**Incident Response Report**

**Date:** August 11, 2025  
**Prepared by:** Nnaji Daniel Chinweoke  
**Environment:** Elastic Stack 7.x (Elasticsearch, Kibana, Filebeat, Logstash)  
**Data Source:** auth\_sim.log (ingested via Filebeat)

**1. Executive Summary**

On August 11, 2025, at 20:00:01, the SIEM system detected suspicious SSH authentication activity targeting the system testhost. The logs indicate a **failed password attempt for an invalid user account (admin)** originating from IP address 10.1.2.3.

This activity matches known patterns of **SSH brute-force or reconnaissance attacks**, where an attacker attempts to gain unauthorized access by repeatedly guessing usernames and passwords.

**2. Incident Timeline**

| **Time (UTC+1)** | **Event Description** |
| --- | --- |
| 20:00:01 | Failed SSH login for invalid user admin from IP 10.1.2.3 on port 5001 |
| (No further events yet) | Further analysis required to check for repeated attempts from same source |

**3. Technical Findings**

**Log Source:** C:\ELK\sample\_logs\auth\_sim.log  
**Filebeat Index:** filebeat-\*  
**Log Extract:**

Aug 11 20:00:01 testhost sshd[1234]: Failed password for invalid user admin from 10.1.2.3 port 5001 ssh2

**Key Observations:**

* **Attacker IP:** 10.1.2.3 (internal simulation; in production this would likely be an external IP)
* **Attack Type:** SSH brute-force / enumeration attempt
* **Target Service:** sshd
* **Target Username:** admin (invalid account on system)
* **Connection Port:** 5001 (non-standard SSH port; attacker is scanning multiple ports or system uses custom configuration)
* **Program:** sshd
* **Host:** testhost

**4. Risk Assessment**

* **Likelihood:** Medium – Brute-force attacks are common and often automated.
* **Impact if Successful:** High – Could result in unauthorized system access, privilege escalation, and data compromise.
* **Current Status:** No successful login detected in this log sample.

**5. Root Cause Analysis**

The log entry shows a **failed SSH login attempt** using an invalid username.  
Such attempts typically originate from:

* Automated scanning tools (e.g., Hydra, Ncrack, or botnets)
* Threat actors probing systems for weak credentials
* Internal penetration testing activities (in this case, simulated)

The non-standard port (5001) may indicate:

* The attacker is scanning multiple ports for SSH services.
* The service is intentionally running on a non-default port to avoid basic scans.

**6. Incident Response Actions**

**Containment:**

* Block IP 10.1.2.3 at firewall:

sudo ufw deny from 10.1.2.3

# or

sudo iptables -A INPUT -s 10.1.2.3 -j DROP

* Enable SSH rate-limiting with fail2ban.

**Eradication:**

* Verify no successful logins from suspicious IP in /var/log/auth.log.
* Check for unauthorized SSH keys in /home/\*/.ssh/authorized\_keys.

**Recovery:**

* Rotate passwords for all accounts.
* Disable password-based SSH authentication; use key-based authentication only.

**7. Recommendations**

1. **Enable Multi-Factor Authentication (MFA)** for privileged accounts.
2. **Harden SSH Configurations** in /etc/ssh/sshd\_config:
   * Set PermitRootLogin no
   * Set PasswordAuthentication no
3. **Implement Network Segmentation** to limit SSH exposure.
4. **Continuous Monitoring** using Kibana dashboards for real-time anomaly detection.
5. **Threat Intelligence Integration** to automatically flag known malicious IPs.

**8. Conclusion**

The SIEM successfully detected and logged a simulated SSH brute-force attempt. While no breach occurred in this test scenario, in a production environment such events require **immediate investigation** and **preventive measures** to reduce the risk of compromise.