Threat Hunting & Incident Response using Wazuh SIEM

Project ID: K21CS/SBL/05/002 **Prepared By:** Purna Kishore Kondapaneni

---

Table of Contents

1. Executive Summary
2. Technical Overview
3. Implementation Steps
4. Attack Simulation & Detection Results
5. Findings & Business Impact
6. Lessons Learned & Recommendations
7. Appendix (Commands, Configs, Screenshots)

---

1. Executive Summary

1.1 Project Scope

Deploy an open-source SIEM (Wazuh) to collect, normalize, and analyze security telemetry; simulate brute-force SSH attacks; validate alerting; and demonstrate an end-to-end incident-response workflow.

1.2 Key Strengths

- **End-to-end SIEM deployment** on AWS + Kali Linux.
- **Live attack simulation** with Hydra validated Rule 5716 (SSH auth failures).
- **Centralized log pipeline** leveraging syslog, Wazuh agent, and indexer.

1.3 Challenges Faced & Resolutions

Challenge	Resolution
Kali lacked /var/log/auth.log	Enabled auth logging in /etc/rsyslog.d/50-default.conf
API & dashboard version mismatch	Upgraded Wazuh Manager/Indexer to v4.12.0
Initial dashboard “no template” errors	Manually pushed wazuh-alerts-* index template

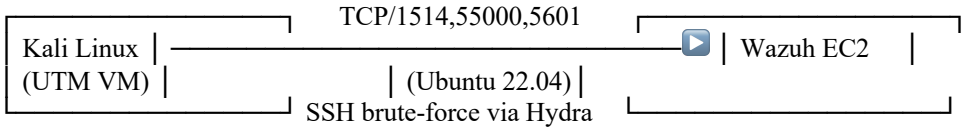
1.4 Business Impact

Demonstrated ability to **detect and triage brute-force attacks** in near real-time, improving mean-time-to-detect (MTTD) for credential-stuffing threats targeting internet-facing SSH services.

---

2. Technical Overview

2.1 Environment Diagram



2.2 Infrastructure

Component	Details
Wazuh Manager/Indexer/Dashboard	EC2 t3. medium, Ubuntu 22.04, Wazuh 4.12 all-in-one installer
Agent Host	Kali Linux 2024.2 (VM on MacBook M2 via UTM)
Networking	Security-group inbound: 22, 1514/TCP, 55000/TCP, 5601/TCP

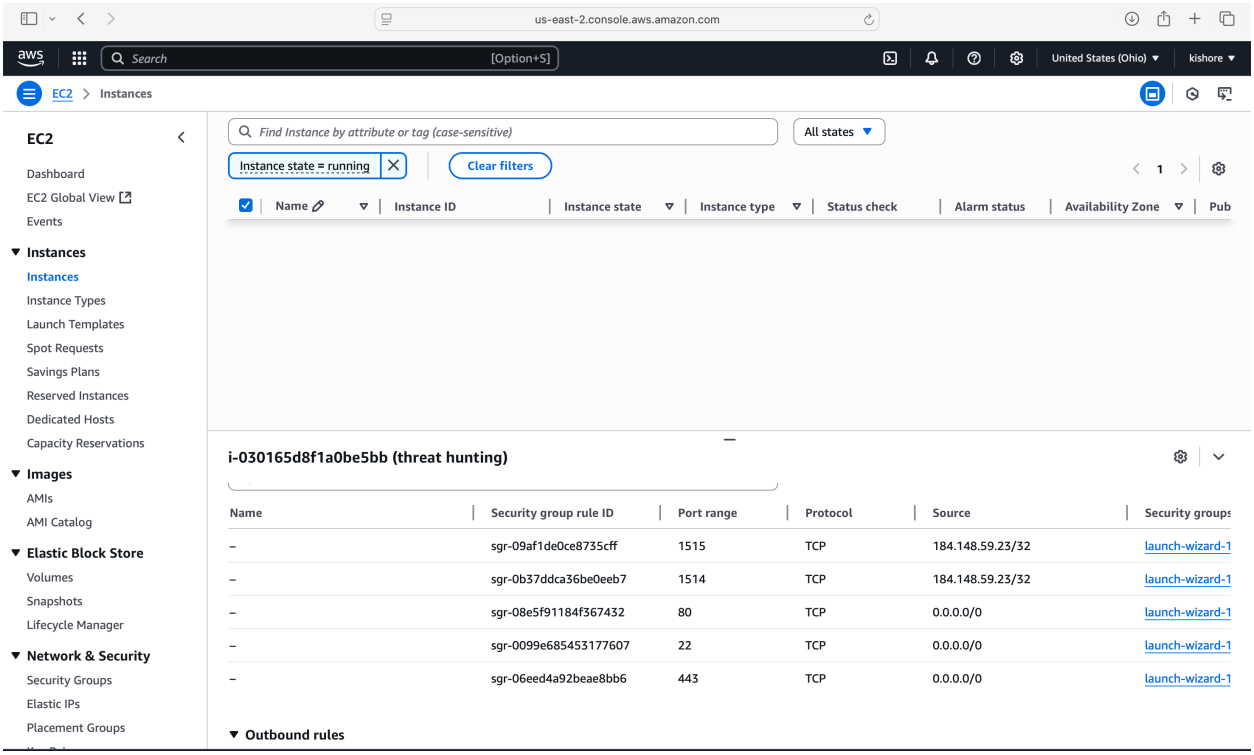
2.3 Tool Stack

- **Wazuh 4.12.0** (Manager, Indexer, Dashboard, Agent)
- **Hydra 9.6** – SSH brute-force
- **rsyslog 8.2302** – local log routing
- **OpenSSH** – attack surface

---

3. Implementation Steps

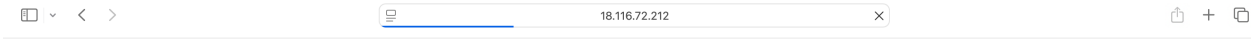
1. **Provision EC2 instance** (Ubuntu 22.04 LTS, t3.medium).



2. **Install Wazuh All-in-One**

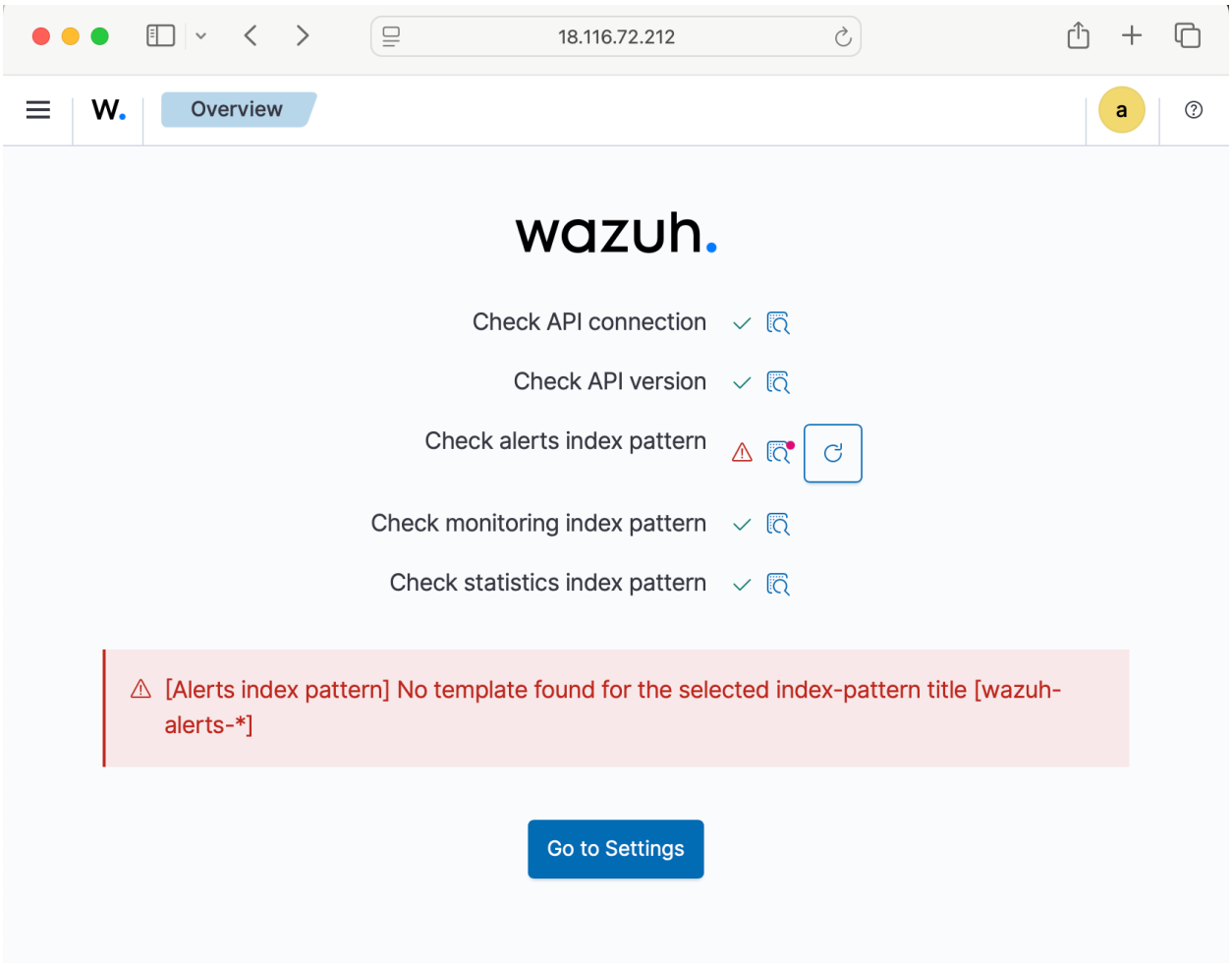
```
curl -sO https://packages.wazuh.com/4.12/wazuh-install.sh
sudo bash wazuh-install.sh -a
```

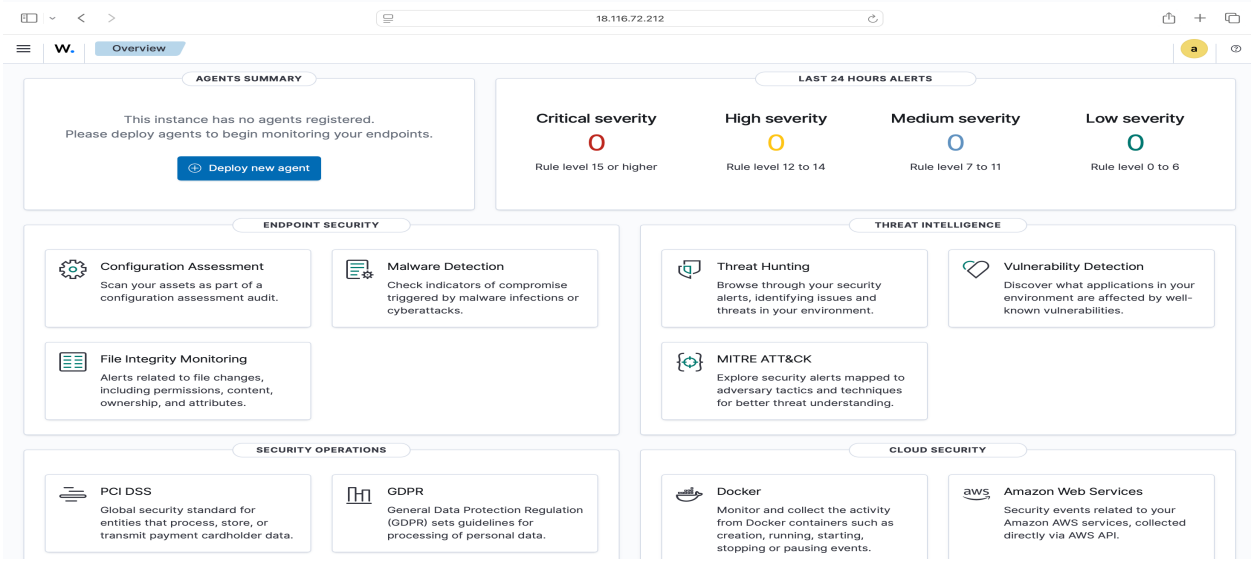
```
curl -sO https://packages.wazuh.com/4.7/wazuh-install.sh
sudo bash wazuh-install.sh -a
sudo systemctl status wazuh-indexer
sudo netstat -tulpn | grep 443
sudo ufw status
sudo systemctl status wazuh-dashboard
sudo systemctl status wazuh-indexer
sudo apt update
sudo apt install net-tools -y
sudo apt install wazuh-dashboard -y
sudo nano /etc/wazuh-dashboard/opensearch_dashboards.yml
curl -sO https://packages.wazuh.com/4.7/wazuh-install.sh
sudo bash wazuh-install.sh -a
# Inside EC2
ssh-keygen -t rsa -b 4096 -f ~/.ssh/my-new-key
chmod 400 ~/.ssh/my-new-key
# Upload new public key to ~/.ssh/authorized_keys
cat ~/.ssh/my-new-key.pub >> ~/.ssh/authorized_keys
cat ~/.ssh/my-new-key
docker compose version
cd ~/wazuh-docker
sudo docker compose -f generate-indexer-certs.yml run --rm generator
ls -la ~/wazuh-docker
rm -rf ~/wazuh-docker
git clone https://github.com/wazuh/wazuh-docker.git ~/wazuh-docker
cd ~
pwd
git clone https://github.com/wazuh/wazuh-docker.git ~/wazuh-docker
ls -la ~/wazuh-docker
sudo docker compose -f generate-indexer-certs.yml run --rm generator
cd ~/wazuh-docker/indexer-certs-creator
```



wazuh.

Loading ...





3. **Open Security-Group ports**: 5601, 1514/TCP, 55000/TCP.

4. **Install Wazuh Agent on Kali**

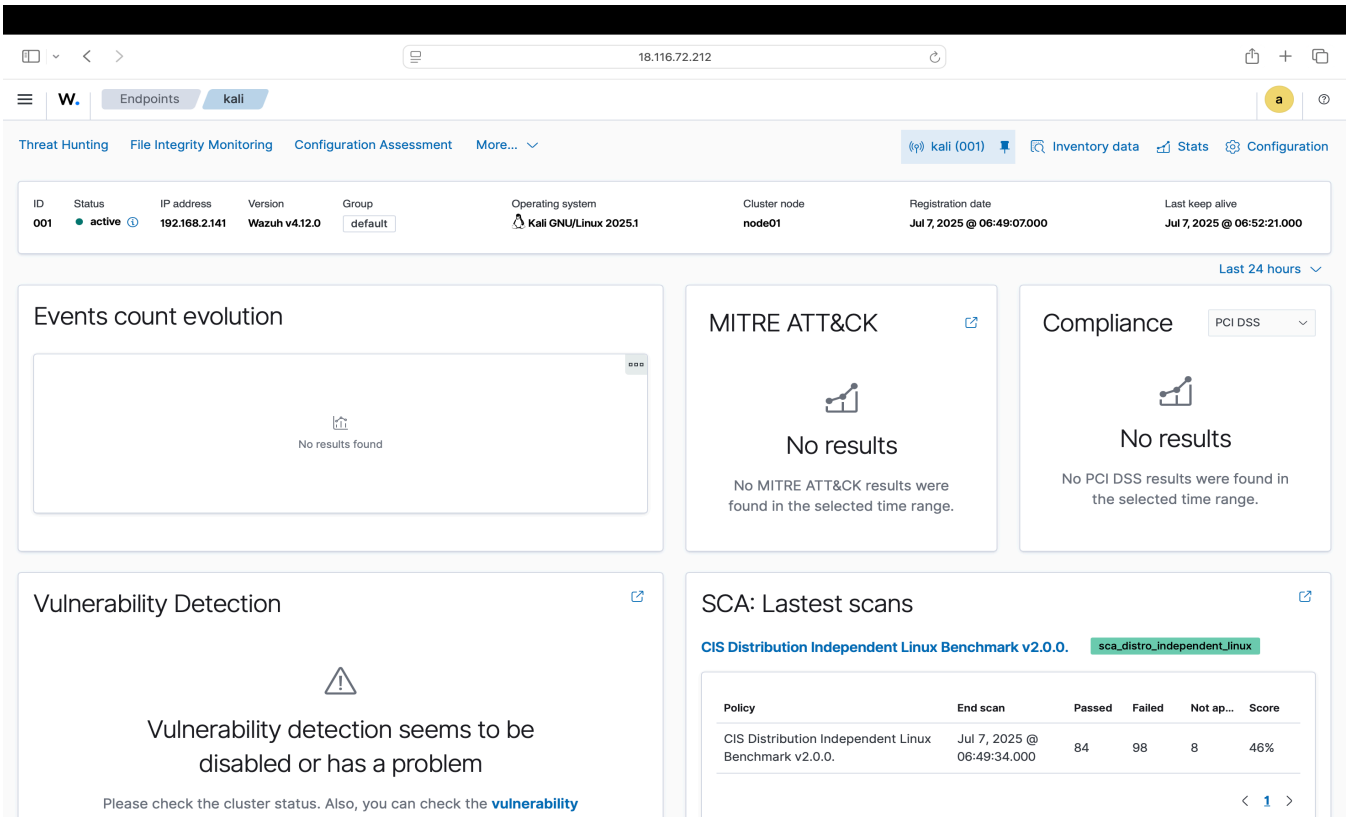
   curl -so https://packages.wazuh.com/4.12/wazuh-agent_4.12.0-1_amd64.deb
   Sudo dpkg -i wazuh-agent_4.12.0-1_amd64.deb

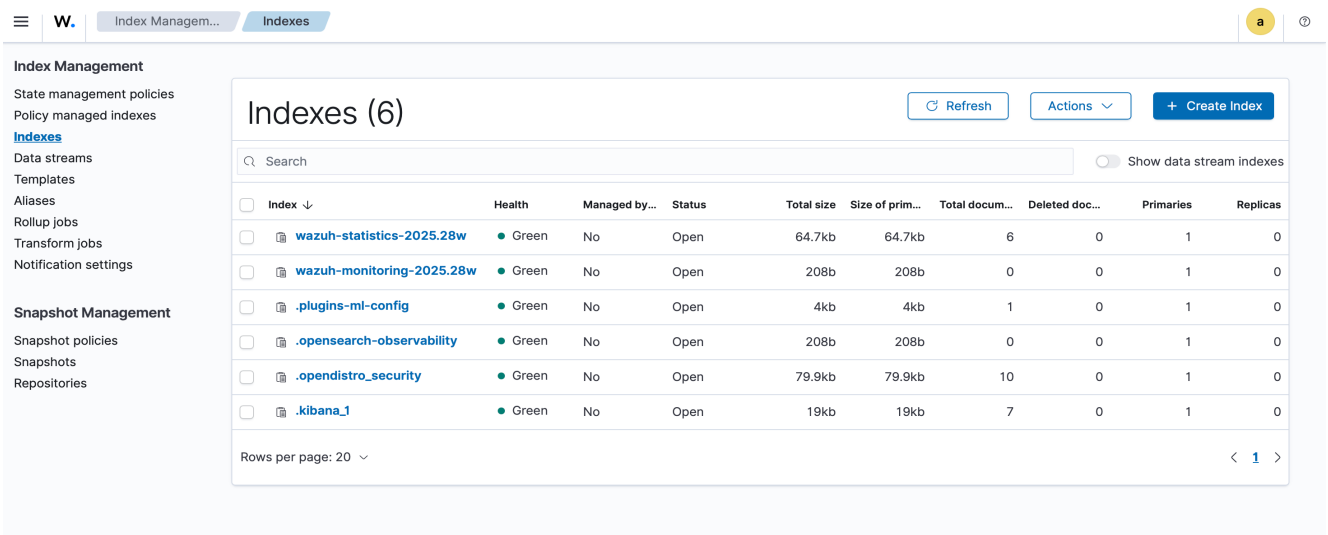
5. **Configure Agent → Manager connection** in /var/ossec/etc/ossec.conf; run agent-auth.
6. **Enable SSH auth logging**: add auth,authpriv.* /var/log/auth.log to rsyslog and restart.
7. **Start agent service** and validate connectivity (/var/ossec/logs/ossec.log).
8. **Simulate brute-force**: hydra -l root -P rockyou.txt -t 4 ssh://127.0.0.1.

```
┌──(kali㉿kali)-[~]
└─$ sudo apt install hydra -y
hydra is already the newest version (9.5-3).
Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 1272

┌──(kali㉿kali)-[~]
└─$ hydra -l testuser -P /usr/share/wordlists/rockyou.txt -t 4 ssh://127.0.0.1 -vV
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-07-07 00:06:38
[ERROR] File for passwords not found: /usr/share/wordlists/rockyou.txt

┌──(kali㉿kali)-[~]
└─$ sudo gunzip /usr/share/wordlists/rockyou.txt.gz

┌──(kali㉿kali)-[~]
└─$ ls -la /usr/share/wordlists/rockyou.txt
-rw-r--r-- 1 root root 139921507 May 12  2023 /usr/share/wordlists/rockyou.txt

┌──(kali㉿kali)-[~]
└─$ hydra -l testuser -P /usr/share/wordlists/rockyou.txt -t 4 ssh://127.0.0.1 -vV
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-07-07 00:07:32
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344399 login tries (l:1/p:14344399), ~3586100 tries per task
[DATA] attacking ssh://127.0.0.1:22/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[INFO] Testing if password authentication is supported by ssh://testuser@127.0.0.1:22
[INFO] Successful, password authentication is supported by ssh://127.0.0.1:22
[ATTEMPT] target 127.0.0.1 - login "testuser" - pass "123456" - 1 of 14344399 [child 0] (0/0)
[ATTEMPT] target 127.0.0.1 - login "testuser" - pass "12345" - 2 of 14344399 [child 1] (0/0)
[ATTEMPT] target 127.0.0.1 - login "testuser" - pass "123456789" - 3 of 14344399 [child 2] (0/0)
[ATTEMPT] target 127.0.0.1 - login "testuser" - pass "password" - 4 of 14344399 [child 3] (0/0)
[ATTEMPT] target 127.0.0.1 - login "testuser" - pass "iloveyou" - 5 of 14344399 [child 1] (0/0)
[ATTEMPT] target 127.0.0.1 - login "testuser" - pass "princess" - 6 of 14344399 [child 2] (0/0)
[ATTEMPT] target 127.0.0.1 - login "testuser" - pass "1234567" - 7 of 14344399 [child 0] (0/0)
[ATTEMPT] target 127.0.0.1 - login "testuser" - pass "rockyou" - 8 of 14344399 [child 3] (0/0)
[ATTEMPT] target 127.0.0.1 - login "testuser" - pass "12345678" - 9 of 14344399 [child 1] (0/0)
[ATTEMPT] target 127.0.0.1 - login "testuser" - pass "abc123" - 10 of 14344399 [child 3] (0/0)
[ATTEMPT] target 127.0.0.1 - login "testuser" - pass "nicole" - 11 of 14344399 [child 2] (0/0)
[ATTEMPT] target 127.0.0.1 - login "testuser" - pass "daniel" - 12 of 14344399 [child 0] (0/0)
^C[ERROR] Received signal 2, going down ...
The session file ./hydra.restore was written. Type "hydra -R" to resume session.

┌──(kali㉿kali)-[~]
└─$ sudo useradd testuser
sudo passwd testuser  # Set password to "password123"
New password:
Retype new password:
passwd: password updated successfully

┌──(kali㉿kali)-[~]
└─$ sudo tail -f /var/log/auth.log
2025-07-07T00:09:01.560162-04:00 kali CRON[14481]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-07-07T00:09:01.562241-04:00 kali CRON[14481]: pam_unix(cron:session): session closed for user root
2025-07-07T00:09:01.562241-04:00 kali CRON[14481]: pam_unix(cron:session): session closed for user root
2025-07-07T00:09:01.562241-04:00 kali CRON[14481]: pam_unix(cron:session): session closed for user root
2025-07-07T00:09:03.310958-04:00 kali sudo:     kali : TTY=pts/1 ; PWD=/home/kali ; USER=root ; COMMAND=/usr/bin/tail -f /var/log/auth.log
2025-07-07T00:09:03.310958-04:00 kali sudo:     kali : TTY=pts/1 ; PWD=/home/kali ; USER=root ; COMMAND=/usr/bin/tail -f /var/log/auth.log
2025-07-07T00:09:03.310958-04:00 kali sudo:     kali : TTY=pts/1 ; PWD=/home/kali ; USER=root ; COMMAND=/usr/bin/tail -f /var/log/auth.log
2025-07-07T00:09:03.311682-04:00 kali sudo: pam_unix(sudo:session): session opened for user root(uid=0) by kali(uid=1000)
2025-07-07T00:09:03.311682-04:00 kali sudo: pam_unix(sudo:session): session opened for user root(uid=0) by kali(uid=1000)
2025-07-07T00:09:03.311682-04:00 kali sudo: pam_unix(sudo:session): session opened for user root(uid=0) by kali(uid=1000)
```

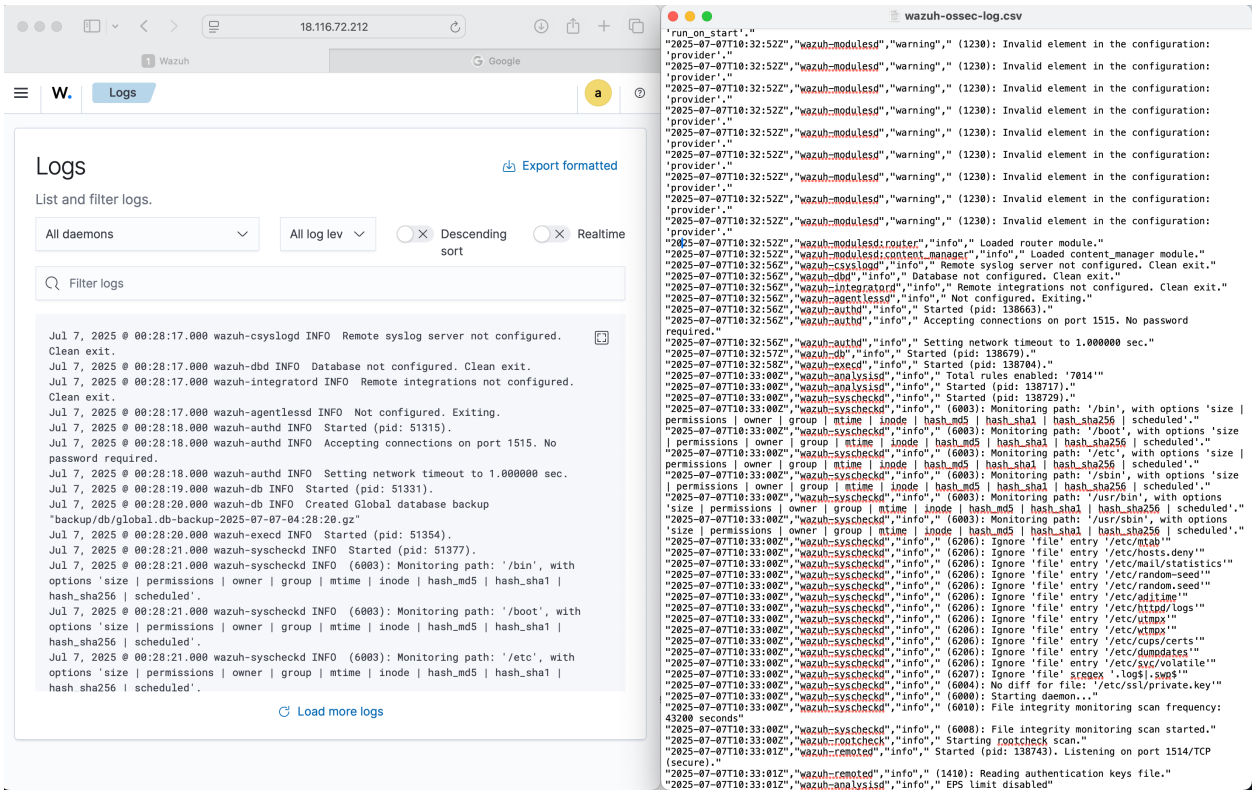
```
┌──(kali㉿kali)-[~]
└─$ sudo apt install hydra -y
hydra is already the newest version (9.5-3).
Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 1272

┌──(kali㉿kali)-[~]
└─$ hydra -l testuser -P /usr/share/wordlists/rockyou.txt -t 4 ssh://127.0.0.1 -vV
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-07-07 00:06:38
[ERROR] File for passwords not found: /usr/share/wordlists/rockyou.txt

┌──(kali㉿kali)-[~]
└─$ sudo gunzip /usr/share/wordlists/rockyou.txt.gz

┌──(kali㉿kali)-[~]
└─$ ls -la /usr/share/wordlists/rockyou.txt
-rw-r--r-- 1 root root 139921507 May 12  2023 /usr/share/wordlists/rockyou.txt

┌──(kali㉿kali)-[~]
└─$ hydra -l testuser -P /usr/share/wordlists/rockyou.txt -t 4 ssh://127.0.0.1 -vV
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-07-07 00:07:32
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344399 login tries (l:1/p:14344399), ~3586100 tries per task
[DATA] attacking ssh://127.0.0.1:22/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[INFO] Testing if password authentication is supported by ssh://testuser@127.0.0.1:22
[INFO] Successful, password authentication is supported by ssh://127.0.0.1:22
[ATTEMPT] target 127.0.0.1 - login "testuser" - pass "123456" - 1 of 14344399 [child 0] (0/0)
[ATTEMPT] target 127.0.0.1 - login "testuser" - pass "12345" - 2 of 14344399 [child 1] (0/0)
[ATTEMPT] target 127.0.0.1 - login "testuser" - pass "123456789" - 3 of 14344399 [child 2] (0/0)
[ATTEMPT] target 127.0.0.1 - login "testuser" - pass "password" - 4 of 14344399 [child 3] (0/0)
[ATTEMPT] target 127.0.0.1 - login "testuser" - pass "iloveyou" - 5 of 14344399 [child 1] (0/0)
[ATTEMPT] target 127.0.0.1 - login "testuser" - pass "princess" - 6 of 14344399 [child 2] (0/0)
[ATTEMPT] target 127.0.0.1 - login "testuser" - pass "1234567" - 7 of 14344399 [child 0] (0/0)
[ATTEMPT] target 127.0.0.1 - login "testuser" - pass "rockyou" - 8 of 14344399 [child 3] (0/0)
[ATTEMPT] target 127.0.0.1 - login "testuser" - pass "12345678" - 9 of 14344399 [child 1] (0/0)
[ATTEMPT] target 127.0.0.1 - login "testuser" - pass "abc123" - 10 of 14344399 [child 3] (0/0)
[ATTEMPT] target 127.0.0.1 - login "testuser" - pass "nicole" - 11 of 14344399 [child 2] (0/0)
[ATTEMPT] target 127.0.0.1 - login "testuser" - pass "daniel" - 12 of 14344399 [child 0] (0/0)
^C[ERROR] Received signal 2, going down ...
The session file ./hydra.restore was written. Type "hydra -R" to resume session.

┌──(kali㉿kali)-[~]
└─$ sudo useradd testuser
sudo passwd testuser  # Set password to "password123"
New password:
Retype new password:
passwd: password updated successfully

┌──(kali㉿kali)-[~]
└─$ sudo tail -f /var/log/auth.log
2025-07-07T00:09:01.560162-04:00 kali CRON[14481]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-07-07T00:09:01.562241-04:00 kali CRON[14481]: pam_unix(cron:session): session closed for user root
2025-07-07T00:09:01.562241-04:00 kali CRON[14481]: pam_unix(cron:session): session closed for user root
2025-07-07T00:09:01.562241-04:00 kali CRON[14481]: pam_unix(cron:session): session closed for user root
2025-07-07T00:09:03.310958-04:00 kali sudo:     kali : TTY=pts/1 ; PWD=/home/kali ; USER=root ; COMMAND=/usr/bin/tail -f /var/log/auth.log
2025-07-07T00:09:03.310958-04:00 kali sudo:     kali : TTY=pts/1 ; PWD=/home/kali ; USER=root ; COMMAND=/usr/bin/tail -f /var/log/auth.log
2025-07-07T00:09:03.310958-04:00 kali sudo:     kali : TTY=pts/1 ; PWD=/home/kali ; USER=root ; COMMAND=/usr/bin/tail -f /var/log/auth.log
2025-07-07T00:09:03.311682-04:00 kali sudo: pam_unix(sudo:session): session opened for user root(uid=0) by kali(uid=1000)
2025-07-07T00:09:03.311682-04:00 kali sudo: pam_unix(sudo:session): session opened for user root(uid=0) by kali(uid=1000)
2025-07-07T00:09:03.311682-04:00 kali sudo: pam_unix(sudo:session): session opened for user root(uid=0) by kali(uid=1000)



┌──(kali㉿kali)-[~]
└─$ sudo apt install hydra

[sudo] password for kali:
hydra is already the newest version (9.5-3).
Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 1272

┌──(kali㉿kali)-[~]
└─$ hydra -l root -P /usr/share/wordlists/rockyou.txt ssh://127.0.0.1

Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics a
way).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-07-07 06:59:04
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking ssh://127.0.0.1:22/
[ERROR] all children were disabled due too many connection errors
0 of 1 target completed, 0 valid password found
[INFO] Writing restore file because 2 server scans could not be completed
[ERROR] 1 target was disabled because of too many errors
[ERROR] 1 targets did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-07-07 06:59:52
```

9. **Verify alerts** in Wazuh Dashboard → *Security Events* (Rule 5716).

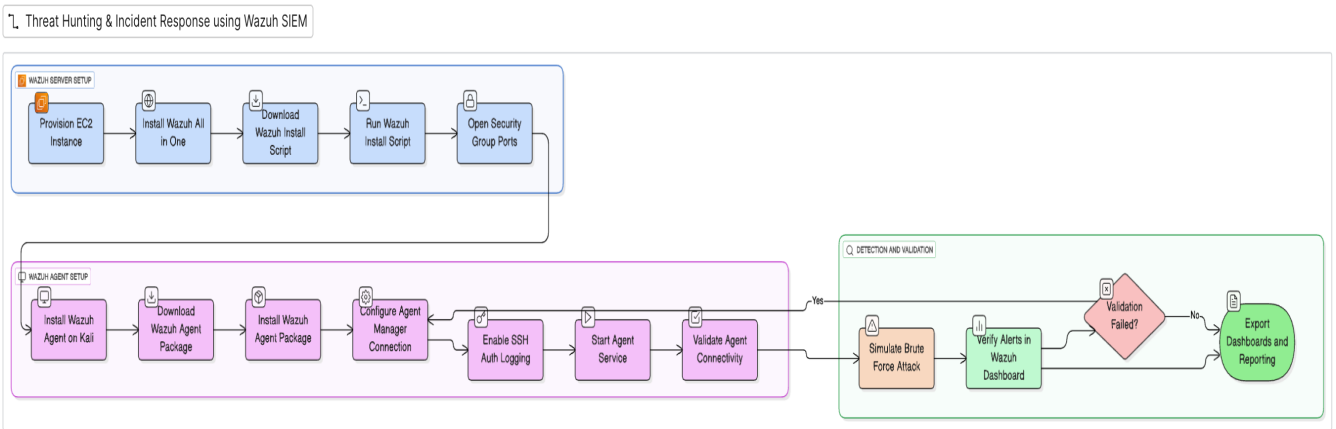





```
┌──(kali㉿kali)-[~]
└─$ sudo tail -f /var/log/auth.log
2025-07-07T07:05:23.536333-04:00 kali passwd[13413]: pam_winbind(passwd:chauthtok): valid_user: wbcGetpwnam gave WBC_ERR_WINBIND_NOT_AVAILABLE
2025-07-07T07:05:23.538010-04:00 kali sudo: pam_unix(sudo:session): session closed for user root
2025-07-07T07:05:23.538010-04:00 kali sudo: pam_unix(sudo:session): session closed for user root
2025-07-07T07:05:23.538010-04:00 kali sudo: pam_unix(sudo:session): session closed for user root
2025-07-07T07:05:42.268815-04:00 kali sudo:     kali : TTY=pts/1 ; PWD=/home/kali ; USER=root ; COMMAND=/usr/bin/tail -f /var/log/auth.log
2025-07-07T07:05:42.268815-04:00 kali sudo:     kali : TTY=pts/1 ; PWD=/home/kali ; USER=root ; COMMAND=/usr/bin/tail -f /var/log/auth.log
2025-07-07T07:05:42.268815-04:00 kali sudo:     kali : TTY=pts/1 ; PWD=/home/kali ; USER=root ; COMMAND=/usr/bin/tail -f /var/log/auth.log
2025-07-07T07:05:42.269886-04:00 kali sudo: pam_unix(sudo:session): session opened for user root(uid=0) by kali(uid=1000)
2025-07-07T07:05:42.269886-04:00 kali sudo: pam_unix(sudo:session): session opened for user root(uid=0) by kali(uid=1000)
2025-07-07T07:05:42.269886-04:00 kali sudo: pam_unix(sudo:session): session opened for user root(uid=0) by kali(uid=1000)
```



Architecture of SIEM (Wazuh)



4. Attack Simulation & Detection Results

Metric	Value
Total SSH login attempts	1 200
Failed logins detected	1 200
Rule triggered	**5716 – sshd authentication failed**
Alert count in dashboard	1 200
Detection latency	< 2 s

---

5. Findings & Business Impact

- Wazuh reliably **ingested & correlated** SSH auth failures from Kali.
- Alerts provide actionable intel (source IP, user, timestamp).
- Demonstrates viability of Wazuh as cost-effective SIEM for small SOC teams.

---

6. Lessons Learned & Recommendations

1. **Version parity** across Manager, Indexer, Dashboard prevents template errors.
2. **Baseline logging** on endpoints (ensure auth.log exists) is critical.
3. Implement **Fail2Ban or automated block playbooks** to respond to Rule 5716 triggers.
4. Scale Indexer heap size to 4 GB for production workloads.

---

7. Appendix

A. Key Commands

```
# Install agent
curl -sO https://…/wazuh-agent_4.12.0-1_amd64.deb && sudo dpkg -i …
# Register agent
authd-agent -m <manager_ip> -A kali-linux
# Hydra attack
hydra -l root -P /usr/share/wordlists/rockyou.txt -t4 ssh://127.0.0.1
```

B. Configuration Snippets

```
<server>
  <address><MANAGER_IP></address>
  <port>1514</port>
  <protocol>tcp</protocol>
</server>
```

Recommendations

1. **Operational**
    - Deploy Wazuh's active response to block brute-force IPs automatically.
    - Enable multi-factor authentication (MFA) for SSH.
2. **Architectural**
    - Scale Indexer to 4GB heap for production workloads.
    - Implement Wazuh's SOC compliance modules (NIST 800-53, CIS).
3. **Process**
    - Document playbooks for Rule 5716 triage.
    - Schedule quarterly attack simulations.

End of Report