Incident Report

SSH Brute Force Attack – Unauthorized System Access

Incident ID: SOC-2025-001
Incident Type: SSH Brute Force with Successful Authentication
Date of Incident: 24 December 2025
Report Date: 25 December 2025
Prepared By: Ronnakrit Woralakpakdee
Environment: Ubuntu Linux Server
Severity: HIGH

1. Executive Summary

On 24 December 2025, the Security Operations Center (SOC) identified suspicious SSH authentication activity targeting an Ubuntu server. Multiple failed login attempts were observed from a single external IP address within a short time window, indicating a brute-force attack. Shortly afterward, a successful authentication was recorded, confirming unauthorized system access.

Based on the available evidence, the incident was classified as a True Positive high-severity security event due to confirmed compromise of valid credentials and the risk of further malicious activity.

2. Incident Scope & Identification

Target System:
Ubuntu Linux Server (SSH service enabled)

Impacted Account:
ubuntu

Source IP Address:
192.168.56.102

Authentication Method:
Password-based SSH login

Incident Timeframe:
24 December 2025 — 18:43:08 to 18:43:41 (UTC+7)

Scope Definition:
This incident covers all SSH authentication attempts against the ubuntu account originating from IP address 192.168.56.102 during the identified timeframe.

3. Timeline Analysis

Authentication logs recorded on the server indicate the following sequence of events:

- 18:43:08 — First failed SSH authentication attempt detected
- 18:43:08–18:43:26 — Multiple failed authentication attempts recorded in rapid succession, targeting the same account (ubuntu) from the same source IP
- 18:43:31 — A successful SSH authentication was recorded
- 18:43:41 — A second successful authentication occurred from the same IP

Interpretation

The frequency and persistence of authentication failures strongly indicate an automated brute-force attack rather than normal user activity.
The subsequent successful authentication confirms credential compromise.

4. Attack Pattern Analysis

Log evidence demonstrates the following characteristics:

- Repeated “Failed password” messages
- Attempts against the same local user account
- Attempts originating from the same source IP
- Frequent connection resets consistent with automated retries
- Eventual successful authentication

Pattern Conclusion

The attack consists of repeated password-guessing attempts until a valid credential is discovered — consistent with SSH brute-force / password-spraying behavior.

5. Incident Classification

This incident was classified as a True Positive Security Incident based on:

- High volume of failed authentication attempts
- Abnormal login behavior
- Subsequent successful login
- Activity originating from a single external IP

- No indication of legitimate user testing

The attack successfully resulted in unauthorized system access.

6. Impact Assessment

Confirmed Impact

- Unauthorized user-level access to the server

Potential Impact

- Credential theft
- Privilege escalation
- Lateral movement inside network
- Sensitive data exposure
- Execution of malicious commands or tools

7. Severity Assessment

Severity Level: HIGH

Justification

- External threat actor
- Valid credentials compromised
- Remote authenticated access obtained
- Business-impacting risk exists
- Further compromise possible

This classification aligns with common SOC severity scoring methodologies.

8. MITRE ATT&CK Mapping

This incident was mapped against the MITRE ATT&CK Framework to classify the adversary behavior and identify the related attack lifecycle stages. The activities observed during the incident correspond to techniques within the **Credential Access** and **Initial Access** tactics.

8.1 Technique — Brute Force (T1110)

Tactic: Credential Access
Technique ID: T1110 — Brute Force

Description:
The attacker repeatedly attempted to authenticate to the SSH service using multiple password guesses in rapid succession. The failed authentication attempts were directed at the same local user account and originated from a single external IP address. This behavior is consistent with automated brute-force password-guessing activity.

Observed Evidence:

- Multiple **"Failed password"** log entries for the user account ubuntu
- Attempts occurred within seconds of each other
- All login attempts originated from the same source IP address 192.168.56.102

SOC Assessment:
This activity demonstrates an intentional effort to gain access through repeated password-guessing attempts, indicating malicious intent rather than normal user behavior.

8.2 Technique — Valid Accounts (T1078)

Tactic: Initial Access
Technique ID: T1078 — Valid Accounts

Description:
After successfully identifying the correct password during the brute-force phase, the attacker authenticated to the server using the compromised account credentials. Because the access was obtained using a legitimate account, the activity would appear valid from an authentication standpoint and may evade basic security controls.

Observed Evidence:

- Log entries showing **"Accepted password"** for the user account ubuntu
- Successful SSH session creation from the same attacking IP address

- No indication that the login was initiated by a legitimate user

SOC Assessment:
This confirms that the attacker obtained valid credentials and used them to gain authenticated access to the target system.

8.3 MITRE-Based Attack Flow Summary

The incident followed this progression:

1. Credential Access – Brute Force (T1110)
The attacker attempted multiple SSH password guesses against the ubuntu account.

2. Initial Access – Valid Accounts (T1078)
Once the correct password was discovered, the attacker successfully authenticated and gained interactive access to the system.

8.4 MITRE Technique Summary Table

Tactic	Technique	Technique ID	Status
Credential Access	Brute Force	T1110	Observed
Initial Access	Valid Accounts	T1078	Observed

8.5 MITRE Summary

Mapping the incident to MITRE ATT&CK confirms that this event represents a **credential-based compromise**, beginning with brute-force password attempts and resulting in successful authenticated system access. This activity aligns with common intrusion techniques used by threat actors to gain initial foothold into target systems.

9. Response & Mitigation Actions

Following the identification of the SSH brute-force attack and confirmation of successful unauthorized authentication, the SOC initiated incident response procedures to contain the threat, limit further exposure, and remediate the affected environment.

9.1 Detection & Verification

The incident was initially identified through abnormal SSH authentication activity recorded in the system authentication logs. Repeated login failures followed by successful authentication from the same external IP address indicated credential compromise. The SOC verified the incident severity based on confirmed user-level system access.

9.2 Containment Actions

Immediate containment steps were taken to prevent further unauthorized access, including:

- Resetting the password associated with the compromised ubuntu account
- Terminating any active SSH sessions originating from the attacker IP
- Reviewing system accounts to ensure no additional credentials were compromised
- Preserving authentication logs for forensic review

These actions ensured that the attacker no longer retained valid system access.

9.3 Eradication & System Review

A focused examination of the affected host was conducted to identify any signs of persistence or privilege escalation. The review included:

- Examination of SSH login history and session artifacts
- Review of **sudo** command logs
- Inspection of **cron** jobs, startup entries, and authorized key files
- Verification of system integrity indicators

No malicious persistence mechanisms or unauthorized privilege escalation attempts were identified during the investigation.

9.4 Recovery Actions

To prevent recurrence of similar credential-based attacks, the following recovery measures were implemented:

- Password-based SSH authentication was disabled
- Key-based authentication was enforced for all SSH access
- SSH access was restricted to trusted IP ranges only
- Brute-force protection controls such as login throttling and lockout policies were implemented
- Centralized authentication log monitoring and alerting were enabled

These changes significantly reduced external attack surface exposure.

10. Lessons Learned

This incident reinforced several key security principles regarding credential protection and external remote access exposure:

- Password-based SSH authentication presents a high-risk entry point for brute-force and credential-stuffing attacks
- Continuous monitoring of authentication activity is essential for early detection of intrusion attempts
- Layered security controls (network restrictions, MFA/key-based authentication, monitoring, and throttling) provide effective defense-in-depth
- Clear incident response procedures enable rapid containment and risk reduction

Going forward, proactive security hardening and ongoing monitoring will remain critical to minimizing the risk of credential-based compromise.

11. Conclusion

This incident confirms that the system was exposed to a credential-based brute-force attack that successfully resulted in unauthorized authenticated SSH access. While no evidence of further malicious activity or persistence was identified, the event represents a high-severity security compromise due to confirmed account credential misuse.

The implementation of preventive security controls — including disabling password authentication, restricting SSH access, and improving monitoring — has significantly strengthened the organization’s security posture and reduced the likelihood of similar incidents recurring in the future.

12. Recommendations

1. Require key-based SSH authentication for all systems
2. Enforce strong credential policies and periodic password rotation
3. Restrict SSH access to trusted networks or VPN-only access
4. Implement account lockout or throttling for repeated failed logins
5. Deploy SIEM-based monitoring and automated alerting
6. Perform periodic authentication log review
7. Conduct regular security awareness training

13. Evidence References

The following evidence supports the conclusions in this report:

- Figure 1 — SSH Timeline Log
  Showing multiple failed authentication events followed by successful logins
- Figure 2 — Filtered SSH Failed Login Attempts
  Demonstrating repetitive brute-force behavior
- Figure 3 — Successful SSH Login Session Screenshot
  Confirming unauthorized system access

Full log files retained separately for forensic integrity.

14. Appendix

```
ubuntu@ubuntu:~$ cat Desktop/SOC-Incident/Evidence/Timeline/incident-timelines.log
2025-12-24T18:43:08.131223+07:00 ubuntu sshd[2815]: Failed password for ubuntu from 192.168.56.102 port 35546 ssh2
2025-12-24T18:43:08.277207+07:00 ubuntu sshd[2815]: Failed password for ubuntu from 192.168.56.102 port 35546 ssh2
2025-12-24T18:43:10.892248+07:00 ubuntu sshd[2827]: Failed password for ubuntu from 192.168.56.102 port 35556 ssh2
2025-12-24T18:43:11.025113+07:00 ubuntu sshd[2827]: Failed password for ubuntu from 192.168.56.102 port 35556 ssh2
2025-12-24T18:43:12.449058+07:00 ubuntu sshd[2829]: Failed password for ubuntu from 192.168.56.102 port 46078 ssh2
2025-12-24T18:43:12.576223+07:00 ubuntu sshd[2829]: Failed password for ubuntu from 192.168.56.102 port 46078 ssh2
2025-12-24T18:43:13.802103+07:00 ubuntu sshd[2831]: Failed password for ubuntu from 192.168.56.102 port 46090 ssh2
2025-12-24T18:43:13.935570+07:00 ubuntu sshd[2831]: Failed password for ubuntu from 192.168.56.102 port 46090 ssh2
2025-12-24T18:43:15.144083+07:00 ubuntu sshd[2833]: Failed password for ubuntu from 192.168.56.102 port 46100 ssh2
2025-12-24T18:43:15.280587+07:00 ubuntu sshd[2833]: Failed password for ubuntu from 192.168.56.102 port 46100 ssh2
2025-12-24T18:43:16.341663+07:00 ubuntu sshd[2835]: Failed password for ubuntu from 192.168.56.102 port 46110 ssh2
2025-12-24T18:43:16.480437+07:00 ubuntu sshd[2835]: Failed password for ubuntu from 192.168.56.102 port 46110 ssh2
2025-12-24T18:43:17.545187+07:00 ubuntu sshd[2837]: Failed password for ubuntu from 192.168.56.102 port 46114 ssh2
2025-12-24T18:43:17.681804+07:00 ubuntu sshd[2837]: Failed password for ubuntu from 192.168.56.102 port 46114 ssh2
2025-12-24T18:43:18.827200+07:00 ubuntu sshd[2840]: Failed password for ubuntu from 192.168.56.102 port 46118 ssh2
2025-12-24T18:43:18.952864+07:00 ubuntu sshd[2840]: Failed password for ubuntu from 192.168.56.102 port 46118 ssh2
2025-12-24T18:43:20.053402+07:00 ubuntu sshd[2842]: Failed password for ubuntu from 192.168.56.102 port 46120 ssh2
2025-12-24T18:43:20.197374+07:00 ubuntu sshd[2842]: Failed password for ubuntu from 192.168.56.102 port 46120 ssh2
2025-12-24T18:43:21.144511+07:00 ubuntu sshd[2844]: Failed password for ubuntu from 192.168.56.102 port 55252 ssh2
2025-12-24T18:43:21.276630+07:00 ubuntu sshd[2844]: Failed password for ubuntu from 192.168.56.102 port 55252 ssh2
2025-12-24T18:43:22.404926+07:00 ubuntu sshd[2846]: Failed password for ubuntu from 192.168.56.102 port 55254 ssh2
2025-12-24T18:43:22.539820+07:00 ubuntu sshd[2846]: Failed password for ubuntu from 192.168.56.102 port 55254 ssh2
2025-12-24T18:43:24.100017+07:00 ubuntu sshd[2848]: Failed password for ubuntu from 192.168.56.102 port 55258 ssh2
2025-12-24T18:43:24.225720+07:00 ubuntu sshd[2848]: Failed password for ubuntu from 192.168.56.102 port 55258 ssh2
2025-12-24T18:43:25.320662+07:00 ubuntu sshd[2850]: Failed password for ubuntu from 192.168.56.102 port 55272 ssh2
2025-12-24T18:43:25.462988+07:00 ubuntu sshd[2850]: Failed password for ubuntu from 192.168.56.102 port 55272 ssh2
2025-12-24T18:43:26.806226+07:00 ubuntu sshd[2852]: Failed password for ubuntu from 192.168.56.102 port 55288 ssh2
2025-12-24T18:43:26.936073+07:00 ubuntu sshd[2852]: Failed password for ubuntu from 192.168.56.102 port 55288 ssh2
2025-12-24T18:43:31.789829+07:00 ubuntu sshd[2854]: Accepted password for ubuntu from 192.168.56.102 port 55294 ssh2
2025-12-24T18:43:41.362757+07:00 ubuntu sshd[2941]: Accepted password for ubuntu from 192.168.56.102 port 54124 ssh2
ubuntu@ubuntu:~$
```

Figure 1 — SSH Timeline Log

```
ubuntu@ubuntu:~/Desktop/SOC-Incident/Evidence/Filtered$ grep "Failed password" incident-ssh.log | sed -n "1,6p"
2025-12-24T10:44:23.879998+07:00 ubuntu sshd[2802]: Failed password for ubuntu from 192.168.56.102 port 39212 ssh2
2025-12-24T10:44:47.254084+07:00 ubuntu sshd[2802]: message repeated 2 times: [ Failed password for ubuntu from 192.168.
56.102 port 39212 ssh2]
2025-12-24T11:27:05.620460+07:00 ubuntu sshd[3065]: Failed password for ubuntu from 192.168.56.102 port 47378 ssh2
2025-12-24T11:27:12.221529+07:00 ubuntu sshd[3065]: message repeated 2 times: [ Failed password for ubuntu from 192.168.
56.102 port 47378 ssh2]
2025-12-24T11:27:17.514484+07:00 ubuntu sshd[3067]: Failed password for ubuntu from 192.168.56.102 port 44420 ssh2
2025-12-24T11:27:17.669961+07:00 ubuntu sshd[3067]: Failed password for ubuntu from 192.168.56.102 port 44420 ssh2
ubuntu@ubuntu:~/Desktop/SOC-Incident/Evidence/Filtered$
```

Figure 2 — Failed Attempts Log

```
┌──(kali㉿kali)-[~]
└─$ ssh ubuntu@192.168.56.101
ubuntu@192.168.56.101's password:
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.14.0-37-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

Expanded Security Maintenance for Applications is not enabled.

151 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your In
ternet connection or proxy settings

Last login: Wed Dec 24 08:27:26 2025 from 192.168.56.102
ubuntu@ubuntu:~$
```

Figure 3 — Successful Login Session