INCIDENT RESPONSE REPORT

SSH Brute Force Attack and Unauthorized Access

Following NIST SP 800-61 Rev. 2 Framework

Prepared by: Ruben

Date: February 27, 2026

Classification: Confidential

Incident ID: IR-2026-001

1. Incident Summary

Field	Details
Incident ID	IR-2026-001
Date of Incident	February 27, 2026
Date of Detection	February 27, 2026
Incident Type	SSH Brute Force Attack with Unauthorized Access
Severity	**High**
Affected System	Ubuntu Server 24.04 LTS (192.168.0.89)
Attack Source	192.168.0.67 (Kali Linux)
Status	Contained and Remediated
Handler	Ruben

2. Phase 1: Preparation

Prior to the incident, the following security controls and monitoring capabilities were in place:

2.1 Security Controls

- UFW firewall configured with default-deny incoming policy (Week 1)
- SSH key-based authentication enabled (Week 1)
- System auditing (auditd) monitoring /etc/passwd, /etc/shadow, and /var/log (Week 1)
- Splunk SIEM deployed and ingesting auth.log, syslog, and audit.log (Week 7)

2.2 Detection Capabilities

- Splunk brute force detection alert: triggers when any IP generates more than 3 failed SSH login attempts within one hour
- Security monitoring dashboard tracking failed logins, successful logins, attacker IPs, and sudo usage
- Auditd rules generating alerts on access to sensitive authentication files

Assessment: The preparation phase was adequate for detecting the attack. The SIEM was operational, log sources were configured, and detection rules were in place before the incident occurred.

3. Phase 2: Detection and Analysis

3.1 Detection Timeline

Time	Event
20:47:17	First failed SSH login attempt detected from 192.168.0.67 for user 'fakeuser'
20:47:17–20:47:34	20 rapid failed SSH login attempts from same source IP — brute force pattern identified
20:47:34	Splunk brute force detection alert triggered — IP 192.168.0.67 exceeded threshold of 3 failed attempts
20:48:xx	Successful SSH login from 192.168.0.67 as user 'ruben' — attacker gained access
20:48:xx	Commands executed: whoami, cat /etc/passwd, sudo cat /etc/shadow — credential harvesting detected
20:49:xx	Auditd alerts generated for access to /etc/passwd and /etc/shadow

3.2 Indicators of Compromise (IOCs)

IOC Type	Value	Context
Source IP	192.168.0.67	Origin of all attack traffic
Username	fakeuser	Non-existent account used in brute force
Log Pattern	20 failed logins in 17 seconds	Automated brute force attack signature
File Access	/etc/passwd, /etc/shadow	Credential harvesting post-exploitation
Log Source	/var/log/auth.log	Authentication events captured by Splunk

3.3 Analysis

The attack followed a classic brute force pattern: rapid automated login attempts against the SSH service from a single source IP. The attack targeted a non-existent username ('fakeuser'), suggesting the attacker did not have prior knowledge of valid accounts.

Following the brute force phase, a successful login occurred from the same IP address using the valid account 'ruben'. This indicates the attacker either guessed the correct credentials or obtained them through another means.

Post-access activity focused on credential harvesting — the attacker accessed /etc/passwd to enumerate user accounts and attempted to read /etc/shadow to obtain password hashes. The auditd rules configured in Week 1 detected both file access events, confirming the value of proactive system monitoring.

The speed of the attack (20 attempts in 17 seconds) confirms this was an automated tool, not a manual attempt. The Splunk brute force detection alert successfully identified the attack within the first hour of its occurrence.

4. Phase 3: Containment, Eradication, and Recovery

4.1 Containment

Immediate containment actions taken:

1. Blocked attacker IP (192.168.0.67) at the firewall: sudo ufw deny from 192.168.0.67
2. Terminated active SSH sessions from the attacker IP
3. Disabled the compromised user account temporarily: sudo usermod -L ruben

4.2 Eradication

Actions taken to eliminate the threat:

4. Reset the password for the compromised 'ruben' account
5. Regenerated SSH key pairs and removed any unauthorized public keys from ~/.ssh/authorized_keys
6. Reviewed all user accounts in /etc/passwd for unauthorized additions — none found
7. Checked for persistence mechanisms (cron jobs, startup scripts, authorized_keys) — none found
8. Verified no additional backdoors or malicious processes were running

4.3 Recovery

Steps taken to restore normal operations:

9. Re-enabled the 'ruben' account with a new strong password
10. Implemented SSH rate limiting using UFW: sudo ufw limit ssh
11. Configured fail2ban to automatically block IPs after 5 failed SSH attempts
12. Verified all services are operating normally
13. Confirmed Splunk is continuing to ingest logs and alerts are functioning

5. Phase 4: Post-Incident Activity

5.1 Lessons Learned

Finding	Gap Identified	Remediation
Brute force succeeded	No automated IP blocking after failed attempts	Deploy fail2ban for automatic IP banning
Password-based login possible	Password authentication was enabled alongside key-based auth	Disable password authentication in sshd_config

No rate limiting on SSH	Unlimited login attempts allowed	Implement UFW rate limiting: ufw limit ssh
Sensitive file access	/etc/shadow was readable with sudo	Review and restrict sudo privileges using the principle of least privilege
Detection delay	Alert runs hourly, attack completed in seconds	Switch to real-time alerting or reduce alert interval

5.2 Recommended Security Improvements

Immediate (within 24 hours):

14. Install and configure fail2ban to automatically ban IPs after 5 failed SSH attempts
15. Disable password authentication — enforce SSH key-only access
16. Apply UFW rate limiting to the SSH port

Short-term (within 1 week):

17. Implement real-time alerting in Splunk for brute force detection
18. Add network-based detection for port scanning activity
19. Configure log forwarding redundancy to prevent log tampering
20. Review and restrict sudo access to only necessary commands

Long-term:

21. Deploy a host-based intrusion detection system (OSSEC or Wazuh)
22. Implement multi-factor authentication for SSH access
23. Establish a formal incident response plan with defined roles and escalation procedures
24. Conduct regular penetration testing to identify new vulnerabilities

6. Conclusion

This incident demonstrated both the effectiveness and limitations of the current security monitoring infrastructure. The SIEM successfully detected the brute force attack through log ingestion and alerting, and the auditd rules provided visibility into post-exploitation credential harvesting activity.

However, the incident also revealed gaps: the absence of automated blocking (fail2ban), the availability of password-based authentication alongside key-based access, and the hourly alert schedule that introduced detection delay. All of these gaps have been addressed in the remediation plan.

The NIST SP 800-61 framework provided a structured approach to handling the incident through all four phases: preparation, detection, containment, and post-incident improvement. Following this framework ensures that each incident not only gets resolved but also strengthens the overall security posture for future events.

7. Evidence and Artifacts

The following evidence was preserved during incident handling:

- Splunk search results showing 20 failed SSH login attempts from 192.168.0.67
- Splunk brute force detection alert trigger log
- Splunk dashboard showing attack activity across all four monitoring panels
- Auditd logs showing /etc/passwd and /etc/shadow access events
- Raw auth.log entries preserved in Splunk index