Home lab Report

Author: Michael Asante Anim
Date: January 13th 2025

---

1. Introduction

This home lab was built to help me strengthen my cybersecurity, networking, scripting and system administration skills in a safe, isolated setup. I used VMware to virtualize multiple operating systems and simulate a small enterprise network for offensive and defensive experiments.

The environment includes:

- **Windows Server** (Domain Controller / Server roles)
- **Windows 10** (Client)
- **Kali Linux** (Offensive security)

---

2. Home lab Goals

- **Experience I wanted**

  A hands-on environment where I can practice Active Directory management, penetration testing, vulnerability scanning, and secure system configuration.

- **What I did**
  I used VMware to install and network four separate virtual machines, each assigned a specific role in the home lab environment.
- **The Result**
  A fully functional mini-enterprise network where I can safely test attacks, automate admin tasks, and practice real-world cybersecurity workflows.

---

3. Hardware & Software Used

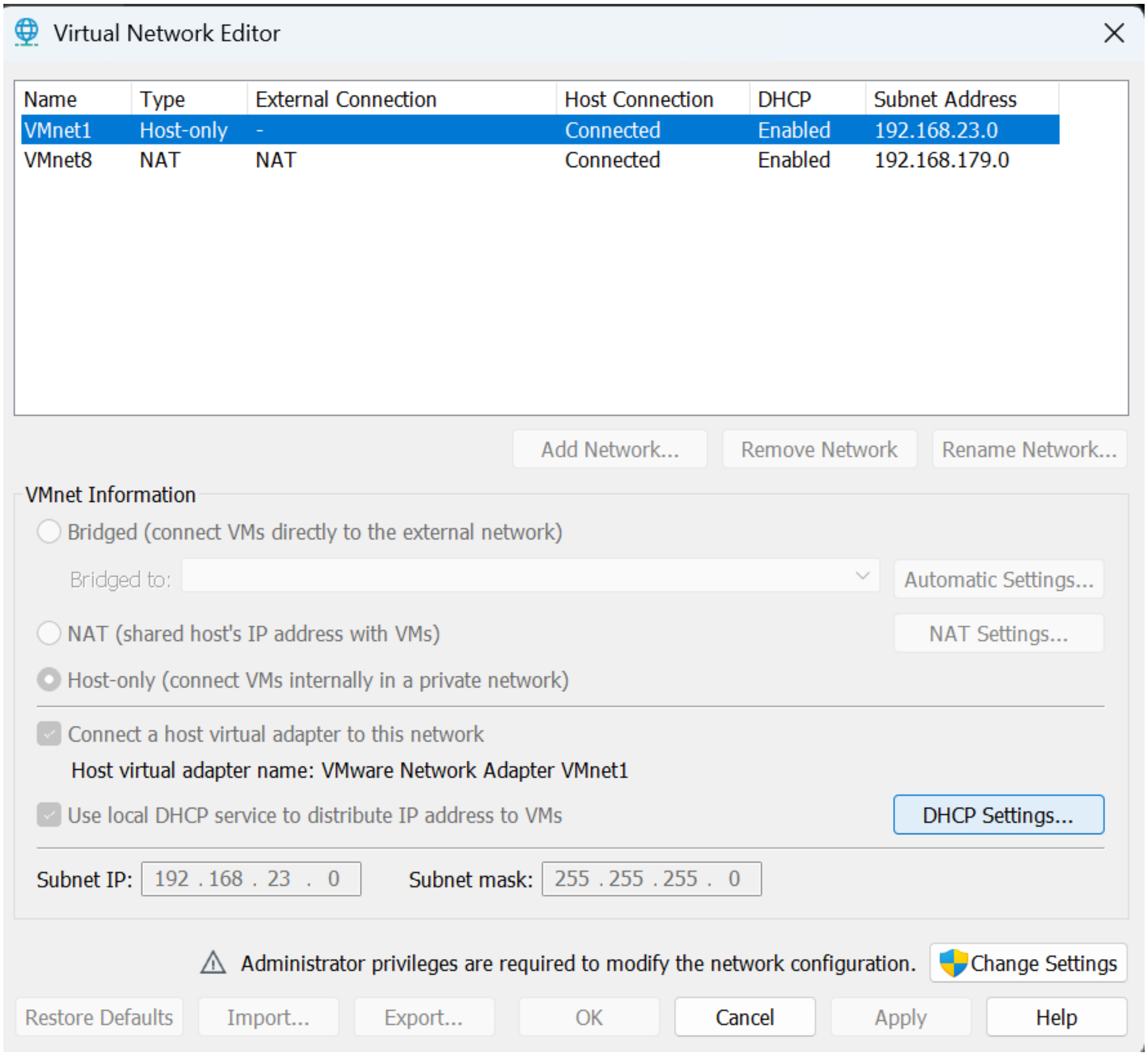
- **Virtualization Platform: VMware Pro**
- Operating Systems Installed:
  - Windows Server 2022
  - Windows 10
  - Kali Linux

4. Network Topology

I configured each virtual machine with two network adapters to separate internal lab traffic from internet access:

- **Adapter 1: Host-Only Network**
  This adapter allows all the virtual machines to communicate with each other in a private, isolated network. Windows Server, Windows 10, Kali Linux, and Parrot OS all share this internal network, which is where domain authentication, scanning, exploitation, and internal traffic take place.
- **Adapter 2: NAT Network**
  This adapter provides internet access to the VMs through the host machine's connection. It lets the operating systems download updates, install tools, and access online repositories without exposing the internal lab network to the public internet.
  This dual-adapter setup keeps the home lab secure and isolated while still giving each machine access to the resources it needs.

VMware Virtual Network Editor screenshot here



Name	Type	External Connection	Host Connection	DHCP	Subnet Address
VMnet1	Host-only	-	Connected	Enabled	192.168.23.0
VMnet8	NAT	NAT	Connected	Enabled	192.168.179.0

VMnet Information

○ Bridged (connect VMs directly to the external network)

Bridged to:

○ NAT (shared host's IP address with VMs)

● Host-only (connect VMs internally in a private network)

☑ Connect a host virtual adapter to this network

Host virtual adapter name: VMware Network Adapter VMnet1

☑ Use local DHCP service to distribute IP address to VMs

Subnet IP: 192 . 168 . 23 . 0   Subnet mask: 255 . 255 . 255 . 0

⚠ Administrator privileges are required to modify the network configuration.

5. Machine Setup & Configuration

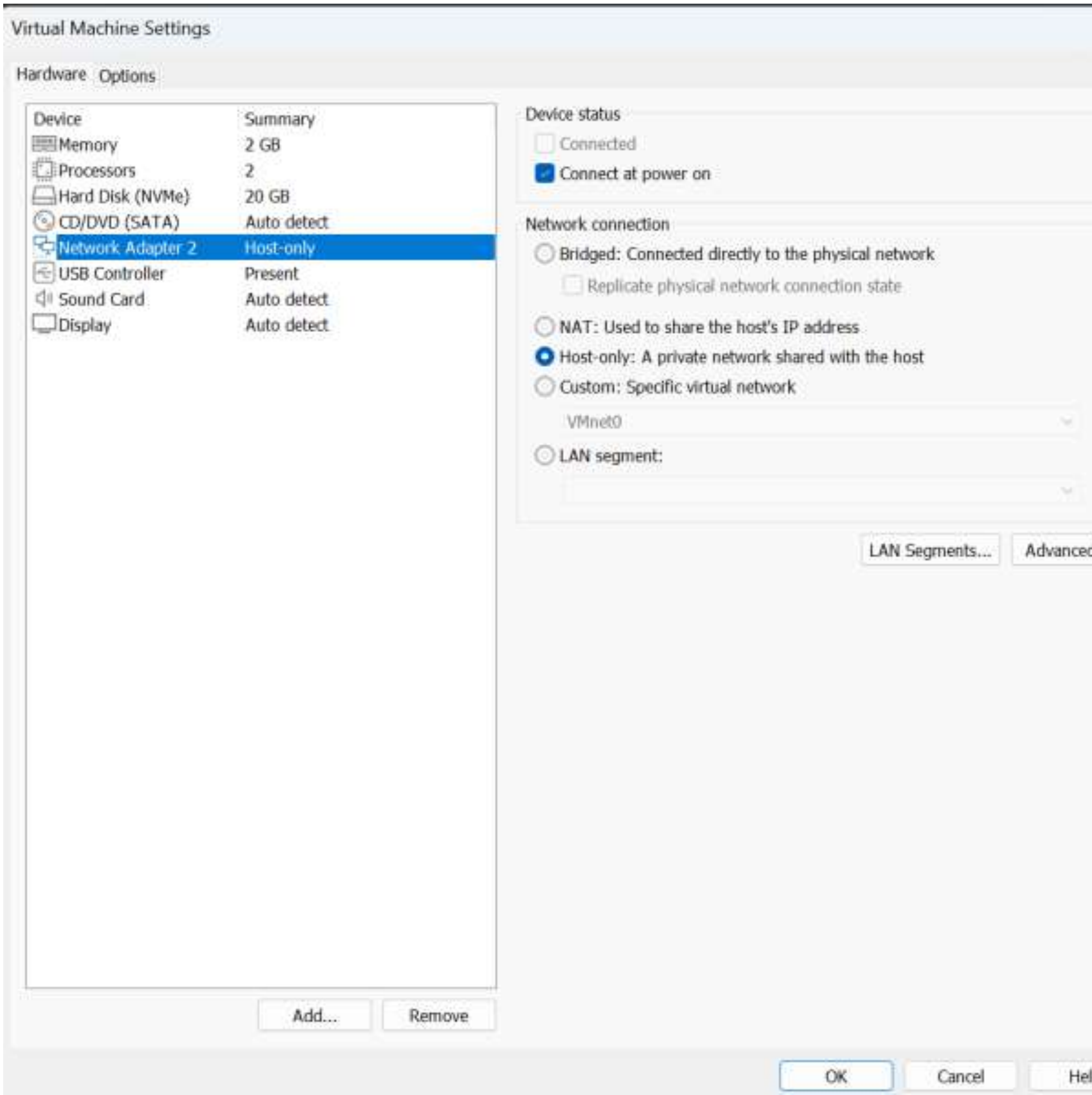
5.1 Windows Server Setup

- **Experience I wanted**

  Set up Active Directory to understand domain management and authentication.

- **What I did**
  - Created a new VMware VM for Windows Server
  - Configured virtual hardware (CPU, RAM, storage, network type)
  - Set a static IP address
  - Installed AD DS
  - Promoted the server to a Domain Controller
  - Created users and Organizational Units

VMware VM settings for Windows Server



Virtual Machine Settings

Device	Summary
Memory	2 GB
Processors	2
Hard Disk (NVMe)	20 GB
CD/DVD (SATA)	Auto detect
Network Adapter 2	Host-only
USB Controller	Present
Sound Card	Auto detect
Display	Auto detect

Device status

□ Connected

☑ Connect at power on

Network connection

○ Bridged: Connected directly to the physical network

□ Replicate physical network connection state

○ NAT: Used to share the host's IP address

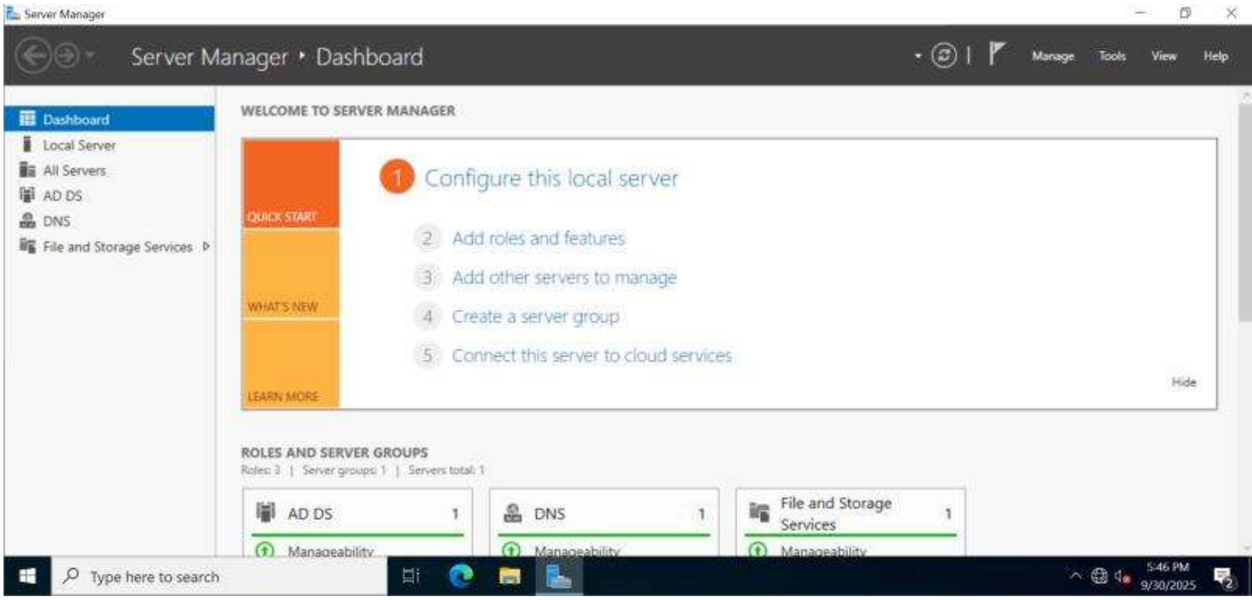
● Host-only: A private network shared with the host

○ Custom: Specific virtual network

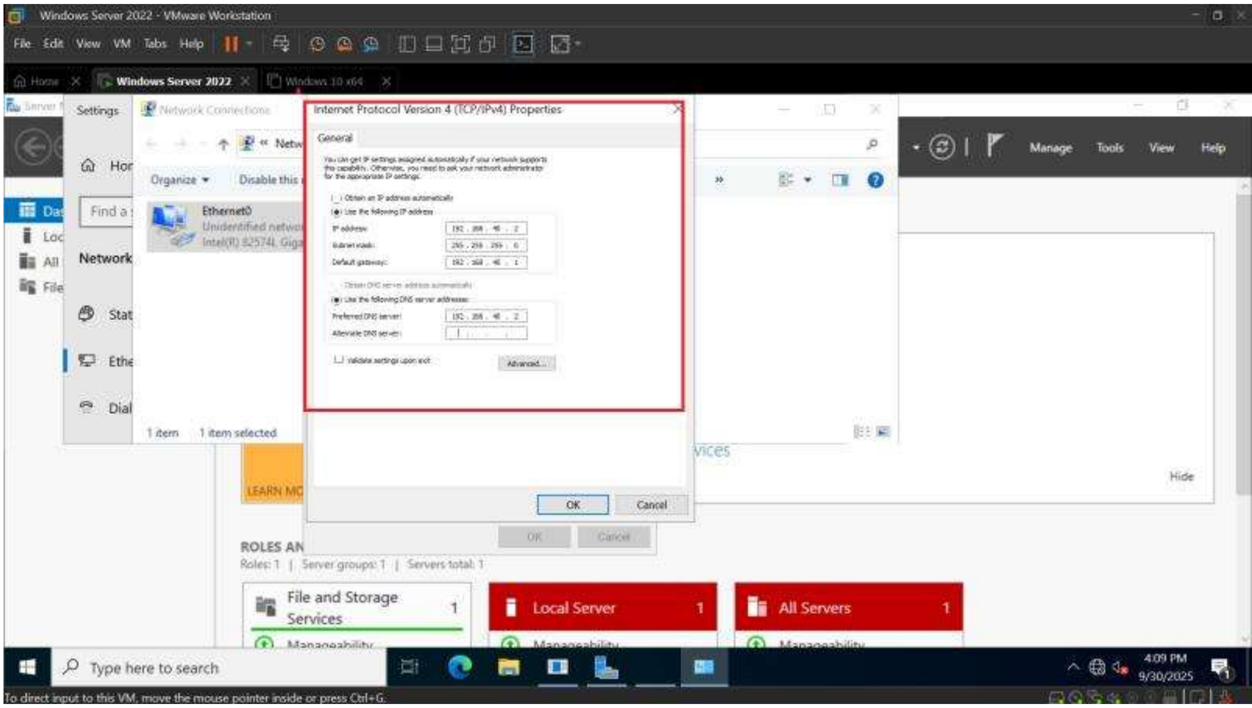
VMnet0

○ LAN segment:

Insert screenshot of AD DS installation


Server Manager
Server Manager • Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
AD DS
DNS
File and Storage Services
WELCOME TO SERVER MANAGER
QUICK START
WHAT'S NEW
LEARN MORE
1 Configure this local server
2 Add roles and features
3 Add other servers to manage
4 Create a server group
5 Connect this server to cloud services
Hide
ROLES AND SERVER GROUPS
Roles: 3 | Server groups: 1 | Servers total: 1
AD DS 1
DNS 1
File and Storage Services 1
Manageability
Type here to search
5:46 PM
9/30/2025

Assigning Static IP



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically
● Use the following IP address:

IP address: 192 . 168 . 40 . 2
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 192 . 168 . 40 . 1

○ Obtain DNS server address automatically
● Use the following DNS server addresses:

Preferred DNS server: 192 . 168 . 40 . 2
Alternate DNS server: . . .

□ Validate settings upon exit

Advanced...

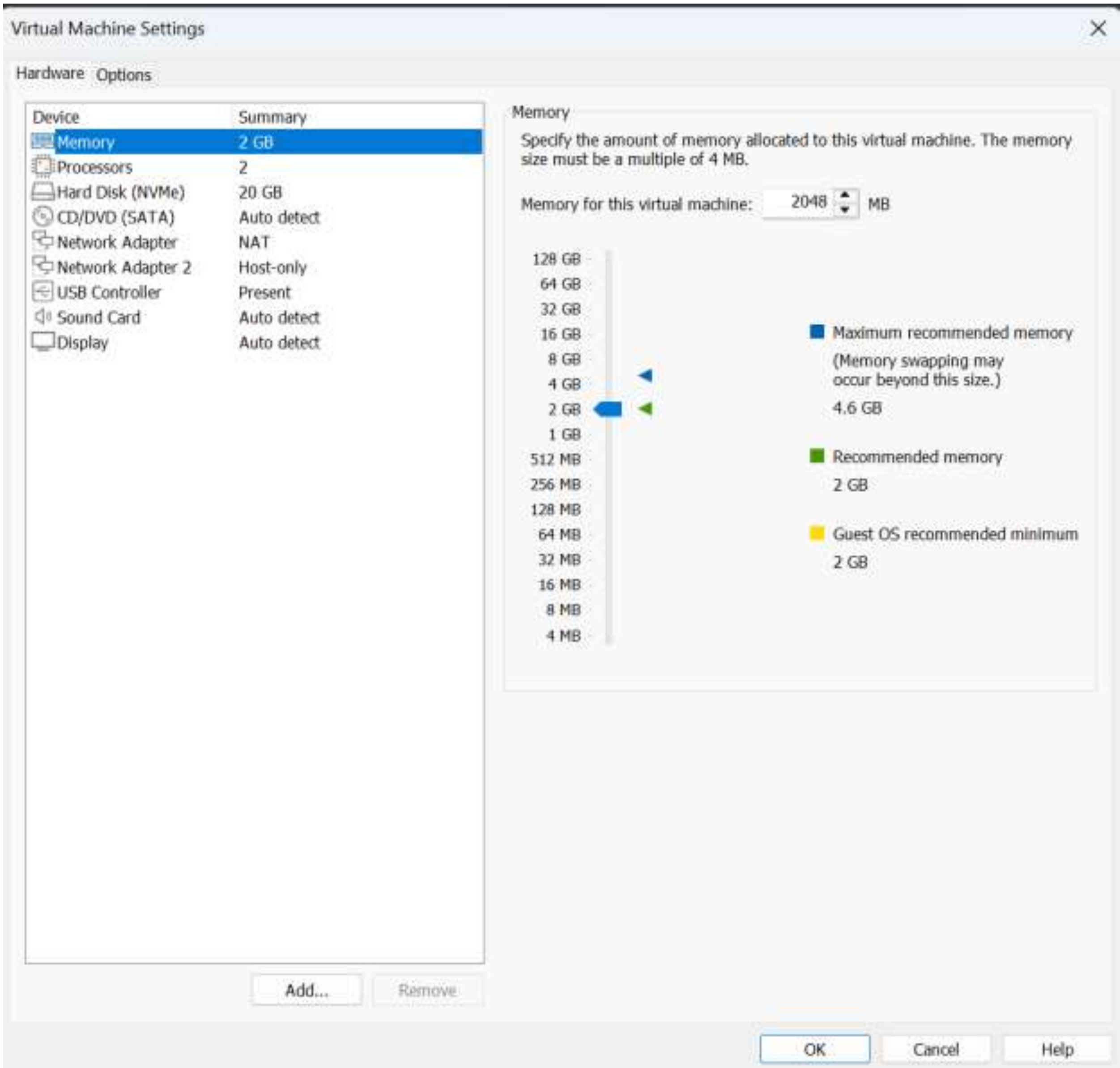
OK Cancel

5.2 Windows 10 Client Setup

- **Experience I wanted**
  - Practice domain joining and policy management.

- **What I did**
  - Installed Windows 10 inside VMware
  - Set IP to point to the domain controller
  - Joined the Windows domain
  - Logged in using domain credentials

VMware VM settings for Windows 10



Device	Summary
Memory	2 GB
Processors	2
Hard Disk (NVMe)	20 GB
CD/DVD (SATA)	Auto detect
Network Adapter	NAT
Network Adapter 2	Host-only
USB Controller	Present
Sound Card	Auto detect
Display	Auto detect

Memory

Specify the amount of memory allocated to this virtual machine. The memory size must be a multiple of 4 MB.

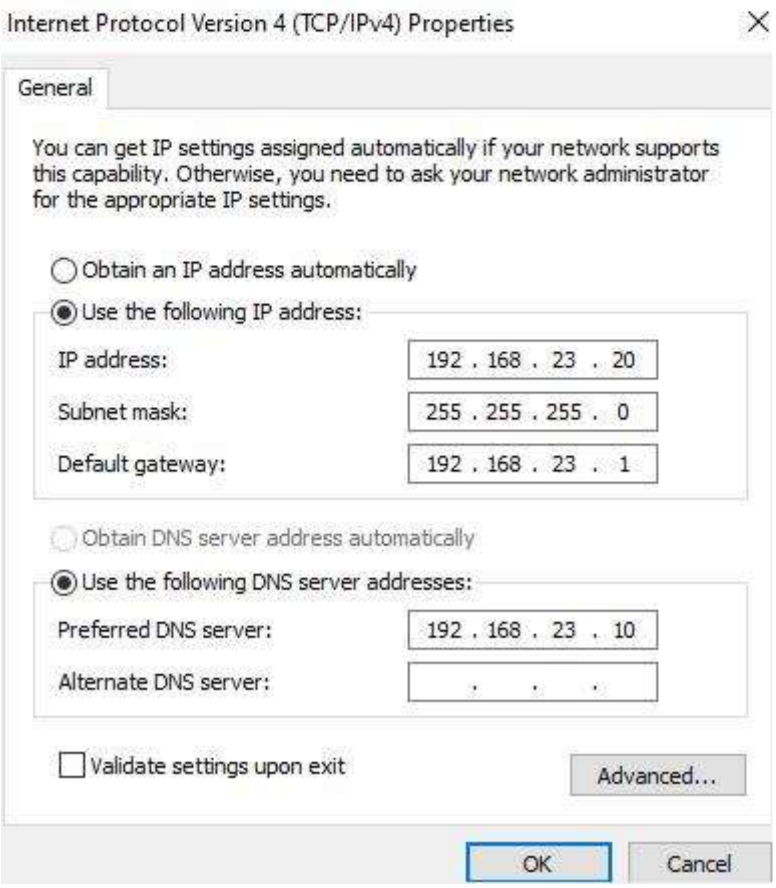
Memory for this virtual machine: 2048 MB

🟦 Maximum recommended memory
(Memory swapping may occur beyond this size.)
4.6 GB

🟩 Recommended memory
2 GB

🟨 Guest OS recommended minimum
2 GB

Insert screenshot of domain join window



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 23 . 20

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 23 . 1

○ Obtain DNS server address automatically

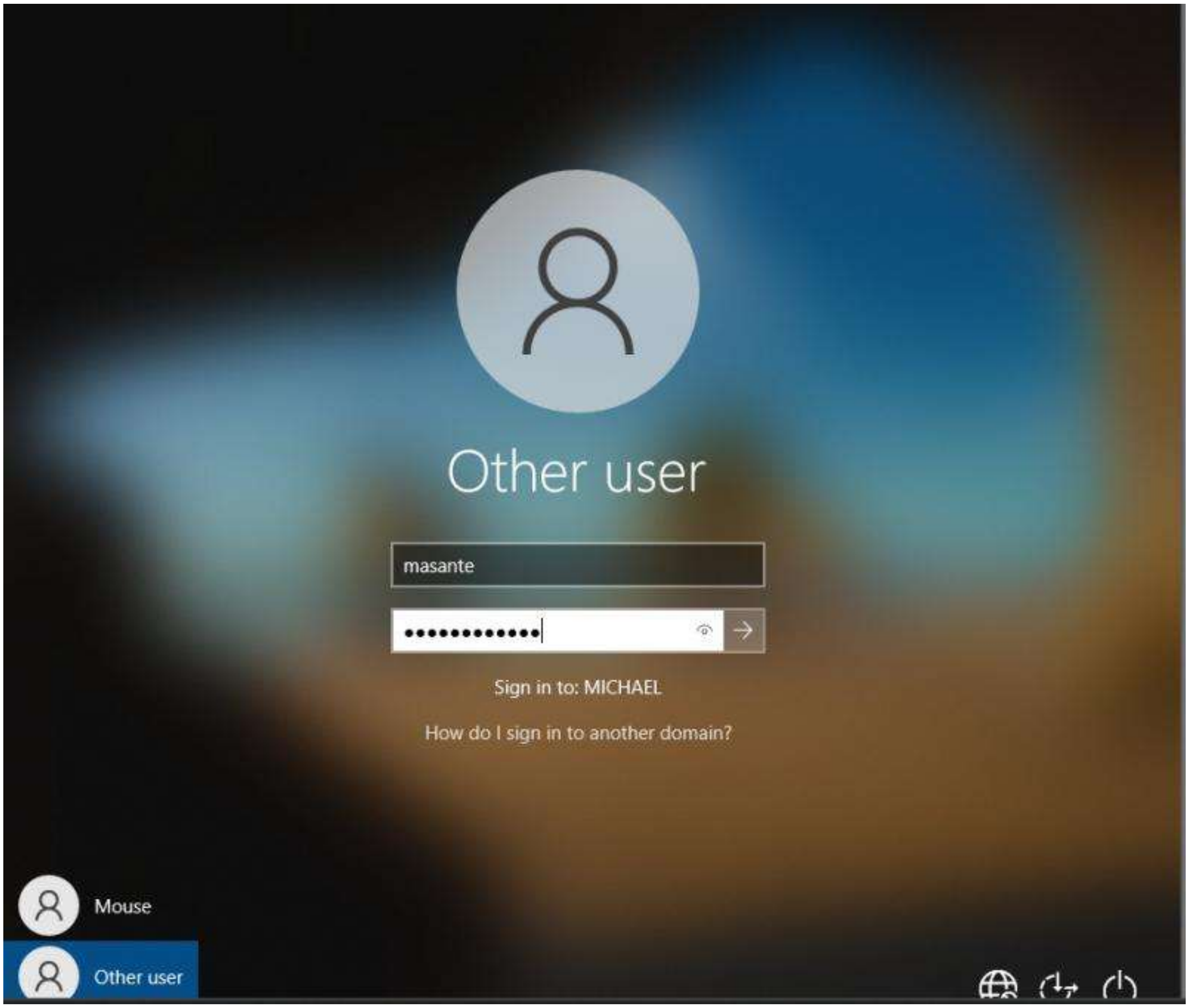
● Use the following DNS server addresses:

Preferred DNS server: 192 . 168 . 23 . 10

Alternate DNS server: . . .

□ Validate settings upon exit

screenshot of successful domain login


Other user

masante

•••••••••••••

Sign in to: MICHAEL

How do I sign in to another domain?

The Result

A domain-connected workstation ready for GPO testing.

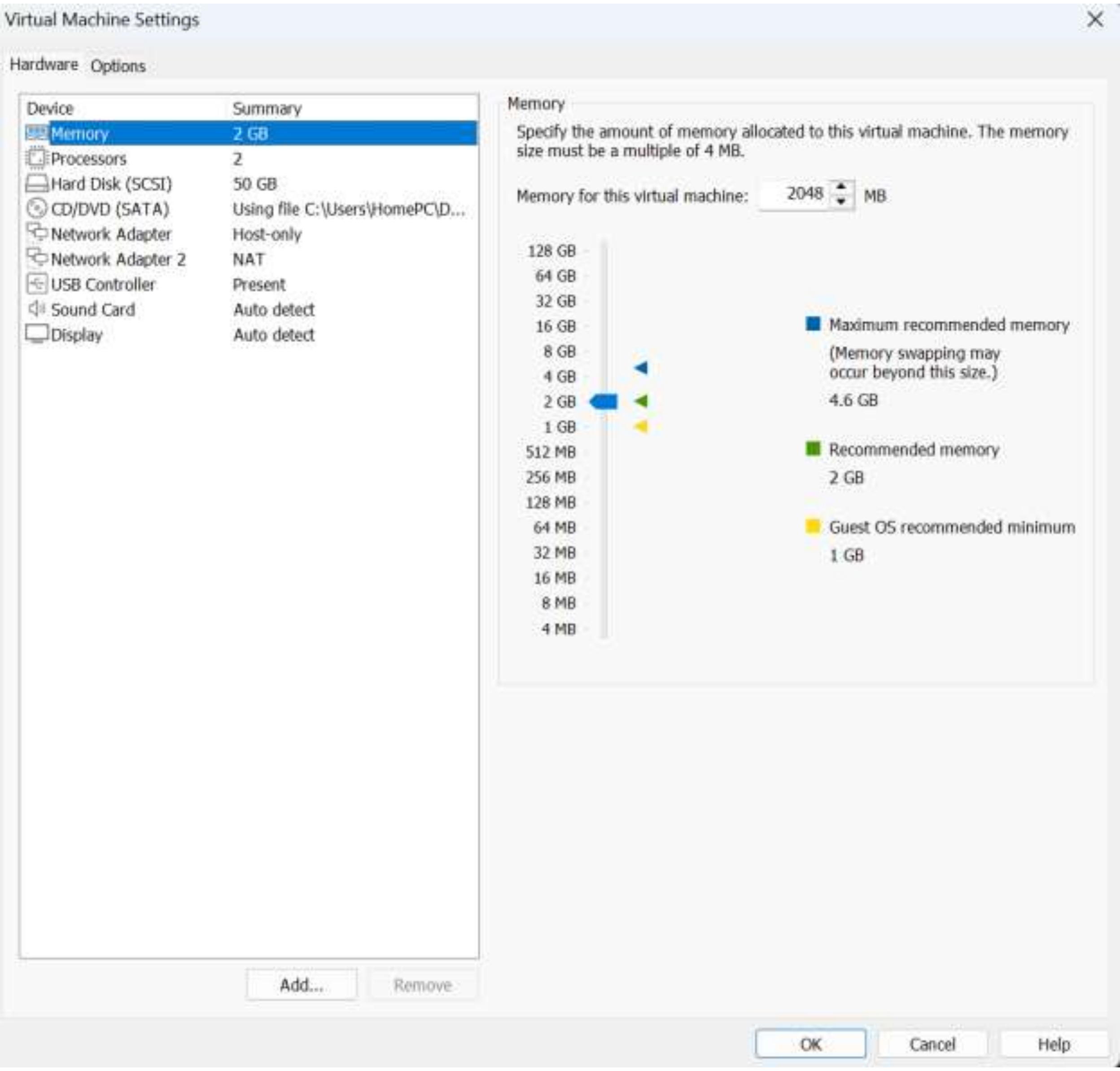
5.3 Kali Linux Setup

- **Experience I wanted**
  - Use Kali as an offensive machine for scanning, exploitation, and enumeration.
- **What I did**
  - Installed Kali Linux on VMware
  - Snapshot taken before major tests
  - Updated all tools (Nmap, Metasploit, Hydra, Burp Suite)
  - Connected Kali to the same virtual network

- Performed initial reconnaissance on Windows machines

VMware VM settings for Kali Linux

VMware VM settings for Kali Linux



Device	Summary
Memory	2 GB
Processors	2
Hard Disk (SCSI)	50 GB
CD/DVD (SATA)	Using file C:\Users\HomePC\D...
Network Adapter	Host-only
Network Adapter 2	NAT
USB Controller	Present
Sound Card	Auto detect
Display	Auto detect

Memory

Specify the amount of memory allocated to this virtual machine. The memory size must be a multiple of 4 MB.

Memory for this virtual machine: 2048 MB

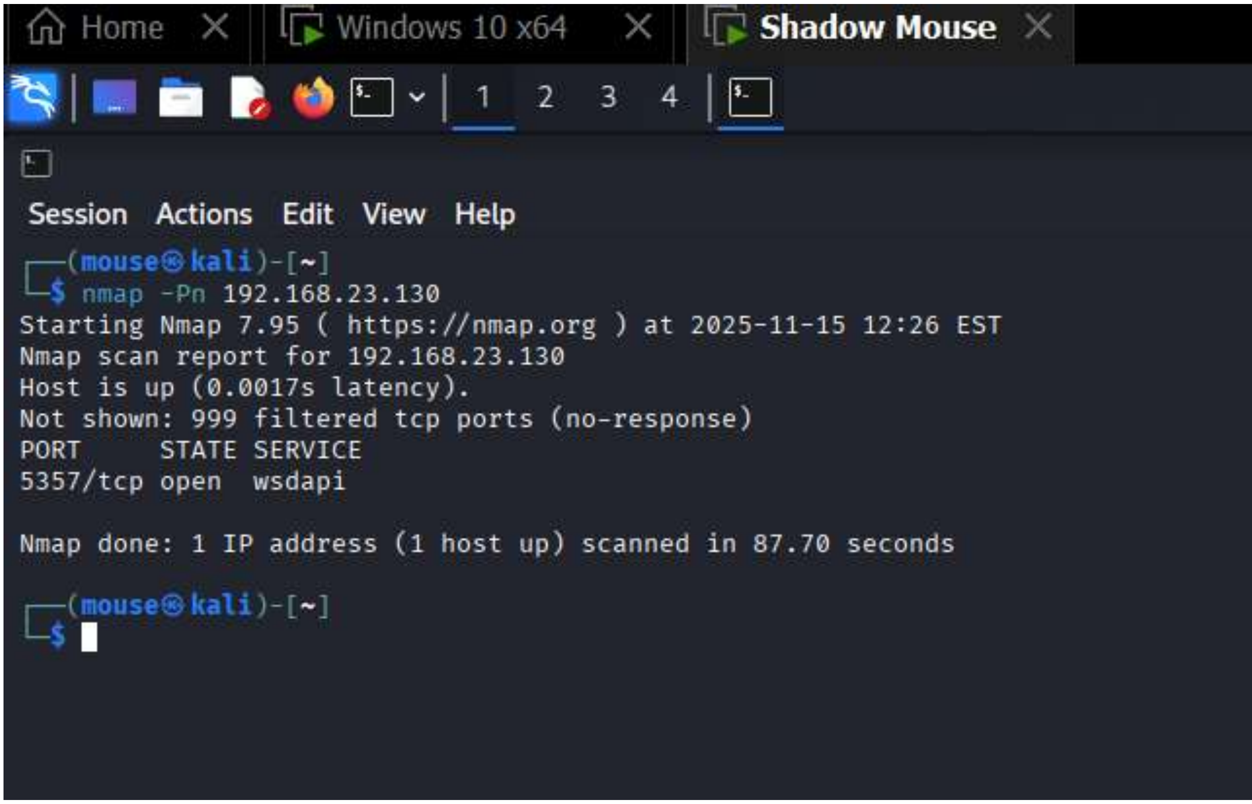
🟦 Maximum recommended memory
(Memory swapping may occur beyond this size.)
4.6 GB

🟩 Recommended memory
2 GB

🟨 Guest OS recommended minimum
1 GB

Kali desktop

Nmap scan results



```
┌──(mouse㉿kali)-[~]
└─$ nmap -Pn 192.168.23.130
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-15 12:26 EST
Nmap scan report for 192.168.23.130
Host is up (0.0017s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT     STATE SERVICE
5357/tcp open  wsdapi

Nmap done: 1 IP address (1 host up) scanned in 87.70 seconds

┌──(mouse㉿kali)-[~]
└─$ 
```

6.Attacks & Defenses Performed

- Nmap scanning
- Password cracking simulations
- Windows Firewall rule testing
- Hardening Windows Server with GPO
- Testing detection gaps
- SMB enumeration

---

7. Issues Faced & Solutions

- VMware network misconfiguration
- IP conflicts
- DNS issues causing failed domain joins
- VMware tools not installing on Linux
- Slow performance due to low RAM allocation

---

8. Key Lessons Learned

- How important DNS is in Active Directory
- The value of snapshots during experiments
- The difference between Kali and Parrot toolsets
- How offensive tools expose weak configurations
- Why patching and hardening matter

---

9. Conclusion

- **Experience I wanted**

  A real environment for practicing cybersecurity concepts end-to-end.

- **What I did**

  Built a multi-OS home lab on VMware, configured server roles, connected client machines, performed attacks, analyzed vulnerabilities, applied defenses, and documented results.

- **The Result**

A strong practical foundation in cybersecurity operations, system administration, and penetration testing—skills directly applicable to real-world environments.

A strong practical foundation in cybersecurity operations, system administration, and penetration testing—skills directly applicable to real-world environments.