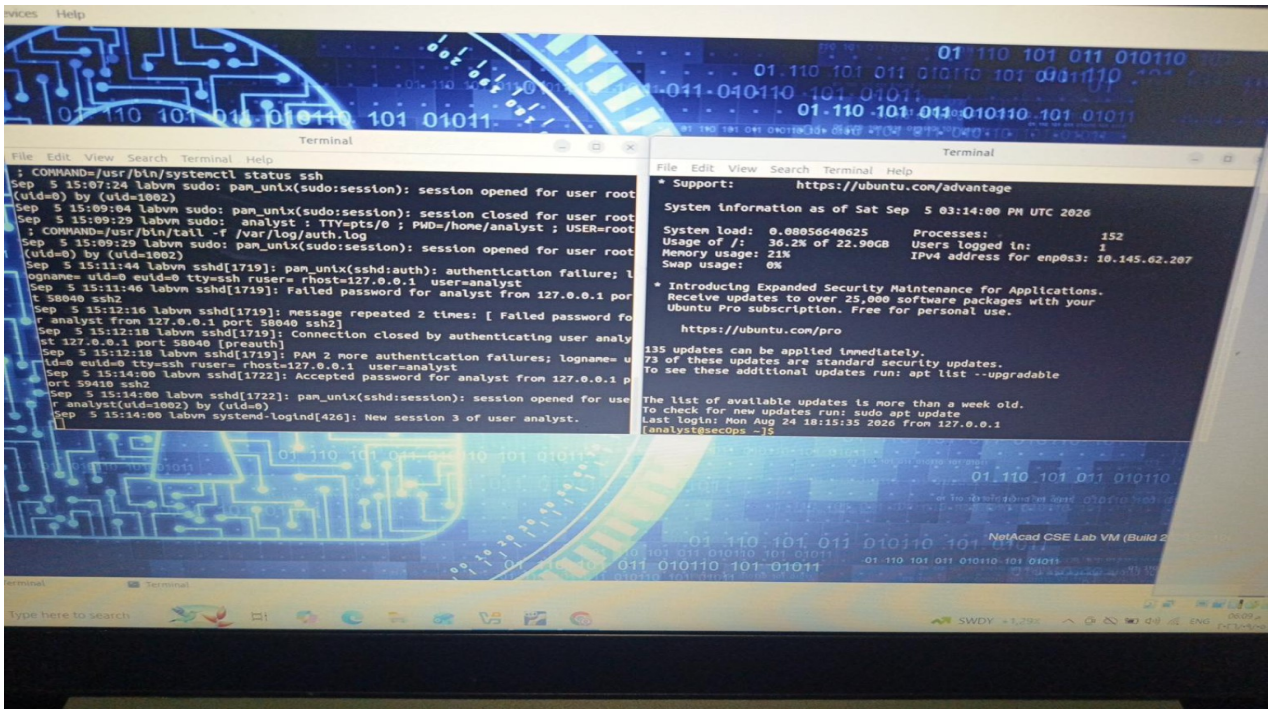
SKILLS DEMONSTRATED

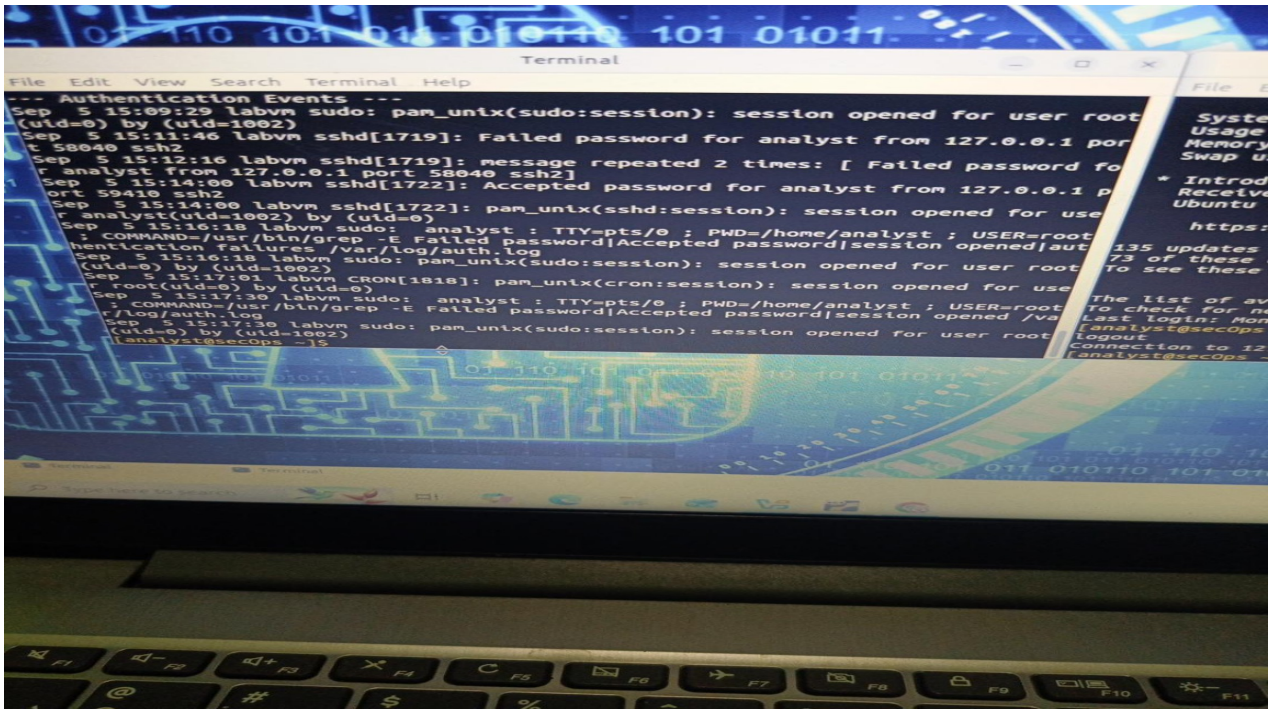
Linux Log Analysis • SSH Monitoring • Brute-Force Detection • Event Correlation • Incident Timeline Analysis • IoC Identification • Severity Assessment • Incident Response Recommendations • SOC Investigation Workflow

PRACTICAL EVIDENCE

Screenshots document the actual controlled lab execution.







IMPORTANT LAB NOTE

This project was performed as a controlled simulation. The source address 127.0.0.1 represents localhost inside the lab and is not evidence of a real external attacker. The project demonstrates the detection and analysis workflow rather than claiming a real-world compromise.

PORTFOLIO VALUE

This case study demonstrates hands-on ability to investigate Linux authentication events and communicate findings in a SOC-oriented format. It can be presented as a practical project for entry-level SOC / CyberOps opportunities.

Project Status: Completed — Practical Lab Evidence Collected