SOC Analyst Home Lab Setup & Walkthrough

Part 1

Mike Arley Morin

Decembre, 2025

Table of Contents

Introduction

In the field of cybersecurity, theoretical concepts are often easier to access than practical, hands-on resources. However, true proficiency requires both a strong theoretical foundation and the ability to apply that knowledge in real-world scenarios.

This Home Lab is designed as a practical learning environment for cybersecurity students and self-learners. It provides a controlled space to practice key skills such as:

- Domain Controller configuration
- Network segmentation
- Firewall rule creation and testing
- Splunk deployment and configuration

Beyond infrastructure setup, the lab also helps develop Security Operations Center (SOC) analyst capabilities, including:

- Writing and executing Splunk searches
- Configuring alerts
- Investigating simulated security incidents

By combining technical implementation with investigative workflows, this lab offers a comprehensive platform to build the skills required for professional cybersecurity roles.

Lab Goals & Scope

The primary goal of this lab is to provide hands-on experience with fundamental cybersecurity infrastructure and monitoring concepts. Specifically, the lab focuses on:

- Understanding and implementing network segmentation
- Configuring and managing firewall rules
- Deploying and using a Security Information and Event Management (SIEM) solution (Splunk)

Learning Outcomes:
By completing this lab, you should be able to:

- Confidently design and implement network segmentation.

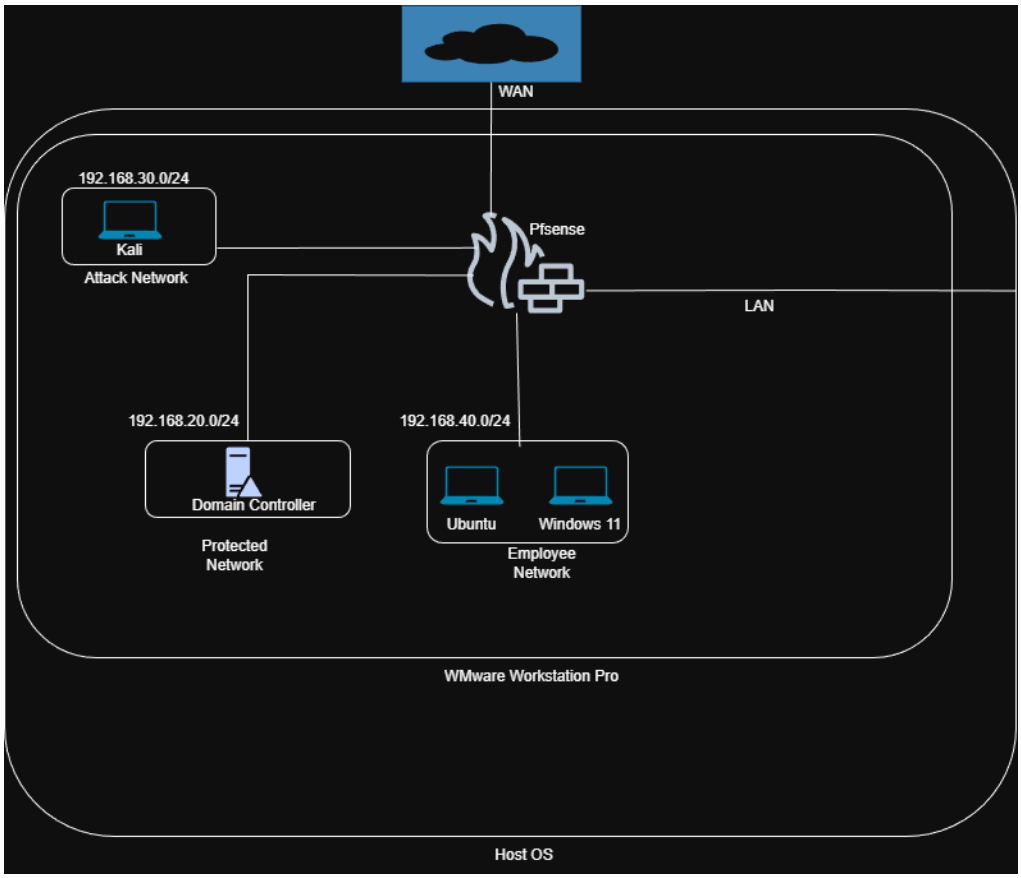
- Configure firewall rules to control and monitor traffic between network segments.
- Deploy Splunk, ingest log data, create searches, and configure alerts.

These skills form the foundation for both system administration and Security Operations Center (SOC) analysis, preparing you for more advanced cybersecurity challenges.

Prerequisites

- VMware Workstation Pro
- Pfsense ISO
- Kali ISO
- Ubuntu ISO
- Windows Server 2022 ISO (Evaluation)
- WIndows 11 Enterprise ISO (Evaluation)

Network Architecture



As shown in the diagram above, the network is divided into multiple segments. Ideally, VLANs should be used to implement this segmentation, since switches with VLAN capabilities provide greater flexibility and allow new segments to be added without installing additional network interfaces. However, because VMware does not support VLANs in this setup, we must create

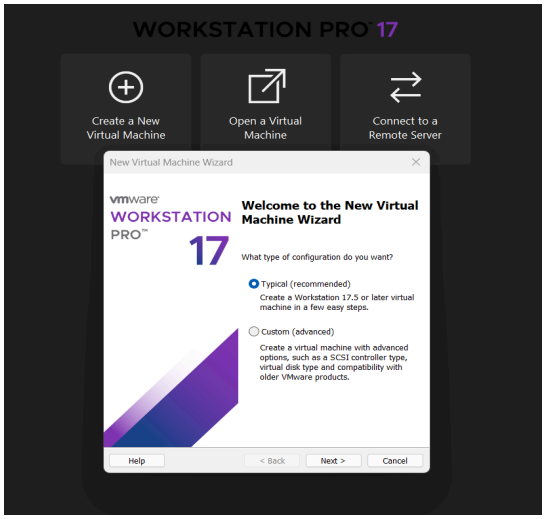
multiple virtual network interfaces and assign each network segment to its corresponding interface.

The network is segmented into five zones: WAN, LAN, Attack Network, Protected Network, and Employee Network. The WAN is configured using NAT to provide internet access to the other network segments. The LAN functions as the local interface for pfSense. The Attack Network is dedicated to conducting simulated attacks against critical network assets. The Protected Network hosts the Domain Controller, with additional private services planned for future deployment. The Employee Network consists of employee workstations.

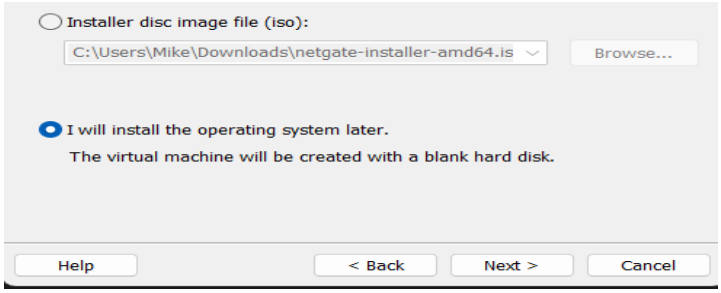
Virtual Machine Deployment

Pfsense

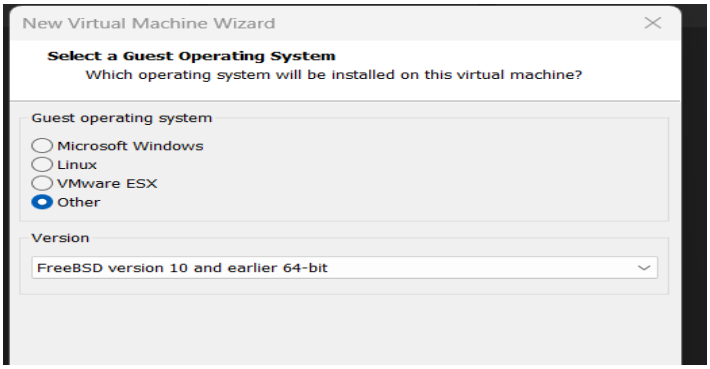
1- from WMware select “Create a New Virtual Machine”

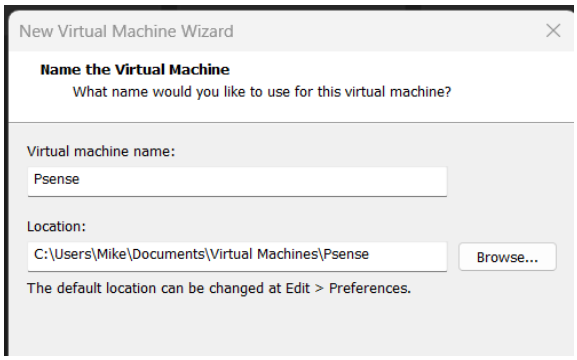


2- I will install the operating system later

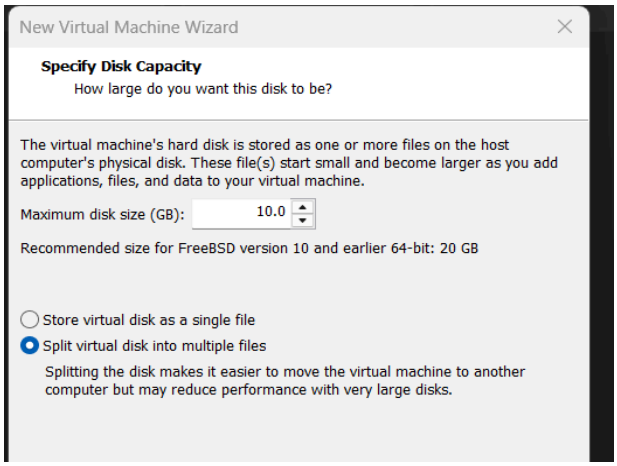


3- Other → FreeBSD 64-bit



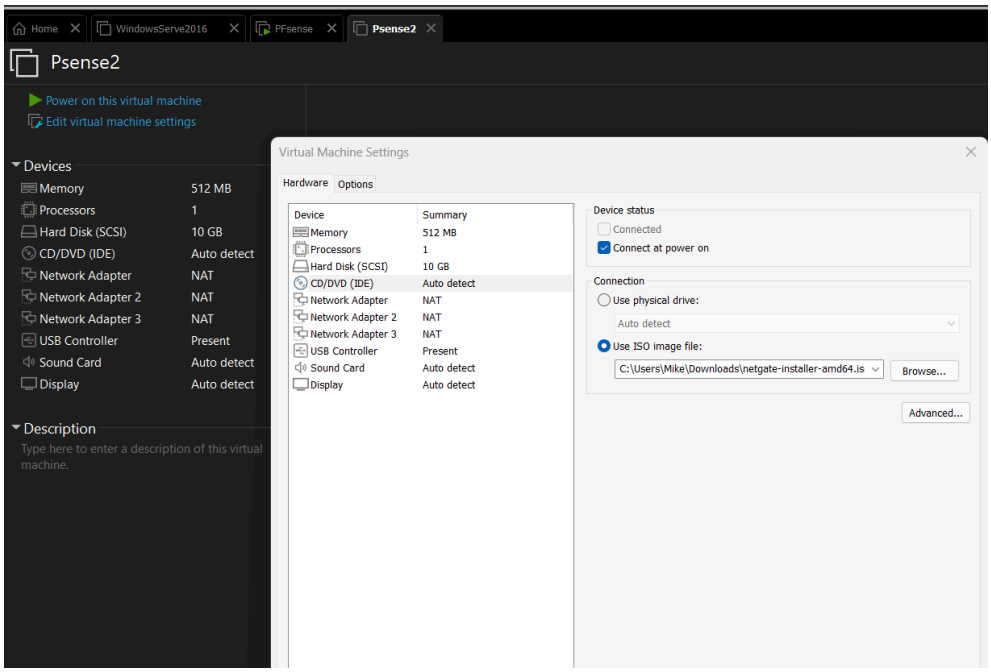


5- For the purpose of this lab, you can allocate 10 GB of disk space and 512 MB of RAM.



6- Click on Network Adapter and add four additional network adapters.

7- Before booting the virtual machine, attach the ISO file to the CD/DVD drive.

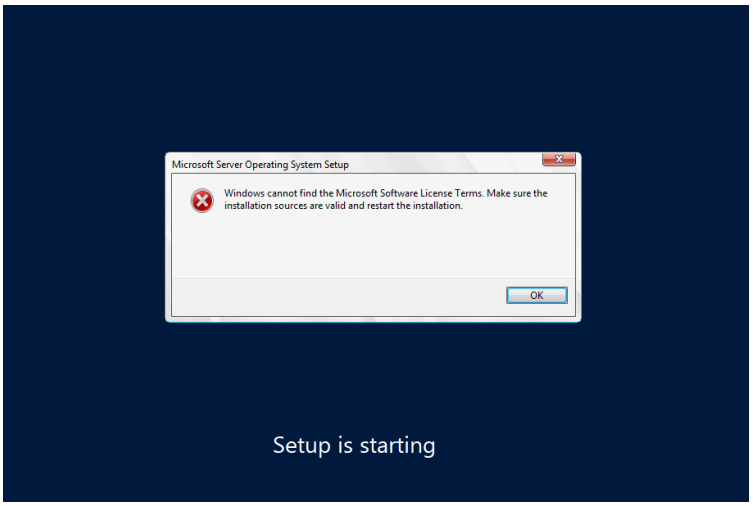


8- Click OK, then power on the pfSense virtual machine.

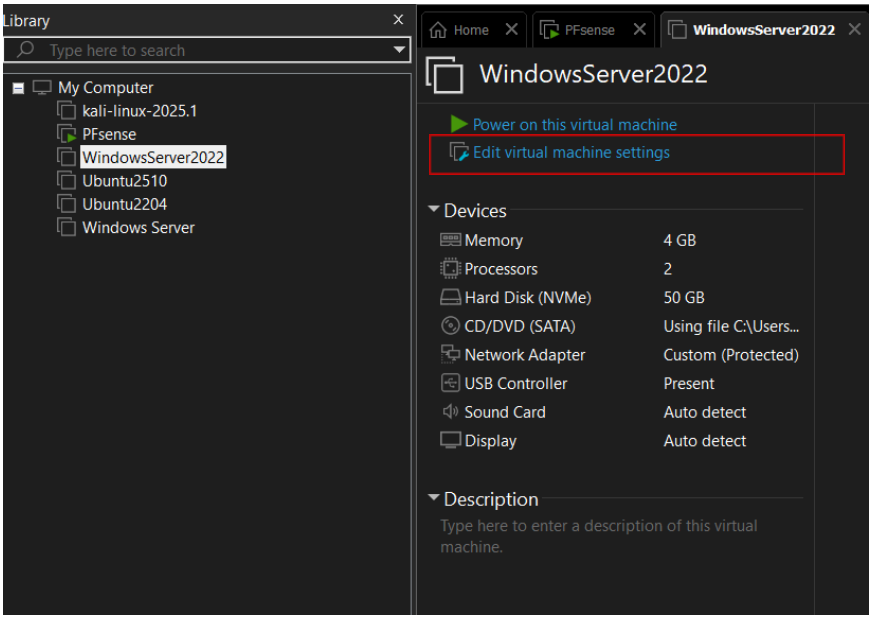
9- Follow the installation wizard.
9- After the installation completes, remove the ISO from the CD/DVD drive and reboot the virtual machine.

Windows Server 2016

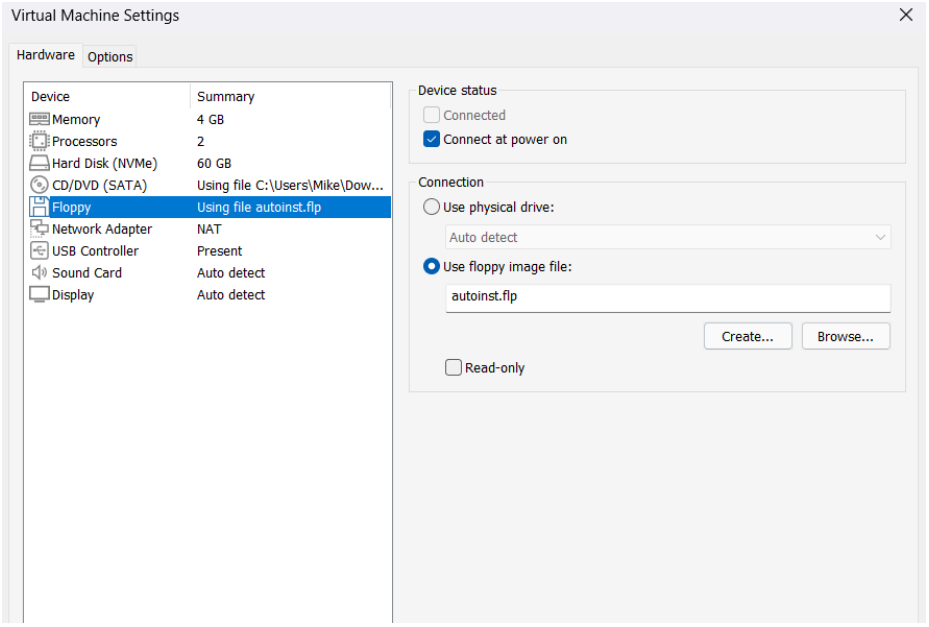
Minimum requirement for windows server 2022 :
CPU: 2 cores
RAM: 4GB
Storage: 60GB



If you encounter the issue shown in the screenshot above during installation, follow the steps below:
1- Shut down the **Windows Server** virtual machine.
2- Click Edit virtual machine settings.



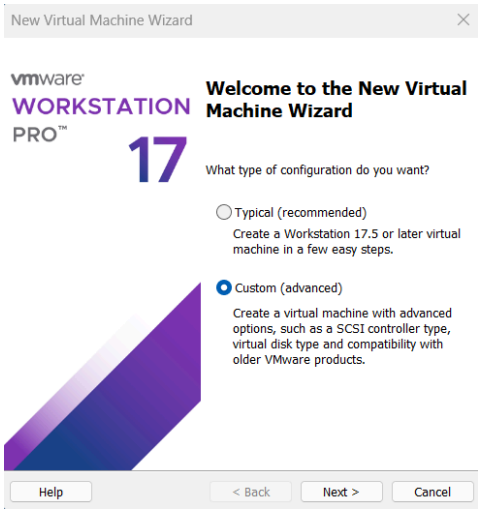
3- Click Floppy, then uncheck Connect at power on.



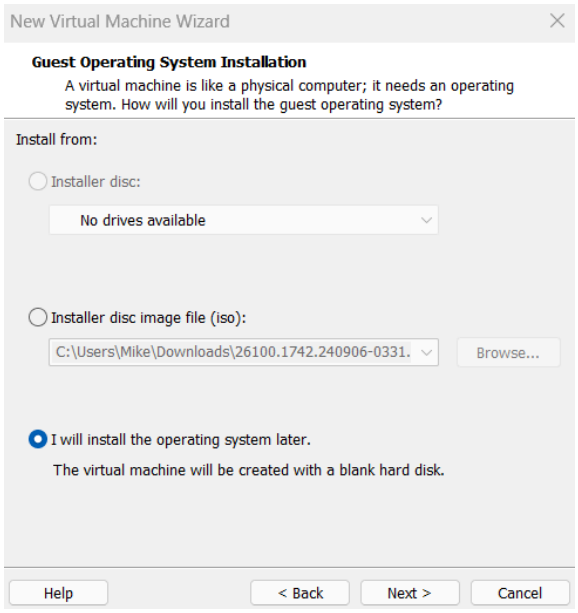
4- Power on the VM and follow the installation Wizard.

Windows 11 Enterprise

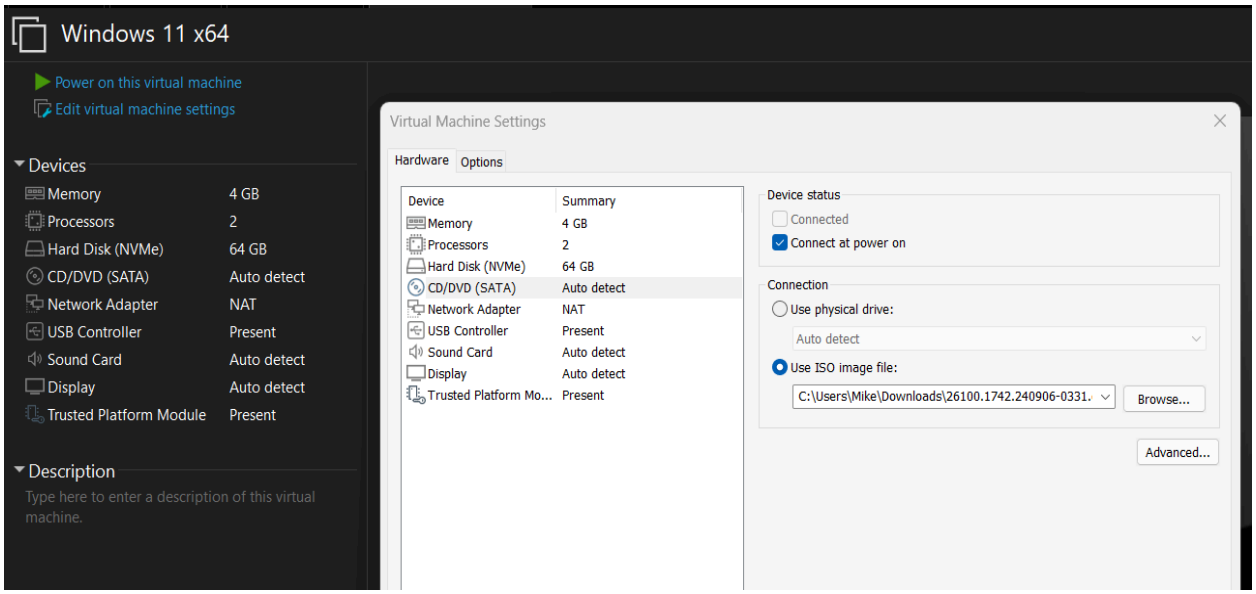
Minimum requirement for windows 11 Enterprise:
CPU: 2 cores
RAM: 4GB
Storage: 60GB
1- Create new virtual machine
2- select Custom (advanced)



3- I will install the operating system later



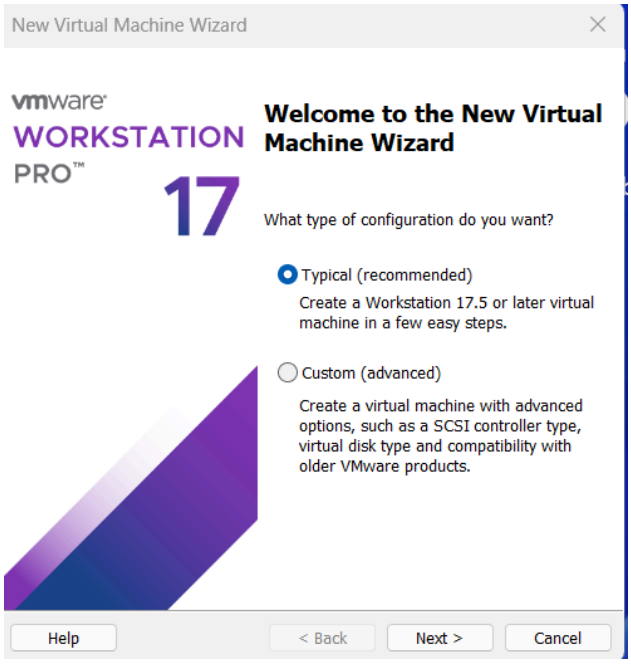
4- Select Microsoft Windows as the guest operating system and Windows 11 x64 as the version.
5- Provide a name for the virtual machine.
6- Create a TPM password.
7- Set the firmware type to UEFI and enable Secure Boot.
8- Once finished, click CD/DVD.



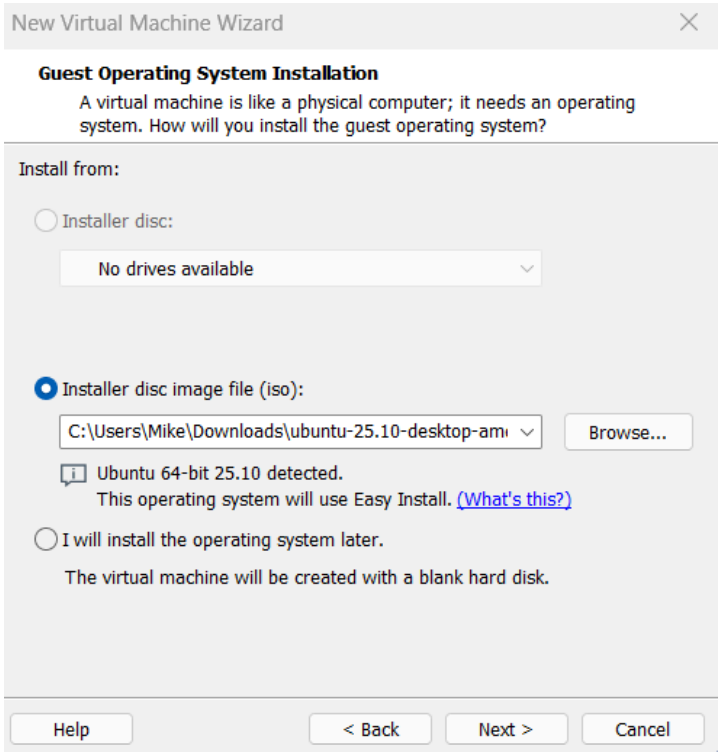
9- Select Use ISO image file, browse your computer for the Windows ISO image, and click OK.
10- Start the virtual machine and follow the installation wizard.

<u>Ubuntu</u>
Minimum requirement for Ubuntu 2510:
CPU: 2 cores

RAM: 4GB
Storage: 20GB
1- Select Typical (recommended)



2- select Installer disc image file (iso), browse your computer for the ubuntu image



3- follow the installation wizard.

Network Configuration

Create four VMnets in VMware

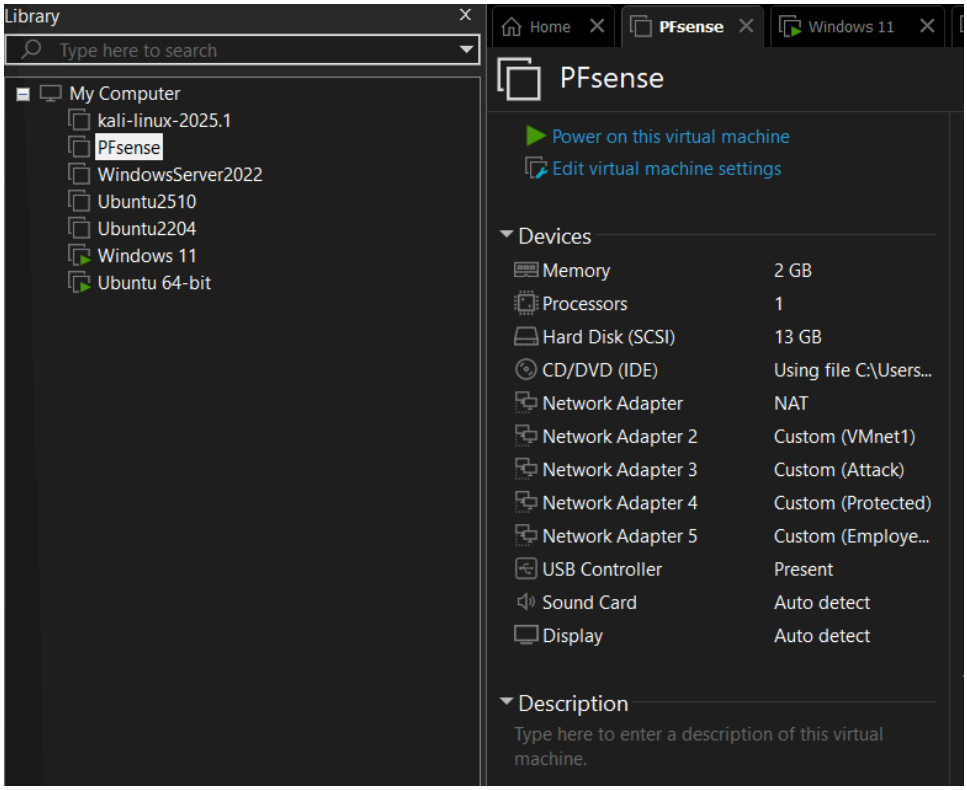
VMnet1 will serve as the LAN network any machine connected to this network will be able to access the Pfsense UI for management purposes.

- VMnet1 (LAN) configuration
    - From VMware click Edit → Virtual Network Editor
    - Select VMnet1→ Change Settings
    - Check Host-only (Connect VMs internally in a private network)
    - Check “Connect a host virtual adapter to this network”
    - Check “Use local DHCP service to distribute IP address to VMs”
    - Assign Subnet IP and Subnet mask (Subnet IP: 192.168.100.0, Subnet mask: 255.255.255.0)
    - Click Apply and OK to save the changes.
- VMnet2 (Protected)
    - Select VMnet2→ Change Setting
    - Rename Network to “Protected”
    - Check Host-only (Connect VMs internally in a private network)
    - Check “Connect a host virtual adapter to this network”
    - Check “Use local DHCP service to distribute IP address to VMs”
    - Assign Subnet IP and Subnet mask (Subnet IP: 192.168.20.0, Subnet mask: 255.255.255.0)
    - Click Apply and OK to save the changes.
- VMnet3 (Employee)
    - Follow the same instructions
    - Assign Subnet IP and Subnet mask (Subnet IP: 192.168.40.0, Subnet mask: 255.255.255.0)
- VMnet4 (Attack)
    - Follow the same instructions
    - Assign Subnet IP and Subnet mask (Subnet IP: 192.168.30.0, Subnet mask: 255.255.255.0)

VMs Configuration

Pfsense

1- Pfsense adapter connection
Before we start the Pfsense configuration we need to connect the adapters to the right networks. Make sure Pfense is turned off, click on Pfsense in the library on the left and the VM’s component will appear. You should see 5 adapters, see image below.



Click on the first adapter and select NAT.
For the second adapter choose “custom: specific virtual network” and select VMnet1 which is the LAN network that will serve for Pfsense management.
Do the same for the third, 4th and 5th adapter and choose VMnet2 (Protected), VMnet3 (Employee), VMnet4 (Attack) respectively. Remember that each VMnet represents a segment of the network where all the machines are connected. The Pfsense rules will be responsible for routing the packets to the intended destination.

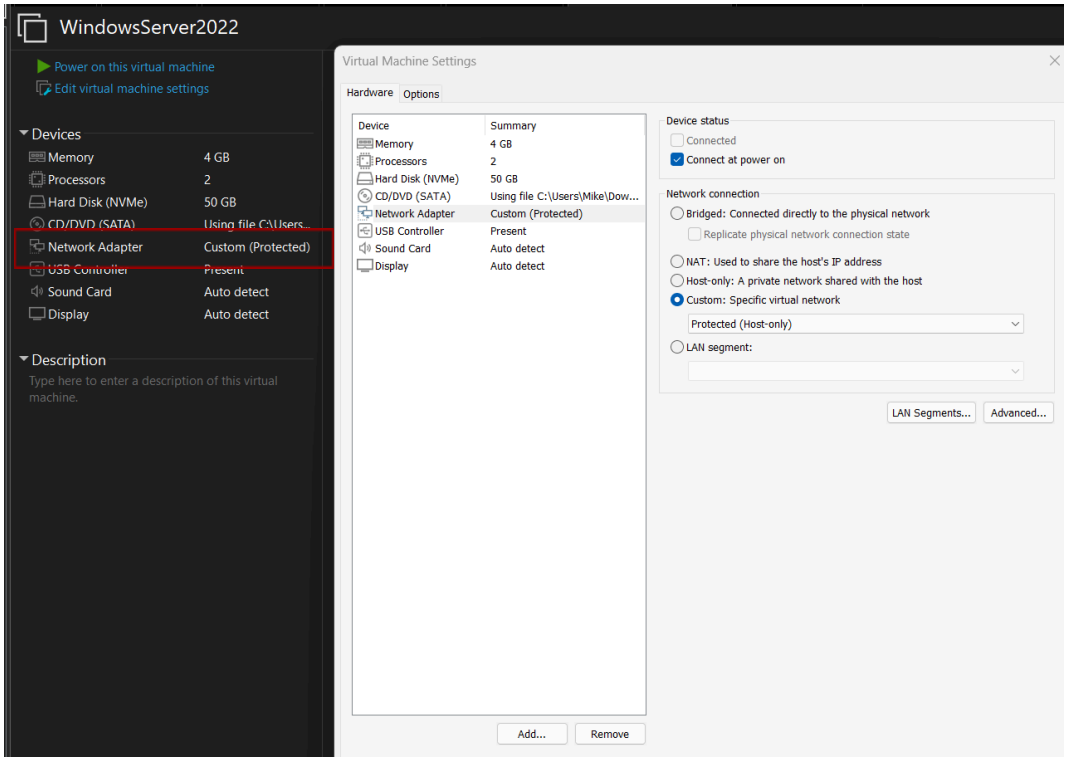
2- Access Pfsense UI management
To access the Pfsense UI management we have two options:

1. Create a virtual machine connected to the same VMnet2 as the Pfsense LAN and assign to the VM an address to the same subnet.
2. Access to Pfsense UI management from your Physical Machine (Host). In the search bar type “Run” open it write “ncpa.cpl” and click Ok. you should see all the VMware network Adapters you created. Right click on the VMnet2 → properties → select “Internet Protocol version 4 → properties → select “Use the following IP address”.
   Assign an address to the same subnet as the VMnet2 you previously created in VMware.

Open a browser, type the address of the Pfsense LAN you should be able to access the UI management. The default username and password is “admin” and “pfsense”

Windows Server 2022 (Domain Controller)

1- Click on the network adapter
2- Select “Custom: Specific virtual network”
3- Chose VMnet2 (Protected)



4- Assign a static IP address to the Domain Controller within the 192.168.20.0/24 subnet.

1. Click on Local Server
2. When the IP address shows Click on the IP address
3. Double click the NIC icon
4. Click on Properties
5. Double click the IPV$ line
6. Select “use the following IP address”
7. assigned IP address (from the subnet noted in the beginning)
8. Update the Default Gateway X.X.X.1
9. Update the Preferred DNS to the DC IP
10. Update the Alternate DNS to 8.8.8.8
11. Click Ok
12. Click Ok
13. Watch sent and received for traffic.
14. Close
15. Close Network Connections Click X at the top right.

5- Install the Active Directory and Domain Services Feature

1. From manage tab
2. Click on “Add Roles and Features Wizard”
3. Click next
4. Click next

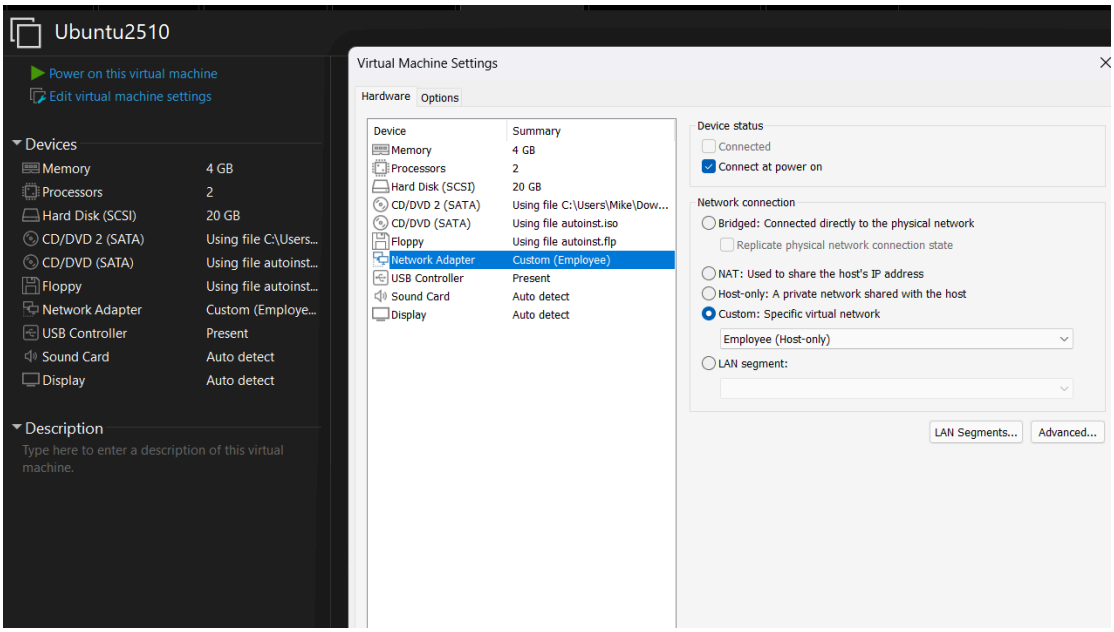
5. Click next
6. Click on the “Active Directory Domain Services” box to check it
7. Click next
8. Click on (in blue) “Promote this Domain Controller”
9. Click “Next
10. Click next
11. Click “Proceed with adding DC”
12. Click next
13. PW = *your_password*
14. Click next
15. Click Promote
16. System will reboot
17. Log into DC
18. PW = your_password

6- Promote Domain Controller

1. Click on the Flag Triangle
2. Click on (in blue) “Promote this server to a domain controller”
3. Click on Add a new forest
4. Root domain name *your_domain_name*
5. Click next
6. PW = *your_password*
7. PW = *yourpassword*
8. Click next
9. Click next
10. Click next
11. Click next
12. Click next
13. At top you will see a green check
14. Click install
15. System will restart

<u>Ubuntu</u>

1- Click on the network adapter
2- Select “Custom: Specific virtual network”
3- Select VMnet3 (employee)



4- Log in to the Ubuntu instance.
5- Open a terminal and switch to root using su or execute commands with sudo.
    1. apt-get update -y
    2. Apt-get upgrade -y
6- Enter the netplan directory
    1. Cd /etc/netplan
7- sudo nano 01-network-manager-all.yaml
8- The file should appear as shown below:

```
network:
  version: 2
  ethernets:
    ens3: #(change to your network adapter)
      dhcp4: true
      match:
        macaddress: fa:16:3e:5f:73:b3 #(change to your VM MAC address)
      mtu: 1450
      set-name: ens3
      nameservers:
        addresses:
          - 192.168.20.12 #(DC IP address)
```

9- save and exit the file
10- Apply the new network configuration:

    1. Sudo netplan apply

If nothing pops up, it should have worked. if you get a 'warning' about permissions change the permission of the file by running: **chmod 600 <filename>**
If you get the warning message "root:Cannot call open vSwitch: ovsdb-server.service is not running", install openvswitch-switch.

11- install the required software packages to adding the ubuntu instance to the Domain Controller (DC)

1. sudo apt -y install realmd libnss-sss libpam-sss sssd sssd-tools adcli samba-common-bin oddjob oddjob-mkhomedir packagekit

12- Discover the domain

1. realm discover *your_domain_name*
   Should get back info indicating the realm exists and needs certain software to be used.

12- Join the Domain/Realm

1. realm join -U administrator *your_domain_name*
2. When prompted, enter the password for Administrator

13- Check if in realm by entering

1. Realm list
   Should give information about the realm

14- Configure the process (PAM) to create a user's home directory automatically

1. Open the pam-configs directory:
   nano /usr/share/pam-configs/mkhomedir
2. Edit it as following:
   Name: activate mkhomedir
   Default: yes
   Priority: 900
   Session-Type: Additional
   Session: Required pam_mkhomedir.so umask=0022 skel=/etc/skel

15- Run the pam-auth-update

1. Pam-auth-update
2. Select the activate mkhomedir option with the spacebar
3. Use TAB to select the Ok option
4. Press enter to accept changes.

16- Restart the sss daemon

1. systemctl restart sssd
   No output should appear

17- Reboot the instance

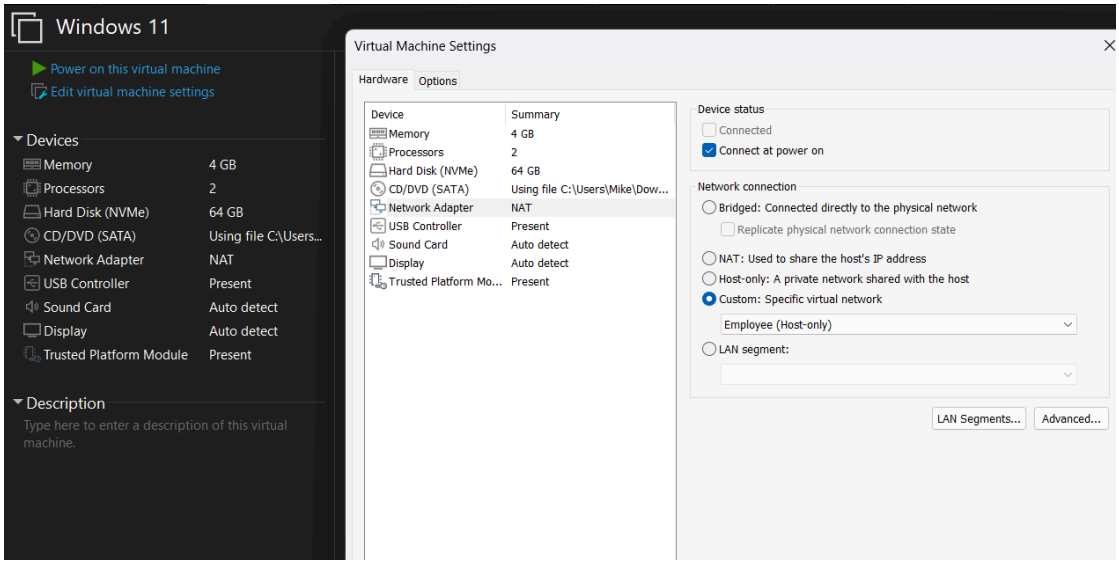
18- log back in as administrator@your_domain_name and password for Administrator

Windows 11 enterprise

1- Click on the network adapter

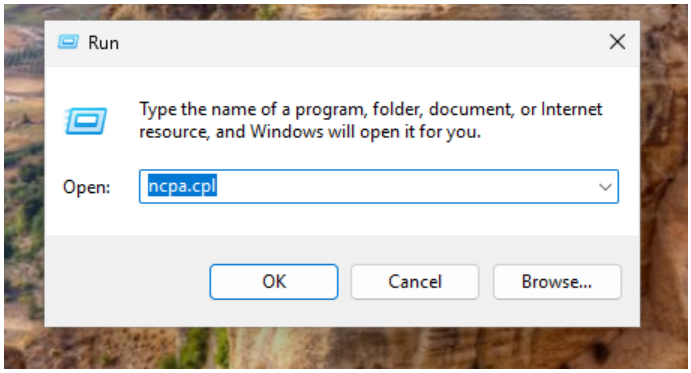
2- Select "Custom: Specific virtual network"

3- Select VMnet3 (employee)

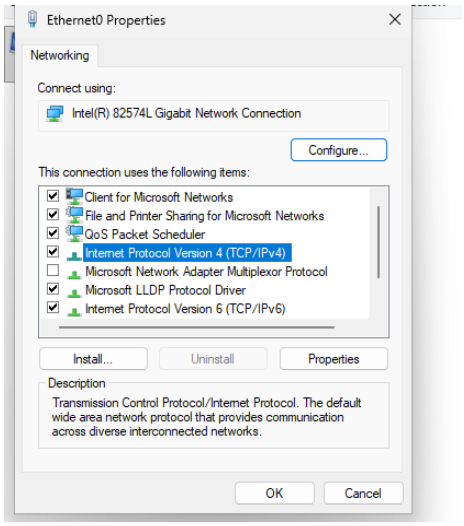


4- Log in to the Windows 11 instance.

5- Open the Run dialog, type ncpa.cpl, and click OK.



6- Right-click the Ethernet adapter, select Internet Protocol Version 4 (TCP/IPv4), and click Properties.



7- Assign a static IP address from the Employee subnet (192.168.40.0/24) to the Ethernet adapter.

8- Set the Preferred DNS server to the IP address of the Domain Controller (DC).
9- Join the Windows 11 VM to the Domain Controller:

1. Right-click Start → System
2. Click Advanced system settings
3. Under Computer Name, click Change
4. Select Domain
5. Enter your domain name
6. When prompted, enter domain admin credentials (Domain\Administrator)
7. Click OK
8. Restart the VM.
9. Log in with a domain account (username@domain_name).

Conclusion

In Part 1 of the lab, we successfully built the foundational elements of our SOC home lab. This included creating all network segments, including Protected, Employee, Attack, LAN and WAN, to simulate a realistic enterprise environment with proper network segmentation. We deployed the virtual machines required for the lab, including pfSense, Windows Server 2022, Ubuntu, and Windows 11, ensuring that each machine has the correct resources allocated for its role. Each VM was connected to its respective network segment, establishing proper isolation. Additionally, we set up and joined the Domain Controller, which provides centralized management.

These steps laid the groundwork for practicing SOC-related tasks, such as monitoring, incident response, and network management. By completing Part 1, we now have a functional network environment where policies can be enforced and traffic can be monitored across segmented networks.

In Part 2, we will build upon this foundation by testing connectivity between the different network segments to verify that routing are functioning correctly. We will implement firewall rules in pfSense to control traffic flow and secure sensitive segments. Finally, we will install Splunk Enterprise and Splunk Forwarders on all relevant endpoints to enable centralized log collection, monitoring, and analysis, which is essential for SOC operations. Completing these next steps will transform the lab from a static network into a fully operational security monitoring environment, allowing for hands-on SOC practice and simulation of real-world scenarios.