Red vs Blue Proxmox Lab Project

Master's Research Project – CYBR-5960-02

Team C – Fall 2025

Saint Louis University

Presented by: Swarupa Jeedimetla, Pranay Garapati, Dheeraj Kumar, Mani Sharan Chakali, Brahmendra Chowdary Ponduri,

Project Phases

1. Build
2. Harden
3. Monitor
4. Attack
5. Defend

Lab Architecture

Core Components

Proxmox

Virtualization platform

VyOS Router

WAN/LAN routing + NAT

pfSense Firewall

LAN protection + DHCP

Windows 10 VM

User endpoint + services (FTP/SSH/SMB/HTTP/NetBIOS)

Ubuntu VM

Internal system + Wazuh Manager

Sysmon

Detailed Windows event logging

Kali Linux

Scanning & recon

WireGuard VPN

Secure access to Red vs Blue target

Data Flow

Windows/Ubuntu → pfSense → VyOS → Internet

Windows → Sysmon → Wazuh → Dashboard

Week 1 - Lab Environment Setup | Mail - Swarupa Jeedimetla - Outl | earsup - Proxmox Virtual Environ

https://proxmox.ears-up-cybersec.com/#v1:0:=node%2Fearsup:4:::::::

PROXMOX Virtual Environment 8.4.0 Search

Documentation | Create VM | Create CT | Swarupa@pve

Server View

- Datacenter
  - earsup
    - 30051 (Team-C-VyOs)
    - 30052 (Team-C-PfSense)
    - 30053 (Team-C-Ubuntu)
    - 30054 (Team-C-Windows10)

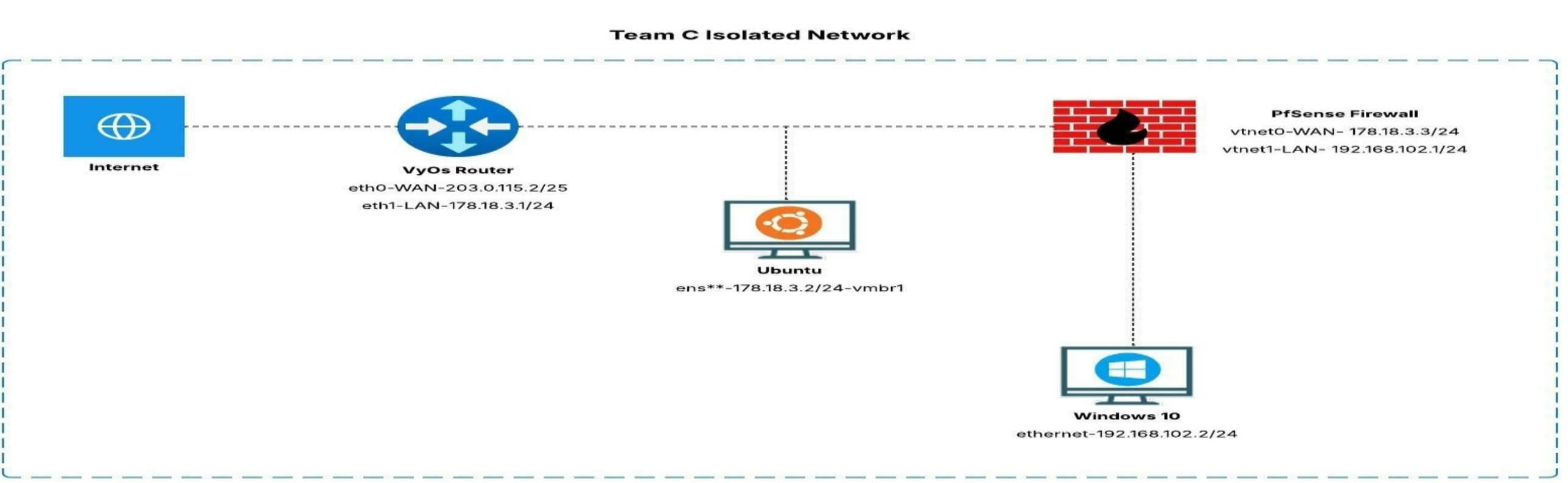
Node 'earsup'

Reboot | Shutdown | Shell | Bulk Actions | Help

Search | Task History | Subscription

Search:

Type	Description	Disk usage…	Memory us…	CPU usage	Uptime	Host CPU …
qemu	30051 (Team-C-VyOs)	0.0 %	84.2 %	0.4% of 2 …	23:22:25	0.9% of 1 …
qemu	30052 (Team-C-PfSense)	0.0 %	76.4 %	2.3% of 2 …	23:29:39	4.6% of 1 …
qemu	30053 (Team-C-Ubuntu)	0.0 %	94.4 %	0.3% of 2 …	23:22:21	0.7% of 1 …
qemu	30054 (Team-C-Windows10)	0.0 %	79.1 %	1.0% of 4 …	17:24:10	3.9% of 1 …



Network Build (Proxmox)- VyOS

What We Did

1. Set IP Address
2. Configured network bridges
   WAN, LAN, Internal
3. Configured DNS and Added source NAT rule
4. Verified connectivity

```
yos@vyos# ping google.com
ING google.com (172.217.4.46) 56(84) bytes of data.
4 bytes from lga15s46-in-f46.1e100.net (172.217.4.46): icmp_seq=1 ttl=113 time=
8.0 ms
4 bytes from lga15s46-in-f14.1e100.net (172.217.4.46): icmp_seq=2 ttl=113 time=
8.0 ms
4 bytes from lga15s46-in-f14.1e100.net (172.217.4.46): icmp_seq=3 ttl=113 time=
6.2 ms
4 bytes from lga15s46-in-f14.1e100.net (172.217.4.46): icmp_seq=4 ttl=113 time=
9.6 ms
C
-- google.com ping statistics ---
 packets transmitted, 4 received, 0% packet loss, time 3005ms
tt min/avg/max/mdev = 16.200/17.956/19.631/1.213 ms
edit]
yos@vyos# ping 8.8.8.8
ING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=113 time=16.8 ms
4 bytes from 8.8.8.8: icmp_seq=2 ttl=113 time=20.4 ms
4 bytes from 8.8.8.8: icmp_seq=3 ttl=113 time=22.7 ms
4 bytes from 8.8.8.8: icmp_seq=4 ttl=113 time=18.6 ms
4 bytes from 8.8.8.8: icmp_seq=5 ttl=113 time=17.7 ms
```

Network Build (Proxmox)-pfSense

What We Did

1. Set IP address
2. Configured network bridges
   WAN, LAN, Internal
3. Enabled DHCP server
4. Verified full connectivity
   router → firewall → Ubuntu → Windows → Internet

Purpose

Build a working enterprise-style network as our project foundation.

```
The IPv4 LAN address has been set to 192.168.102.1/24
You can now access the webConfigurator by opening the following URL in your web
browser:
                    http://192.168.102.1/

Press <ENTER> to continue.
QEMU Guest - Netgate Device ID: 658b7a3f465d42ee92cd

*** Welcome to pfSense 2.8.0-RELEASE (amd64) on pfSense ***

 WAN (wan)  -> vtnet0 -> v4: 172.18.3.3/24
 LAN (lan)  -> vtnet1 -> v4: 192.168.102.1/24

 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:
```

```
 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: 7


Enter a host name or IP address: 192.168.102.2

PING 192.168.102.2 (192.168.102.2): 56 data bytes
64 bytes from 192.168.102.2: icmp_seq=0 ttl=128 time=0.594 ms
64 bytes from 192.168.102.2: icmp_seq=1 ttl=128 time=0.600 ms
64 bytes from 192.168.102.2: icmp_seq=2 ttl=128 time=0.710 ms

--- 192.168.102.2 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.594/0.635/0.710/0.053 ms

Press ENTER to continue.
```

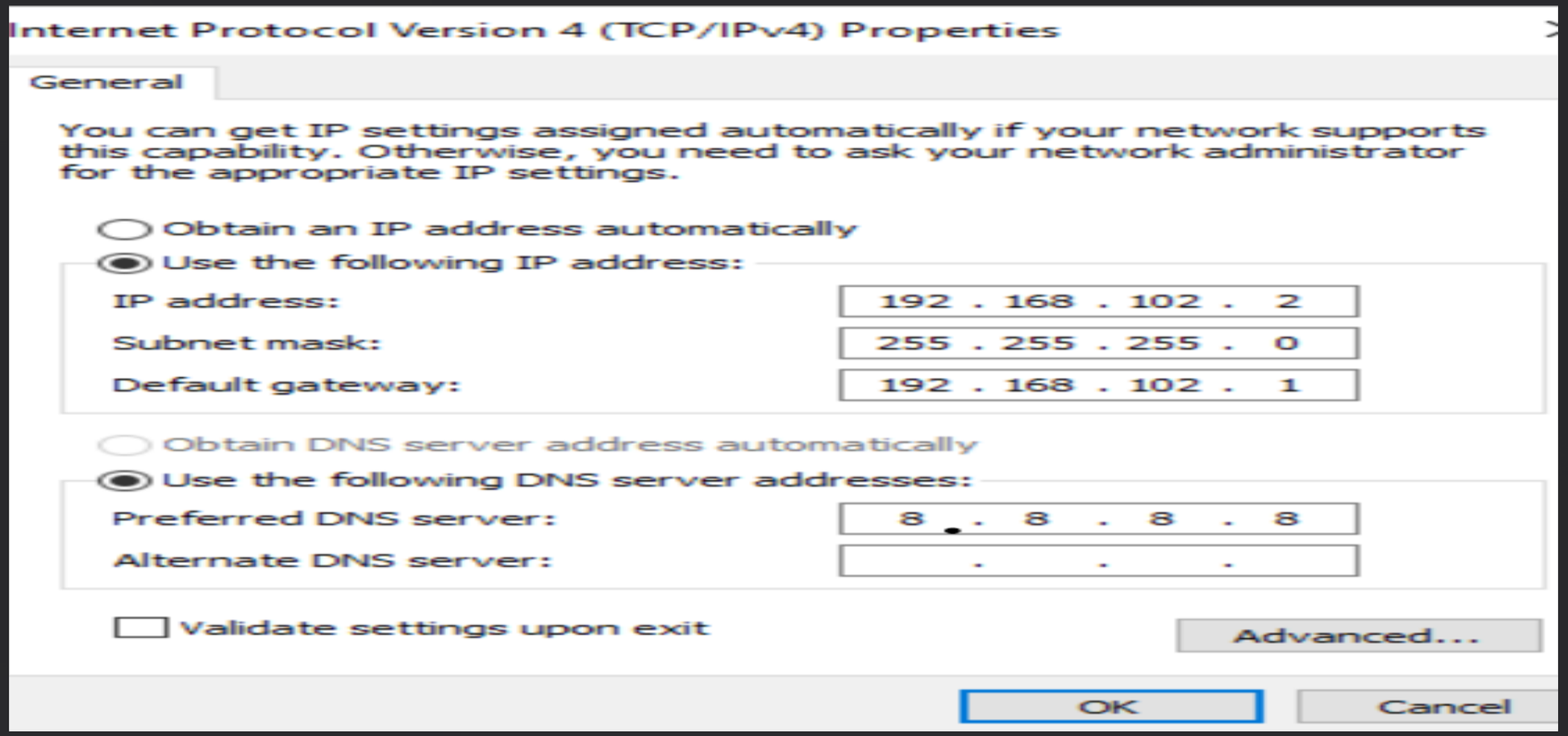
Network Build (Proxmox)- Windows

What We Did

1. Configured IPv4 properties
2. Configured DNS
3. Added pfsense Rules
4. Verified full connectivity

   router → firewall → Ubuntu → Windows → Internet

IPv4 Properties and pfSense Rules



Automatic Rules

	Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description
✓	WAN	127.0.0.0/8 ::1/128 192.168.102.0/24	*	*	500	WAN address	*	✓	Auto created rule for ISAKMP
✓	WAN	127.0.0.0/8 ::1/128 192.168.102.0/24	*	*	*	WAN address	*		

Network 3
Connected

Command Prompt

```
Ping statistics for 178.18.3.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\Admin>ping 178.18.3.3

Pinging 178.18.3.3 with 32 bytes of data:
Reply from 178.18.3.3: bytes=32 time<1ms TTL=64
Reply from 178.18.3.3: bytes=32 time<1ms TTL=64
Reply from 178.18.3.3: bytes=32 time<1ms TTL=64
Reply from 178.18.3.3: bytes=32 time<1ms TTL=64

Ping statistics for 178.18.3.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Admin>ping 192.168.102.1

Pinging 192.168.102.1 with 32 bytes of data:
Reply from 192.168.102.1: bytes=32 time<1ms TTL=64
Reply from 192.168.102.1: bytes=32 time<1ms TTL=64
Reply from 192.168.102.1: bytes=32 time<1ms TTL=64
Reply from 192.168.102.1: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.102.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Admin>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=20ms TTL=111
Reply from 8.8.8.8: bytes=32 time=14ms TTL=111
Reply from 8.8.8.8: bytes=32 time=16ms TTL=111
Reply from 8.8.8.8: bytes=32 time=16ms TTL=111

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 14ms, Maximum = 20ms, Average = 16ms
```

Network Build (Proxmox)- Ubuntu

What We Did

1. Removed old addresses
2. Assign New Address
3. Corrected Ubuntu IP

   178.18.3.2
4. Set DNS resolver
5. Verified full connectivity

   router → firewall → Ubuntu → Windows → Internet

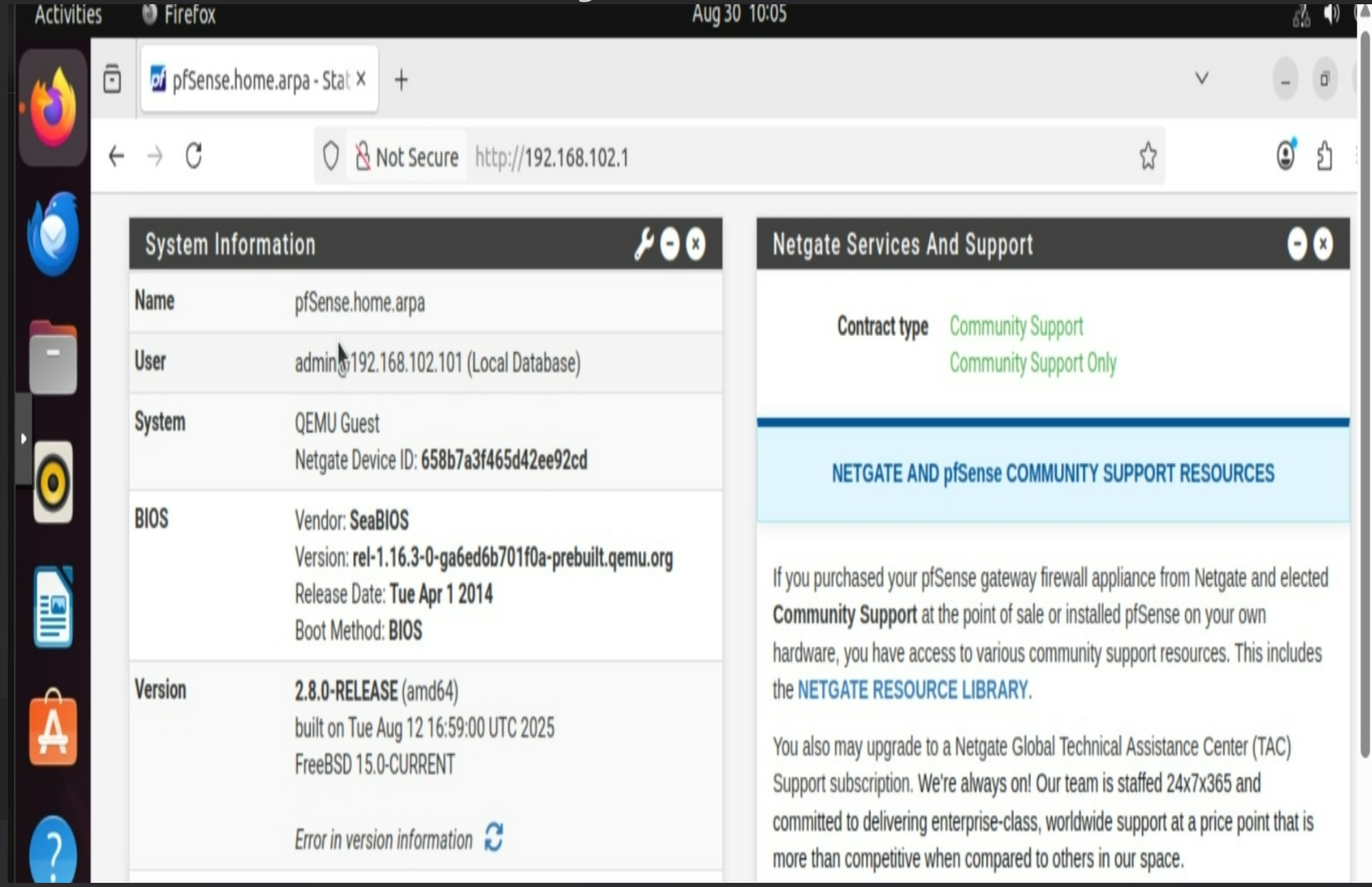
```
anonymous@anonymous-Standard-PC-i440FX-PIIX-1996:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens18: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether bc:24:11:90:08:41 brd ff:ff:ff:ff:ff:ff
    altname enp0s18
    inet 172.18.3.2/24 scope global ens18
       valid_lft forever preferred_lft forever
anonymous@anonymous-Standard-PC-i440FX-PIIX-1996:~$ sudo ip addr flush dev eth0
Device "eth0" does not exist.
anonymous@anonymous-Standard-PC-i440FX-PIIX-1996:~$
```

```
anonymous@anonymous-Standard-PC-i440FX-PIIX-1996:~$ sudo ip link set ens18 up
anonymous@anonymous-Standard-PC-i440FX-PIIX-1996:~$ sudo ip route add default via 178.18.3.1
anonymous@anonymous-Standard-PC-i440FX-PIIX-1996:~$ sudo bash -c 'echo "nameserver 8.8.8.8" > /etc/resolv.conf'
anonymous@anonymous-Standard-PC-i440FX-PIIX-1996:~$ ping -c 3 178.18.3.1
PING 178.18.3.1 (178.18.3.1) 56(84) bytes of data.
64 bytes from 178.18.3.1: icmp_seq=1 ttl=64 time=0.664 ms
64 bytes from 178.18.3.1: icmp_seq=2 ttl=64 time=0.306 ms
64 bytes from 178.18.3.1: icmp_seq=3 ttl=64 time=0.301 ms

--- 178.18.3.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2083ms
rtt min/avg/max/mdev = 0.301/0.423/0.664/0.169 ms
anonymous@anonymous-Standard-PC-i440FX-PIIX-1996:~$ ping -c 3 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=112 time=19.6 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=112 time=20.2 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=112 time=18.8 ms

--- 8.8.8.8 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 18.781/19.538/20.219/0.589 ms
anonymous@anonymous-Standard-PC-i440FX-PIIX-1996:~$ ping -c 3 google.com
PING google.com (172.217.4.46) 56(84) bytes of data.
64 bytes from ord38s18-in-f14.1e100.net (172.217.4.46): icmp_seq=1 ttl=112 time=18.5 ms
64 bytes from lga15s46-in-f46.1e100.net (172.217.4.46): icmp_seq=2 ttl=112 time=16.9 ms
64 bytes from lga15s46-in-f46.1e100.net (172.217.4.46): icmp_seq=3 ttl=112 time=17.8 ms

--- google.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 16.898/17.736/18.465/0.644 ms
anonymous@anonymous-Standard-PC-i440FX-PIIX-1996:~$
```

Routing & Firewall Connectivity

Ubuntu VM

- Can ping VyOS, pfSense, and access internet
- Opened pfSense GUI via browser (validation)



Full Connectivity Matrix

All connections tested : Connections Verified

All systems operational

Connection	Status
VyOS → Internet	✓
VyOS → Ubuntu	✓
VyOS → pfSense	✓
Ubuntu → Internet	✓
pfSense → Internet	✓
Windows → pfSense	✓
Windows → Internet	✓

Every system can talk to every required destination with **no failures**.

Architecture Interpretation

- VyOS = main router
- pfSense = firewall protecting Windows
- Ubuntu = internal machine
- Windows = endpoint behind firewall
- NAT ensures internet access for all VMs

Windows Services + Firewall Controls

Windows Configuration

- Verified internet with ping 8.8.8.8
- We created a Non-Admin User called Jimmy

Services Enabled

FTP (21)	SSH (22)	HTTP (80)
SMB (445)	NetBIOS (137–139)	

pfSense Rules

- Allowed only these ports via LAN rules
- Added NAT port-forwarding to Windows
- Controlled which services are exposed/blocked

Ubuntu Validation

Successfully reached all 5 services via commands + browser (FTP, SSH, SMB, HTTP, NetBIOS)

Purpose: Simulate real-world attack surface and protect it with firewall rules.

QEMU (Team-C-Windows10) - noVNC - Google Chrome

proxmox.ears-up-cybersec.com/?console=kvm&novnc=1&vmid=30054&vmname=Team-C-Windows10&node=earsup&resize=off

69°F
Mostly cloudy

Search

5:59 PM
9/5/2025

proxmox.ears-up-cybersec.com/?console=kvm&novnc=1&vmid=30053&vmname=Team-C-Ubuntu&node=earsup&resize=off

Floating WAN LAN

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓	0/92.79 MiB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	
✓	0/0 B	IPv4 TCP/ UDP	*	*	192.168.102.2	137 - 139	*	none			
✓	0/0 B	IPv4 TCP	*	*	192.168.102.2	445 (MS DS)	*	none			
✓	0/0 B	IPv4 TCP	*	*	192.168.102.2	80 (HTTP)	*	none			
✓	0/0 B	IPv4 TCP	*	*	192.168.102.2	22 (SSH)	*	none			
✓	0/0 B	IPv4 TCP	*	*	192.168.102.2	21 (FTP)	*	none			
✓	0/0 B	IPv4 TCP	LAN subnets	*	This Firewall (self)	80 (HTTP)	*	none			
✓	0/27.09 GiB	IPv4 *	LAN subnets	*	*	*	*	none			

73°F
Sunny

Search

5:47 PM
9/7/2025

Wazuh Manager Setup (Ubuntu)

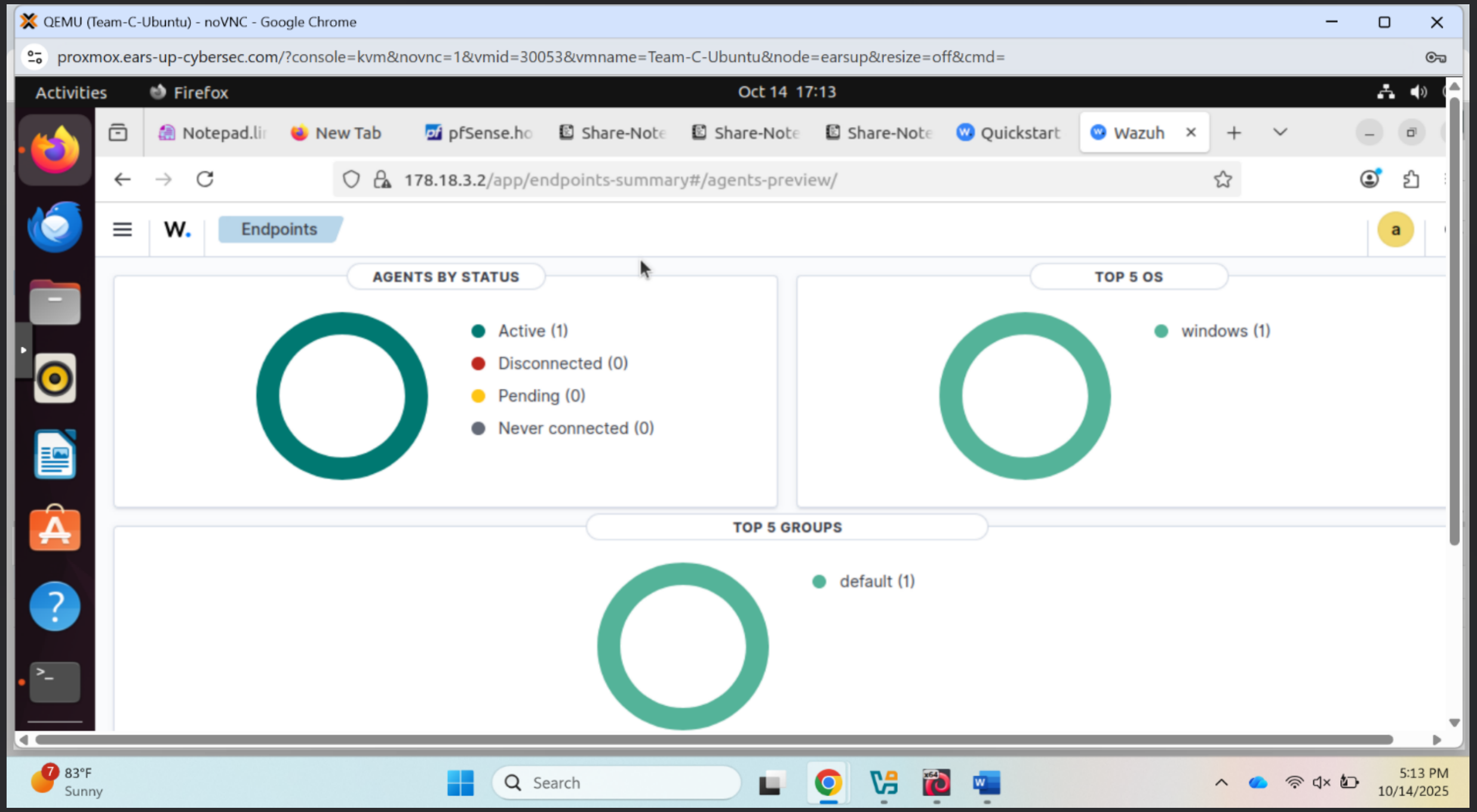
What We Did

- Installed **Wazuh Manager** on Ubuntu
- Started the service and accessed the Wazuh Dashboard
- Verified that the SIEM is running correctly.

Why It Matters

- Wazuh acts as the central log collector
- It allows Blue Team to monitor all system activity from one place

Pipeline Begins: Windows → pfSense → Wazuh Manager → Dashboard

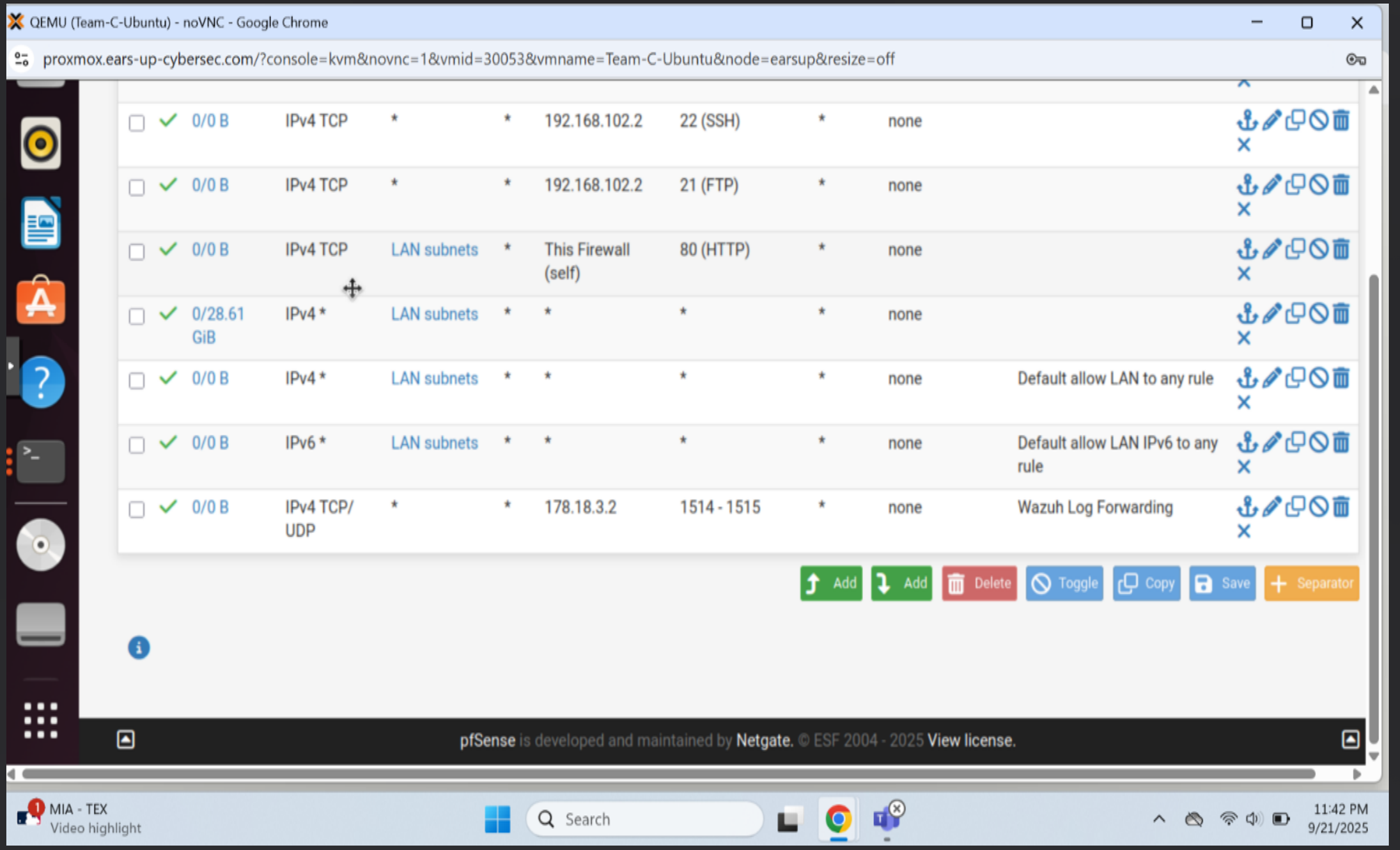

QEMU (Team-C-Ubuntu) - noVNC - Google Chrome
proxmox.ears-up-cybersec.com/?console=kvm&novnc=1&vmid=30053&vmname=Team-C-Ubuntu&node=earsup&resize=off&cmd=
Activities
Firefox
Oct 14 17:13
Notepad.li
New Tab
pfSense.ho
Share-Note
Share-Note
Share-Note
Quickstart
Wazuh
178.18.3.2/app/endpoints-summary#/agents-preview/
Endpoints
a
AGENTS BY STATUS
Active (1)
Disconnected (0)
Pending (0)
Never connected (0)
TOP 5 OS
windows (1)
TOP 5 GROUPS
default (1)
83°F
Sunny
Search
5:13 PM
10/14/2025

Firewall Rules + Log Flow Verification

pfSense Firewall Rules

Allowed essential Wazuh communication ports:

- **1514** – log events
- **1515** – agent registration (From Week 4: Fig 3)
- The rules were saved, accessed and verified as live in the firewall logs.


QEMU (Team-C-Ubuntu) - noVNC - Google Chrome
proxmox.ears-up-cybersec.com/?console=kvm&novnc=1&vmid=30053&vmname=Team-C-Ubuntu&node=earsup&resize=off
0/0 B IPv4 TCP * * 192.168.102.2 22 (SSH) * none
0/0 B IPv4 TCP * * 192.168.102.2 21 (FTP) * none
0/0 B IPv4 TCP LAN subnets * This Firewall (self) 80 (HTTP) * none
0/28.61 GiB IPv4 * LAN subnets * * * * none
0/0 B IPv4 * LAN subnets * * * * none Default allow LAN to any rule
0/0 B IPv6 * LAN subnets * * * * none Default allow LAN IPv6 to any rule
0/0 B IPv4 TCP/ UDP * * 178.18.3.2 1514 - 1515 * none Wazuh Log Forwarding
Add
Add
Delete
Toggle
Copy
Save
Separator
pfSense is developed and maintained by Netgate. © ESF 2004 - 2025 View license.
MIA - TEX
Video highlight
Search
11:42 PM
9/21/2025

Wazuh Agent + Sysmon Setup (Windows)

Wazuh Agent

- Installed on Windows and connected to Manager IP (178.18.3.2)
- Status: Connected but **Not Active** (initially)

Sysmon Installation

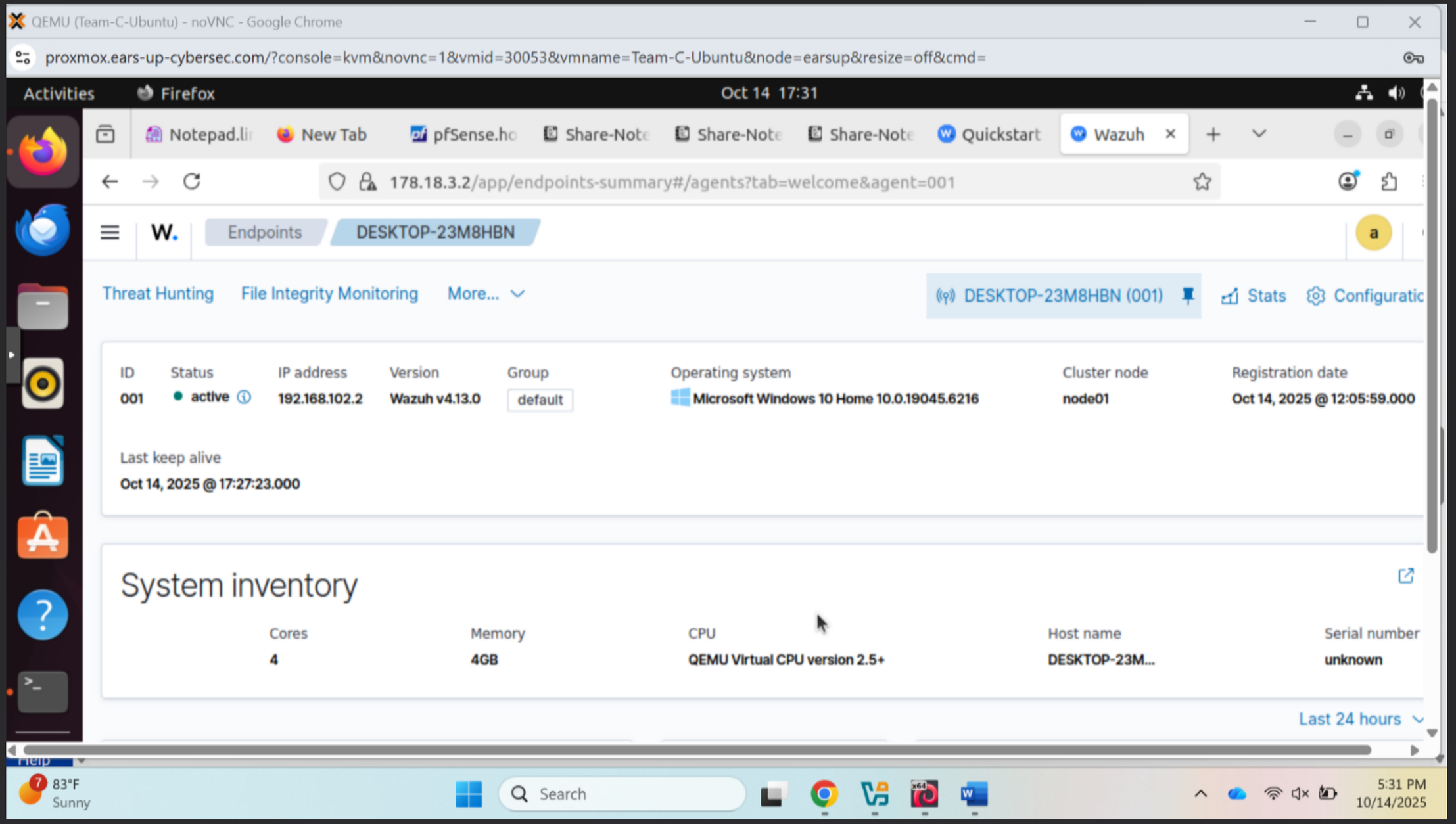
- Installed Sysmon service
- Applied Sysmon XML configuration (From Week 4: Fig 5–6)

Purpose

Sysmon generates detailed logs:

- Process creation
- Network connections
- File changes
- Possible attack behaviors

Wazuh collects and alerts on these events


QEMU (Team-C-Ubuntu) - noVNC - Google Chrome
proxmox.ears-up-cybersec.com/?console=kvm&novnc=1&vmid=30053&vmname=Team-C-Ubuntu&node=earsup&resize=off&cmd=
Activities
Firefox
Oct 14 17:31
Notepad.li
New Tab
pfSense.ho
Share-Note
Share-Note
Share-Note
Quickstart
Wazuh
178.18.3.2/app/endpoints-summary#/agents?tab=welcome&agent=001
Endpoints
DESKTOP-23M8HBN
Threat Hunting
File Integrity Monitoring
More...
DESKTOP-23M8HBN (001)
Stats
Configuratic
ID
001
Status
active
IP address
192.168.102.2
Version
Wazuh v4.13.0
Group
default
Operating system
Microsoft Windows 10 Home 10.0.19045.6216
Cluster node
node01
Registration date
Oct 14, 2025 @ 12:05:59.000
Last keep alive
Oct 14, 2025 @ 17:27:23.000
System inventory
Cores
4
Memory
4GB
CPU
QEMU Virtual CPU version 2.5+
Host name
DESKTOP-23M...
Serial number
unknown
Last 24 hours
83°F
Sunny
Search
5:31 PM
10/14/2025

```
PS C:\Windows\system32> Get-Service  sysmon64

Status   Name               DisplayName
------   ----               -----------
Running  Sysmon64           sysmon64

PS C:\Windows\system32>
```

Administrator: Command Prompt

```
website.

Specify -accepteula to automatically accept the EULA on installation, otherwise you will be interactively prompted to
accept it.

Neither install nor uninstall requires a reboot.


F:\test\Sysmon>sysmon64.exe -c Sysmonconfig.xml


System Monitor v15.15 - System activity monitor
By Mark Russinovich and Thomas Garnier
Copyright (C) 2014-2024 Microsoft Corporation
Using libxml2. libxml2 is Copyright (C) 1998-2012 Daniel Veillard. All Rights Reserved.
Sysinternals - www.sysinternals.com

Loading configuration file with schema version 4.50
Sysmon schema version: 4.90
Configuration file validated.
Configuration updated.


F:\test\Sysmon>
```

Administrator: Command Prompt

```
      <data name="ProcessGuid" inType="win:GUID" />
      <data name="ProcessId" inType="win:UInt32" outType="win:PID" />
      <data name="User" inType="win:UnicodeString" outType="xs:string" />
      <data name="Image" inType="win:UnicodeString" outType="xs:string" />
      <data name="TargetFilename" inType="win:UnicodeString" outType="xs:string" />
      <data name="Hashes" inType="win:UnicodeString" outType="xs:string" />
    </event>
    <event name="SYSMONEVENT_FILE_BLOCK_SHREDDING" value="28" level="Informational" template="File Block Shredding" rulename="FileBlockShredding" version="5"
>
      <data name="RuleName" inType="win:UnicodeString" outType="xs:string" />
      <data name="UtcTime" inType="win:UnicodeString" outType="xs:string" />
      <data name="ProcessGuid" inType="win:GUID" />
      <data name="ProcessId" inType="win:UInt32" outType="win:PID" />
      <data name="User" inType="win:UnicodeString" outType="xs:string" />
      <data name="Image" inType="win:UnicodeString" outType="xs:string" />
      <data name="TargetFilename" inType="win:UnicodeString" outType="xs:string" />
      <data name="Hashes" inType="win:UnicodeString" outType="xs:string" />
      <data name="IsExecutable" inType="win:Boolean" />
    </event>
    <event name="SYSMONEVENT_FILE_EXE_DETECTED" value="29" level="Informational" template="File Executable Detected" rulename="FileExecutableDetected" versio
n="5">
      <data name="RuleName" inType="win:UnicodeString" outType="xs:string" />
      <data name="UtcTime" inType="win:UnicodeString" outType="xs:string" />
      <data name="ProcessGuid" inType="win:GUID" />
      <data name="ProcessId" inType="win:UInt32" outType="win:PID" />
      <data name="User" inType="win:UnicodeString" outType="xs:string" />
      <data name="Image" inType="win:UnicodeString" outType="xs:string" />
      <data name="TargetFilename" inType="win:UnicodeString" outType="xs:string" />
      <data name="Hashes" inType="win:UnicodeString" outType="xs:string" />
    </event>
  </events>
</manifest>

F:\test\Sysmon>Sysmon64.exe -c sysmonconfig.xml


System Monitor v15.15 - System activity monitor
By Mark Russinovich and Thomas Garnier
Copyright (C) 2014-2024 Microsoft Corporation
```

QEMU (Team-C-Ubuntu) - noVNC - Google Chrome

proxmox.ears-up-cybersec.com/?console=kvm&novnc=1&vmid=30053&vmname=Team-C-Ubuntu&node=earsup&resize=off

Filter by type 0

Add filter

Selected fields

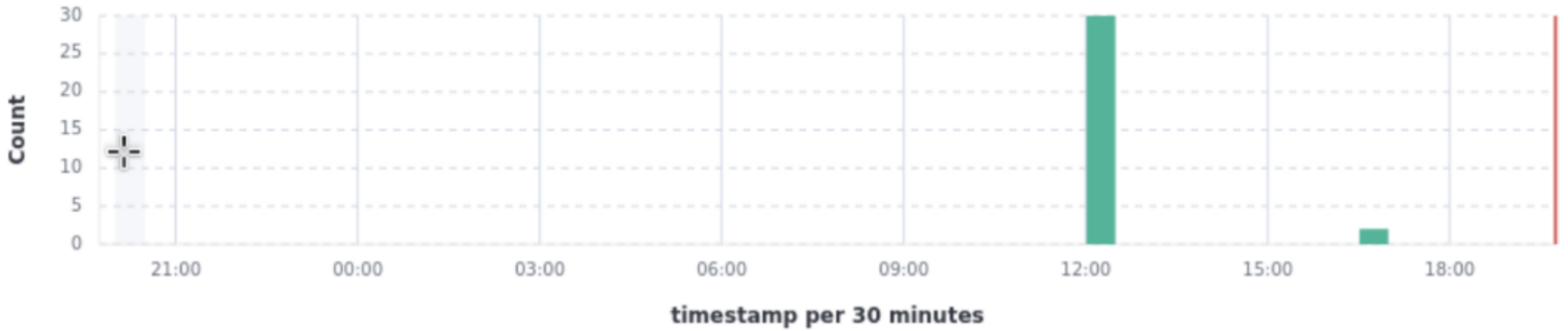
_source

Available fields

- _index
- agent.id
- agent.ip
- agent.name
- data.dstuser
- data.extra_data
- data.sca.check.command
- data.sca.check.compliance.cis
- data.sca.check.compliance.cis_csc
- data.sca.check.compliance.gdpr_IV
- data.sca.check.compliance.gpg_13

32 hits

Oct 13, 2025 @ 19:44:36.895 - Oct 14, 2025 @ 19:44:36.895 per Auto



timestamp per 30 minutes

t	manager.name	anonymous-Standard-PC-i440FX-PIIX-1996
t	rule.description	C:\\Windows\\SysWOW64\\SecEdit.exe binary in a suspicious location launched by C:\\Windows\\SysWOW64\\WindowsPowerShell\\v1.0\\powershell.exe
#	rule.firedtimes	1
t	rule.groups	sysmon, sysmon_eid1_detections, windows
t	rule.id	92066
#	rule.level	4
◯	rule.mail	false

Temps to plum...
Saturday

Search

7:50 PM
10/14/2025

Windows 10 Hardening

Security Improvements Applied

- System Updates & Defense
  - Installed all Windows updates
  - Verified Windows Defender is active
  - Enabled all firewall profiles (Domain, Private, Public)
  - Added firewall rule for Wazuh (port 1514)
- Access & Service Controls
  - Turned on **Ransomware Protection** (Controlled Folder Access)
  - Set **minimum password length = 12**
  - Disabled Guest account
  - Disabled unnecessary services (e.g., RemoteRegistry)
- Monitoring & Logging
  - Reviewed Event Logs (4624 and 4625 login records)

Goal: Reduce attack surface and enforce strong security posture.

Ubuntu Hardening (Internal System)

Configured Security Controls

- Checked and restricted Sudo users
- Applied stronger password policies
- Enabled **UFW firewall**:
  - Allowed only required ports: 22, 80, 443, 1514
- Disabled unneeded services (ex: CUPS)
- Reviewed logs using journalctl and /var/log/syslog

Purpose: Ensure the Linux system is hardened and only running what is needed.

Baseline Validation (Network, Services, SIEM)

Connectivity Validation

All systems reached expected destinations :

VyOS ⇔ Ubuntu ⇔ pfSense ⇔ Windows ⇔ Internet

Service Port Validation

Confirmed all Windows services still working:

- FTP (21)
- SSH (22)
- HTTP (80)
- SMB (445)
- NetBIOS (137–139)

Wazuh Verification

- Sysmon logs flowing into Wazuh Manager
- Alerts visible on dashboard

Why This Matters: Ensures no misconfigurations before Red vs Blue testing.

External Recon on OWASP Juice Shop

Passive Recon (No Touching Target)

- WHOIS: No domain info (Heroku subdomain)
- DNS Lookup (dig + nslookup):
  - IPs: 46.137.15.86, 54.73.53.134, 54.220.192.176 → Hosted on AWS

Active Scanning

- Nmap host discovery: All 3 IPs alive
- Port scan results: → **Only 80 (HTTP) and 443 (HTTPS) open**, everything else filtered (Table 1 + Fig 5–7)

Web Vulnerability Scan (Nikto) Findings:

- Missing security headers (HSTS, X-Content-Type-Options)
- Possible BREACH vulnerability
- Exposed directories: /ftp/
- Backup/certificate files (.war, .tar, .pem) (From Fig 10)

Enumeration

- Netcat → 403 Forbidden
- enum4linux → No SMB/LDAP services

Purpose: Understand public-facing attack surface; no exploitation performed.

WireGuard VPN (Red vs Blue Lab Access)

Setup

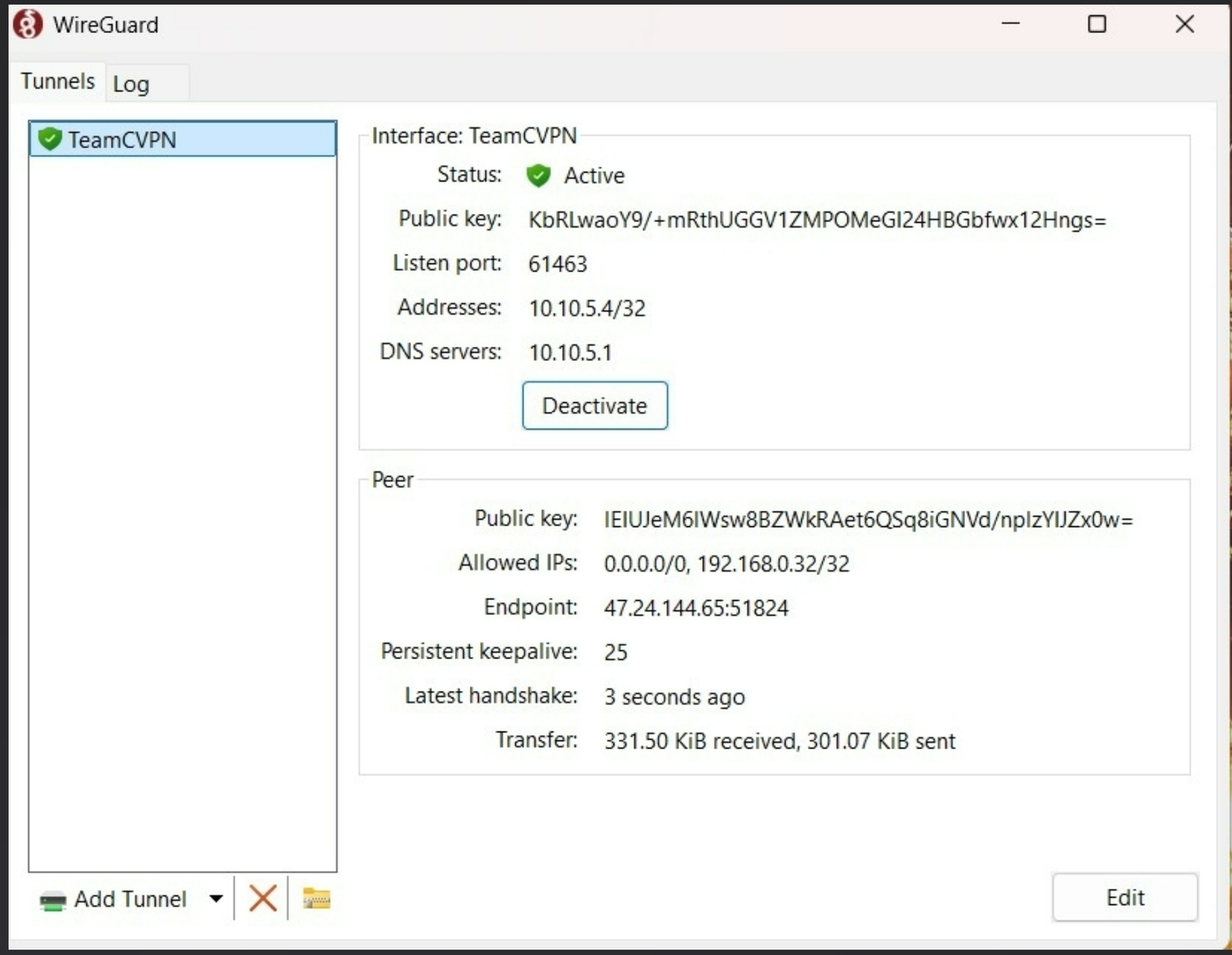
- Installed WireGuard
- Imported team VPN configuration
- Tunnel activated → **Status: Active** (Fig 1)

Connectivity Tests

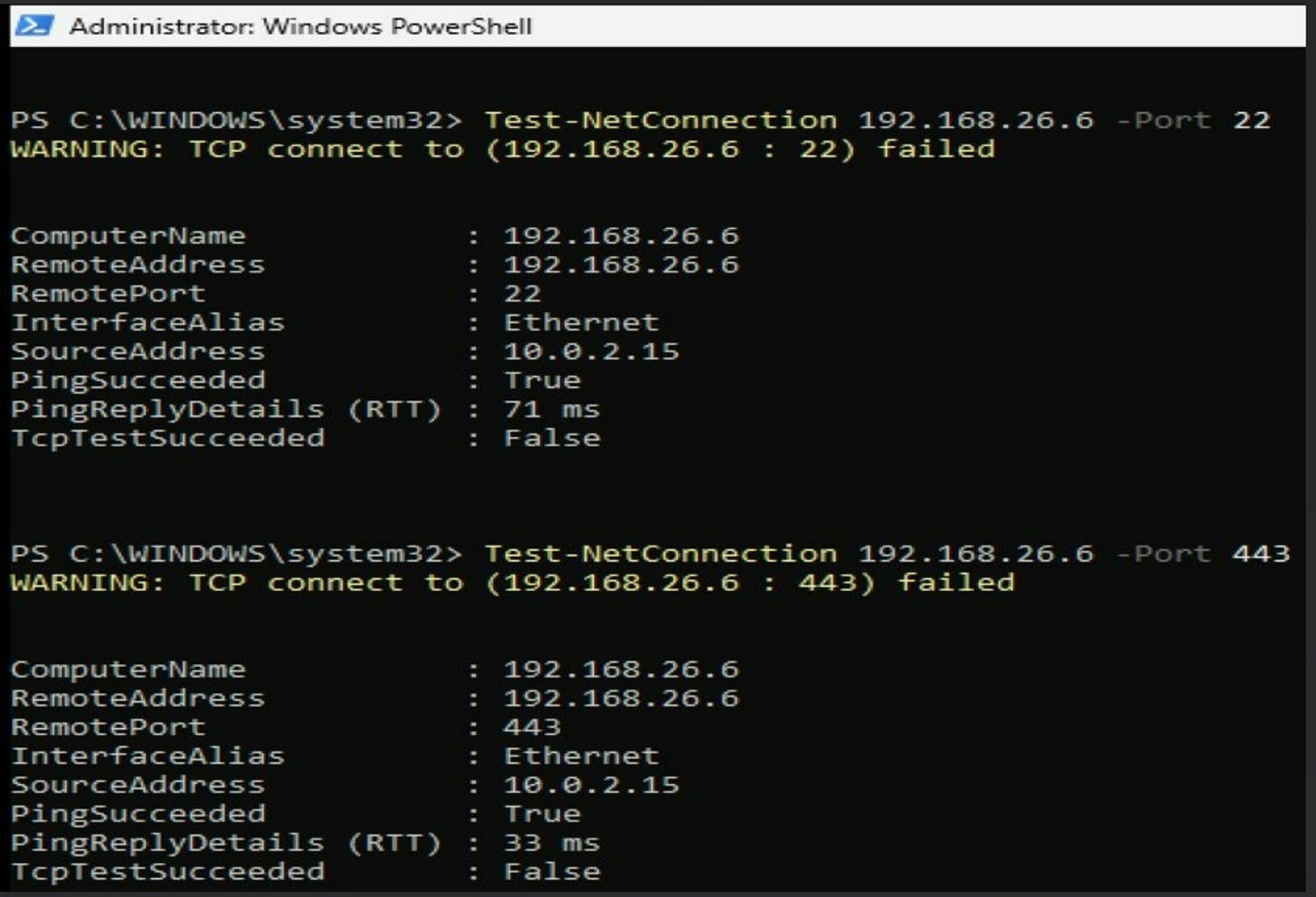
- Ping 192.168.26.6 → 0% loss (VPN working) (Fig 3)
- Port 80 (HTTP) → **Open**
- Port 22 (SSH) → Closed
- Port 443 (HTTPS) → Closed (Fig 2)

Why VPN Matters

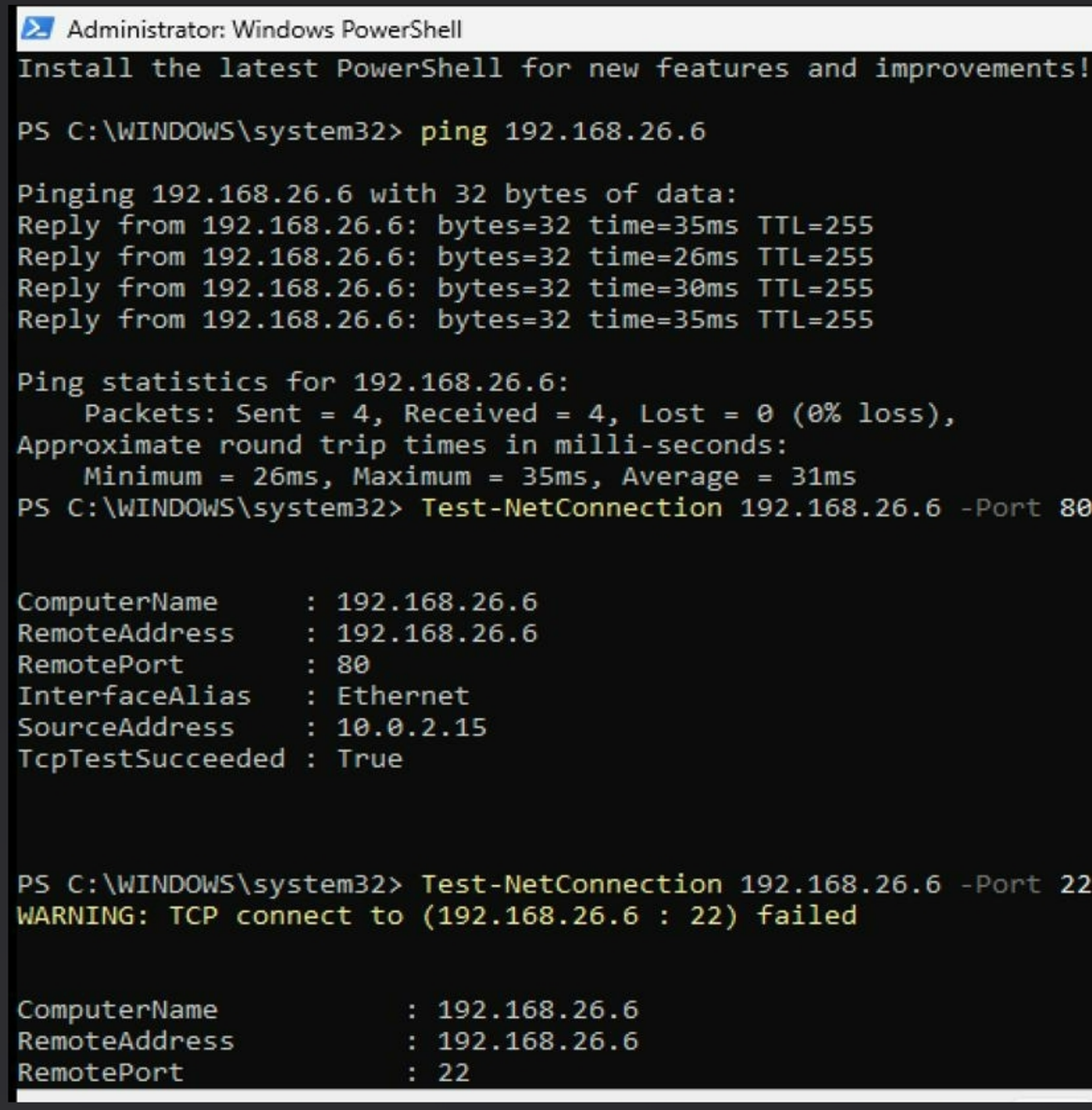
- Encrypts all traffic
- Isolates the lab from the real internet
- Allows safe Red Team attacks
- Helps Blue Team monitor network traffic (Page 5–6)



Port 22 Connection Testing:



Ping Testing:



Red Team Results

Target: 192.168.26.6 (Secure Windows Computer)

What We Could Access

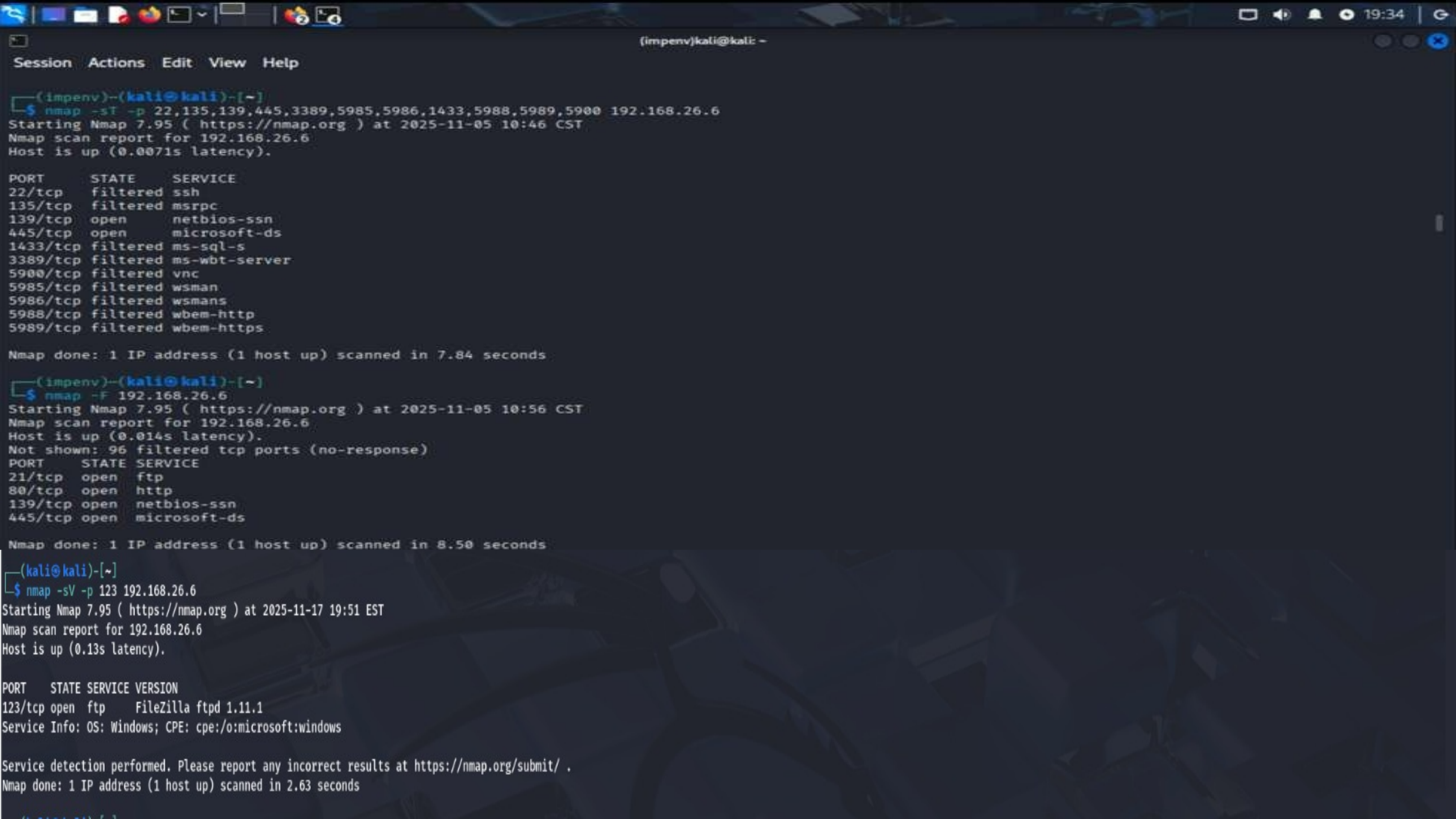
- Only FTP, SMB, and HTTP were available.
- We logged into SMB using test credentials (**admin : password**).
- We saw shared folders: ADMIN$, C$, F$, IPC$
- We logged into FTP using default credentials (Anonymous: Anonymous)

Findings

- The web server (IIS) showed its default page and had TRACE enabled. This could let attackers steal cookies .
- Our scans (Nmap & Legion) found only SMB, FTP, and HTTP were open .
- Repeated attempts to guess SMB passwords were blocked (the password policy worked well) .
- SMB signing was off, meaning someone could trick us into connecting to a fake server (Man-in-the-Middle attack risk).
- RPC showed details about the operating system

Outcome: We could access SMB, but we could not gain higher access or run remote code.

Active scanning with **Nmap** and **Legion** revealed multiple open ports and active services on the target


(impenv)kali@kali: ~
Session Actions Edit View Help
(impenv)-(kali@kali)-[~]
$ nmap -sT -p 22,135,139,445,3389,5985,5986,1433,5988,5989,5900 192.168.26.6
Starting Nmap 7.95 (https://nmap.org) at 2025-11-05 10:46 CST
Nmap scan report for 192.168.26.6
Host is up (0.0071s latency).
PORT STATE SERVICE
22/tcp filtered ssh
135/tcp filtered msrpc
139/tcp open netbios-ssn
445/tcp open microsoft-ds
1433/tcp filtered ms-sql-s
3389/tcp filtered ms-wbt-server
5900/tcp filtered vnc
5985/tcp filtered wsman
5986/tcp filtered wsmans
5988/tcp filtered wbem-http
5989/tcp filtered wbem-https
Nmap done: 1 IP address (1 host up) scanned in 7.84 seconds
(impenv)-(kali@kali)-[~]
$ nmap -F 192.168.26.6
Starting Nmap 7.95 (https://nmap.org) at 2025-11-05 10:56 CST
Nmap scan report for 192.168.26.6
Host is up (0.014s latency).
Not shown: 96 filtered tcp ports (no-response)
PORT STATE SERVICE
21/tcp open ftp
80/tcp open http
139/tcp open netbios-ssn
445/tcp open microsoft-ds
Nmap done: 1 IP address (1 host up) scanned in 8.50 seconds
(kali@kali)-[~]
$ nmap -sV -p 123 192.168.26.6
Starting Nmap 7.95 (https://nmap.org) at 2025-11-17 19:51 EST
Nmap scan report for 192.168.26.6
Host is up (0.13s latency).
PORT STATE SERVICE VERSION
123/tcp open ftp FileZilla ftpd 1.11.1
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.63 seconds

Finding 2: SMB Access Achieved

- Successful login allowed access to SMB shares:
ADMIN$, C$, F$, IPC$

- No guest or null sessions were allowed, indicating restricted unauthenticated access


(impenv)kali@kali: ~
Session Actions Edit View Help
└─$ smbclient -L //192.168.26.6 -U 'admin%password'
Sharename Type Comment
ADMIN$ Disk Remote Admin
C$ Disk Default share
F$ Disk Default share
IPC$ IPC Remote IPC
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 192.168.26.6 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
┌──(impenv)─(kali㉿kali)-[~]
└─$ smbmap -H 192.168.26.6 -u admin -p password
SMBMap - Samba Share Enumerator v1.10.7 | Shawn Evans - ShawnDEvans@gmail.com
https://github.com/ShawnDEvans/smbmap
[*] Detected 1 hosts serving SMB
[*] Established 1 SMB connections(s) and 1 authenticated session(s)
[+] IP: 192.168.26.6:445 Name: 192.168.26.6 Status: Authenticated
Disk Permissions Comment
ADMIN$ NO ACCESS Remote Admin
C$ NO ACCESS Default share
F$ NO ACCESS Default share
IPC$ READ ONLY Remote IPC
[*] Closed 1 connections
┌──(impenv)─(kali㉿kali)-[~]
└─$ enum4linux -a 192.168.26.6
Starting enum4linux v0.9.1 (http://labs.portcullis.co.uk/application/enum4linux/) on Wed Nov 5 11:06:09 2025

Finding 3: SMB Login Brute-Force Attempts Blocked

- A brute-force login attempt was executed using Metasploit’s smb_login module
- Multiple username/password combinations were tested against the SMB service
- All login attempts failed, indicating effective authentication protections

```
File  Actions  Edit  View  Help
Metasploit Documentation: https://docs.metasploit.com/

msf6 > use auxiliary/scanner/smb/smb_login
msf6 auxiliary(scanner/smb/smb_login) > set RHOSTS 192.168.26.6
RHOSTS => 192.168.26.6
msf6 auxiliary(scanner/smb/smb_login) > set USER_FILE /home/kali/Downloads/usernames.txt
USER_FILE => /home/kali/Downloads/usernames.txt
msf6 auxiliary(scanner/smb/smb_login) > set PASS_FILE /tmp/passlist_safe.txt
PASS_FILE => /tmp/passlist_safe.txt
msf6 auxiliary(scanner/smb/smb_login) > run

[*] 192.168.26.6:445      - 192.168.26.6:445 - Starting SMB login bruteforce
[-] 192.168.26.6:445      - 192.168.26.6:445 - Failed: '.\3d:!!!4545',
[-] 192.168.26.6:445      - 192.168.26.6:445 - Failed: '.\3d:!"123',
[-] 192.168.26.6:445      - 192.168.26.6:445 - Failed: '.\3d:!";1234',
[-] 192.168.26.6:445      - 192.168.26.6:445 - Failed: '.\3d:!"")',
[-] 192.168.26.6:445      - 192.168.26.6:445 - Failed: '.\3d:!()*#"EL',
[-] 192.168.26.6:445      - 192.168.26.6:445 - Failed: '.\3d:!)QPA:Z?',
[-] 192.168.26.6:445      - 192.168.26.6:445 - Failed: '.\3d:!4543435',
[-] 192.168.26.6:445      - 192.168.26.6:445 - Failed: '.\3d:!@#!@#',
[-] 192.168.26.6:445      - 192.168.26.6:445 - Failed: '.\3d:!@#$%^&',
[-] 192.168.26.6:445      - 192.168.26.6:445 - Failed: '.\3d:!@#$%^&*(',
[-] 192.168.26.6:445      - 192.168.26.6:445 - Failed: '.\3d:!@#$%^&*()',
[-] 192.168.26.6:445      - 192.168.26.6:445 - Failed: '.\3d:!@#dsa3',
[-] 192.168.26.6:445      - 192.168.26.6:445 - Failed: '.\3d:!@$@@',
[-] 192.168.26.6:445      - 192.168.26.6:445 - Failed: '.\3d:!@QWASZX',
[-] 192.168.26.6:445      - 192.168.26.6:445 - Failed: '.\3d:!AWX#DRV%G',
[-] 192.168.26.6:445      - 192.168.26.6:445 - Failed: '.\3d:!Q@W#E',
[-] 192.168.26.6:445      - 192.168.26.6:445 - Failed: '.\3d:!QAZ@WSX#EDC',
[-] 192.168.26.6:445      - 192.168.26.6:445 - Failed: '.\3d:!("5"',
[-] 192.168.26.6:445      - 192.168.26.6:445 - Failed: '.\3d:##$#%@!',
[-] 192.168.26.6:445      - 192.168.26.6:445 - Failed: '.\3d:#*eidkc,',
[-] 192.168.26.6:445      - 192.168.26.6:445 - Failed: '.\3d:#@!',
[-] 192.168.26.6:445      - 192.168.26.6:445 - Failed: '.\3d:#J-{;BX',
[-] 192.168.26.6:445      - 192.168.26.6:445 - Failed: '.\3d:#JO25s',
[-] 192.168.26.6:445      - 192.168.26.6:445 - Failed: '.\3d:$"-E*(',
[-] 192.168.26.6:445      - 192.168.26.6:445 - Failed: '.\3d:$#@!',
[-] 192.168.26.6:445      - 192.168.26.6:445 - Failed: '.\3d:$dd',
[-] 192.168.26.6:445      - 192.168.26.6:445 - Failed: '.\3d:%,r<xr77',
[-] 192.168.26.6:445      - 192.168.26.6:445 - Failed: '.\3d:%`U%LbL',
[-] 192.168.26.6:445      - 192.168.26.6:445 - Failed: '.\3d:')(@#',
[-] 192.168.26.6:445      - 192.168.26.6:445 - Failed: '.\3d:'0-)@',
[-] 192.168.26.6:445      - 192.168.26.6:445 - Failed: '.\3d:'=*Xw0y`',
[-] 192.168.26.6:445      - 192.168.26.6:445 - Failed: '.\3d:(4958',
[-] 192.168.26.6:445      - 192.168.26.6:445 - Failed: '.\3d:(CBB&"',
[-] 192.168.26.6:445      - 192.168.26.6:445 - Failed: '.\3d:(e"&<N(P',
[-] 192.168.26.6:445      - 192.168.26.6:445 - Failed: '.\3d:)#s0#as',
[-] 192.168.26.6:445      - 192.168.26.6:445 - Failed: '.\3d:)$DFS',
[-] 192.168.26.6:445      - 192.168.26.6:445 - Failed: '.\3d:)*&>+$m',
[-] 192.168.26.6:445      - 192.168.26.6:445 - Failed: '.\3d:)@##(*',
```

Finding 4: SMB Signing Disabled

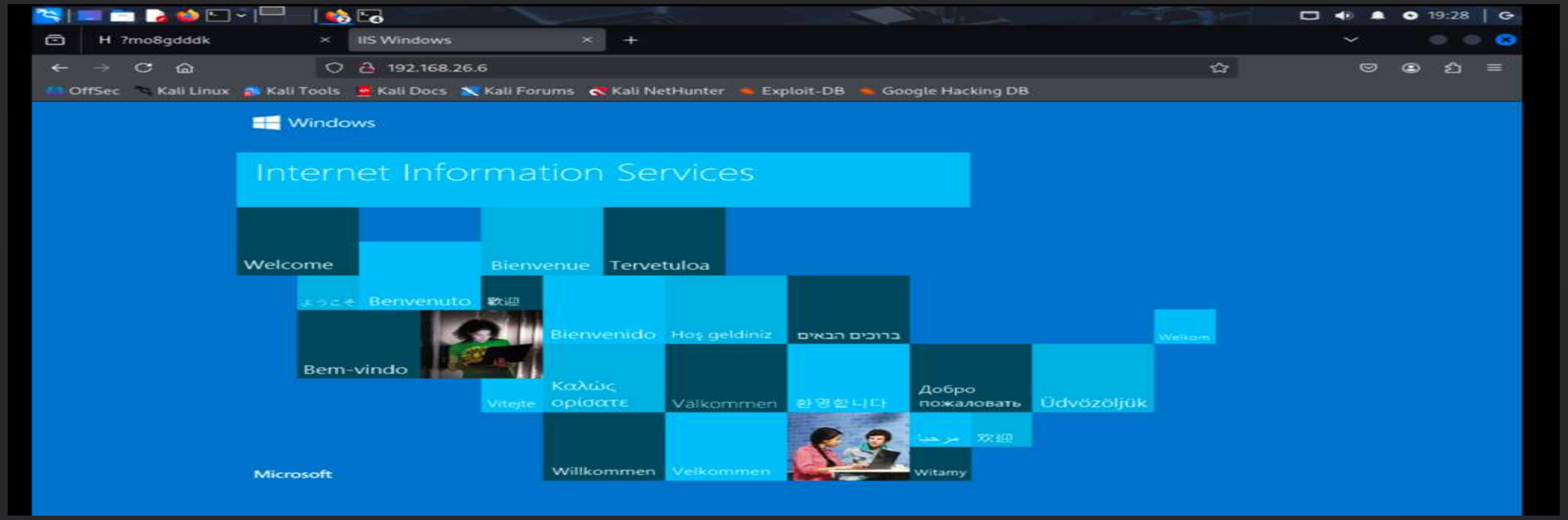
- Using CrackMapExec, we confirmed that the target's SMB service had SMB signing disabled.

```
┌──(kali㉿kali)-[~]
└─$ cat /home/kali/Downloads/passlist.txt | tr -cd '[:print:]\n' > /tmp/passlist_safe.txt

┌──(kali㉿kali)-[~]
└─$ cat /home/kali/Downloads/passlist.txt | tr -cd '[:print:]\n' > /tmp/passlist_safe.txt

┌──(kali㉿kali)-[~]
└─$ crackmapexec smb 192.168.26.6 -u /home/kali/Downloads/usernames.txt -p /tmp/passlist_safe.txt
SMB         192.168.26.6    445    DESKTOP-ONSK8JU  [*] Windows 10.0 Build 19041 (name:DESKTOP-ONSK8JU) (domain:DESKTOP-ONSK8JU) (signing:False) (SMBv1:False)
SMB         192.168.26.6    445    DESKTOP-ONSK8JU  [-] DESKTOP-ONSK8JU\3d:!!!4545 STATUS_LOGON_FAILURE
SMB         192.168.26.6    445    DESKTOP-ONSK8JU  [-] DESKTOP-ONSK8JU\3d:!"123 STATUS_LOGON_FAILURE
SMB         192.168.26.6    445    DESKTOP-ONSK8JU  [-] DESKTOP-ONSK8JU\3d:!";1234 STATUS_LOGON_FAILURE
SMB         192.168.26.6    445    DESKTOP-ONSK8JU  [-] DESKTOP-ONSK8JU\3d:!"") STATUS_LOGON_FAILURE
SMB         192.168.26.6    445    DESKTOP-ONSK8JU  [-] DESKTOP-ONSK8JU\3d:!()*#"EL STATUS_LOGON_FAILURE
SMB         192.168.26.6    445    DESKTOP-ONSK8JU  [-] DESKTOP-ONSK8JU\3d:!)QPA:Z? STATUS_LOGON_FAILURE
SMB         192.168.26.6    445    DESKTOP-ONSK8JU  [-] DESKTOP-ONSK8JU\3d:!4543435 STATUS_LOGON_FAILURE
SMB         192.168.26.6    445    DESKTOP-ONSK8JU  [-] DESKTOP-ONSK8JU\3d:!@#!@# STATUS_LOGON_FAILURE
SMB         192.168.26.6    445    DESKTOP-ONSK8JU  [-] DESKTOP-ONSK8JU\3d:!@#$%^& STATUS_LOGON_FAILURE
SMB         192.168.26.6    445    DESKTOP-ONSK8JU  [-] DESKTOP-ONSK8JU\3d:!@#$%^&*( STATUS_LOGON_FAILURE
SMB         192.168.26.6    445    DESKTOP-ONSK8JU  [-] DESKTOP-ONSK8JU\3d:!@#$%^&*() STATUS_LOGON_FAILURE
SMB         192.168.26.6    445    DESKTOP-ONSK8JU  [-] DESKTOP-ONSK8JU\3d:!@#dsa3 STATUS_LOGON_FAILURE
SMB         192.168.26.6    445    DESKTOP-ONSK8JU  [-] DESKTOP-ONSK8JU\3d:!@$@@ STATUS_LOGON_FAILURE
SMB         192.168.26.6    445    DESKTOP-ONSK8JU  [-] DESKTOP-ONSK8JU\3d:!@QWASZX STATUS_LOGON_FAILURE
SMB         192.168.26.6    445    DESKTOP-ONSK8JU  [-] DESKTOP-ONSK8JU\3d:!AWX#DRV%G STATUS_LOGON_FAILURE
SMB         192.168.26.6    445    DESKTOP-ONSK8JU  [-] DESKTOP-ONSK8JU\3d:!Q@W#E STATUS_LOGON_FAILURE
SMB         192.168.26.6    445    DESKTOP-ONSK8JU  [-] DESKTOP-ONSK8JU\3d:!QAZ@WSX#EDC STATUS_LOGON_FAILURE
SMB         192.168.26.6    445    DESKTOP-ONSK8JU  [-] DESKTOP-ONSK8JU\3d:!("5" STATUS_LOGON_FAILURE
SMB         192.168.26.6    445    DESKTOP-ONSK8JU  [-] DESKTOP-ONSK8JU\3d:##$#%@! STATUS_LOGON_FAILURE
SMB         192.168.26.6    445    DESKTOP-ONSK8JU  [-] DESKTOP-ONSK8JU\3d:#*eidkc, STATUS_LOGON_FAILURE
SMB         192.168.26.6    445    DESKTOP-ONSK8JU  [-] DESKTOP-ONSK8JU\3d:#@! STATUS_LOGON_FAILURE
SMB         192.168.26.6    445    DESKTOP-ONSK8JU  [-] DESKTOP-ONSK8JU\3d:#J-{;BX STATUS_LOGON_FAILURE
SMB         192.168.26.6    445    DESKTOP-ONSK8JU  [-] DESKTOP-ONSK8JU\3d:#JO25s STATUS_LOGON_FAILURE
SMB         192.168.26.6    445    DESKTOP-ONSK8JU  [-] DESKTOP-ONSK8JU\3d:$"-E*( STATUS_LOGON_FAILURE
SMB         192.168.26.6    445    DESKTOP-ONSK8JU  [-] DESKTOP-ONSK8JU\3d:$#@! STATUS_LOGON_FAILURE
SMB         192.168.26.6    445    DESKTOP-ONSK8JU  [-] DESKTOP-ONSK8JU\3d:$dd STATUS_LOGON_FAILURE
SMB         192.168.26.6    445    DESKTOP-ONSK8JU  [-] DESKTOP-ONSK8JU\3d:%,r<xr77 STATUS_LOGON_FAILURE
SMB         192.168.26.6    445    DESKTOP-ONSK8JU  [-] DESKTOP-ONSK8JU\3d:%`U%LbL STATUS_LOGON_FAILURE
SMB         192.168.26.6    445    DESKTOP-ONSK8JU  [-] DESKTOP-ONSK8JU\3d:')(@# STATUS_LOGON_FAILURE
SMB         192.168.26.6    445    DESKTOP-ONSK8JU  [-] DESKTOP-ONSK8JU\3d:'0-)@ STATUS_LOGON_FAILURE
SMB         192.168.26.6    445    DESKTOP-ONSK8JU  [-] DESKTOP-ONSK8JU\3d:'=*Xw0y` STATUS_LOGON_FAILURE
SMB         192.168.26.6    445    DESKTOP-ONSK8JU  [-] DESKTOP-ONSK8JU\3d:(4958 STATUS_LOGON_FAILURE
SMB         192.168.26.6    445    DESKTOP-ONSK8JU  [-] DESKTOP-ONSK8JU\3d:(CBB&" STATUS_LOGON_FAILURE
SMB         192.168.26.6    445    DESKTOP-ONSK8JU  [-] DESKTOP-ONSK8JU\3d:(e"&<N(P STATUS_LOGON_FAILURE
SMB         192.168.26.6    445    DESKTOP-ONSK8JU  [-] DESKTOP-ONSK8JU\3d:)#s0#as STATUS_LOGON_FAILURE
SMB         192.168.26.6    445    DESKTOP-ONSK8JU  [-] DESKTOP-ONSK8JU\3d:)$DFS STATUS_LOGON_FAILURE
SMB         192.168.26.6    445    DESKTOP-ONSK8JU  [-] DESKTOP-ONSK8JU\3d:)*&>+$m STATUS_LOGON_FAILURE
SMB         192.168.26.6    445    DESKTOP-ONSK8JU  [-] DESKTOP-ONSK8JU\3d:)@##(* STATUS_LOGON_FAILURE
SMB         192.168.26.6    445    DESKTOP-ONSK8JU  [-] DESKTOP-ONSK8JU\3d:)@*6+d6 STATUS_LOGON_FAILURE
SMB         192.168.26.6    445    DESKTOP-ONSK8JU  [-] DESKTOP-ONSK8JU\3d:*aj!Ws STATUS_LOGON_FAILURE
```

Finding 5: Remote Service Information Disclosure via RPC

- Although most enumeration attempts were blocked, the srvinfo command successfully revealed Windows OS details
- The disclosed information included the system version and configuration data.


19:36
(impenv)kali@kali: ~
Log Out...
Session Actions Edit View Help
┌──(impenv)─(kali㉿kali)-[~]
└─$ rpcclient -U 'admin%password' 192.168.26.6
rpcclient $> srvinfo
192.168.26.6 Wk Sv NT
platform_id : 500
os version : 10.0
server type : 0×1003
rpcclient $> enumdomusers
result was NT_STATUS_CONNECTION_DISCONNECTED
rpcclient $> querydominfo
result was NT_STATUS_CONNECTION_DISCONNECTED
rpcclient $> netshareenumall
result was WERR_ACCESS_DENIED
rpcclient $> nmap - 5985,5896 192.168.26.6
command not found: nmap
rpcclient $> nmap -p 5985,5896 192.168.26.6
command not found: nmap
rpcclient $> nmap -p 5985,5896 192.168.26.6^C
┌──(impenv)─(kali㉿kali)-[~]
└─$ nmap -p 5895,5986 192.168.26.6
Starting Nmap 7.95 (https://nmap.org) at 2025-11-05 12:21 CST
Nmap scan report for 192.168.26.6
Host is up (0.00028s latency).
PORT STATE SERVICE
5895/tcp filtered unknown
5986/tcp filtered wsmans
Nmap done: 1 IP address (1 host up) scanned in 7.91 seconds
┌──(impenv)─(kali㉿kali)-[~]
└─$ secretsdump.py admin:password@192.168.26.6
Impacket v0.13.0 - Copyright Fortra, LLC and its affiliated companies
[-] RemoteOperations failed: DCERPC Runtime Error: code: 0×5 - rpc_s_access_denied
[*] Cleaning up...
┌──(impenv)─(kali㉿kali)-[~]
└─$ nmap -sn 192.168.26.0/24

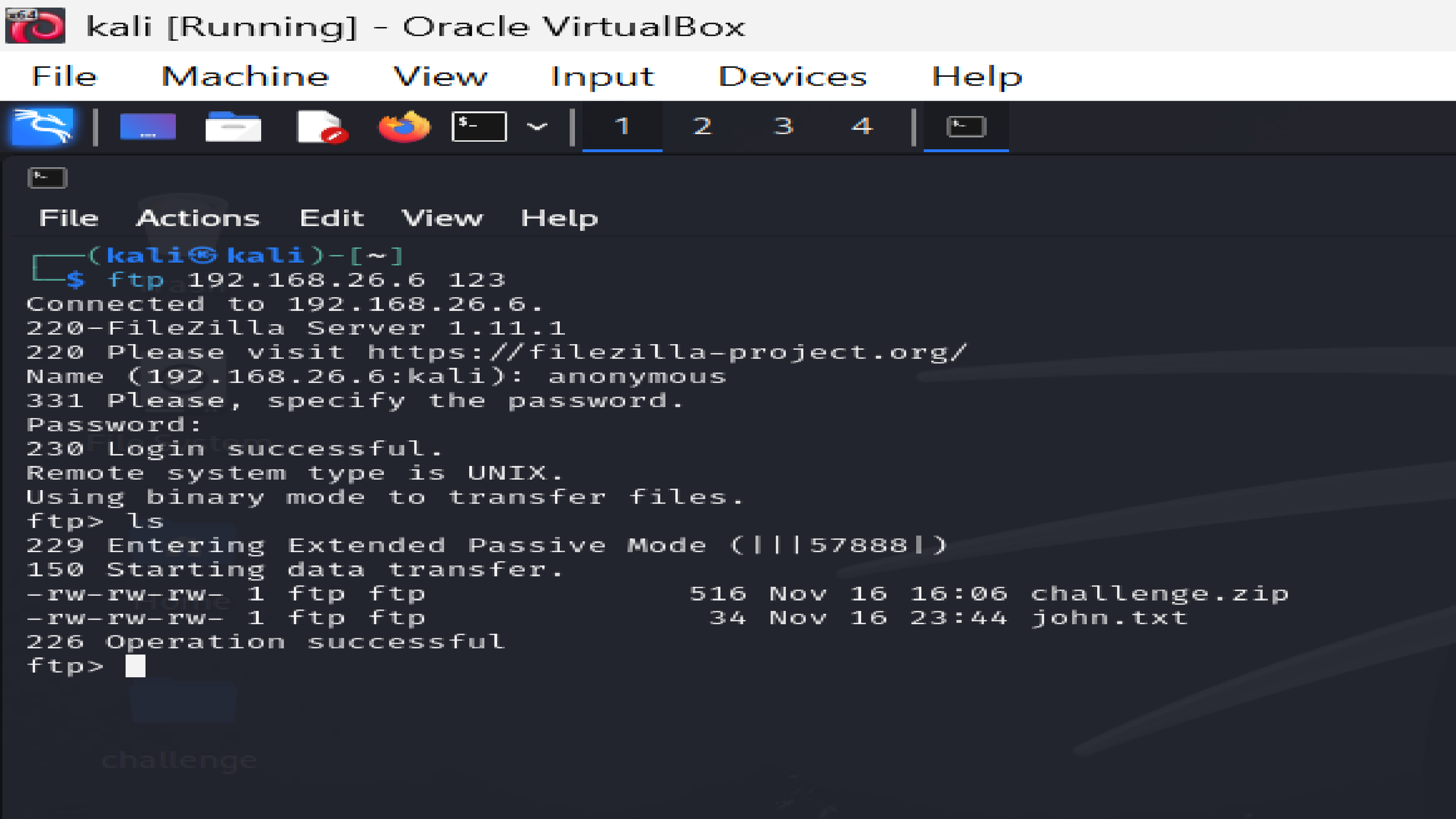


Finding 6: IIS Running with Default Configuration & TRACE Enabled

- Discovered **IIS Default Welcome Page**
- Web surface exists but no sensitive pages found

Finding 7: FTP Access on Port 123

- Port 123 was identified running an FTP service
- Two files were retrieved from the FTP directory:
  - John.txt
  - Challenge.zip


kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
File Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ ftp 192.168.26.6 123
Connected to 192.168.26.6.
220-FileZilla Server 1.11.1
220 Please visit https://filezilla-project.org/
Name (192.168.26.6:kali): anonymous
331 Please, specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||57888|)
150 Starting data transfer.
-rw-rw-rw- 1 ftp ftp 516 Nov 16 16:06 challenge.zip
-rw-rw-rw- 1 ftp ftp 34 Nov 16 23:44 john.txt
226 Operation successful
ftp>

```
┌──(kali㉿kali)-[~]
└─$ cat john.txt
I am not easy! Chat GPT will crash
```

```
┌──(kali㉿kali)-[~]
└─$ cat main.c
#include <stdio.h>
#include <string.h>
#include <stdlib.h>

void transform(char *s) {
    for (int i = 0; s[i]; i++) {
        s[i] = s[i] ^ (0x5A - (i % 3));    // XOR + pattern shift
    }
}

int main() {
    char input[64];

    unsigned char encoded[] = {
        0x08, 0x37, 0x1F, 0x08, 0x2E, 0x3B, 0x35, 0x08,
        0x0F, 0x3A, 0x1F, 0x08, 0x2E, 0x3B, 0x35, 0x00
    };

    for (int i = 0; encoded[i] != 0; i++) {
        encoded[i] ^= (0x5A - (i % 3));    // decode at runtime
    }

    printf("Enter the flag: ");
    fgets(input, sizeof(input), stdin);
    input[strcspn(input, "\n")] = 0;

    char check[64];
    strcpy(check, input);
    transform(check);

    if (strcmp(check, encoded) == 0) {
        printf("Correct! Flag: %s\n", input);
    } else {
        printf("Wrong flag!\n");
    }

    return 0;
}
```

main.c

Share Run

```c

    // DEBUG: show decoded target
    printf("[DEBUG] Decoded target string: %s\n", encoded);
    printf("[DEBUG] Decoded target hex: ");
    for (int i = 0; encoded[i] != 0; i++) {
        printf("%02X ", encoded[i]);
    }
    printf("\n");

    // Step 2: read user input normally
    printf("Enter the flag: ");
    fgets(input, sizeof(input), stdin);
    input[strcspn(input, "\n")] = 0;

    // DEBUG: just show raw input
    printf("[DEBUG] Raw input string: %s\n", input);

    // Step 3: compare input directly to decoded encoded[]
    if (strcmp(input, (char *)encoded) == 0) {
        printf("Correct! Flag: %s\n", input);
    } else {
        printf("Wrong flag!\n");
    }

    return 0;
}

```

Output

```
[DEBUG] Decoded target string: RnGRwcoQW`FPtbm
[DEBUG] Decoded target hex: 52 6E 47 52 77 63 6F 51 57 60 46 5
Enter the flag: RnGRwcoQW`FPtbm
[DEBUG] Raw input string: RnGRwcoQW`FPtbm
Correct! Flag: RnGRwcoQW`FPtbm


=== Code Execution Successful ===
```

Summary of Attacks

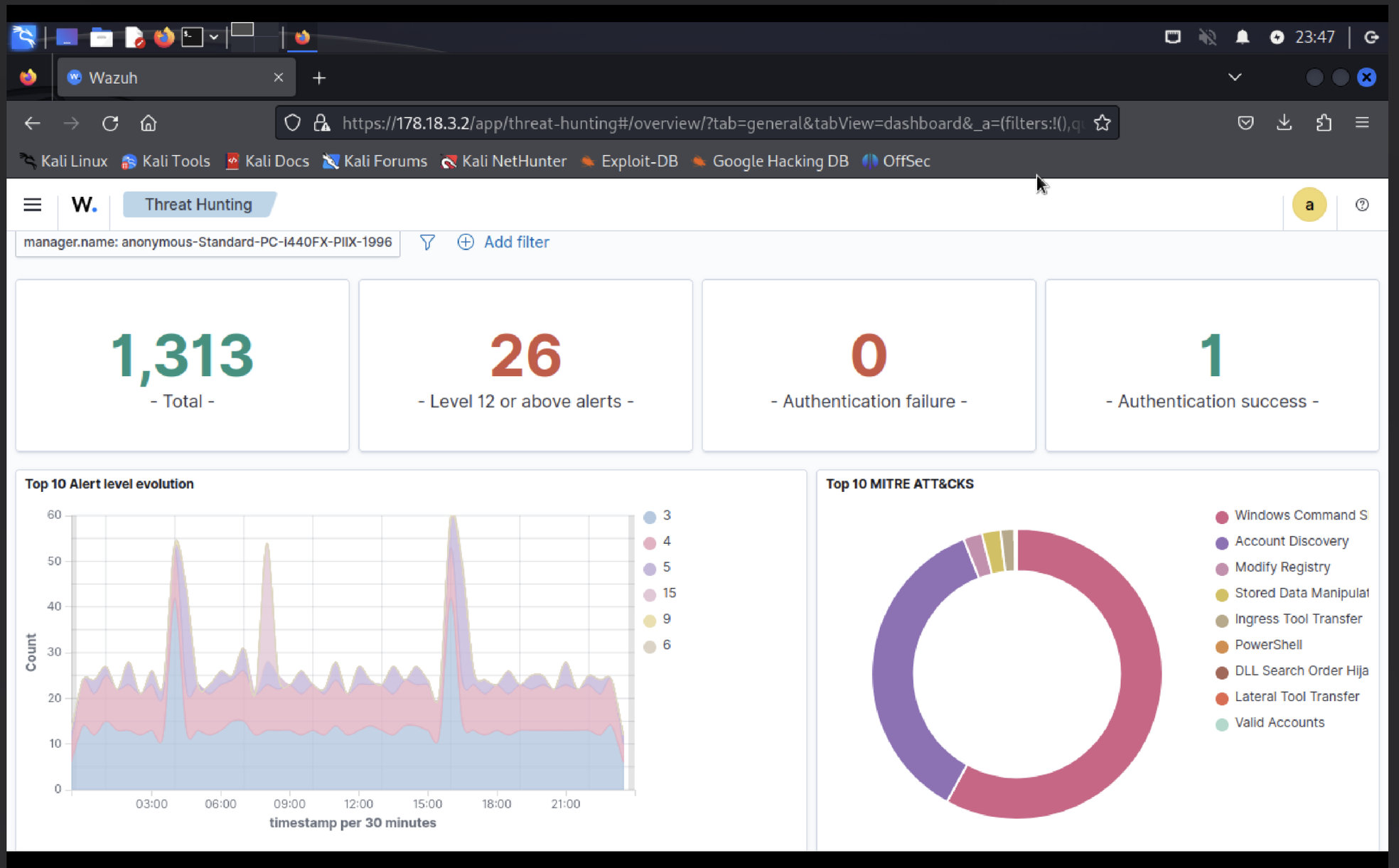
Successful

- Credential validation (SMB & FTP)
- Share and pipe enumeration
- Service identification via IPC$
- Files Extraction

Unsuccessful (Execution/Control Blocked)

- Remote PowerShell execution
- File upload/write to ADMIN$/C$
- Secrets dump

Blue Team Analysis



Highest-Severity Rules Observed

Rule ID	Level	Meaning
92213	15	Executable dropped in malware-common folders
92032	3	Suspicious cmd shell execution
92052	4	cmd.exe spawned by abnormal parent
60132	5	System time changed
60702	5	Volume Shadow Copy Service stopped
61104	3	Service startup type modified

	timestamp	agent.name	rule.description	rule.level	rule.id
	Dec 2, 2025 @ 08:28:32.775	DESKTOP-23M8HBN	Executable file dropped in folder commonly used by malware	15	92213
	Dec 2, 2025 @ 08:28:32.760	DESKTOP-23M8HBN	Executable file dropped in folder commonly used by malware	15	92213
	Dec 2, 2025 @ 08:28:32.746	DESKTOP-23M8HBN	Executable file dropped in folder commonly used by malware	15	92213
	Nov 30, 2025 @ 07:44:03.9...	DESKTOP-23M8HBN	Suspicious Windows cmd shell execution	3	92032
	Nov 30, 2025 @ 07:39:03.9...	DESKTOP-23M8HBN	Suspicious Windows cmd shell execution	3	92032
	Nov 30, 2025 @ 07:39:03.9...	DESKTOP-23M8HBN	Suspicious Windows cmd shell execution	3	92032
	Dec 3, 2025 @ 01:19:02.983	DESKTOP-23M8HBN	Windows command prompt started by an abnormal process	4	92052
	Dec 3, 2025 @ 01:18:03.485	DESKTOP-23M8HBN	Windows command prompt started by an abnormal process	4	92052
	Dec 3, 2025 @ 01:14:02.975	DESKTOP-23M8HBN	Windows command prompt started by an abnormal process	4	92052
	Dec 2, 2025 @ 08:28:42.805	DESKTOP-23M8HBN	System time changed	5	60132
	Dec 2, 2025 @ 08:28:42.790	DESKTOP-23M8HBN	System time changed	5	60132
	Dec 2, 2025 @ 08:28:42.784	DESKTOP-23M8HBN	System time changed	5	60132
	Nov 30, 2025 @ 08:31:25.4...	DESKTOP-23M8HBN	The VSS service is shutting down due to idle timeout.	5	60702
	Nov 27, 2025 @ 08:31:26.5...	DESKTOP-23M8HBN	The VSS service is shutting down due to idle timeout.	5	60702
	Nov 24, 2025 @ 08:31:46.6...	DESKTOP-23M8HBN	The VSS service is shutting down due to idle timeout.	5	60702
	Dec 2, 2025 @ 06:32:46.216	DESKTOP-23M8HBN	Service startup type was changed	3	61104
	Dec 2, 2025 @ 06:30:29.890	DESKTOP-23M8HBN	Service startup type was changed	3	61104
	Nov 30, 2025 @ 04:32:41.5...	DESKTOP-23M8HBN	Service startup type was changed	3	61104

Key Sysmon Events

Event ID 1 – Process Creation

The system runs this event whenever any new process begins execution. The Event ID 1 logs show continuous suspicious activity because cmd.exe and powershell.exe commands keep running which indicates automated malware dropper and script execution patterns.

Event ID 3 – Network Connection

The system logs all instances when a process creates an outgoing network connection. The system maintained continuous operation through Defender subdirectory connections to multiple cloud IPs at port 443 which handled command-and-control (C2) beaconing activity.

Event ID 11 – File Creation

The system produces this alert when users perform file saves to their disk storage. The system generated multiple Level 15 alerts (Rule 92213) because it detected malware through executable file placement in directories which malware targets frequently. The system shows payload deployment through this particular alert sequence.

Event ID 13 – Registry Modification

The system tracks all modifications made to the Logs registry value through its logs. The system logs display multiple entries which document service creation activities and startup modifications and additional persistence operations.

t data.win.system.channel	Microsoft-Windows-Sysmon/Operational
t data.win.system.computer	DESKTOP-23M8HBN
t data.win.system.eventID	1
t data.win.system.eventRecordID	106726
t data.win.system.keywords	0x8000000000000000
t data.win.system.level	4
t data.win.system.message	"Process Create: RuleName:

timestamp per 12 hours

t data.win.system.channel	Microsoft-Windows-Sysmon/Operational
t data.win.system.computer	DESKTOP-23M8HBN
t data.win.system.eventID	3
t data.win.system.eventRecordID	104741
t data.win.system.keywords	0x8000000000000000
t data.win.system.level	4
t data.win.system.message	"Network connection detected: RuleName: -

t data.win.system.channel	Microsoft-Windows-Sysmon/Operational
t data.win.system.computer	DESKTOP-23M8HBN
t data.win.system.eventID	11
t data.win.system.eventRecordID	99222
t data.win.system.keywords	0x8000000000000000
t data.win.system.level	4
t data.win.system.message	"File created: RuleName: DLL

t data.win.eventdata.utcTime	2025-11-18 00:28:27.328
t data.win.system.channel	Microsoft-Windows-Sysmon/Operational
t data.win.system.computer	DESKTOP-23M8HBN
t data.win.system.eventID	13
t data.win.system.eventRecordID	71963
t data.win.system.keywords	0x8000000000000000

MITRE ATT&CK Mapping

Technique	MITRE ID	Evidence Source
Command Execution	**T1059**	Suspicious cmd.exe + PowerShell drops
Account Discovery	**T1087**	net.exe enumeration events
Discovery	**T1082**	Discovery rule triggers (92031)
Ingress Tool Transfer	**T1105**	Multiple Level 15 executable drops
Modify Registry	**T1112**	Registry-based service creation
Persistence via Services	**T1547.001**	Service startup type modified
Defense Evasion	**T1070.004**	VSS shutdown, time modification
Execution via Services	**T1569**	Service creation/log start events

	Nov 12, 2025 @ 08:45:36.9...	DESKTOP-23M8HBN	T1059 T1105	Execution, Command and Control	Scripting file created under Windows Temp or ...	6	92
	Nov 12, 2025 @ 08:45:36.9...	DESKTOP-23M8HBN	T1059 T1105	Execution, Command and Control	Scripting file created under Windows Temp or ...	6	92
	Nov 12, 2025 @ 08:45:36.8...	DESKTOP-23M8HBN	T1059 T1105	Execution, Command and Control	Scripting file created under Windows Temp or ...	6	92

	Nov 24, 2025 @ 02:19:02.9...	DESKTOP-23M8HBN	T1087 T1059.003	Discovery, Execution	Suspicious Windows cmd shell execution	3
	Nov 24, 2025 @ 02:19:02.9...	DESKTOP-23M8HBN	T1087 T1059.003	Discovery, Execution	Suspicious Windows cmd shell execution	3
	Nov 24, 2025 @ 02:19:02.9...	DESKTOP-23M8HBN	T1059.003	Execution	Windows command prompt started by an abno...	4

	Nov 23, 2025 @ 16:34:17.6...	DESKTOP-23M8HBN	T1565.001 T1112	Impact, Defense Evasion	Registry Value Integrity Checksum Changed	5
	Nov 23, 2025 @ 16:34:17.5...	DESKTOP-23M8HBN	T1565.001 T1112	Impact, Defense Evasion	Registry Key Integrity Checksum Changed	5
	Nov 23, 2025 @ 16:34:12.1...	DESKTOP-23M8HBN	T1565.001 T1112	Impact, Defense Evasion	Registry Value Integrity Checksum Changed	5

	Nov 23, 2025 @ 16:34:25.3...	DESKTOP-23M8HBN	T1070.004 T1485 T1112	Defense Evasion, Impact	Registry Value Entry Deleted.	5
	Nov 23, 2025 @ 16:34:25.3...	DESKTOP-23M8HBN	T1070.004 T1485 T1112	Defense Evasion, Impact	Registry Value Entry Deleted.	5
	Nov 23, 2025 @ 16:34:25.3...	DESKTOP-23M8HBN	T1070.004 T1485 T1112	Defense Evasion, Impact	Registry Value Entry Deleted.	5

	Nov 18, 2025 @ 17:29:47.4...	DESKTOP-23M8HBN	T1547.001	Persistence, Privilege Escalation	An executable file has been copied to Windows...	6
	Nov 18, 2025 @ 17:29:24.7...	DESKTOP-23M8HBN	T1547.001	Persistence, Privilege Escalation	Registry entry to be executed on next logon wa...	6
	Nov 2, 2025 @ 13:39:12.890	DESKTOP-23M8HBN	T1547.001	Persistence, Privilege Escalation	An executable file has been copied to Windows...	6

Key Findings and Lessons Learned

- Implemented a virtual enterprise network using Proxmox, VyOS, pfSense, Ubuntu, and Windows 10, and learned about IP planning, DNS, NAT, and the gateway configuration, and ensured that all hosts and network segments were connected.
- Known attack vectors in SMB and FTP, discovered vulnerabilities such as disabled SMB signing and IIS TRACE enabled, and learned how to correct configurations to minimize the risks of lateral movement.
- Installation of Wazuh and Sysmon to monitor attacks and discovered that proper log configuration and dashboard filtering are essential in responding to incidents.
- Firm Windows 10 and Ubuntu systems with security controls, service restrictions, and permissions management, supporting the fact that CIS compliance enhances to withstand attacks.
- Tools such as Proxmox, VyOS, pfSense, Wazuh, Sysmon, and Nmap were used, and MITRE ATT&CK was applied to match the techniques of attackers with alerts.

Reflection

- Roles separation, task division, and frequent updates enhanced efficiency and minimized mistakes.
- The necessity to perform meticulous verification, version control, and documentation was illustrated by complex network layers, firewall and NAT conflicts, Wazuh and Sysmon troubleshooting, and configuration changes by a teammate.
- Got to know the importance of planning, documenting, testing in baby steps, the views of the attackers and defenders, and responsible troubleshooting.

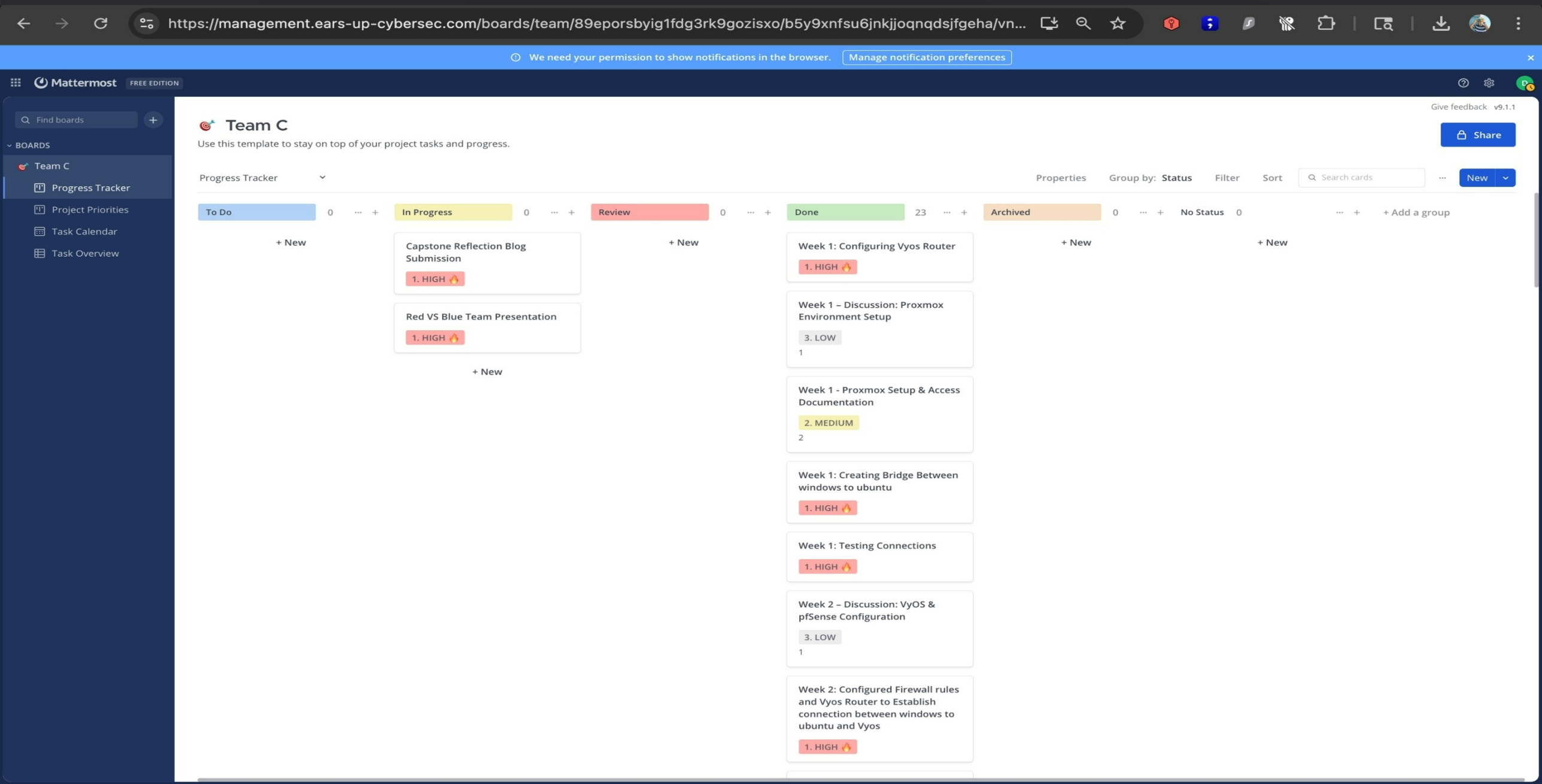
How project can be marketed

- Knows how to design, secure, and monitor enterprise networks, Red and Blue Team methods, and is conversant with MITRE ATT&CK, Wazuh, Sysmon, and network hardening best practices.

- Demonstrates the skills of strategizing and implementing an integrated cybersecurity project and provides valuable experience with attack and defense scenarios for research purposes.

- Presentations, Network diagrams, dashboards, and discovery to exhibit end-to-end capabilities, collaboration, and troubleshooting in a realistic lab environment of enterprise cybersecurity.

Mattermost Dashboard



https://management.ears-up-cybersec.com/boards/team/89eporsbyig1fdg3rk9gozisxo/b5y9xnfsu6jnkjjoqnqdsjfgeha/ve...

We need your permission to show notifications in the browser. Manage notification preferences

Mattermost FREE EDITION

Find boards

BOARDS

- Team C
- Progress Tracker
- Project Priorities
- Task Calendar
- Task Overview

Give feedback v9.1.1

Team C

Use this template to stay on top of your project tasks and progress.

Share

Task Calendar | Properties | Display by: Due Date | Filter | Search cards | New

December 2025

Week | Month | TODAY

Sun	Mon	Tue	Wed	Thu	Fri	Sat
30	1	2	3	4	5	6
7 Red VS Blue Team Presentation	8	9	10 Capstone Reflection Blog Submission	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31	1	2	3
4	5	6	7	8	9	10

Support Team, Professor Syam Sai, Classmates and Faculty for this learning opportunity