
🛡️Security Incident Report: SSH Access Review

📅Date Range Reviewed

July 11, 2025 — July 12, 2025 (UTC)

🖥️Affected System

- **Hostname:** `ip-172-31-38-189`
- **Instance ID:** `i-0cfa212979575969f`
- **Cloud Provider:** AWS EC2
- **OS:** Ubuntu 24.04.2 LTS (Noble Numbat)
- **Architecture:** x86_64
- **Agent:** Filebeat 9.0.3
- **Logging Source:** `/var/log/auth.log`

🔍Summary

This report analyzes SSH login activity captured on the EC2 instance from authentication logs collected via Filebeat and visualized in Kibana. The review covers both legitimate access and potentially malicious login attempts, with a focus on geolocation, frequency, and authentication outcomes.

🔗Successful SSH Logins

Legitimate access was detected from a consistent IP block in San Antonio, Texas. All logins used the `publickey` method, indicating key-based authentication.

Timestamp (UTC)	Source IP	City, Region	Org (ASN)	User	Method	Outcome
2025-07-11 22:08:02	216.76.55.177	San Antonio, TX	BELLSOUTH-NET-BLK	ubuntu	publickey	✅ Accepted
2025-07-11 22:17:10	216.76.55.177	San Antonio, TX	BELLSOUTH-NET-BLK	ubuntu	publickey	✅ Accepted
2025-07-11 23:13:26	216.76.55.177	San Antonio, TX	BELLSOUTH-NET-BLK	ubuntu	publickey	✅ Accepted

Timestamp (UTC)	Source IP	City, Region	Org (ASN)	User	Method	Outcome
2025-07-11 23:46:12	216.76.55.177	San Antonio, TX	BELLSOUTH-NET-BLK	ubuntu	publickey	✅ Accepted
2025-07-12 13:45:56	216.76.55.145	San Antonio, TX	BELLSOUTH-NET-BLK	ubuntu	publickey	✅ Accepted

---

🔩Failed SSH Attempts (Suspicious Activity)

Multiple failed SSH login attempts were recorded from globally distributed IPs, likely indicative of brute-force or credential stuffing bots.

Timestamp (UTC)	Source IP	Location	Org (ASN)	Username	Outcome
2025-07-11 22:08:26	166.155.4.51	Oklahoma City, OK	CELLCO-PART (Verizon)	`a`	❌ Invalid
2025-07-12 00:37:05	47.239.244.99	Hong Kong	Alibaba US Technology Co.	*(blank)*	❌ Invalid
2025-07-12 01:29:57	47.251.168.129	California, US	Alibaba US Technology Co.	*(blank)*	❌ Invalid
2025-07-12 09:32:30	138.2.109.83	Singapore	Oracle-BMC	*(blank)*	❌ Invalid

---

🔍Threat Analysis

- **Consistency in Source IP:** All successful logins originated from Texas IPs under the same ASN, suggesting a likely trusted admin or service.
- **Geographic Disparity:** Failed logins came from Asia, California, and Oklahoma — not previously associated with successful sessions.
- **Username Patterns:** Most failed attempts lacked a username or used a single character (e.g., `a`), a common brute-force signature.
- **Timing:** Clustered attempts in early UTC hours indicate automated scanning behavior.

🛡️Recommendations

🔒Access Control

- Restrict SSH access via AWS Security Groups to known static IPs.
- Change SSH port from `22` to a high-numbered, non-standard port.
- Disable password authentication in `/etc/ssh/sshd_config`:

```
PasswordAuthentication no
PermitRootLogin no
AllowUsers ubuntu
```

🦯Detection & Response

- Install and configure **Fail2Ban** or equivalent to block brute-force attempts.
- Monitor logs for repeated failed SSH attempts from the same IPs.
- Set Kibana/Elastic alerts:
- More than 5 failed logins in 5 minutes
- SSH from unknown geographic regions

🔐SSH Key Hygiene

- Audit `~/.ssh/authorized_keys` for unauthorized or outdated keys.
- Rotate all SSH keys and reissue them only to trusted users.

📊Suggested Kibana Visualizations

- Geo map of login attempts
- Bar chart: Success vs. Failure counts per hour
- Table: Top IPs by login failures

Conclusion

While no unauthorized access was successful, your logs indicate that your EC2 instance is **actively targeted** by external IPs. The best defense includes reducing the attack surface, tightening authentication controls, and enabling real-time detection.

Report generated via log analysis and enrichment from Filebeat/Kibana data on 2025-07-12.