

INCIDENT FINAL REPORT – SOC Capstone (BazTech)

Executive Summary

On August 8, 2025, the BazTech SOC team conducted a controlled simulation of brute-force attacks across a segmented network environment. A Kali Linux host attempted to gain unauthorized access to:

- Ubuntu DMZ server (SSH) – 45 failed login attempts against user accounts 'admin' and 'sage2025'.
- Windows 10 workstation (RDP) – 6 failed login attempts against 'Administrator'.

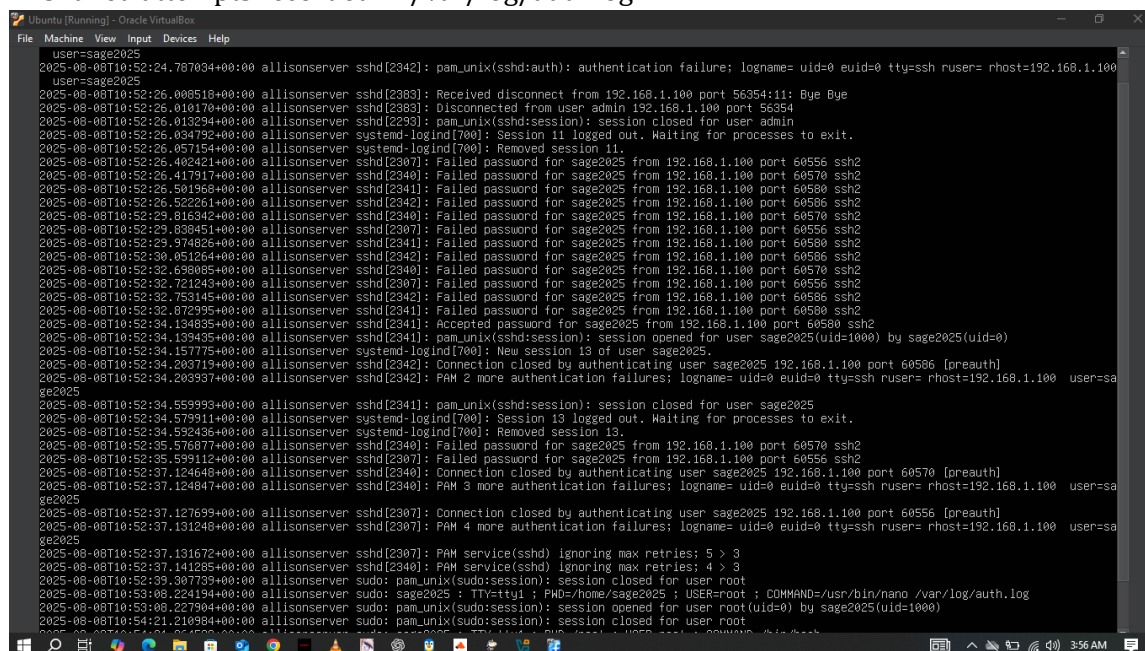
Both attacks originated from the same attacker IP (192.168.1.100). No successful compromises occurred. Detection was achieved through Wazuh agents on both endpoints, which correlated the events across systems.

This exercise demonstrated effective SOC monitoring and correlation capabilities and provided insights into areas for improvement.

Timeline

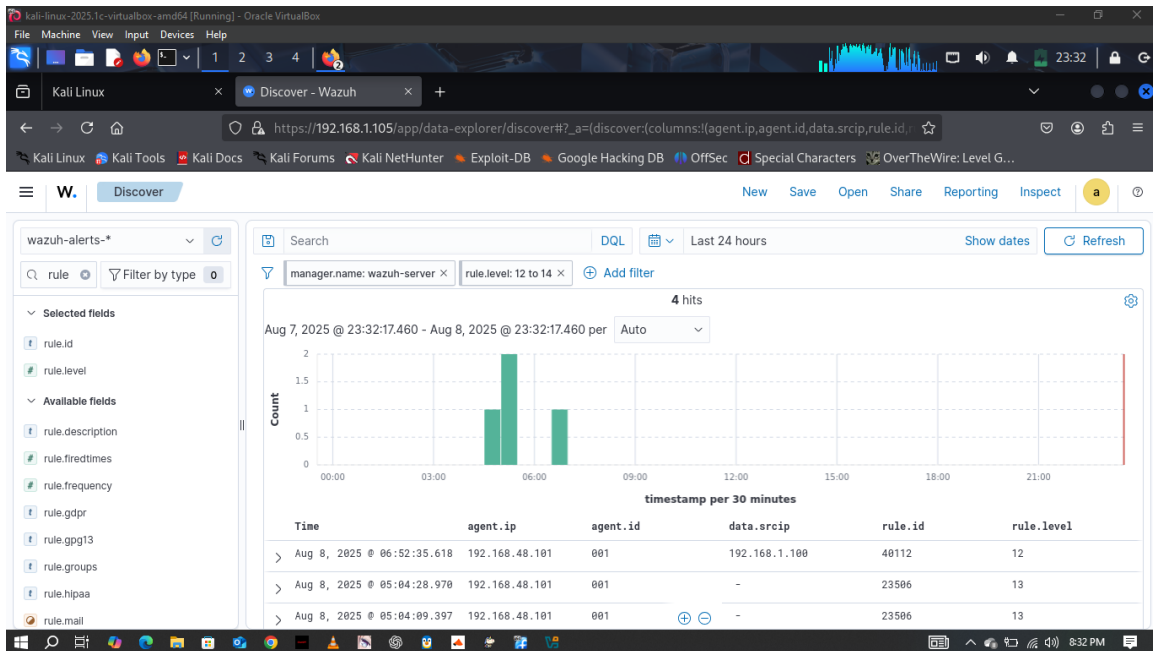
- 10:52 p.m. – Kali Linux attacker initiated SSH brute-force attempts against Ubuntu DMZ server.

- 45 failed attempts recorded in /var/log/auth.log.

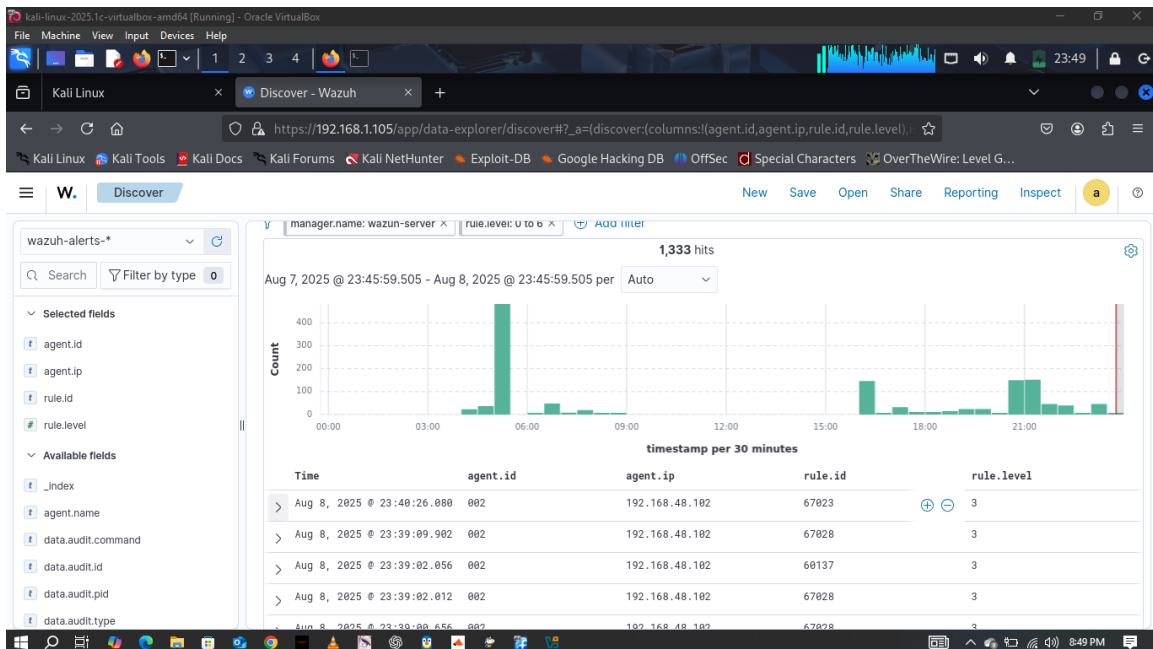


```
2025-08-08T10:52:24.787034+00:00 allisonserver sshd[2342]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.1.100
2025-08-08T10:52:24.787034+00:00 allisonserver sshd[2342]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.1.100
2025-08-08T10:52:26.008518+00:00 allisonserver sshd[2383]: Received disconnect from 192.168.1.100 port 56354:11: Bye Bye
2025-08-08T10:52:26.010170+00:00 allisonserver sshd[2383]: Disconnected from user admin 192.168.1.100 port 56354
2025-08-08T10:52:26.013294+00:00 allisonserver sshd[2293]: pam_unix(sshd:session): session closed for user admin
2025-08-08T10:52:26.024732+00:00 allisonserver systemd-logind[700]: Session 11 logged out. Waiting for processes to exit.
2025-08-08T10:52:26.057154+00:00 allisonserver systemd-logind[700]: Removed session 11.
2025-08-08T10:52:26.462421+00:00 allisonserver sshd[2307]: Failed password for sage2025 from 192.168.1.100 port 60556 ssh2
2025-08-08T10:52:26.417917+00:00 allisonserver sshd[2340]: Failed password for sage2025 from 192.168.1.100 port 60570 ssh2
2025-08-08T10:52:26.501968+00:00 allisonserver sshd[2341]: Failed password for sage2025 from 192.168.1.100 port 60580 ssh2
2025-08-08T10:52:26.522261+00:00 allisonserver sshd[2342]: Failed password for sage2025 from 192.168.1.100 port 60586 ssh2
2025-08-08T10:52:29.816342+00:00 allisonserver sshd[2340]: Failed password for sage2025 from 192.168.1.100 port 60570 ssh2
2025-08-08T10:52:29.838451+00:00 allisonserver sshd[2307]: Failed password for sage2025 from 192.168.1.100 port 60556 ssh2
2025-08-08T10:52:29.974826+00:00 allisonserver sshd[2341]: Failed password for sage2025 from 192.168.1.100 port 60580 ssh2
2025-08-08T10:52:30.051264+00:00 allisonserver sshd[2342]: Failed password for sage2025 from 192.168.1.100 port 60586 ssh2
2025-08-08T10:52:32.630805+00:00 allisonserver sshd[2340]: Failed password for sage2025 from 192.168.1.100 port 60570 ssh2
2025-08-08T10:52:32.721243+00:00 allisonserver sshd[2307]: Failed password for sage2025 from 192.168.1.100 port 60556 ssh2
2025-08-08T10:52:32.753145+00:00 allisonserver sshd[2342]: Failed password for sage2025 from 192.168.1.100 port 60586 ssh2
2025-08-08T10:52:32.872995+00:00 allisonserver sshd[2341]: Failed password for sage2025 from 192.168.1.100 port 60580 ssh2
2025-08-08T10:52:34.194835+00:00 allisonserver sshd[2341]: Accepted password for sage2025 from 192.168.1.100 port 60580 ssh2
2025-08-08T10:52:34.139495+00:00 allisonserver sshd[2341]: pam_unix(sshd:session): session opened for user sage2025(uid=1000) by sage2025(uid=0)
2025-08-08T10:52:34.157775+00:00 allisonserver systemd-logind[700]: New session 13 of user sage2025.
2025-08-08T10:52:34.203719+00:00 allisonserver sshd[2342]: Connection closed by authenticating user sage2025 192.168.1.100 port 60586 [preauth]
2025-08-08T10:52:34.203937+00:00 allisonserver sshd[2342]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.1.100 user=sage2025
2025-08-08T10:52:34.559993+00:00 allisonserver sshd[2341]: pam_unix(sshd:session): session closed for user sage2025
2025-08-08T10:52:34.579911+00:00 allisonserver systemd-logind[700]: Session 13 logged out. Waiting for processes to exit.
2025-08-08T10:52:34.592436+00:00 allisonserver systemd-logind[700]: Removed session 13.
2025-08-08T10:52:35.576877+00:00 allisonserver sshd[2340]: Failed password for sage2025 from 192.168.1.100 port 60570 ssh2
2025-08-08T10:52:35.593112+00:00 allisonserver sshd[2307]: Failed password for sage2025 from 192.168.1.100 port 60556 ssh2
2025-08-08T10:52:37.124648+00:00 allisonserver sshd[2340]: Connection closed by authenticating user sage2025 192.168.1.100 port 60570 [preauth]
2025-08-08T10:52:37.124647+00:00 allisonserver sshd[2340]: PAM 3 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.1.100 user=sage2025
2025-08-08T10:52:37.127699+00:00 allisonserver sshd[2307]: Connection closed by authenticating user sage2025 192.168.1.100 port 60556 [preauth]
2025-08-08T10:52:37.131248+00:00 allisonserver sshd[2307]: PAM 4 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.1.100 user=sage2025
2025-08-08T10:52:37.131672+00:00 allisonserver sshd[2307]: PAM service(sshd) ignoring max retries: 5 > 3
2025-08-08T10:52:37.141285+00:00 allisonserver sshd[2340]: PAM service(sshd) ignoring max retries: 4 > 3
2025-08-08T10:52:39.307739+00:00 allisonserver sudo: pam_unix(sudo:session): session closed for user root
2025-08-08T10:53:08.224194+00:00 allisonserver sudo: sage2025 : TTY=ttty : PWD=/home/sage2025 : USER=root : COMMAND=/usr/bin/nano /var/log/auth.log
2025-08-08T10:53:08.227994+00:00 allisonserver sudo: pam_unix(sudo:session): session opened for user root(uid=0) by sage2025(uid=1000)
2025-08-08T10:54:21.210984+00:00 allisonserver sudo: pam_unix(sudo:session): session closed for user root
```

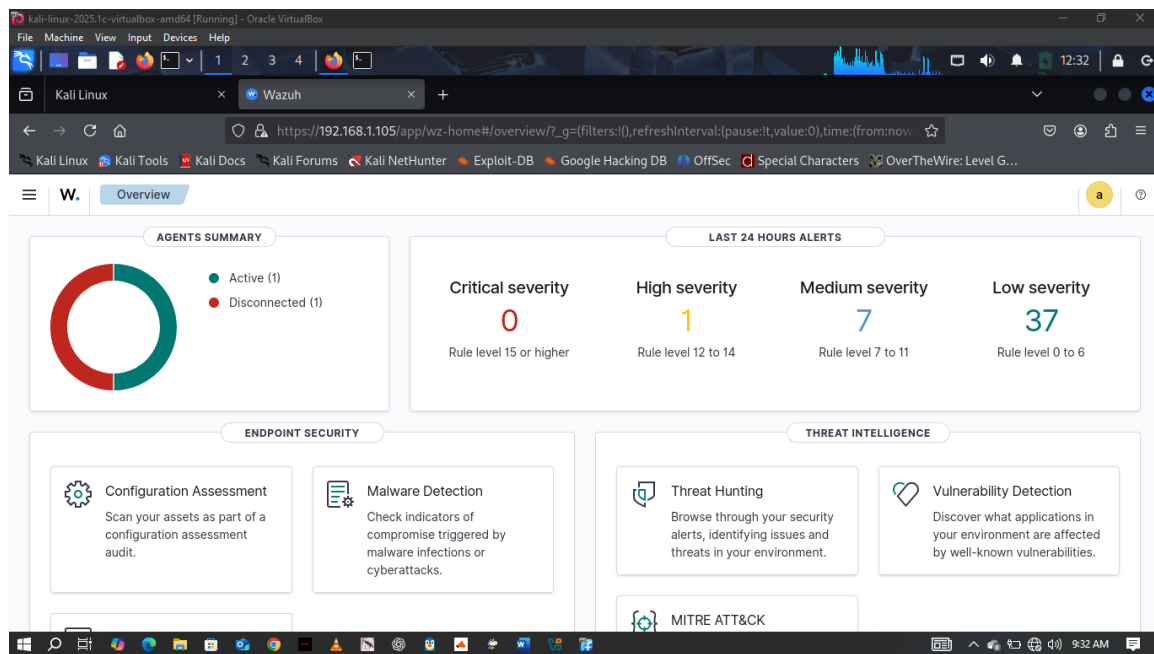

- 10:56 p.m. – Wazuh generated alerts:
- Ubuntu: 'Multiple SSH authentication failures.'



- Windows: 'Multiple RDP authentication failures.'



- 11:00 p.m. – SOC correlated attacker activity across both endpoints.
- Same source IP confirmed.
- Attack pattern aligned with credential brute-force reconnaissance.



Investigation

- SOC analysts examined Ubuntu logs (/var/log/auth.log) and identified repeated 'Failed password' entries.
- Windows Security logs (Event ID 4625) confirmed RDP brute-force attempts.
- Wazuh rules ##### (SSH brute-force) and ##### (RDP brute-force) triggered alerts.
- Correlation showed attacker targeting multiple network segments from the same source, consistent with early-stage lateral movement attempts.

Response and Remediation

Short-term actions:

- Blocked SSH (22/tcp) and RDP (3389/tcp) from untrusted networks in pfSense firewall.
- Enabled Fail2Ban on Ubuntu DMZ server (ban after 3 failed attempts).
- Enforced Windows account lockout policy (lock after 3 failed logons).
- [Insert Screenshot 6: pfSense firewall rule or Fail2Ban logs if available]

Long-term actions:

- Disabled password-based SSH logins (key-based only).
- Recommended multi-factor authentication (MFA) for Windows RDP access.
- Plan to deploy IDS/IPS (Suricata/Snort) for deeper packet inspection.
- Scheduled regular vulnerability scans and penetration testing.

Recommendations

1. Network Hardening

- Restrict administrative access to management subnets only.
- Implement allowlisting for RDP and SSH.

2. Endpoint Security

- Continue tuning Fail2Ban and Windows lockout thresholds.
- Deploy endpoint detection tools for enhanced visibility.

3. SOC Operations

- Configure advanced correlation rules in Wazuh for multi-host brute-force patterns.
- Improve alert thresholds to reduce false positives.

4. Strategic Improvements

- Provide security awareness training for employees.
- Establish an incident response playbook for brute-force/lateral movement detection.