

Operation AgroDefend SOC Capstone Project Report

Prepared by: Ogbuagu Anayo Godson

May 23, 2025.

Table Of Contents

1.0 Executive Summary.....	3
2.0 Project Objective.....	3
3.0 Project Methodology.....	3
3.1 Network Segmentation Design.....	3
3.2 Lab Environment Setup (VirtualBox).....	4
3.3 Virtual Machines Deployed.....	4
4.0 pfSense Configuration.....	7
4.1 Interfaces.....	7
4.2 Firewall Rules.....	7
4.3 NAT & Port Forwarding.....	7
5.0 Attack Simulation from Corpnet to DMZ.....	9
5.1 Threat Emulation Using Kali Linux.....	9
5.2 Attack Scenario.....	11
6.0 Log Monitoring with Wazuh (IT-dept Network).....	11
6.1 Wazuh Components.....	11
6.2 Log Sources Monitored.....	12
6.3 Detection Rules.....	12
7.0 Incident Response Workflow.....	14
8. Key Findings.....	14
9. Recommendations.....	14
10. Conclusion.....	15
11. Appendices.....	16

1. Executive Summary

Agrodefend firm is an agricultural technology firm focused on securing data and infrastructure across multiple digital platforms and departments. Due to cyber threats to critical sectors like food and agriculture, the company is determined to enhance its cybersecurity capabilities by implementing a segmented SOC (Security Operations Center) environment. This project addressed these challenges by setting up a network with four logical segments (**WAN**, **DMZ**, **Corpnet**, and **IT-dept**) using **pfSense** as the core firewall/router. The focus is to simulate cyber-attacks from the **Corpnet** (Kali Linux) to Ubuntu servers in the **Demilitarized Zone (DMZ)**, while the **IT-dept** segment houses the Wazuh monitoring infrastructure for centralized detection, alerting, response and also provide actionable recommendations for the firm to enhance their security posture.

2. Project Objectives

AgroDefend, as an agricultural firm in the cyberspace is posed with significant threats to data and infrastructure across its departments. The firm lacked the understanding of how to identify, respond to and mitigate real-world cyber threats through segmentation, and log monitoring. This project aimed to:

- Build a virtualized, segmented network using pfSense.
- Simulate real-world cyber-attacks from Corpnet to DMZ using Kali Linux.
- Monitor logs and detect threats using Wazuh in the IT-dept network.
- Enforce network segmentation to minimize risk and isolate intrusions.
- Develop incident response procedures based on Wazuh alerts.

3.0 Project Methodology

3.1 Network Segmentation Design

A network with four logical segments was created on pfSense with their respective gateways, static IP addresses were assigned and firewall rules were also configured to restrict lateral movement:

Network	Description	IP Range
WAN:	Internet-facing network (external)	192.168.30.4/24
DMZ:	Exposed servers (e.g. Ubuntu web server)	192.168.50.1/24
Corpnet:	Employee network (includes Kali attacker)	192.168.60.1/24
IT-dept:	SOC & security monitoring (Wazuh)	192.168.40.1/24

Network	Description	IP Range
---------	-------------	----------

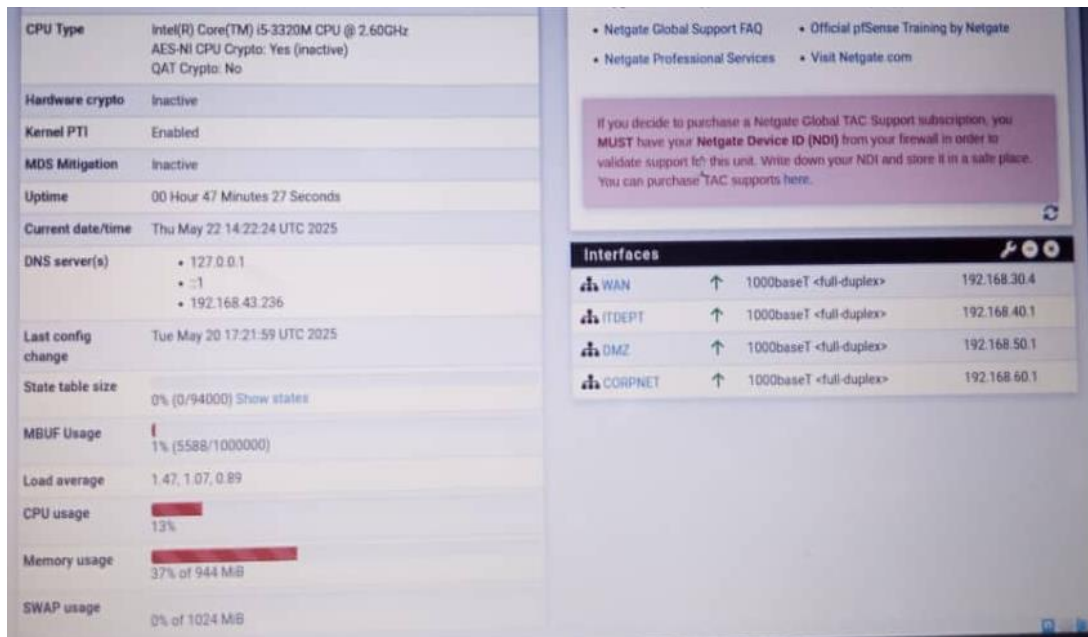


Figure 1: pfSense Interface Showing Four Configured Network Segments.

3.2 Lab Environment Setup (VirtualBox)

3.3 Virtual Machines Deployed

Host	Role	OS	Network
pfSense	Firewall & Routing	pfSense	All 4 networks
Ubuntu Web Server	Target	Ubuntu 22.04	DMZ
Kali Linux	Attacker	Kali Linux	Corpnet
Wazuh Server	SIEM	Linux 2.6/3.x/4.x/5.x(64-bit)	IT-dept
Windows 10	Target	Windows 10 (64-bit)	IT-dept

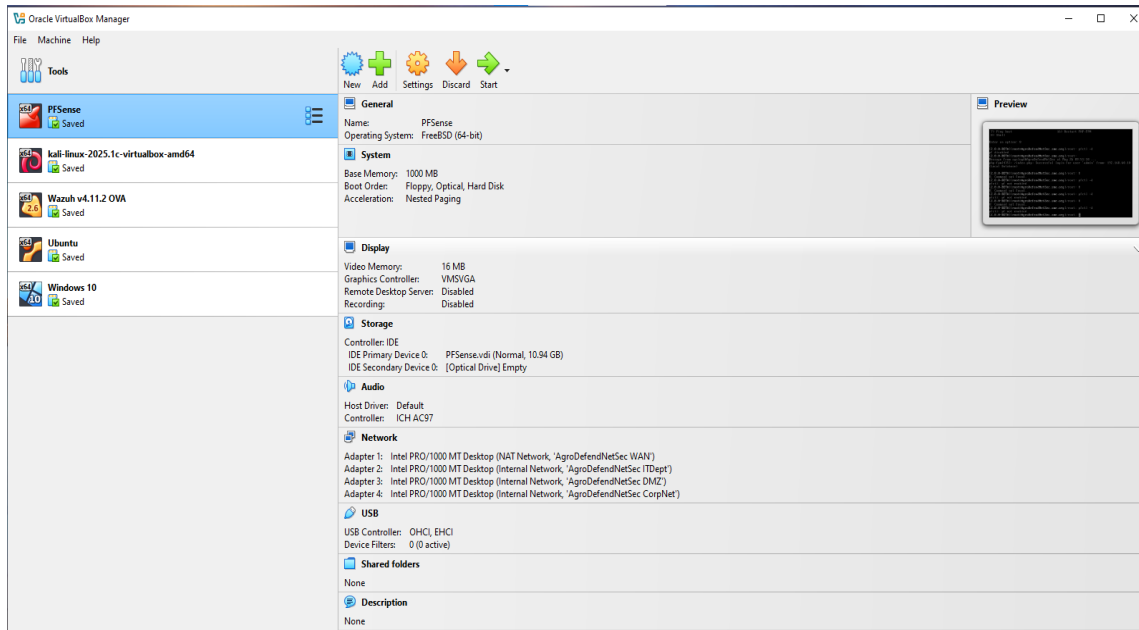


Figure 2: pfSense interface showing the four Configured Network Segments in the VirtualBox.

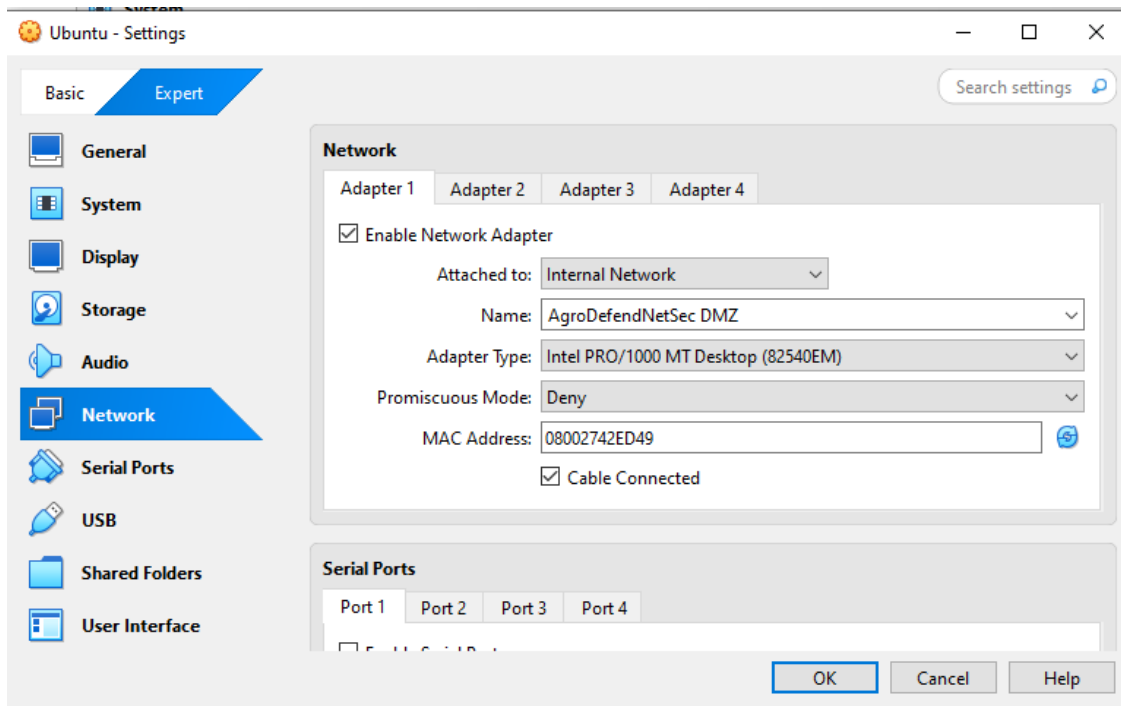


Figure 3: Showing Ubuntu VM Configured to DMZ Network in the VirtualBox.

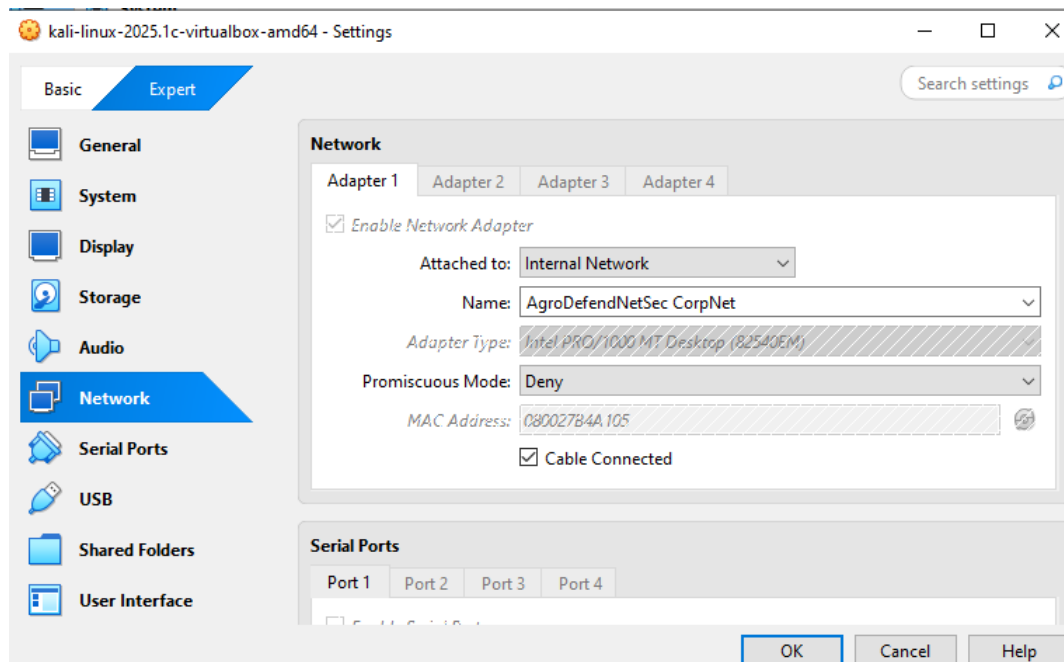


Figure 4: Showing Kali VM Configured to Corpnet Network in the VirtualBox

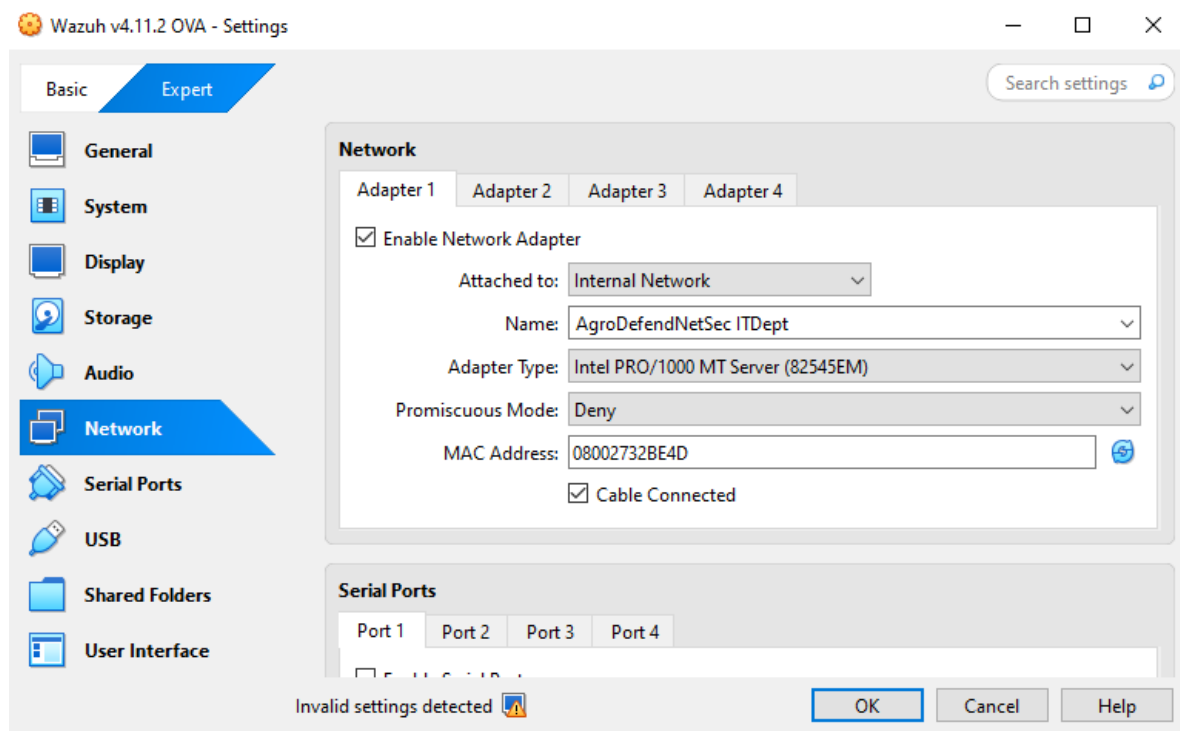


Figure 5: Showing Wazuh VM Configured to IT-dept Network in the VirtualBox

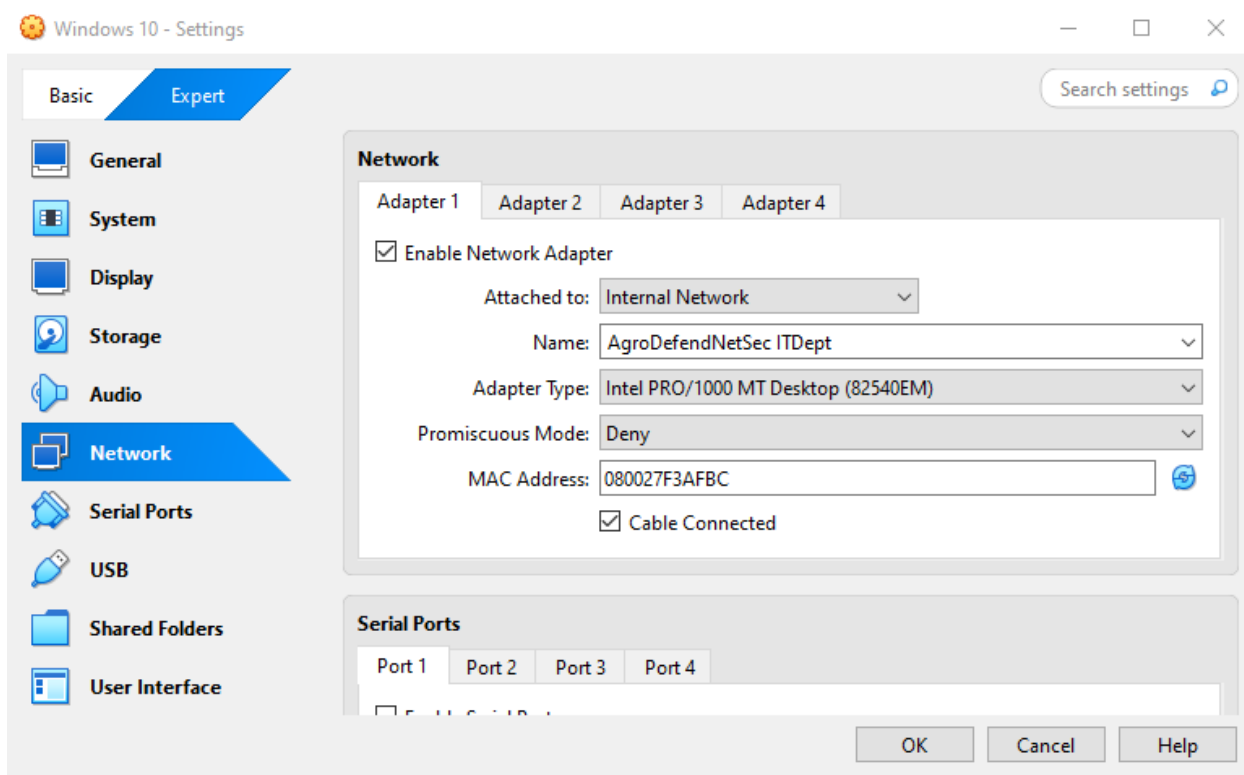


Figure 6: Showing Windows 10 VM Configured to IT-dept Network in the VirtualBox

4.0 pfSense Configuration

4.1 Interfaces: The individual interfaces were configured with VLANs for each zone.

4.2 Firewall Rules:

- Block all inter-network traffic except required (Corpnet to DMZ: allow only HTTP/HTTPS for test)
- Allow IT-dept to access all zones for monitoring.

4.3 NAT & Port Forwarding: Optional access from WAN to DMZ server for testing public attack exposure.

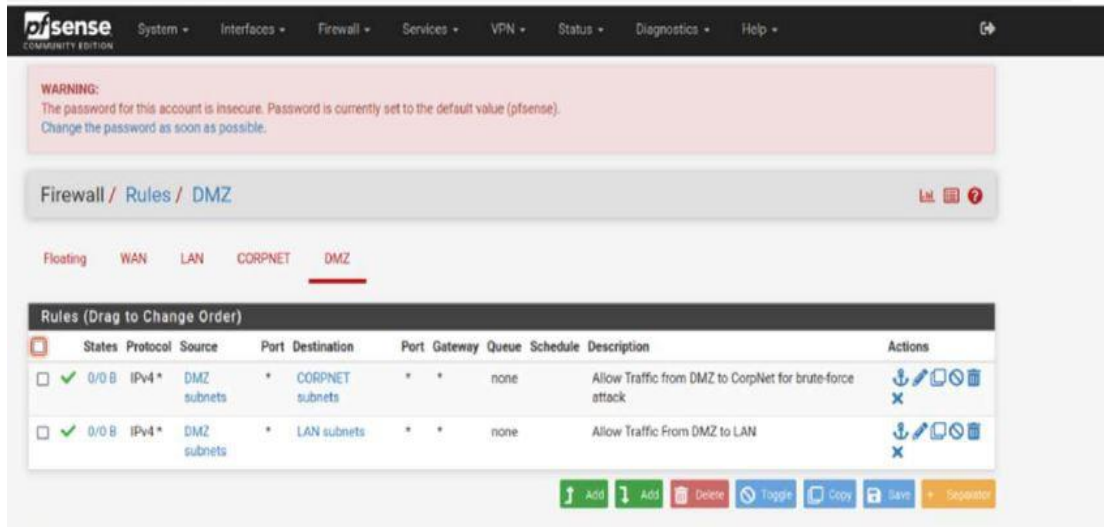


Figure 7: Showing Firewall rules Configured from DMZ interface in the pfSense

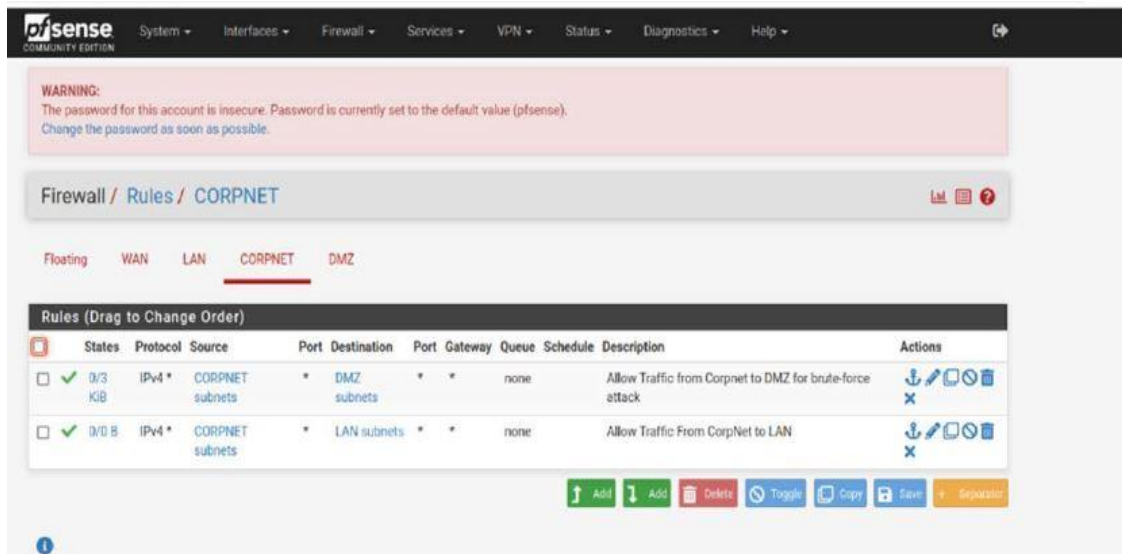


Figure 8: Showing Firewall rules Configured from Corpnet interface in the pfSense

5.0 Attack Simulation from Corpnet to DMZ

5.1 Threat Emulation Using Kali Linux

Phase	ToolsUsed	Description
Reconnaissance	nmap,	Scanned DMZ and IT-dept subnet from Corpnet.
Exploitation	hydra	SSH brute-force against Ubuntu and windows 10 from Kali Linux.

```
kali@kali ~
$ nmap 192.168.50.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-25 19:36 EDT
Nmap scan report for 192.168.50.1
Host is up (0.00064s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
443/tcp   open  https
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
Device type: general purpose/game console
Running (JUST GUESSING): FreeBSD 11.X|12.X|13.X (91%), Sony embedded (86%)
OS CPE: cpe:/o:freebsd:freebsd:11.2 cpe:/o:freebsd:freebsd:11.0 cpe:/o:freebs
d:freebsd:12 cpe:/o:freebsd:freebsd:13
Aggressive OS guesses: FreeBSD 11.2-RELEASE (91%), Sony PS5 (FreeBSD 11.0) (8
6%), FreeBSD 11.3-RELEASE (85%), FreeBSD 12.0-RELEASE - 12.1-RELEASE (85%), F
reeBSD 12.2-RELEASE - 13.0-RELEASE (85%)
No exact OS matches for host (test conditions non-ideal).

Nmap scan report for 192.168.50.10
Host is up (0.0014s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE
22/tcp    open  ssh
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
Aggressive OS guesses: Linux 4.15 - 5.19 (97%), Linux 4.19 (97%), Linux 5.0 -
5.14 (97%), OpenMrt 21.02 (Linux 5.4) (97%), Mikrotik RouterOS 7.2 - 7.5 (Li
nux 5.6.3) (97%), Linux 6.0 (94%), Linux 5.4 - 5.10 (91%), Linux 2.6.32 (91%)
, Linux 2.6.32 - 3.13 (91%), Linux 3.10 - 4.11 (91%)
No exact OS matches for host (test conditions non-ideal).

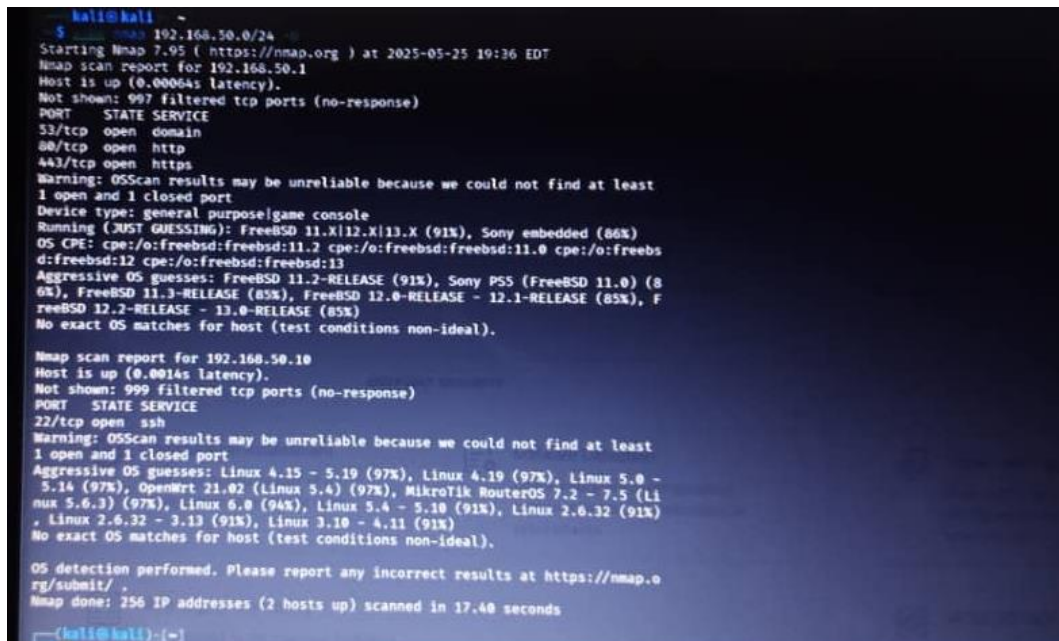
OS detection performed. Please report any incorrect results at https://nmap.o
rg/submit/.
Nmap done: 256 IP addresses (2 hosts up) scanned in 17.40 seconds

kali@kali) ~
```

Figure 9: Showing nmap scan report of DMZ subnet from Corpnet

5.2 Attack Scenario

- Attacker used nmap to discover open ports on 192.168.50.10 (Ubuntu server) and 192.168.40.11 (Windows 10).
- Finds HTTP (port 80) and SSH (port 22) open.
- Uses hydra to brute-force SSH login.



```
kali@kali ~  
$ nmap 192.168.50.0/24  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-25 19:36 EDT  
Nmap scan report for 192.168.50.1  
Host is up (0.00064s latency).  
Not shown: 997 filtered tcp ports (no-response)  
PORT      STATE SERVICE  
53/tcp    open  domain  
80/tcp    open  http  
443/tcp   open  https  
Warning: OSScan results may be unreliable because we could not find at least  
1 open and 1 closed port  
Device type: general purpose/game console  
Running (JUST GUESSING): FreeBSD 11.X|12.X|13.X (91%), Sony embedded (86%)  
OS CPE: cpe:/o:freebsd:freebsd:11.2 cpe:/o:freebsd:freebsd:11.0 cpe:/o:freebsd:freebsd:12 cpe:/o:freebsd:freebsd:13  
Aggressive OS guesses: FreeBSD 11.2-RELEASE (91%), Sony PS5 (FreeBSD 11.0) (86%), FreeBSD 11.3-RELEASE (85%), FreeBSD 12.0-RELEASE - 12.1-RELEASE (85%), FreeBSD 12.2-RELEASE - 13.0-RELEASE (85%)  
No exact OS matches for host (test conditions non-ideal).  
  
Nmap scan report for 192.168.50.10  
Host is up (0.0014s latency).  
Not shown: 999 filtered tcp ports (no-response)  
PORT      STATE SERVICE  
22/tcp    open  ssh  
Warning: OSScan results may be unreliable because we could not find at least  
1 open and 1 closed port  
Aggressive OS guesses: Linux 4.15 - 5.19 (97%), Linux 4.19 (97%), Linux 5.0 - 5.14 (97%), OpenWrt 21.02 (Linux 5.4) (97%), MikroTik RouterOS 7.2 - 7.5 (Linux 5.6.3) (97%), Linux 6.0 (94%), Linux 5.4 - 5.10 (91%), Linux 2.6.32 (91%), Linux 2.6.32 - 3.13 (91%), Linux 3.10 - 4.11 (91%)  
No exact OS matches for host (test conditions non-ideal).  
  
OS detection performed. Please report any incorrect results at https://nmap.org/submit/.  
Nmap done: 256 IP addresses (2 hosts up) scanned in 17.40 seconds  
kali@kali ~
```

Figure 12: Showing discovered open ports 22, port 80 and so on

6.0 Log Monitoring with Wazuh (IT-dept Network)

6.1 Wazuh Architecture

Component	Description
Wazuh Manager	Central server collecting and analyzing logs.
Wazuh Agent	Installed on Ubuntu DMZ server and Windows 10 machine
Wazuh Dashboard	Web interface for log visualization and rule tuning.

6.2 Log Sources Monitored

- /var/log/auth.log
- /var/log/apache2/access.log
- SSH login attempts
- File integrity monitoring (FIM)

6.3 Detection Rules

- Multiple failed SSH logins (Brute-force)
- Web server anomaly detection (e.g., shell upload)

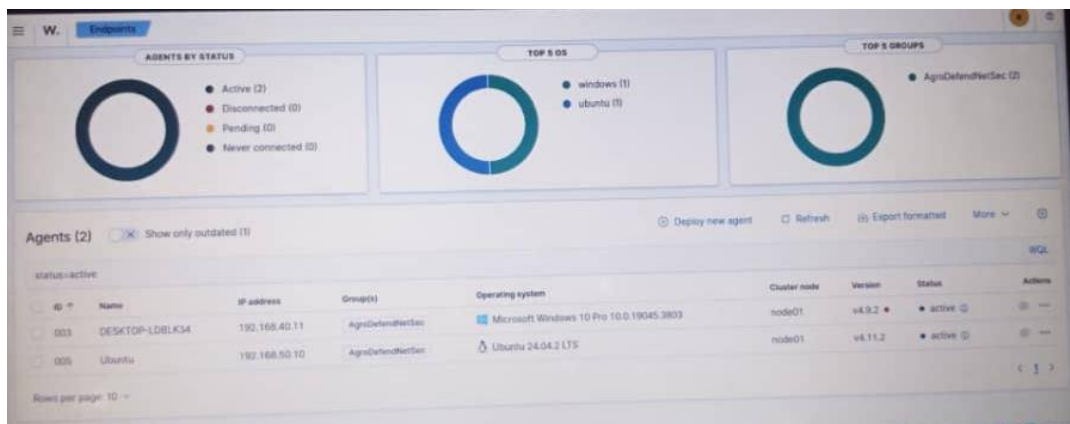


Figure 13: Showing the two active endpoints (Ubuntu and Windows 10) on wazuh dashboard

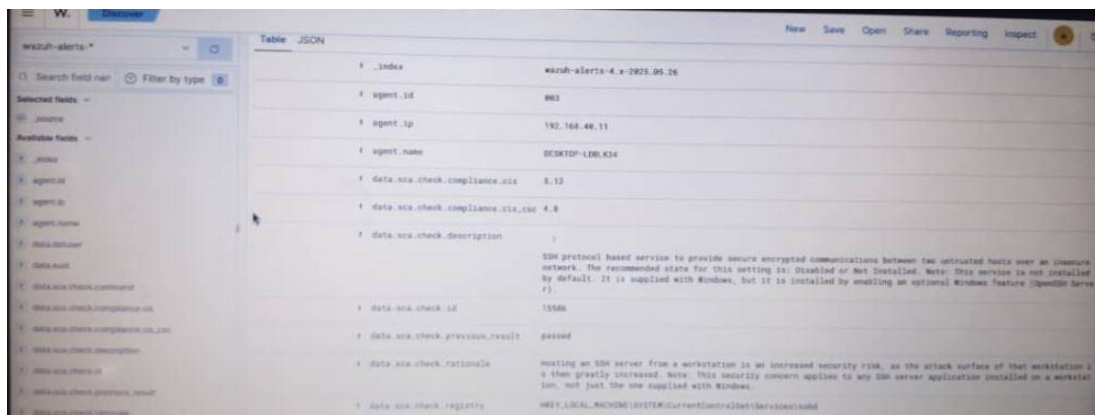


Figure 14: Showing the detected brute force attack on windows 10 via wazuh monitoring dashboard

The screenshot shows the Wazuh Alerts dashboard. On the left, there's a sidebar with 'Selected Fields' and 'Available Fields'. The main area displays a table of alerts. The first alert is for a brute force attack on Ubuntu.

Field	Value
_index	wazuh-alerts-4.x-2025.05.26
agent.id	003
agent.ip	192.168.48.11
agent.name	DESKTOP-LDBK34
data.sca.check.compliance.cis	5.12
data.sca.check.compliance.cis_csc	4.8
data.sca.check.description	SSH protocol based service to provide secure encrypted communications between two untrusted hosts over an insecure network. The recommended state for this setting is: Disabled or Not Installed. Note: This service is not installed by default. It is supplied with Windows, but it is installed by enabling an optional Windows feature (OpenSSH Server).
data.sca.check.id	15586
data.sca.check.previous.result	passed
data.sca.check.rationale	Hosting an SSH server from a workstation is an increased security risk, as the attack surface of the workstation is then greatly increased. Note: This security concern applies to any SSH server application installed on a workstation, not just the one supplied with Windows.
data.sca.check.registry	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\sshd

Figure 15: Showing the detected bruteforce attack on Ubuntu via wazuh monitoring dashboard

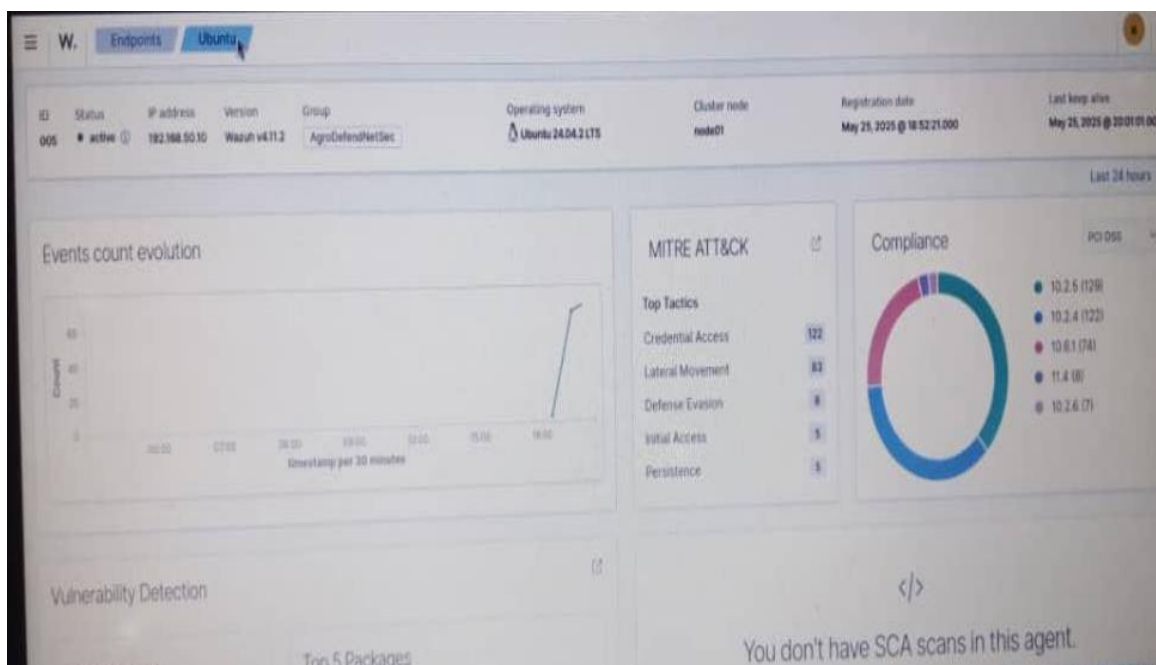


Figure 16: Showing Wazuh Mitre Att&ck Dashboard of Ubuntu Brute-force Attack

7. Incident Response Workflow

Step	Action
1. Detection	Wazuh detects brute-force attempt on SSH
2. Alerting	Wazuh received medium/high alert from both Targets via dashboard
3. Investigation	Analyst inspects logs, confirms source IP 192.168.60.10 from Corpnet
4. Containment	pfSense updated to block attacking IP
5. Eradication	Cleanup of payloads/shells from Ubuntu
6. Recovery	System restored from snapshot
7.LessonsLearned	Tuning Wazuh rules, firewall policy updates

8. Key Findings

Threat	Detected	Response
SSH Brute-Force	Yes (Wazuh Rule ID 5710)	IP blocked via pfSense
HTTP Exploit	Yes (via Apache logs)	Patch applied to Ubuntu
Reverse Shell	Partial (Improved by custom rule)	Manual analysis triggered

9. Recommendations

- **Enhance segmentation rules:** Restrict unnecessary ports, add alerts on inter-segment scans.
- **Automated firewall updates:** Integrate Wazuh with pfSense for dynamic blocking.
- **Patch management:** Ensure DMZ services are hardened and patched regularly.
- **Regular simulations:** Schedule red team simulations quarterly.
- **Honeypots:** Deploy honeypots to detect early intrusion attempts.

- **Rule tuning:** Continuously improve detection accuracy in Wazuh.
 - **Security Training:** Agrodefend firm should train employees regularly on security awareness. The use of strong passwords and MFA codes for login should be encouraged.
 - **Service Banners:** exposure of service banners and OS information should be discouraged by the SOC team.
 - **Layered Defense:** The SOC team should create a strong layered defense for all segmented networks to strengthen security.
-

10. Conclusion

This project demonstrates the effectiveness of a segmented SOC environment in identifying, responding to, and mitigating threats targeting Ubuntu and Windows 10 systems. Using Kali Linux for emulation and Wazuh for monitoring, Agrodefend firm can proactively defend against real-world cyber threats.

11. Appendices

A. Network Diagram (Textual Representation)

