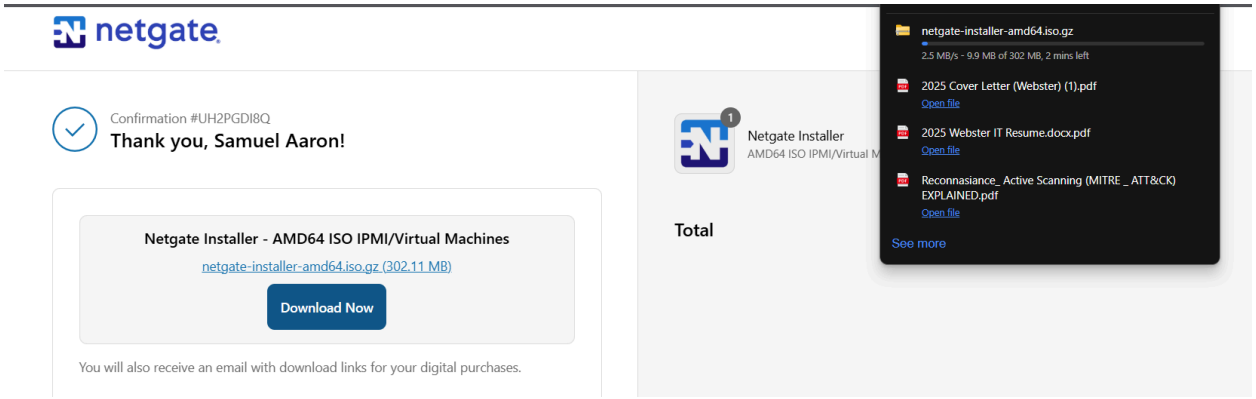
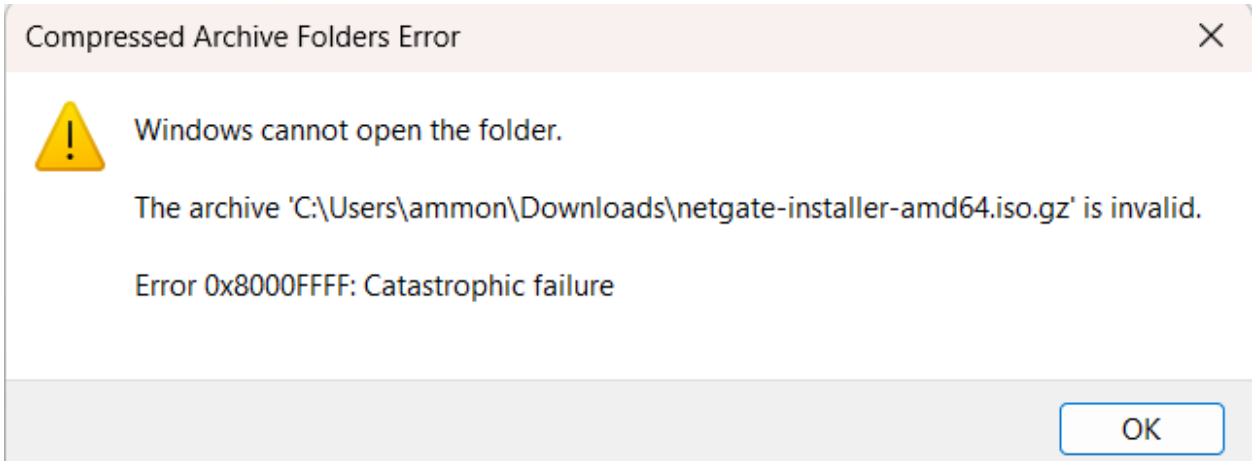
pfSense

pfSense is a free and open source firewall and router software. It is a great tool and one of the key parts of our SOC Lab infrastructure.

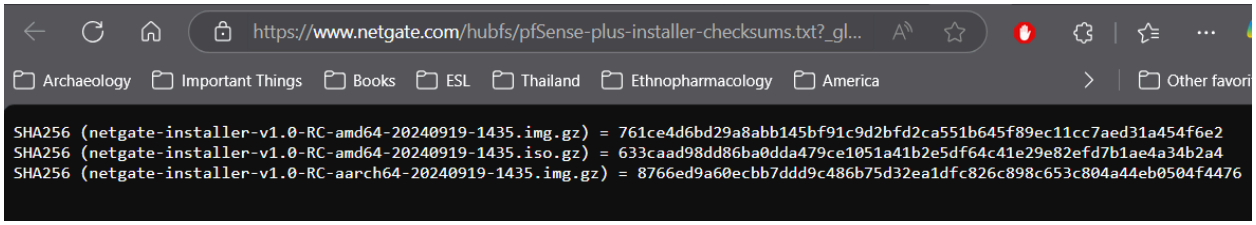


First, I installed [netgate](), which is an installer that you must use to install pfSense.



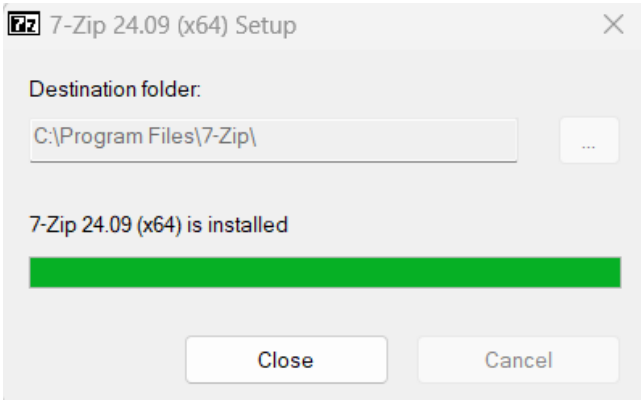
The file is a *.iso.gz* file so I couldn't simply unzip it. I kept getting an error message.

```
PS C:\windows\system32> Set-Location -Path "C:\Users\ammon\Downloads"
PS C:\Users\ammon\Downloads> Get-FileHash -Algorithm SHA256 .\netgate-installer-amd64.img.gz
Resolve-Path : Cannot find path 'C:\Users\ammon\Downloads\netgate-installer-amd64.img.gz' because it does not exist.
At
C:\windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1:110
char:36
+                $pathsToProcess += Resolve-Path $Path | Foreach-Objec ...
+                                   ~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : ObjectNotFound: (C:\Users\ammon\...er-amd64.img.gz:String) [Resolve-Path], ItemNotFoundE
   xception
    + FullyQualifiedErrorId : PathNotFound,Microsoft.PowerShell.Commands.ResolvePathCommand

PS C:\Users\ammon\Downloads> Get-FileHash -Algorithm SHA256 "C:\Users\ammon\Downloads\netgate-installer-amd64.iso.gz"

Algorithm       Hash                                                                   Path
---------       ----                                                                   ----
SHA256          633CAAD98DD86BA0DDA479CE1051A41B2E5DF64C41E29E82EFD7B1AE4A34B2A4       C:\Users\ammon\Downloads\netg...
```

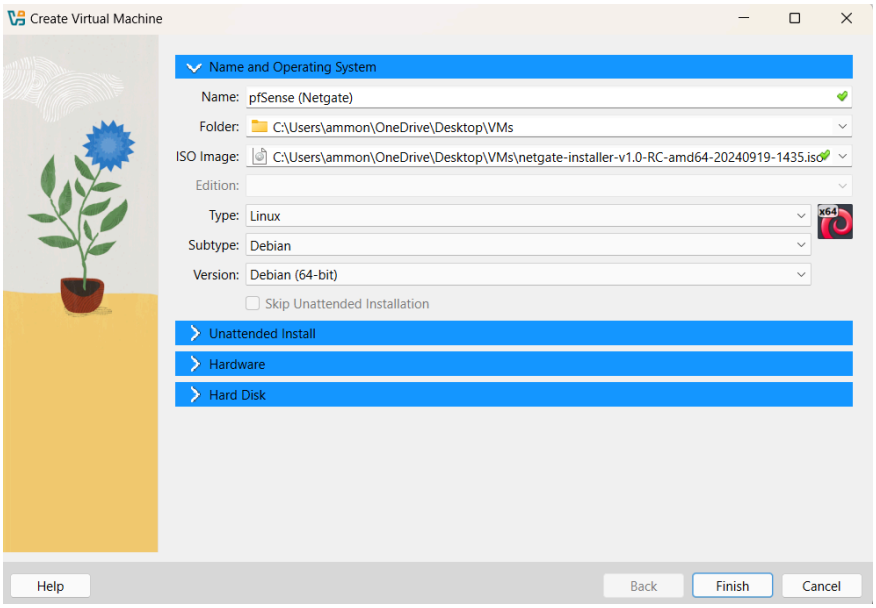


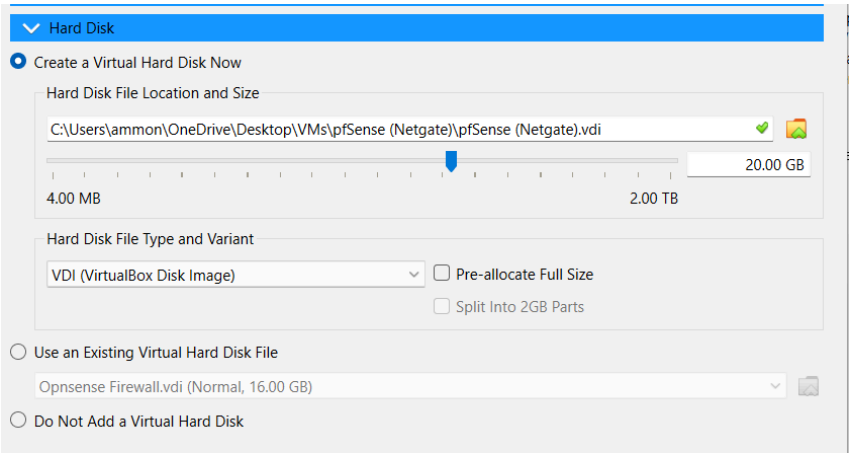
So I checked to see if the SHA256 hash of the file I downloaded matched the true SHA256 hash. They matched.

I wasn't sure how to get **pfSense** onto a virtual machine from here, so I began using the netgate installation guide.

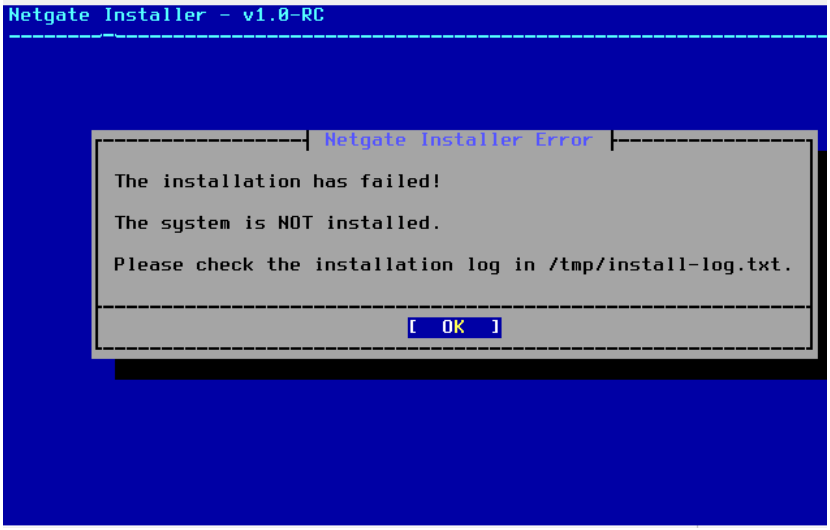


I had to download **7-Zip** in order to extract the *.iso* file.

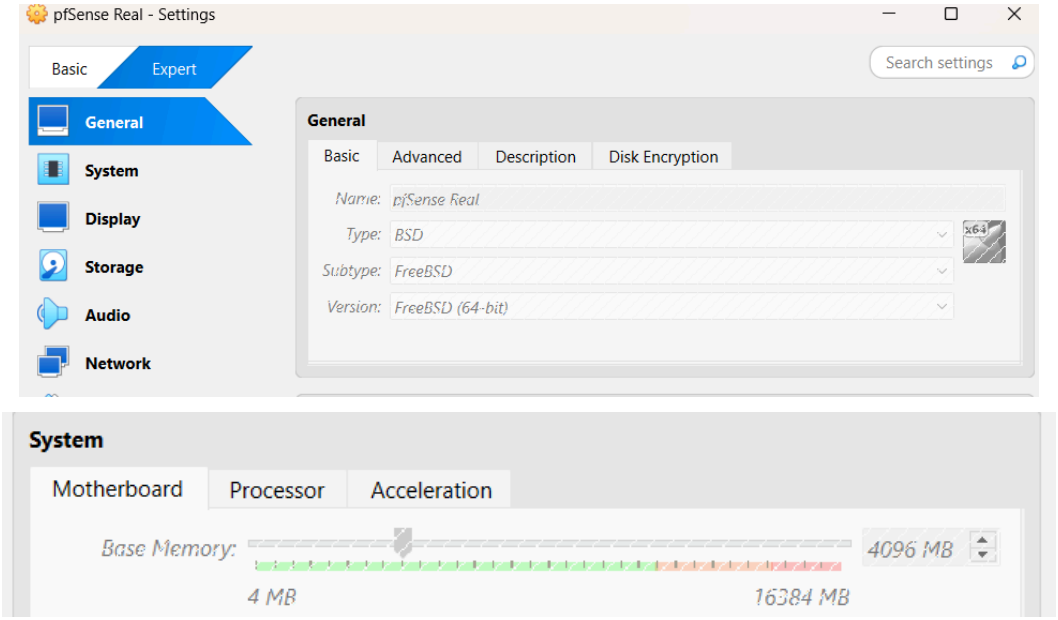




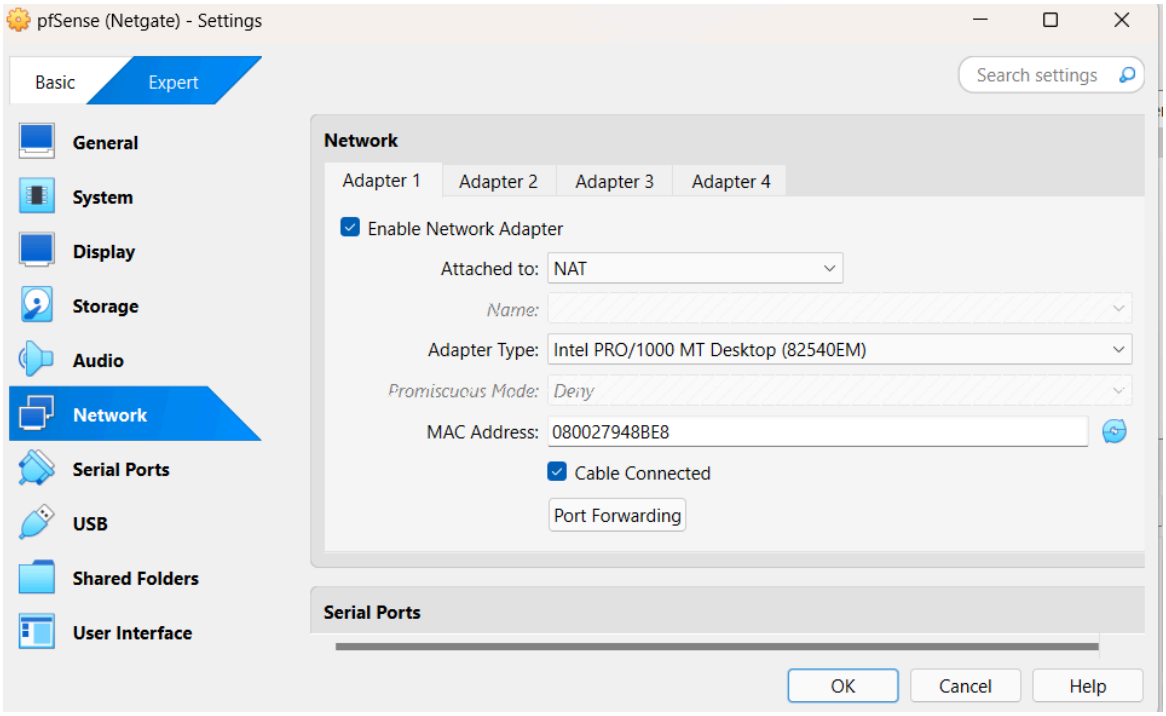
After extracting the *.iso* file using **7-Zip** I started making a VM in **VirtualBox**. It should be noted I ran into an issue later in the installation process. The issue was with this step. I should not have made the type Linux, subtype Debian, and the version Debian 64-bit.

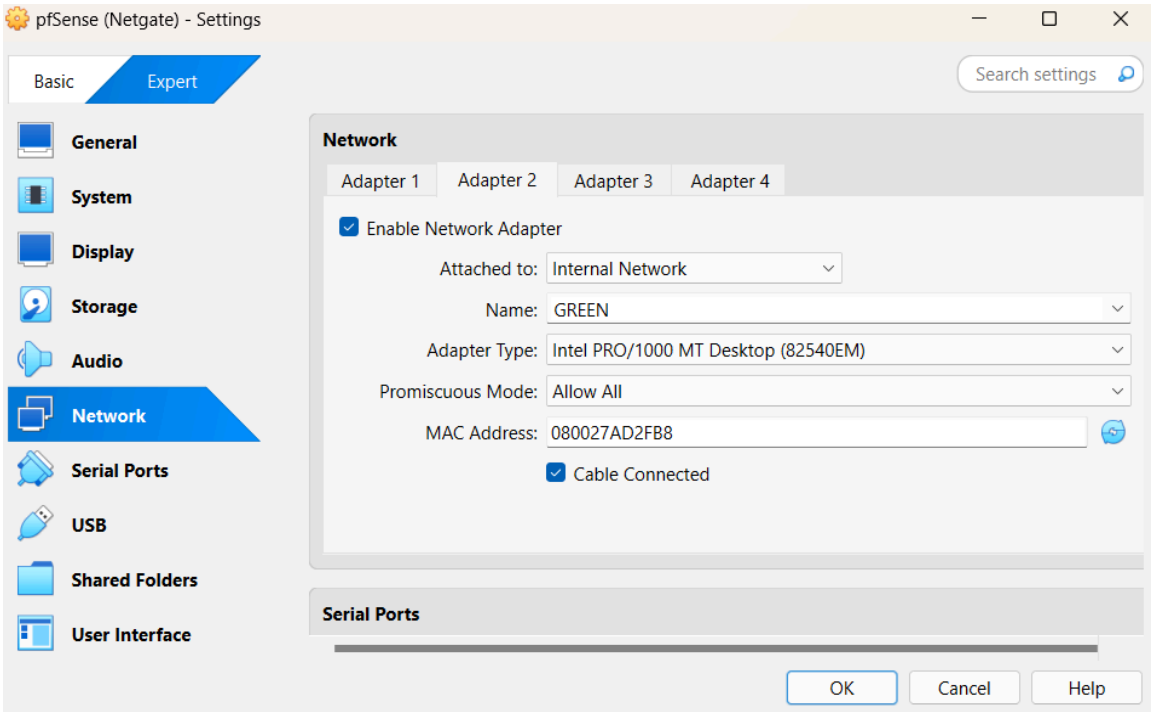


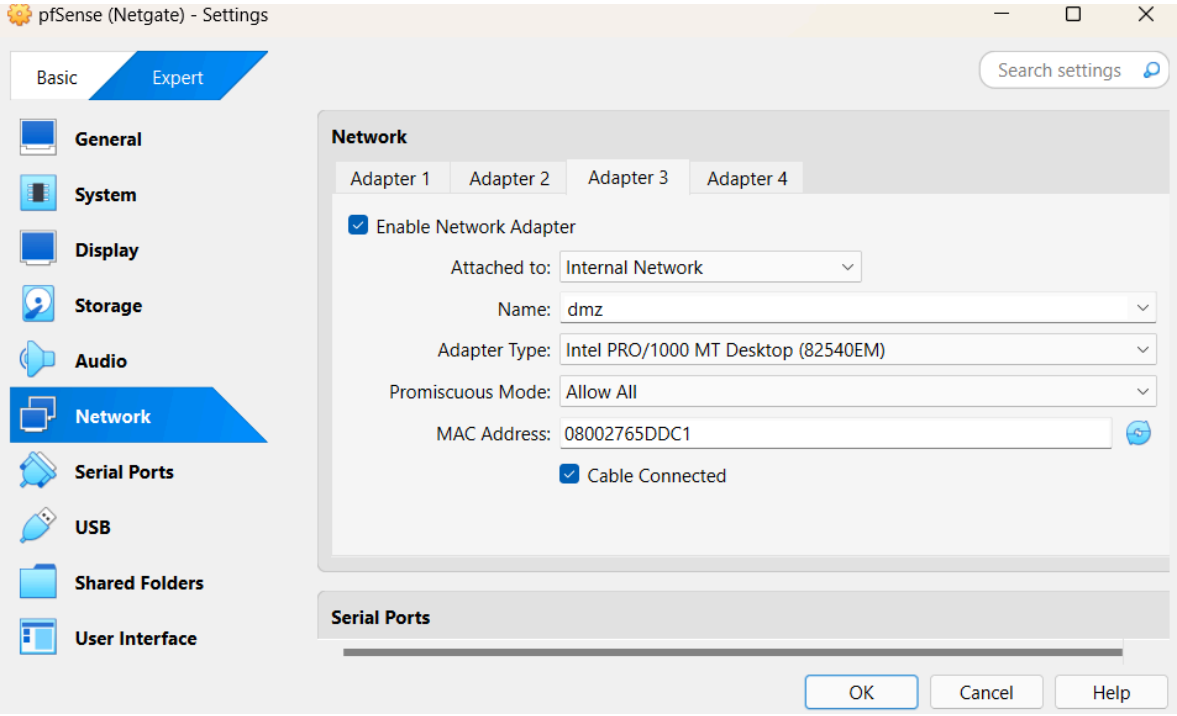
As you can see it ended up causing my installation to fail. So I had to go back and create a new VM.



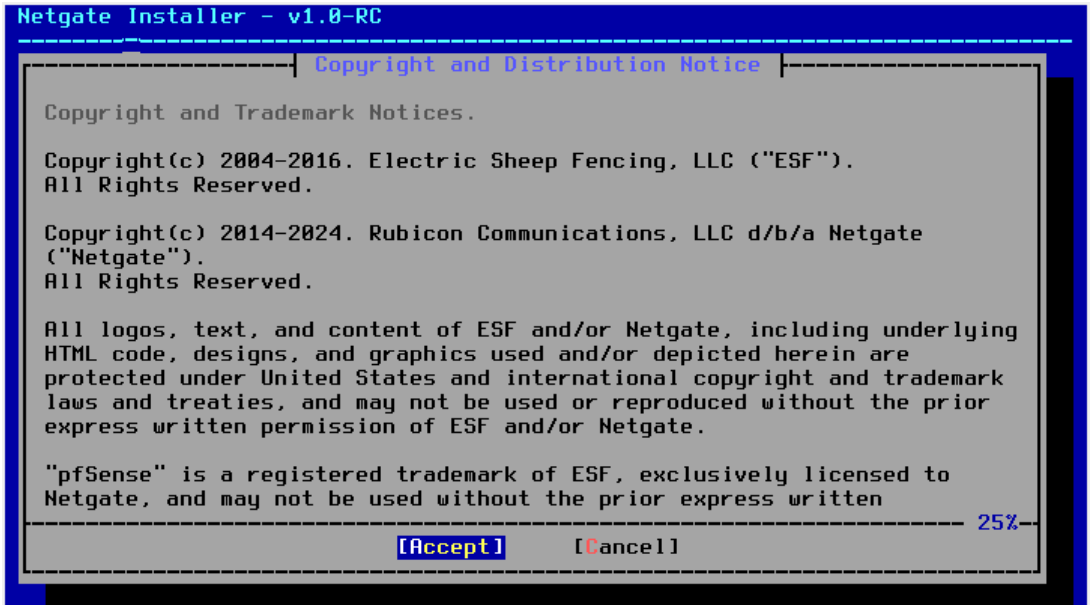
The main thing I did differently with the new VM is change the “Type”. Previously I made the type Linux, the subtype Debian , and the version Debian 64-bit. With the new VM I made the type BSD, the subtype FreeBSD, and the version FreeBSD 64-bit. The other adjustment I made was increasing the Base Memory to 4096 MB. After making these adjustments the installation was successful.


pfSense (Netgate) - Settings
Basic
Expert
Search settings
General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
User Interface
Network
Adapter 1
Adapter 2
Adapter 3
Adapter 4
Enable Network Adapter
Attached to: NAT
Name:
Adapter Type: Intel PRO/1000 MT Desktop (82540EM)
Promiscuous Mode: Deny
MAC Address: 080027948BE8
Cable Connected
Port Forwarding
Serial Ports
OK
Cancel
Help

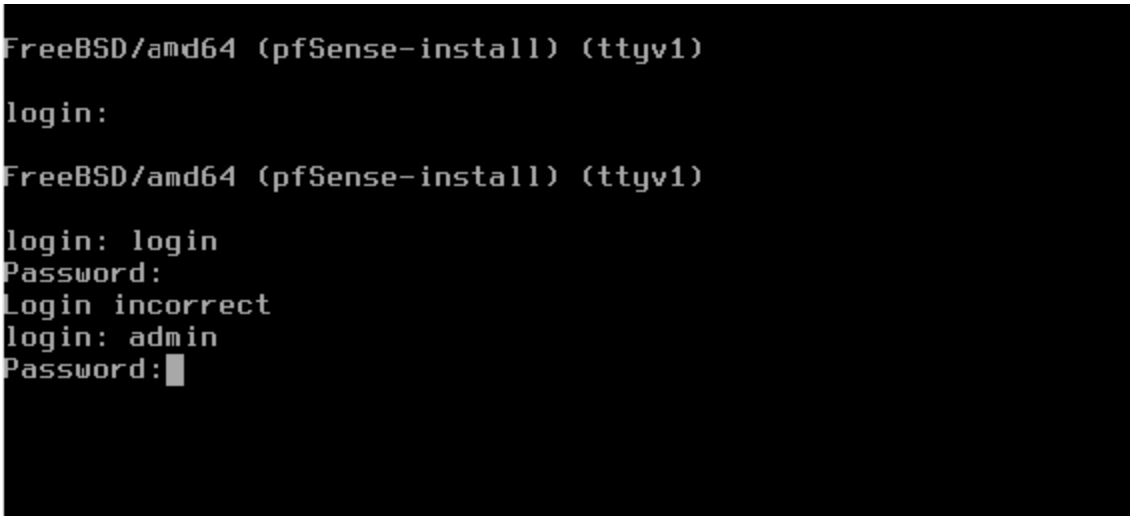

pfSense (Netgate) - Settings
Basic
Expert
Search settings
General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
User Interface
Network
Adapter 1
Adapter 2
Adapter 3
Adapter 4
Enable Network Adapter
Attached to: Internal Network
Name: GREEN
Adapter Type: Intel PRO/1000 MT Desktop (82540EM)
Promiscuous Mode: Allow All
MAC Address: 080027AD2FB8
Cable Connected
Serial Ports
OK
Cancel
Help



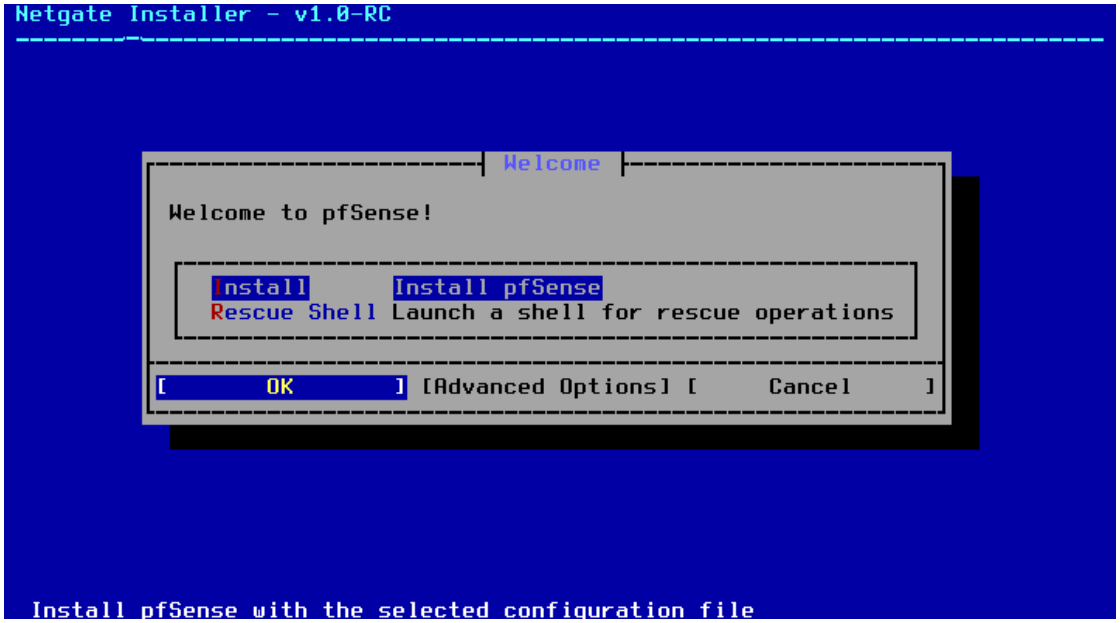
After adding the new VM you need to go to **Settings -> Network** and then we establish 3 adapters like you see above.

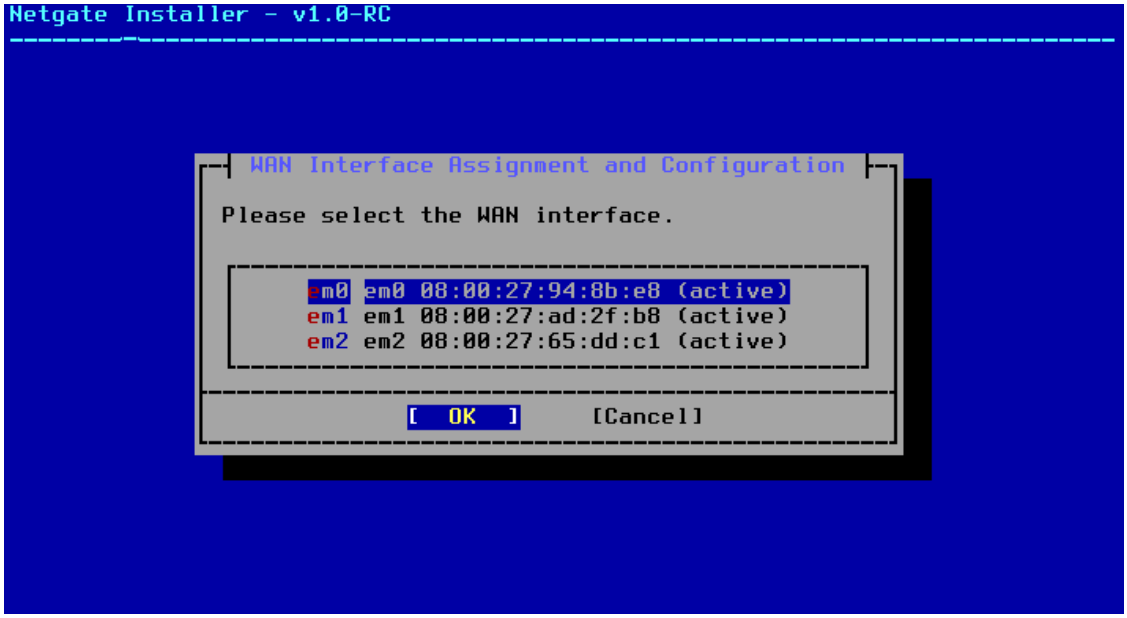


After opening the new VM we must accept the copyright agreement.

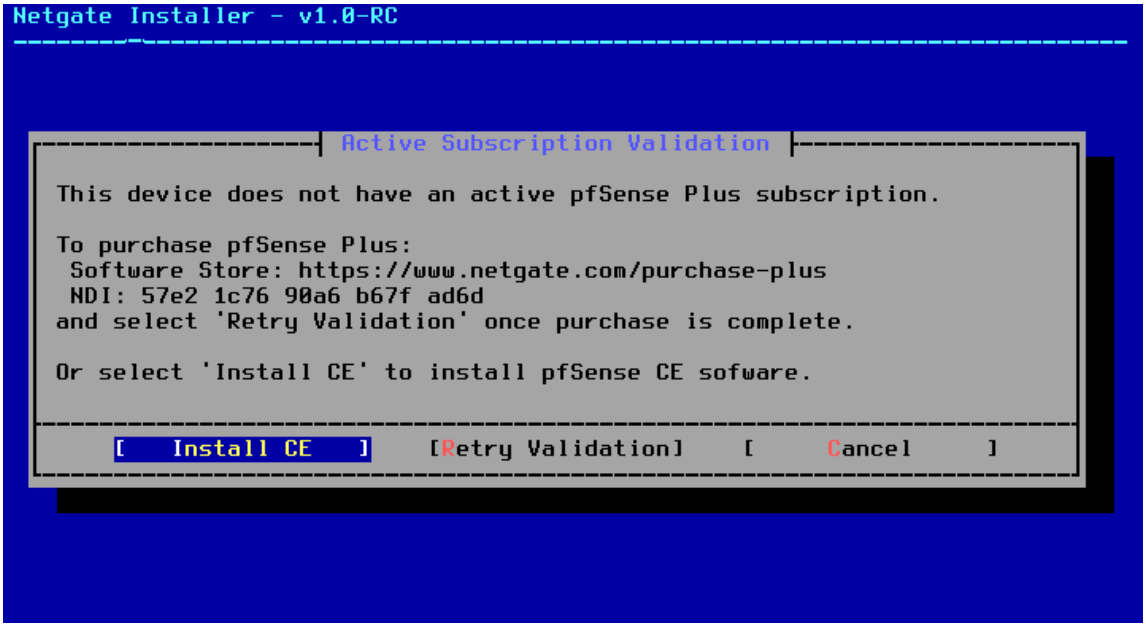


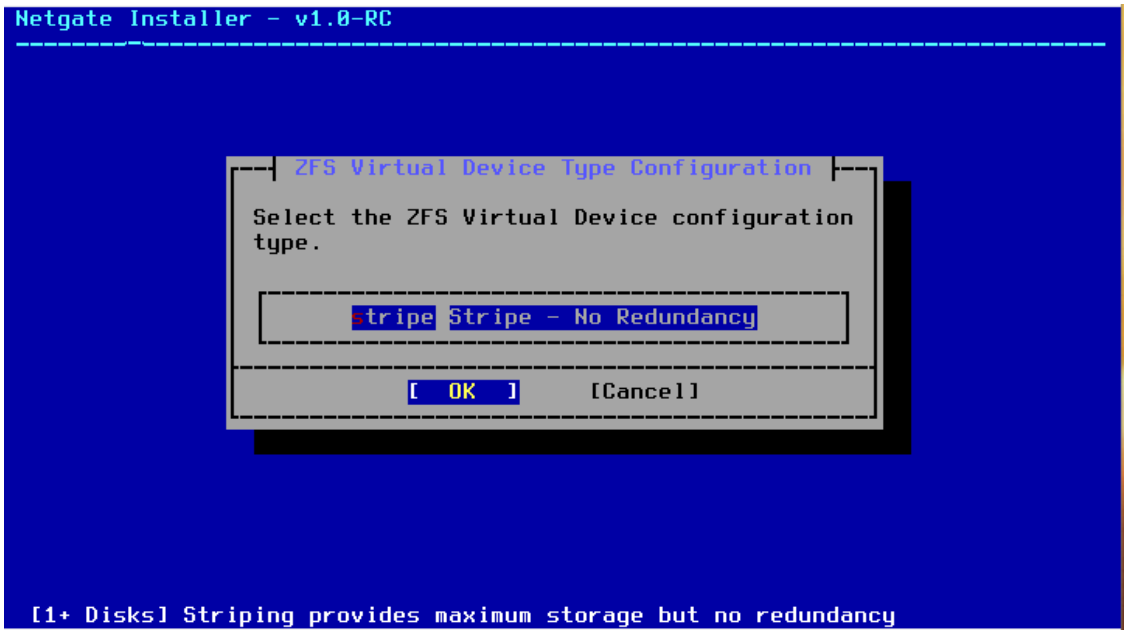
If you don’t interact with the VM window for a few minutes it makes you login again. (Login: admin / Password: pfsense)

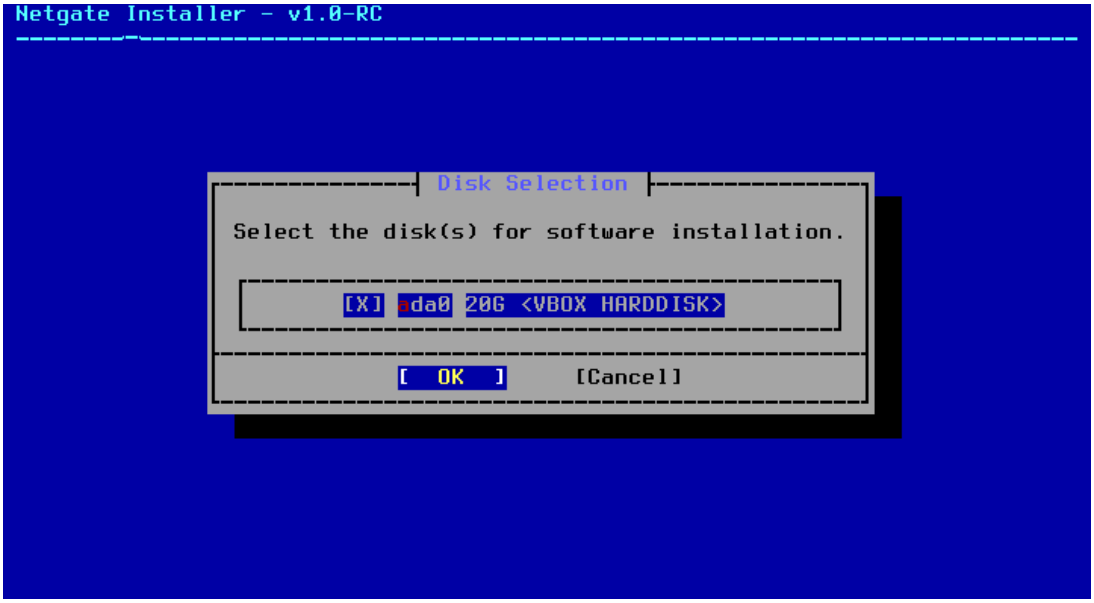




I made em0 the WAN and em1 the LAN

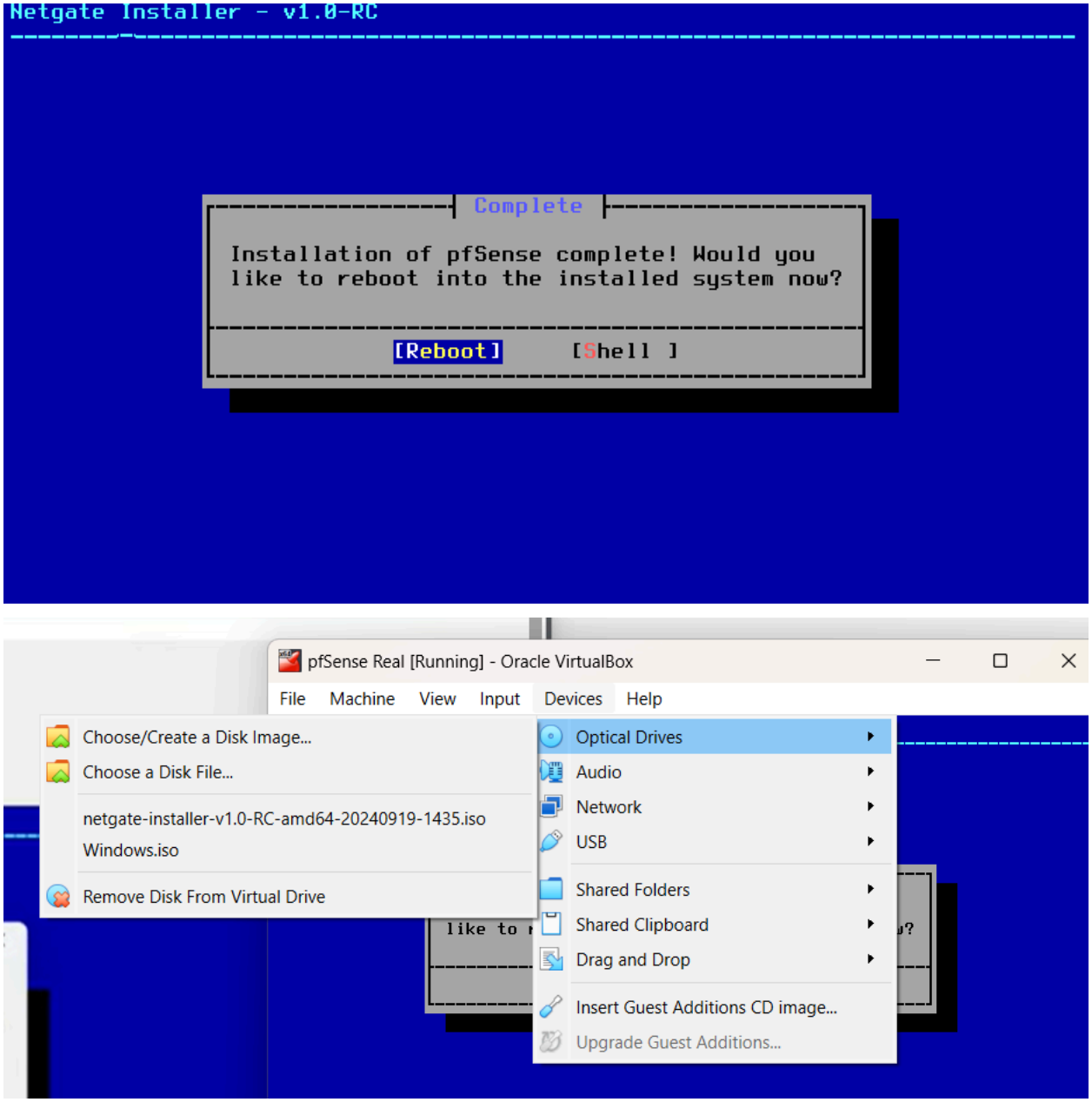



Netgate Installer - v1.0-RC
ZFS Virtual Device Type Configuration
Select the ZFS Virtual Device configuration type.
stripe Stripe - No Redundancy
[OK]
[Cancel]
[1+ Disks] Striping provides maximum storage but no redundancy


Netgate Installer - v1.0-RC
Disk Selection
Select the disk(s) for software installation.
[X] da0 20G <VBOX HARDDISK>
[OK]
[Cancel]

```
Number of packages to be installed: 1

The process will require 144 MiB more space.
139 MiB to be downloaded.
[1/1] Fetching pfSense-base-2.7.2.pkg: .......... done
Checking integrity... done (0 conflicting)
[1/1] Installing pfSense-base-2.7.2...
[1/1] Extracting pfSense-base-2.7.2: ... done
===> Removing schg flag from base files
===> Extracting new base tarball
===> Removing static obsoleted files

Installing pfSense kernel

pkg-static: Warning: Major OS version upgrade detected.  Running "pkg boot
Updating pfSense-core repository catalogue...
```

```
[9/169] Fetching dpinger-3.3.pkg: . done
[10/169] Fetching php82-pear-Crypt_CHAP-1.5.0_2.pkg: . done
[11/169] Fetching libidn2-2.3.4.pkg: ....... done
[12/169] Fetching devcpu-data-20230617_1.pkg: . done
[13/169] Fetching hostapd-2.10_8.pkg: ....... done
[14/169] Fetching filterdns-2.2.pkg: . done
[15/169] Fetching libxslt-1.1.37.pkg: ...... done
[16/169] Fetching libuv-1.46.0.pkg: ..... done
[17/169] Fetching boost-libs-1.83.0.pkg: .......... done
[18/169] Fetching uclcmd-0.2.20211204.pkg: . done
[19/169] Fetching bsnmp-ucd-0.4.5.pkg: . done
[20/169] Fetching lzo2-2.10_1.pkg: ...... done
[21/169] Fetching nss_ldap-1.265_14.pkg: .. done
[22/169] Fetching php82-pear-Net_Socket-1.2.2.pkg: . done
[23/169] Fetching libunistring-1.1.pkg: ......... done
[24/169] Fetching cpdup-1.22.pkg: .. done
[25/169] Fetching php82-zlib-8.2.11.pkg: . done
[26/169] Fetching cpu-microcode-amd-20230808.pkg: .. done
[27/169] Fetching php82-dom-8.2.11.pkg: ... done
```



Before rebooting make sure you unmount the *.iso* file from the drive so when we reboot the machine we will be able to use **pfSense**. If you don't do this step you will have to reinstall it again and again.

```
Starting CRON... done.
pfSense 2.7.2-RELEASE amd64 20240304-1953
Bootup complete

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

VirtualBox Virtual Machine - Netgate Device ID: 59b9ddba2e676631cab2

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

 WAN (wan)       -> em0        -> v4/DHCP4: 10.0.2.15/24
                                  v6/DHCP6: fd00::a00:27ff:feb0:2d8f/64
 LAN (lan)       -> em1        -> v4: 192.168.1.1/24

 0) Logout (SSH only)                  9) pfTop
 1) Assign Interfaces                 10) Filter Logs
 2) Set interface(s) IP address       11) Restart webConfigurator
 3) Reset webConfigurator 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:
```

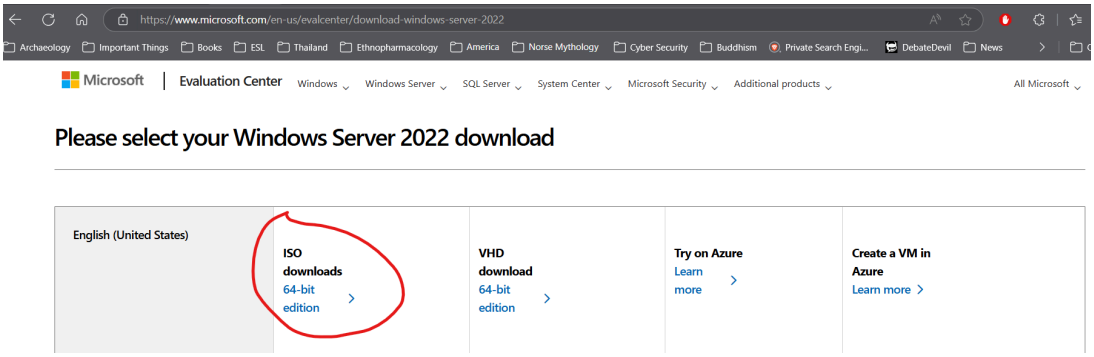
After reboot we arrive inside **pfSense**. The last step we want to complete now is assigning network interfaces. So we typed “1” to assign network interfaces.

```
say no here and use the webConfigurator to configure VLANs later, if required.

Should VLANs be set up now [y|n]? n

If the names of the interfaces are not known, auto-detection can
be used instead. To use auto-detection, please disconnect all
interfaces before pressing 'a' to begin the process.

Enter the WAN interface name or 'a' for auto-detection
(em0 em1 em2 or a): em0

Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(em1 em2 a or nothing if finished): em1

Enter the Optional 1 interface name or 'a' for auto-detection
(em2 a or nothing if finished): em2

The interfaces will be assigned as follows:

WAN  -> em0
LAN  -> em1
OPT1 -> em2

Do you want to proceed [y|n]? y
```

After assigning the network interfaces as seen above, we are done. For the next part in the SOC lab series we will work on setting up **Active Directory.**

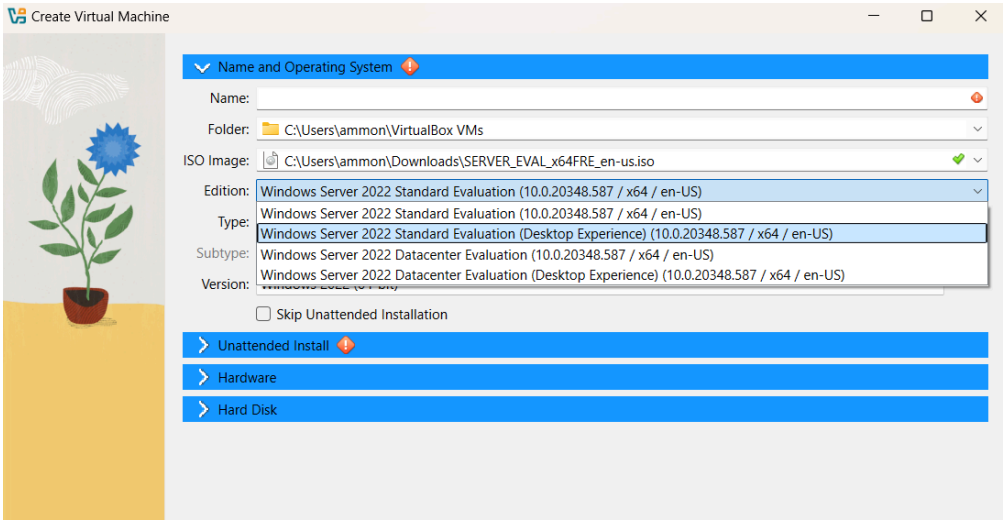
Active Directory

Active Directory is an important tool in SOC. It is used to manage user accounts, groups, and permissions across the entire network. It plays an important role in the Principle of Least Privilege and in Identity and Access Management. Active Directory logs every password change, login attempt, and access change. It can also create Group Policy Objects to enforce security settings. Lastly, Active Directory logs can be forwarded to SIEMs.

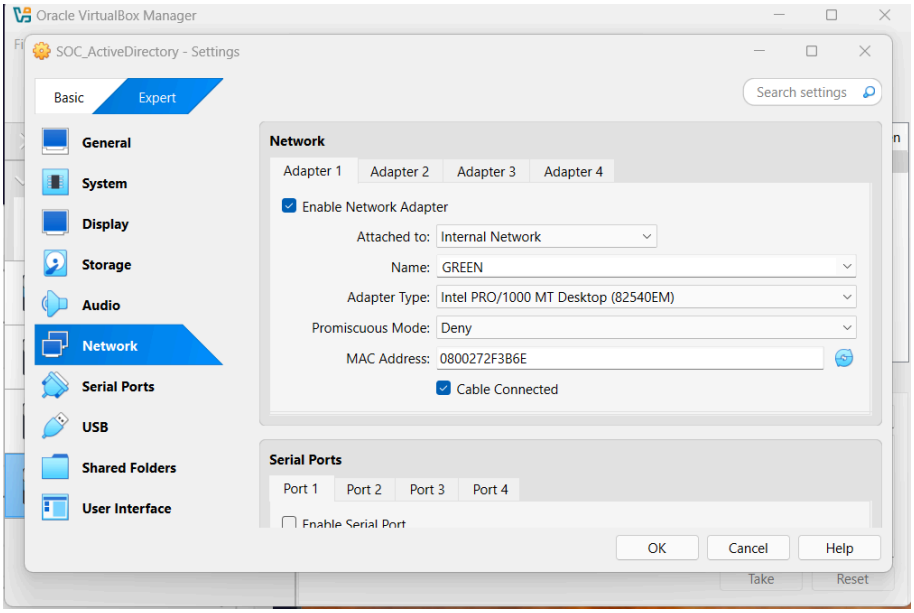


First, we downloaded Windows Server 2022 ISO file.
[Windows Server 2022 | Microsoft Evaluation Center]

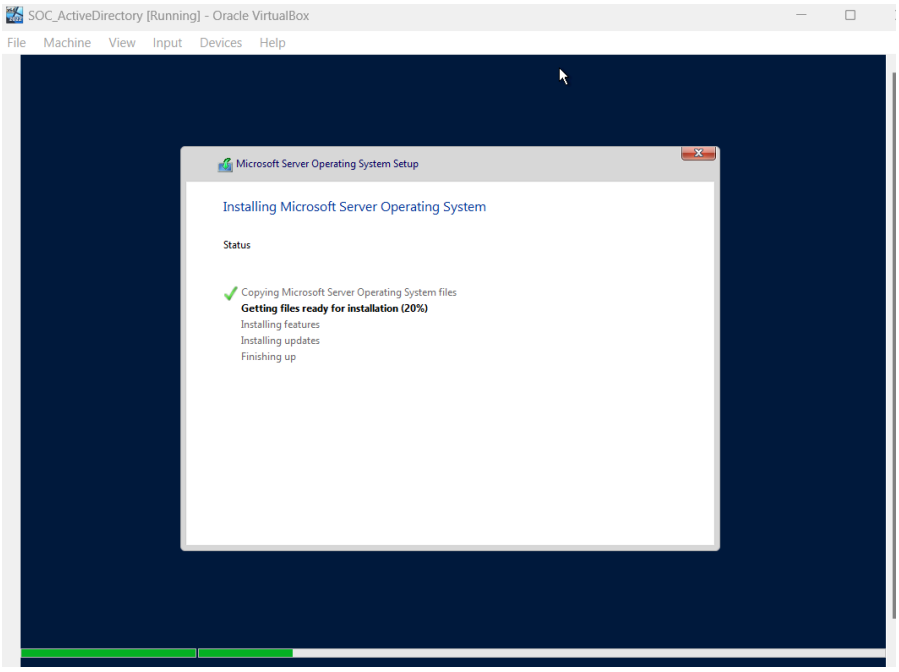
After downloading the *.iso* file I created a new machine with the file.



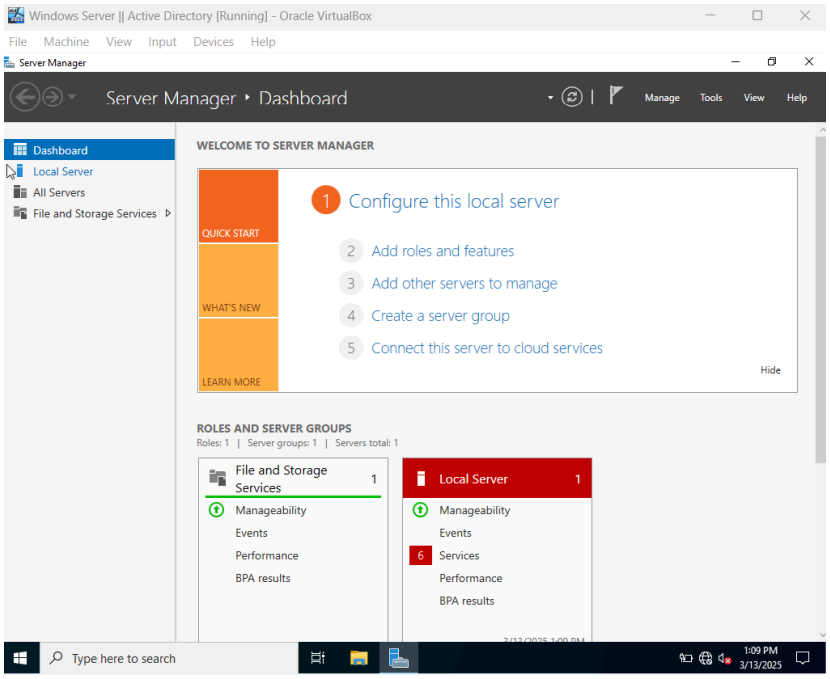
Make sure when you create the VM that you select Windows Server 2022 Standard Evaluation (Desktop Experience). I originally selected the other option and there was no GUI.



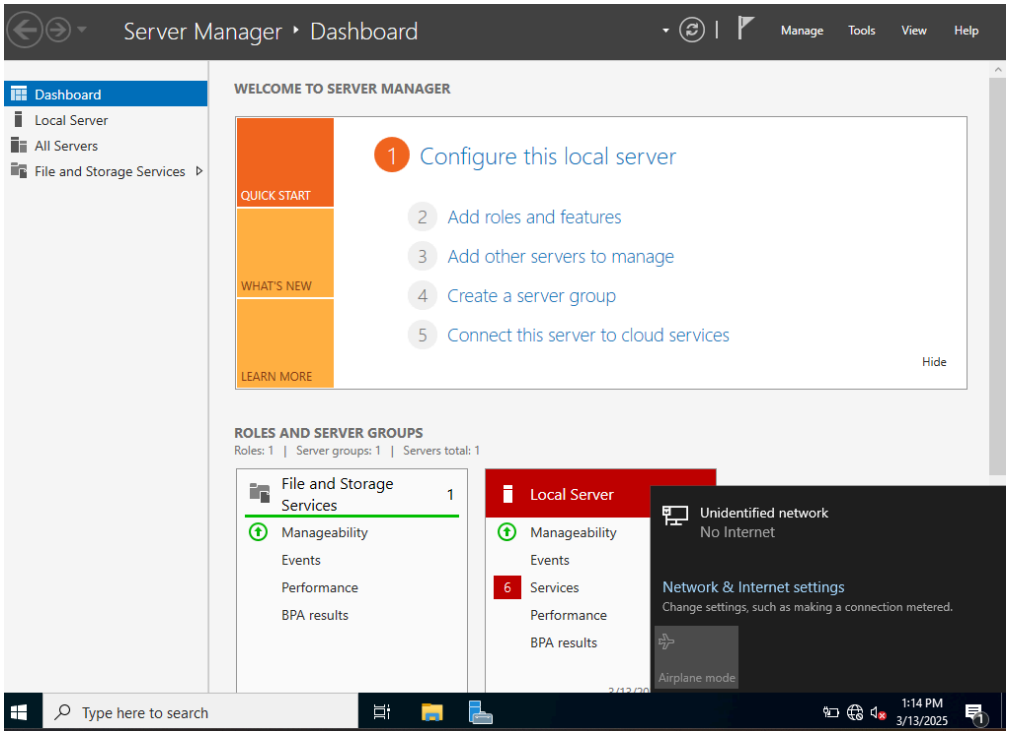
After creating it, I established one adapter attached to the Internal Network and named it Green.



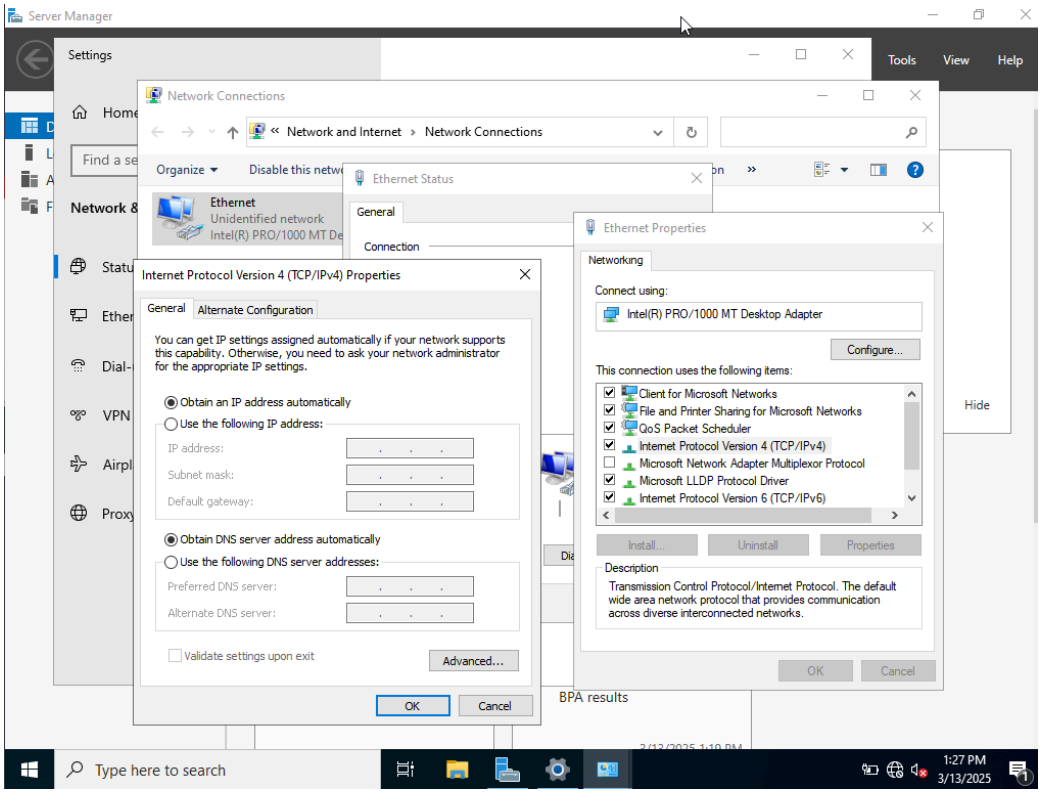
After starting the machine, the Microsoft Server OS begins to install.



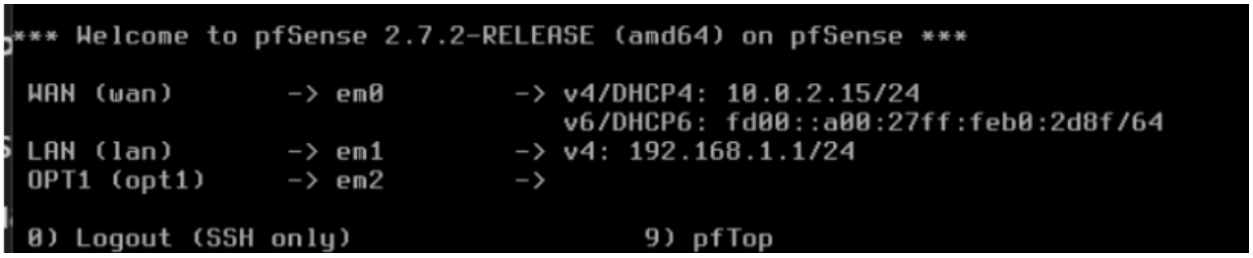
After instillation I was automatically logged in and Server Manager automatically opened.

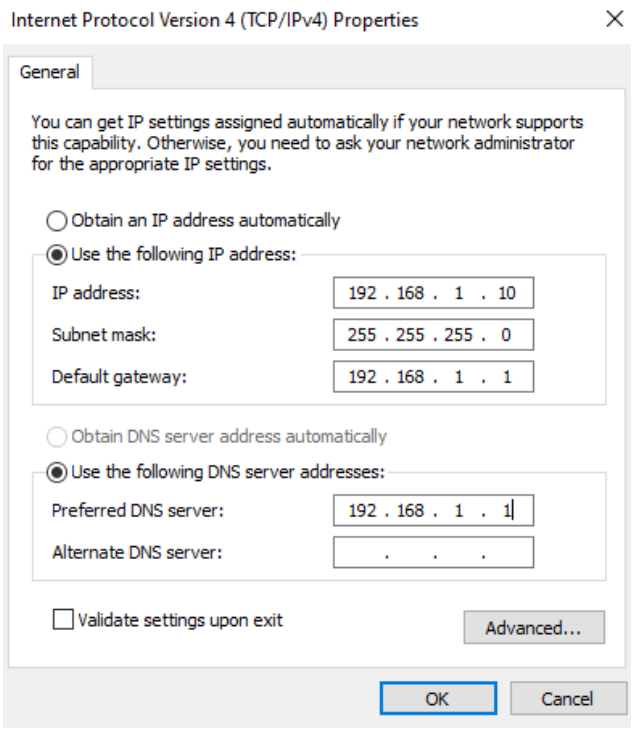


Go to Network and Internet Settings.

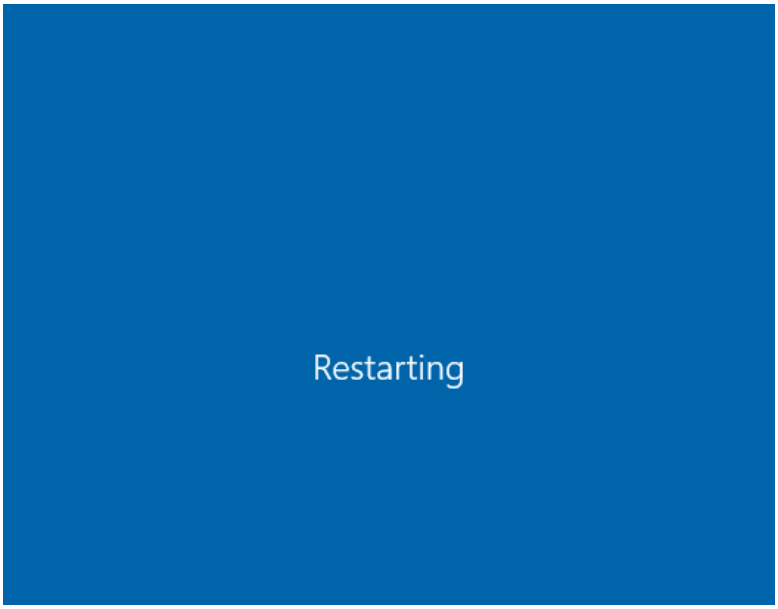


Click on Ethernet, then Ethernet Properties, then IPV 4 Properties.

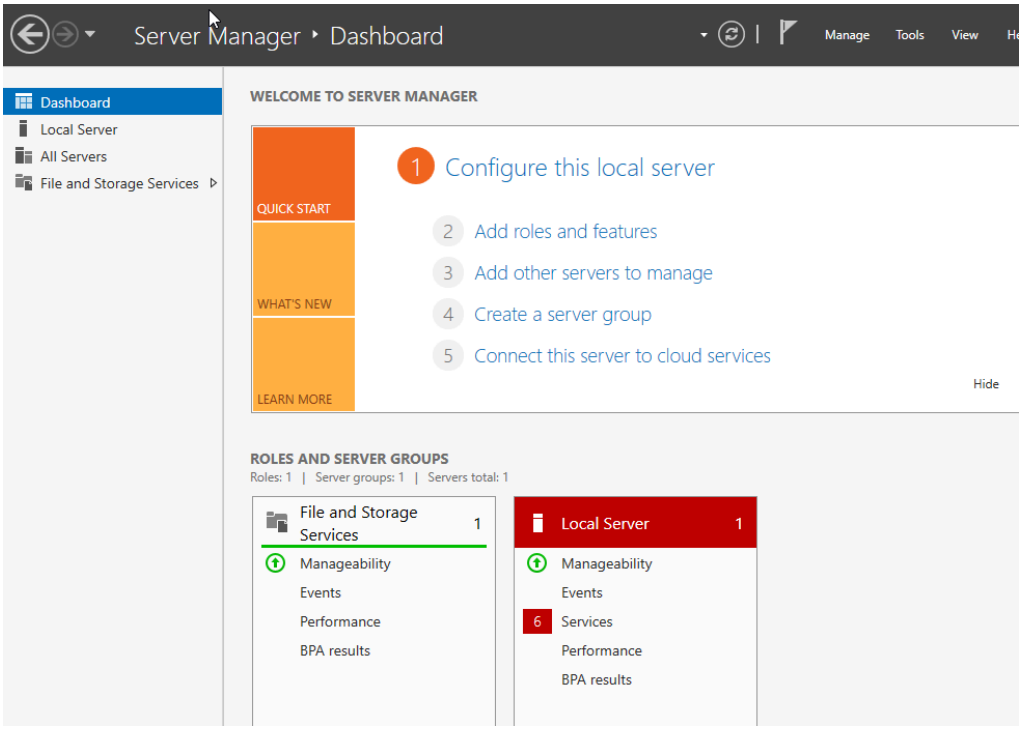




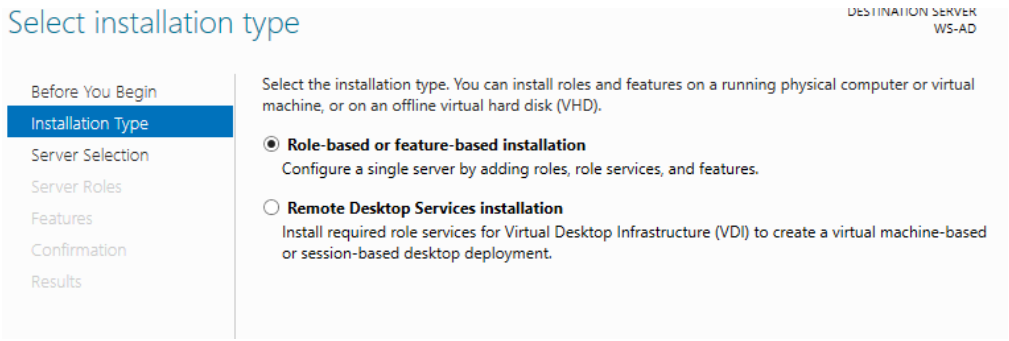
We want our Windows Server 2022 IPV4 IP address to be in the same range as the **pfSense** LAN (192.168.1.1/24). We want the Default Gateway to match the IP for **pfSense** LAN, The DNS server address can also be the same.

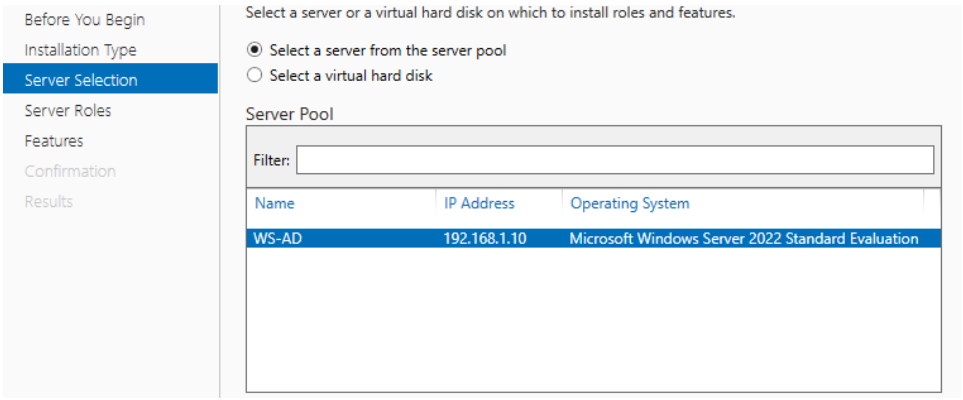


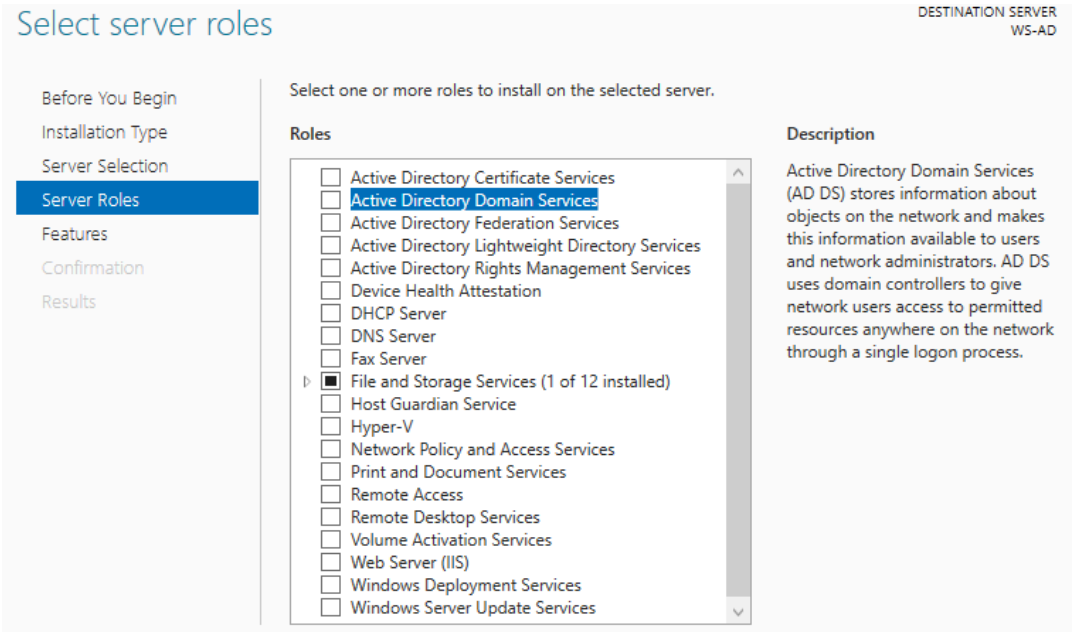
Afterwards we restart the VM.

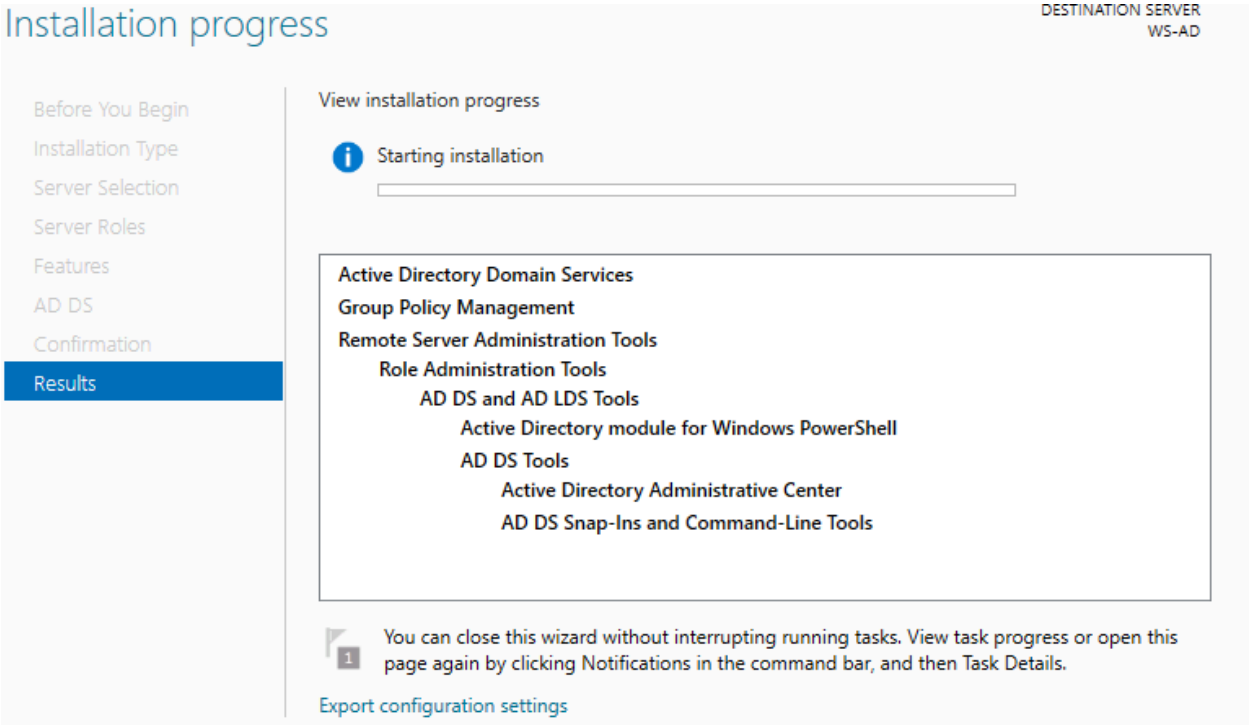


After restart, we click “Add roles and features”.

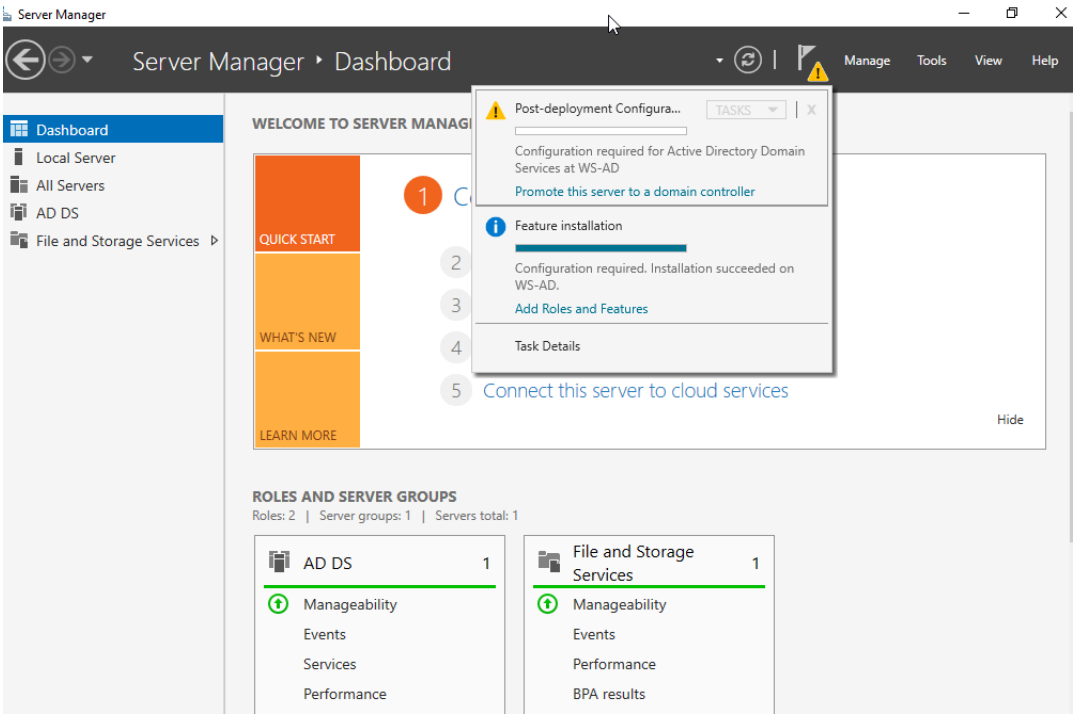




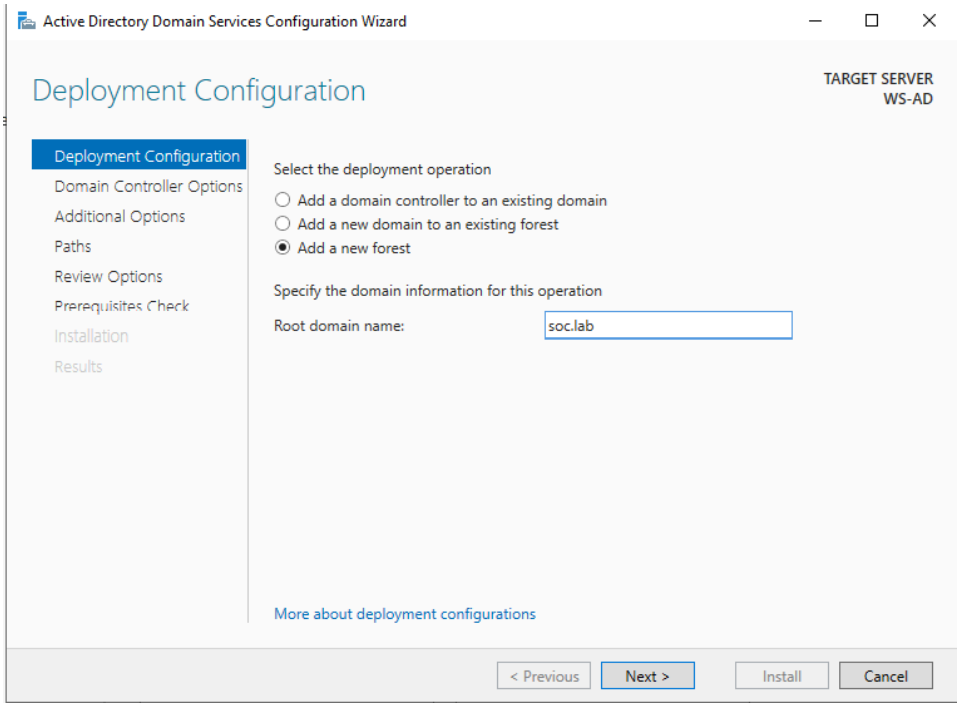




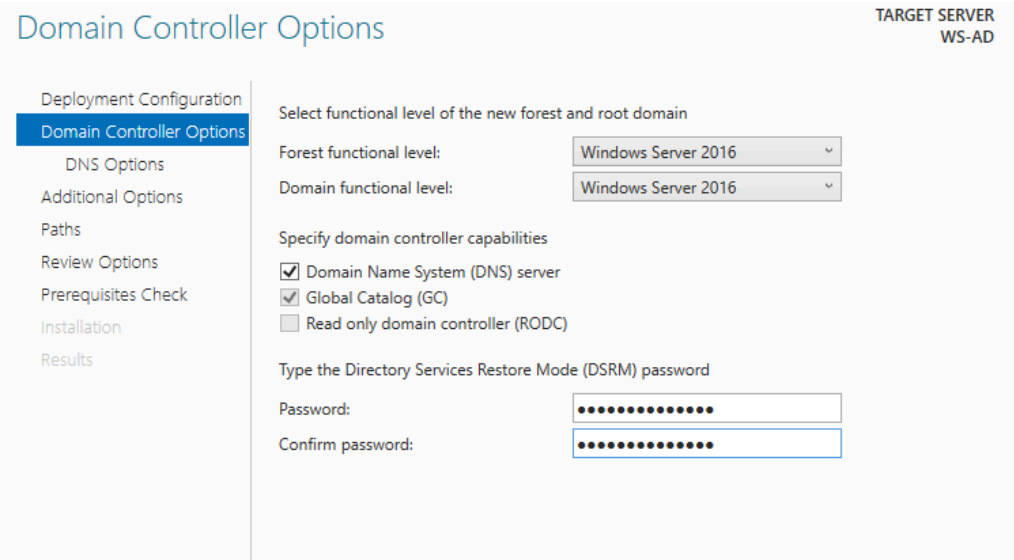
Follow all of the above steps to successfully install **Active Directory.**



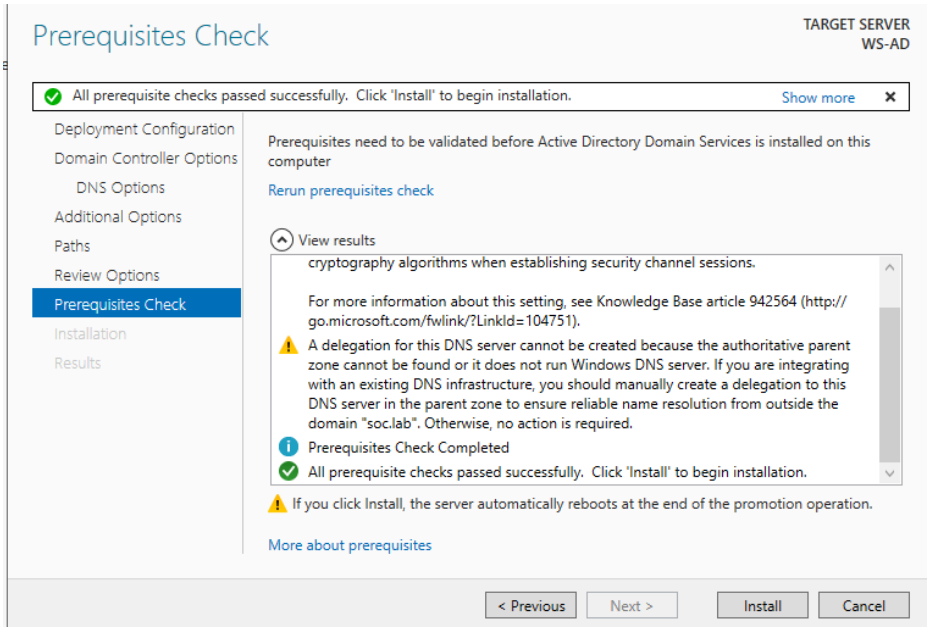
Next, we click “Promote this server to a domain controller”.



Then we “Add a new forest” and name the Root domain name.

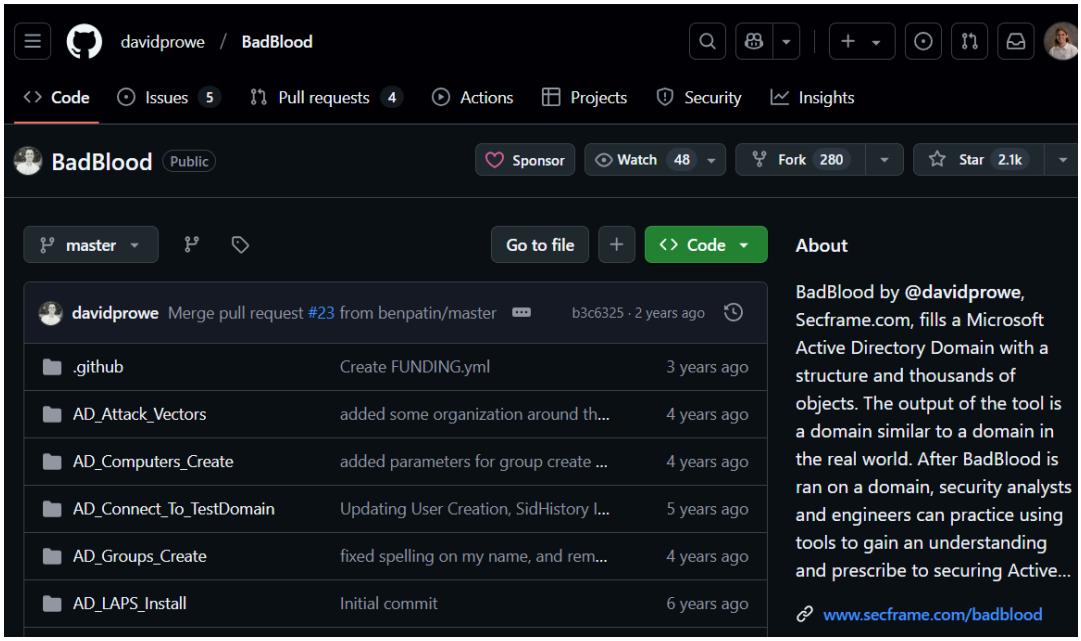


Leave these settings on default and assign a DSRM password. Just leave the DNS Options as is. Click “Next”.



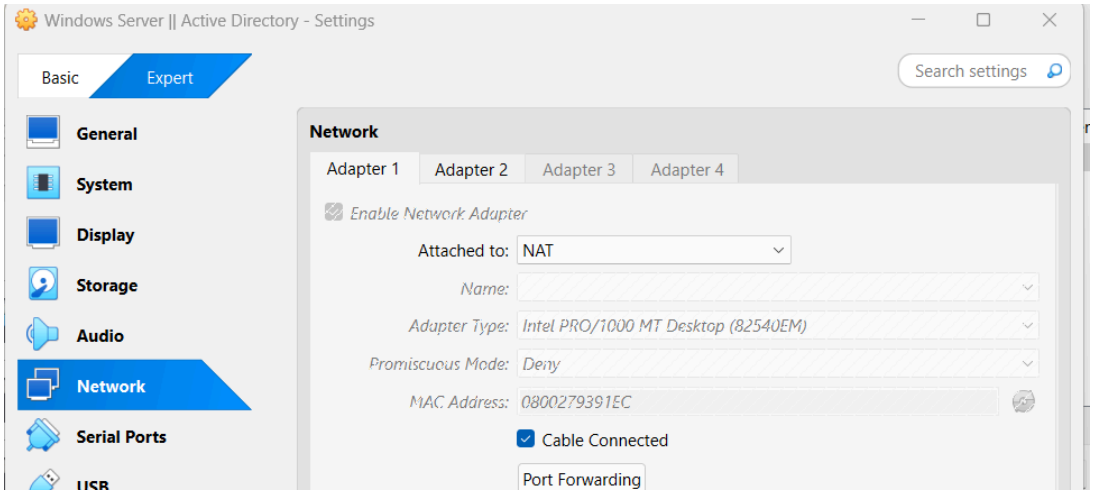
Click “Next” for the rest of the settings and then install it.

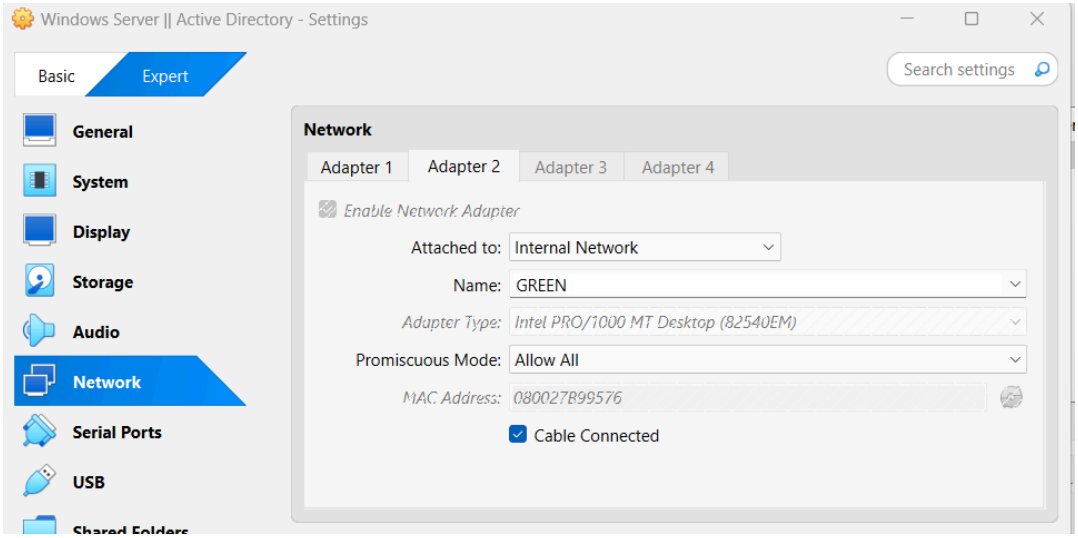
It automatically restarted.

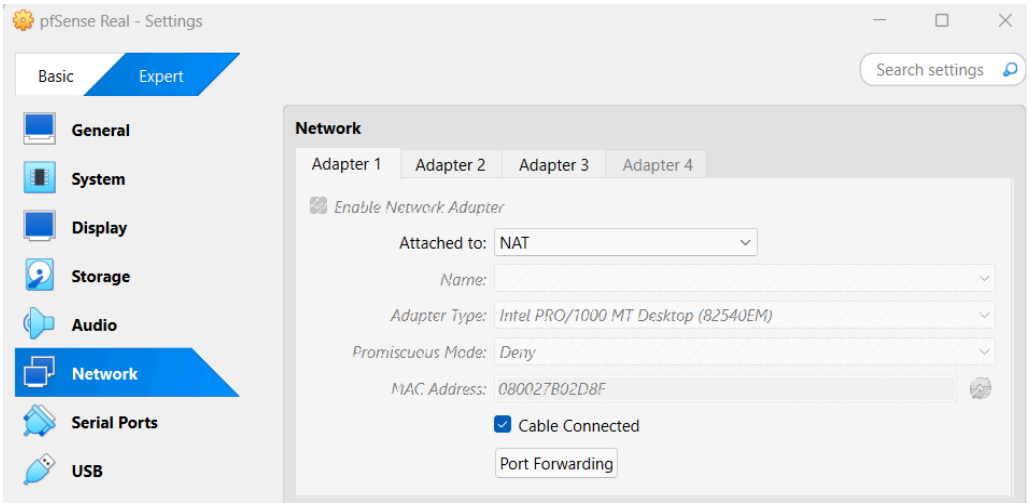


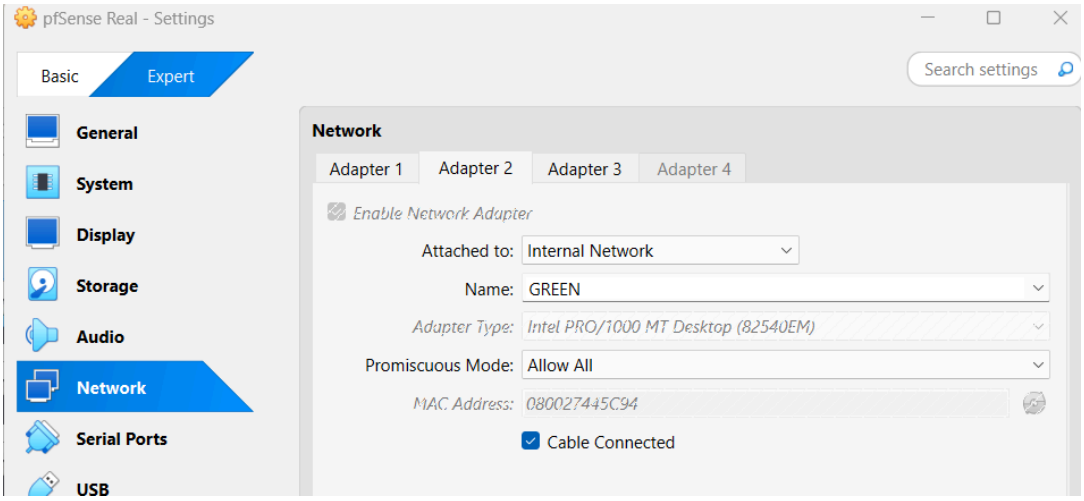
Next, we will install BadBlood, which will populate Active Directory with fake users, groups, and permissions. This will be a good way to simulate a real SOC environment and practice.

I had some issues connecting my Windows Server 2022 VM to the internet and installing Git so that I could install BadBlood. So I spent some time troubleshooting. Then I found the issue…

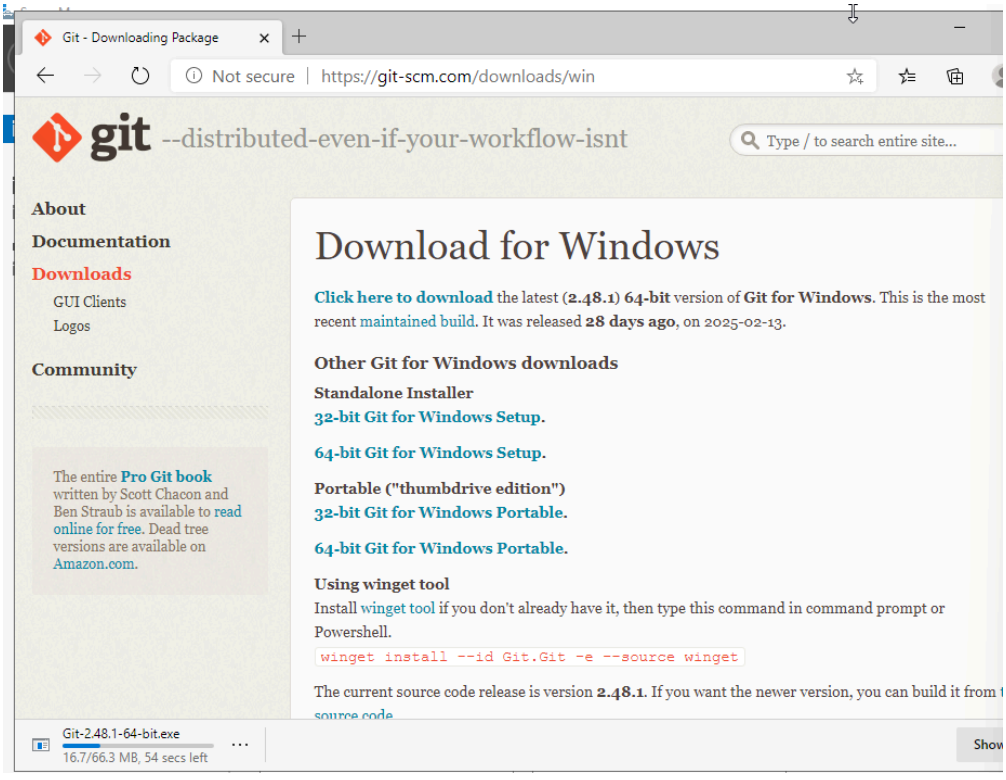

Windows Server || Active Directory - Settings
Basic
Expert
Search settings
General
System
Display
Storage
Audio
Network
Serial Ports
USB
Network
Adapter 1
Adapter 2
Adapter 3
Adapter 4
Enable Network Adapter
Attached to: NAT
Name:
Adapter Type: Intel PRO/1000 MT Desktop (82540EM)
Promiscuous Mode: Deny
MAC Address: 0800279391EC
Cable Connected
Port Forwarding

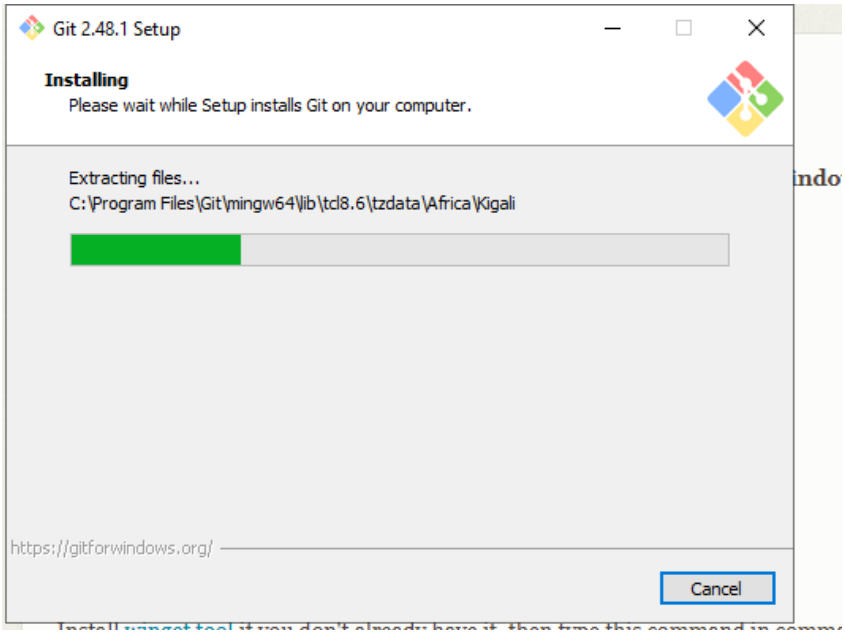

Windows Server || Active Directory - Settings
Basic
Expert
Search settings
General
System
Display
Storage
Audio
Network
Serial Ports
USB
Network
Adapter 1
Adapter 2
Adapter 3
Adapter 4
Enable Network Adapter
Attached to: Internal Network
Name: GREEN
Adapter Type: Intel PRO/1000 MT Desktop (82540EM)
Promiscuous Mode: Allow All
MAC Address: 080027B99576
Cable Connected


pfSense Real - Settings
Basic
Expert
Search settings
General
System
Display
Storage
Audio
Network
Serial Ports
USB
Network
Adapter 1
Adapter 2
Adapter 3
Adapter 4
Enable Network Adapter
Attached to: NAT
Name:
Adapter Type: Intel PRO/1000 MT Desktop (82540EM)
Promiscuous Mode: Deny
MAC Address: 080027B02D8F
Cable Connected
Port Forwarding

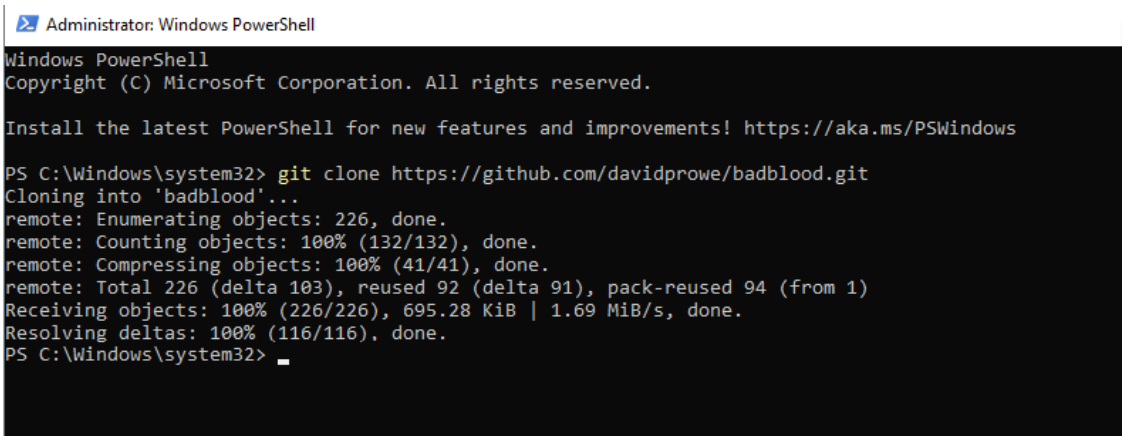


The issue was that my pfSense adapter 1 was NAT and adapter 2 was Internal Network (Green), but on Windows Server it was reversed, so adapter 1 was Internal Network (Green) and adapter 2 was NAT. Each adapter should match, like displayed above.The internet is now working. Another point is that **pfSense** must be open in order for the Windows Server 2022 VM to have internet access.

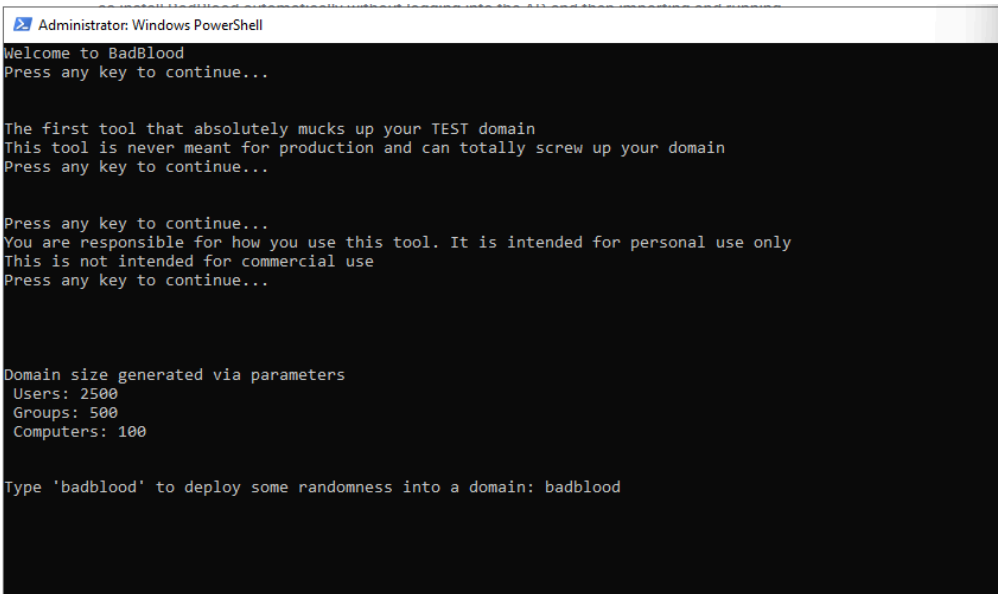


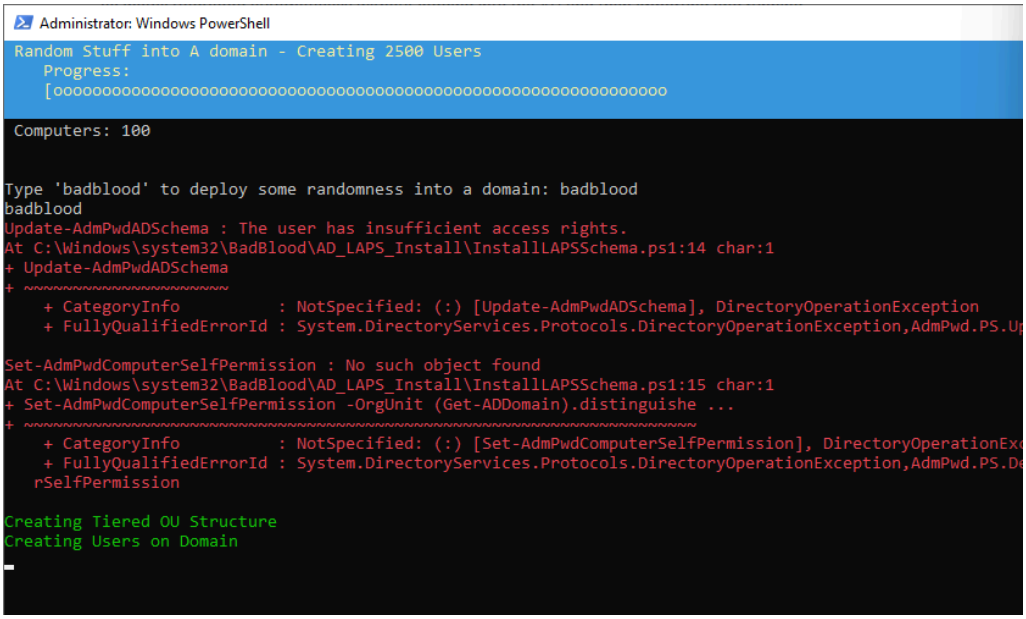


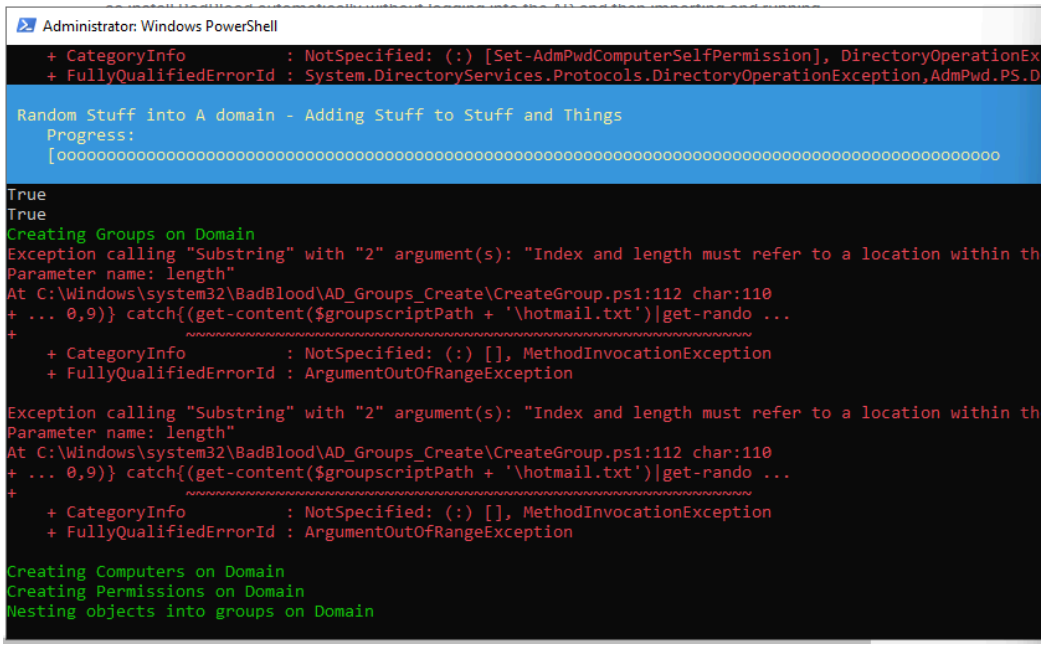
First I had to install Git so that I could install the BadBlood package.

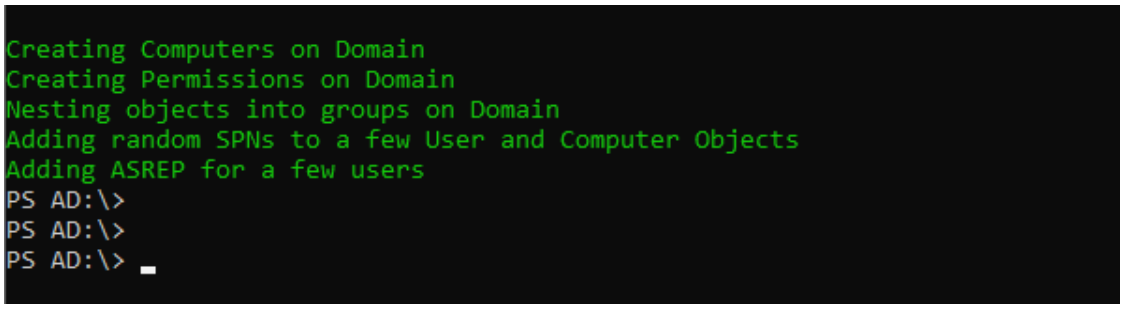


After installing Git, I entered this command to install the BadBlood package.


Administrator: Windows PowerShell
Welcome to BadBlood
Press any key to continue...
The first tool that absolutely mucks up your TEST domain
This tool is never meant for production and can totally screw up your domain
Press any key to continue...
Press any key to continue...
You are responsible for how you use this tool. It is intended for personal use only
This is not intended for commercial use
Press any key to continue...
Domain size generated via parameters
Users: 2500
Groups: 500
Computers: 100
Type 'badblood' to deploy some randomness into a domain: badblood


Administrator: Windows PowerShell
Random Stuff into A domain - Creating 2500 Users
Progress:
[ooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooo
Computers: 100
Type 'badblood' to deploy some randomness into a domain: badblood
badblood
Update-AdmPwdADSchema : The user has insufficient access rights.
At C:\Windows\system32\BadBlood\AD_LAPS_Install\InstallLAPSSchema.ps1:14 char:1
+ Update-AdmPwdADSchema
+ ~~~~~~~~~~~~~~~~~~~~~
+ CategoryInfo : NotSpecified: (:) [Update-AdmPwdADSchema], DirectoryOperationException
+ FullyQualifiedErrorId : System.DirectoryServices.Protocols.DirectoryOperationException,AdmPwd.PS.Up
Set-AdmPwdComputerSelfPermission : No such object found
At C:\Windows\system32\BadBlood\AD_LAPS_Install\InstallLAPSSchema.ps1:15 char:1
+ Set-AdmPwdComputerSelfPermission -OrgUnit (Get-ADDomain).distinguishe ...
+ ~~~~~~
+ CategoryInfo : NotSpecified: (:) [Set-AdmPwdComputerSelfPermission], DirectoryOperationExc
+ FullyQualifiedErrorId : System.DirectoryServices.Protocols.DirectoryOperationException,AdmPwd.PS.De
rSelfPermission
Creating Tiered OU Structure
Creating Users on Domain

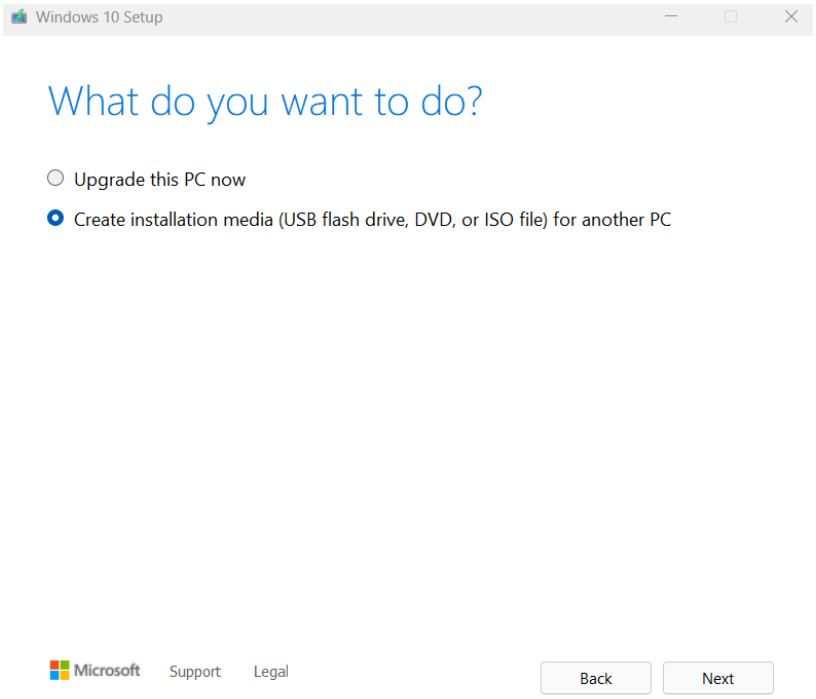


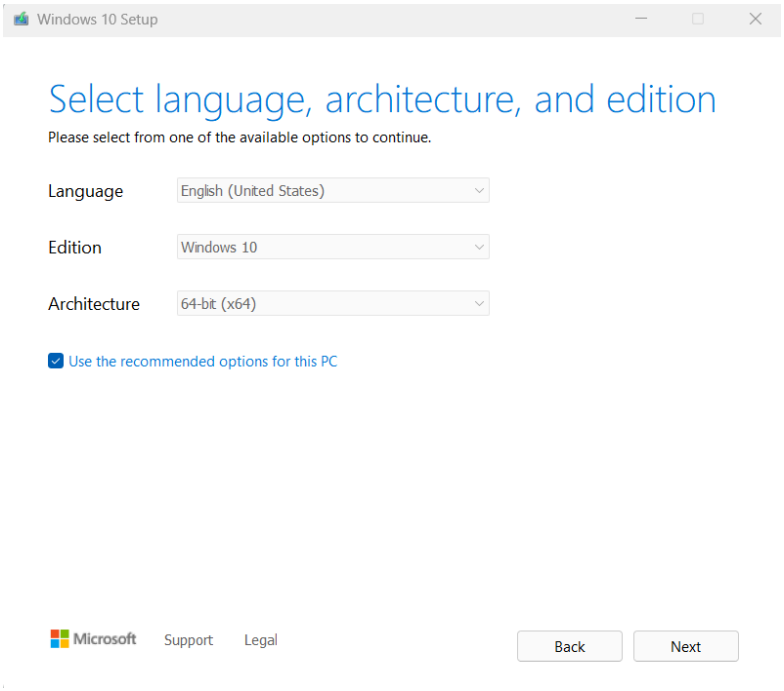


The BadBlood installation finished and now Active Directory has 2500 users, 500 groups, OU, 100 computers, etc. This will allow us to simulate a real SOC environment. For the next addition to our SOC lab we will set up **Windows Workstation**.

Windows Workstation

Use this windows tool to create your own Windows VM. We will create a Windows Workstation VM to simulate a regular user's computer, which will help us in simulating cyber attacks.





Choose which media to use

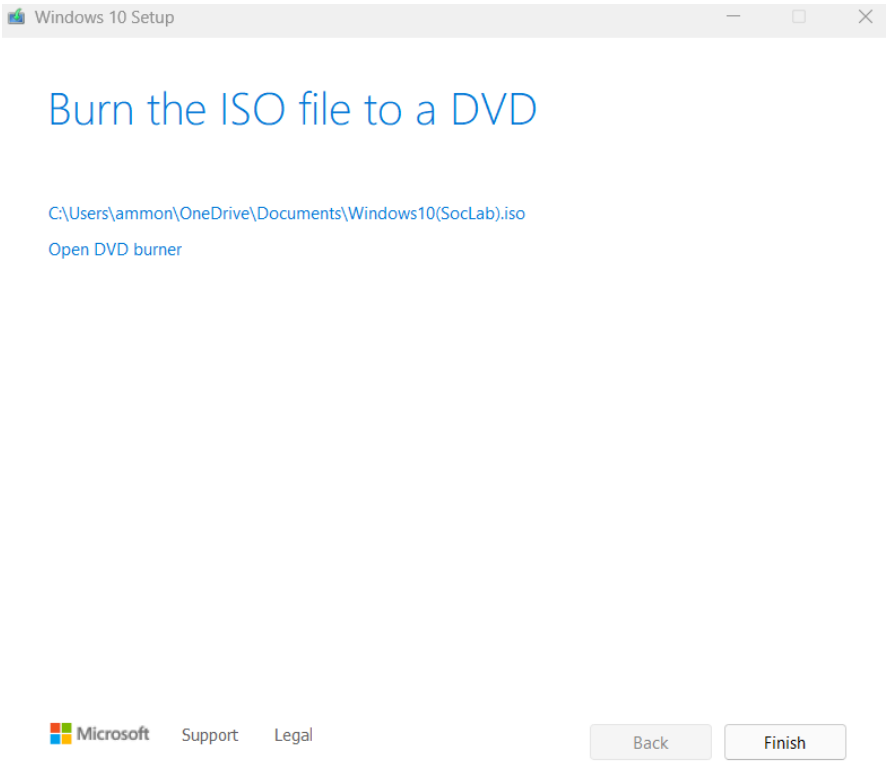
If you want to install Windows 10 on another partition, you need to create and then run the media to install it.

○ USB flash drive

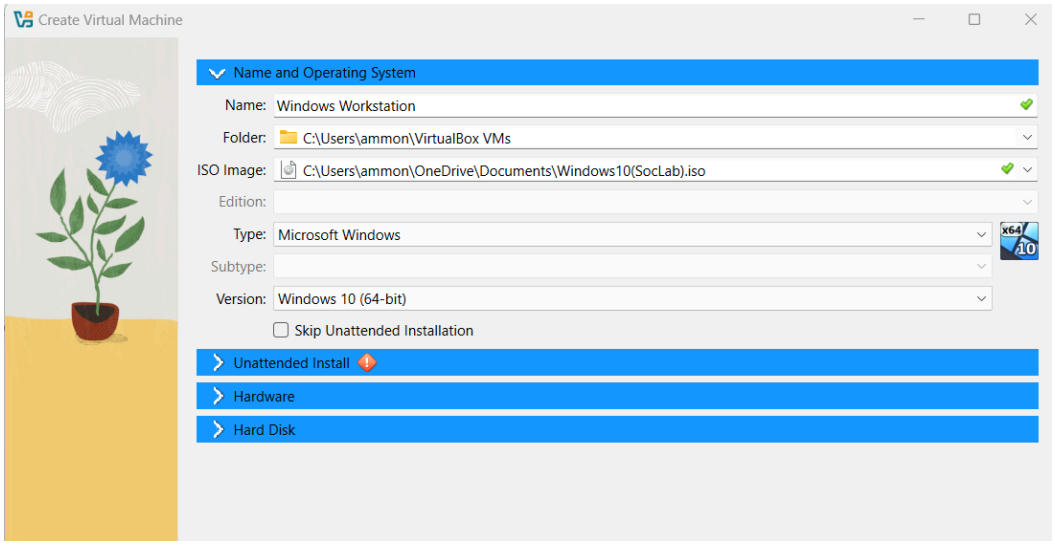
It needs to be at least 8 GB.

◉ ISO file

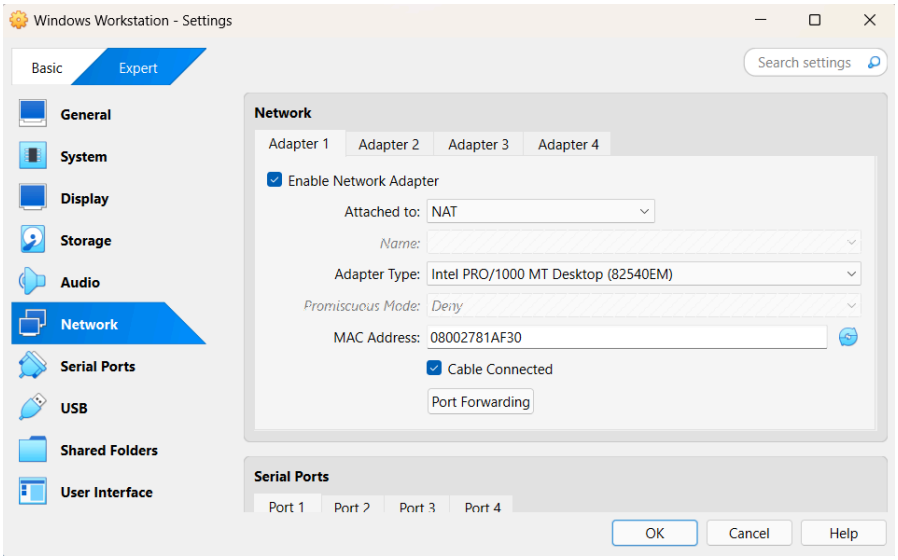
You'll need to burn the ISO file to a DVD later.

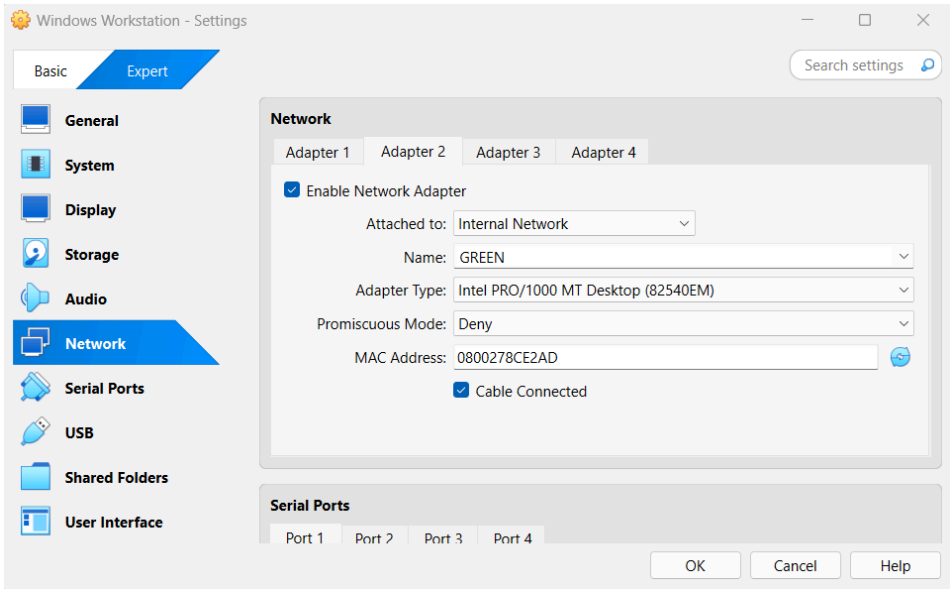


We finished creating and downloading the Windows VM.

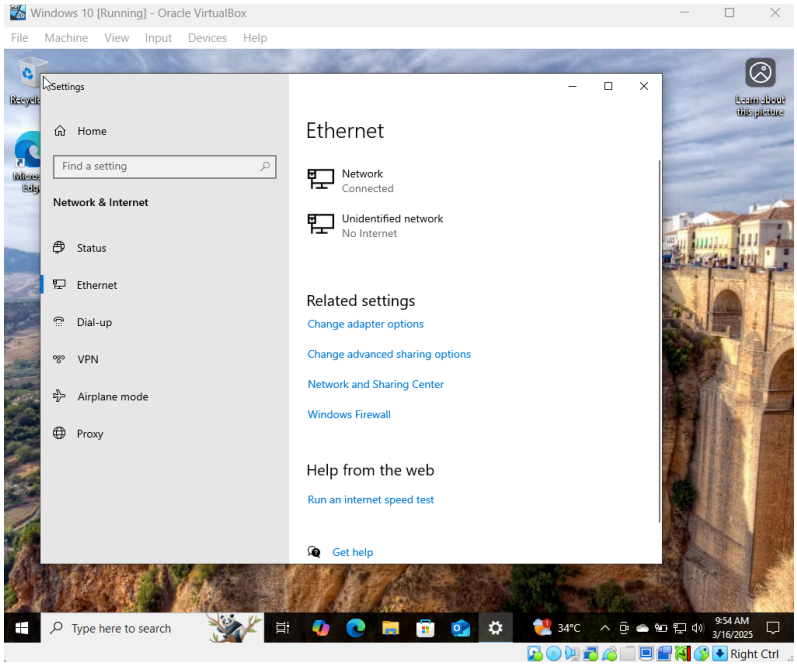


Next, we add the Windows VM we just created to VirtualBox.

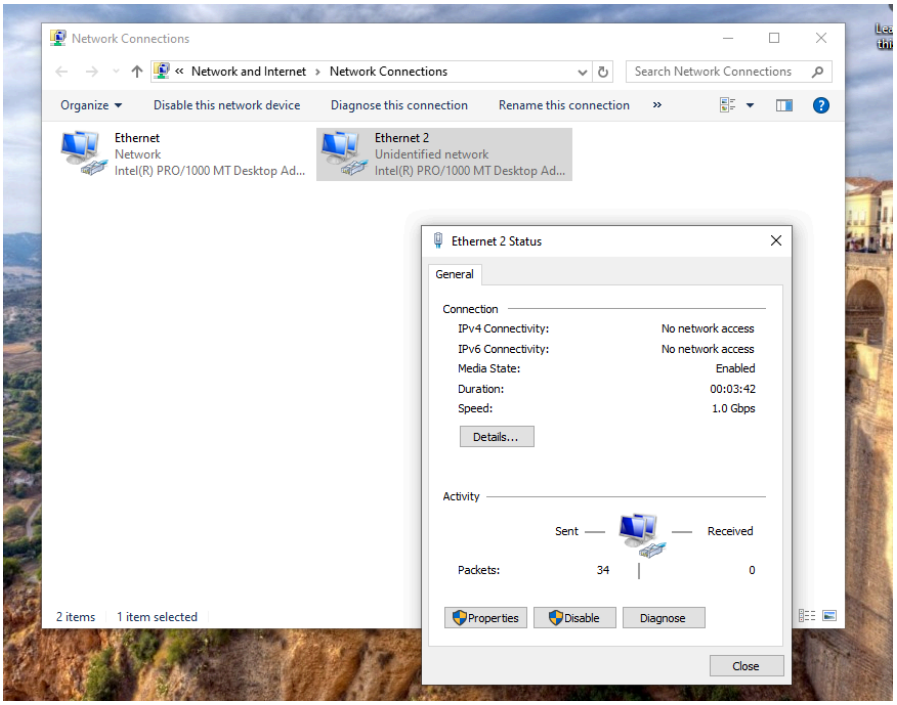


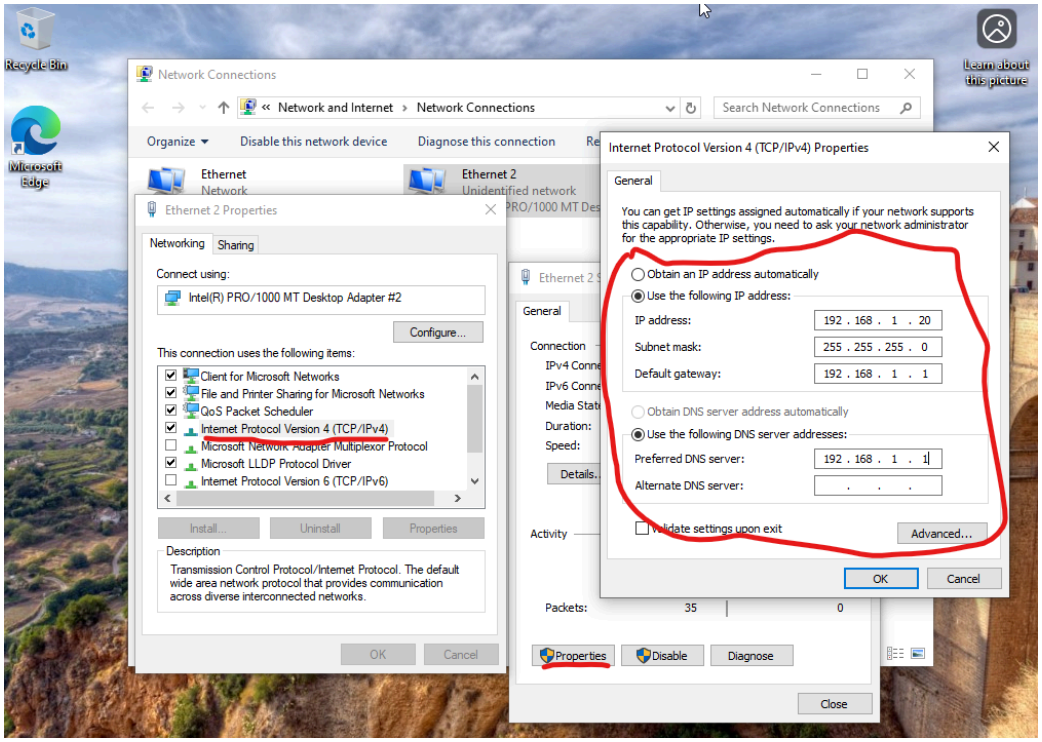


We configured the network the exact same way as the previous machine, Windows Server 2022.

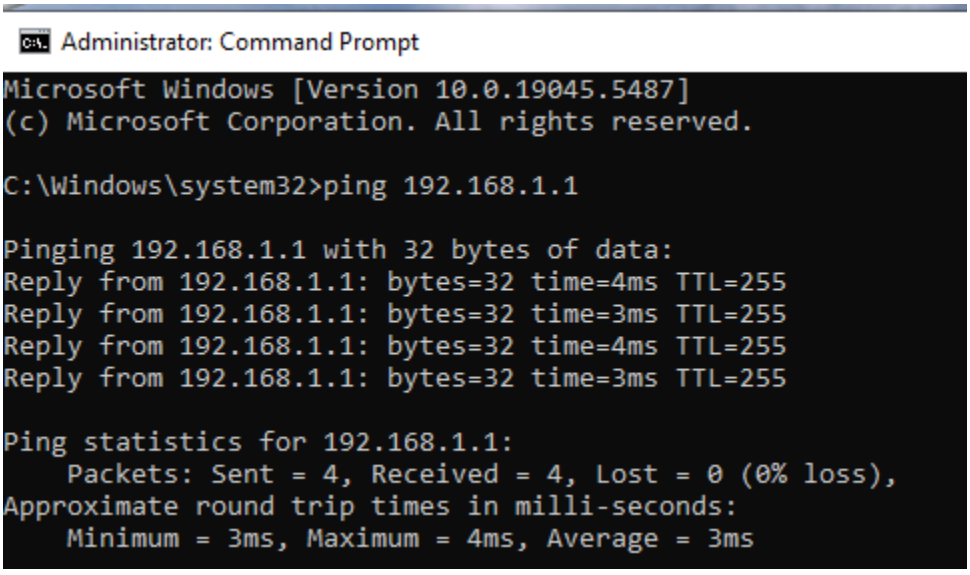


After installing it, go to Network & Internet settings. Then click Change adapter options.





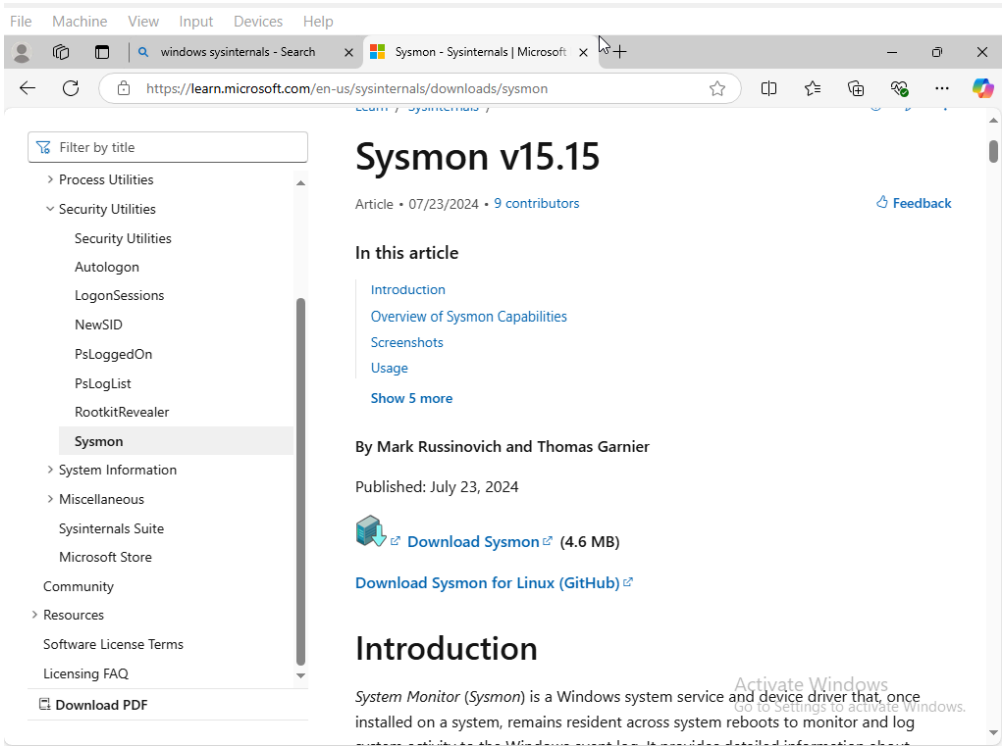
We want this Windows Workstation to be connected the the LAN with **pfSense** and **Active Directory**. So we make the IP address within the same subnet as our other machines. For the Default Gateway and the DNS server we use the **pfSense** address.



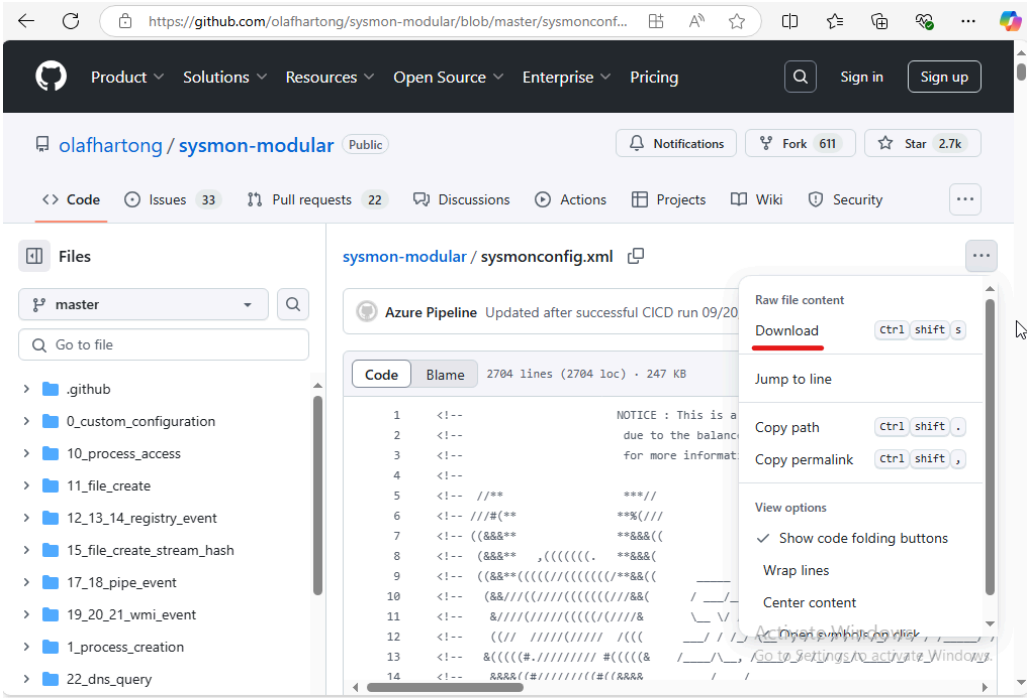
We sent a ping to the default gateways (pfSense's LAN interface) to test the connection. It worked.

Sysmom

We will now download **Sysmon** on both our Windows Workstation VM and our Windows Server 2022 VM (Active Directory). Sysmon provides cybersecurity analysts detailed system logs, which allow us to detect suspicious behavior, malware execution, or persistence techniques. Sysmon on Windows Workstation will allow us to monitor endpoint activity, including process creation, network connections, and file modifications. Sysmom on Windows Server 2022 will allow us to detect suspicious activities, privilege escalation, lateral movement, and unauthorized access attempts.



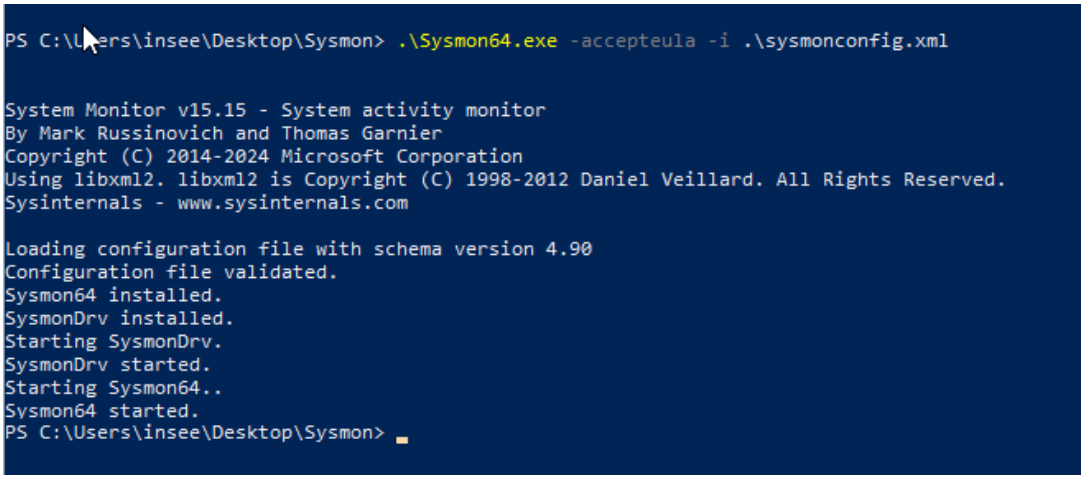
In the **Windows Workstation** VM download the Sysmon zip.



[Download sysmonconfig.xml]

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Windows\system32> cd /
PS C:\> cd .\Users\insee\Desktop\Sysmon\
PS C:\Users\insee\Desktop\Sysmon> ls


    Directory: C:\Users\insee\Desktop\Sysmon


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         3/16/2025   1:00 PM           7490 Eula.txt
-a----         3/16/2025   1:00 PM        8480560 Sysmon.exe
-a----         3/16/2025   1:00 PM        4563248 Sysmon64.exe
-a----         3/16/2025   1:00 PM        4993440 Sysmon64a.exe


PS C:\Users\insee\Desktop\Sysmon> ls


    Directory: C:\Users\insee\Desktop\Sysmon


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         3/16/2025   1:00 PM           7490 Eula.txt
-a----         3/16/2025   1:00 PM        8480560 Sysmon.exe
-a----         3/16/2025   1:00 PM        4563248 Sysmon64.exe
-a----         3/16/2025   1:00 PM        4993440 Sysmon64a.exe
-a----         3/16/2025   1:10 PM         253169 sysmonconfig.xml
```

After extracting the zip file, go to the folder in PowerShell. Make sure you add the sysmonconfig.xml file.

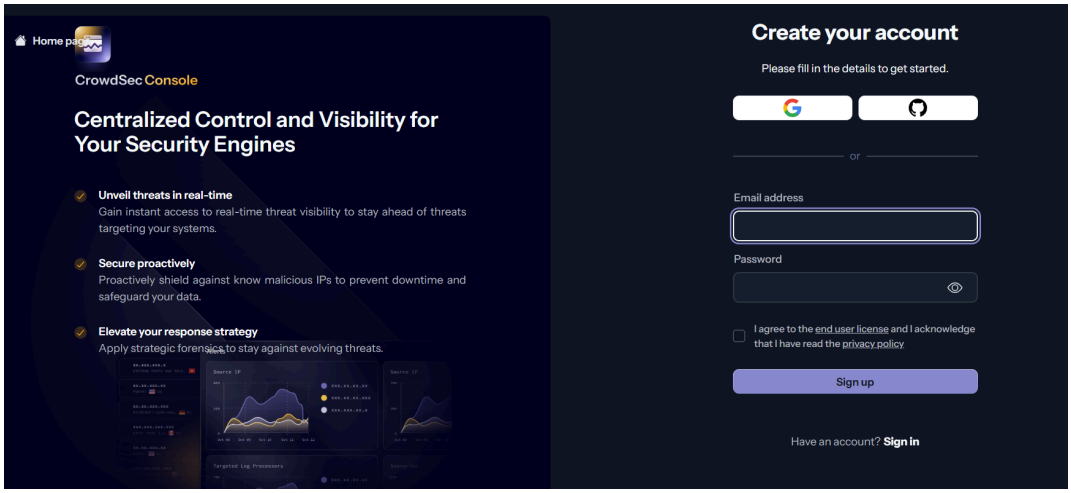


Use “ .\sysmon64.exe -accepteula -i YOURFILE.xml" to install **Sysmon**.

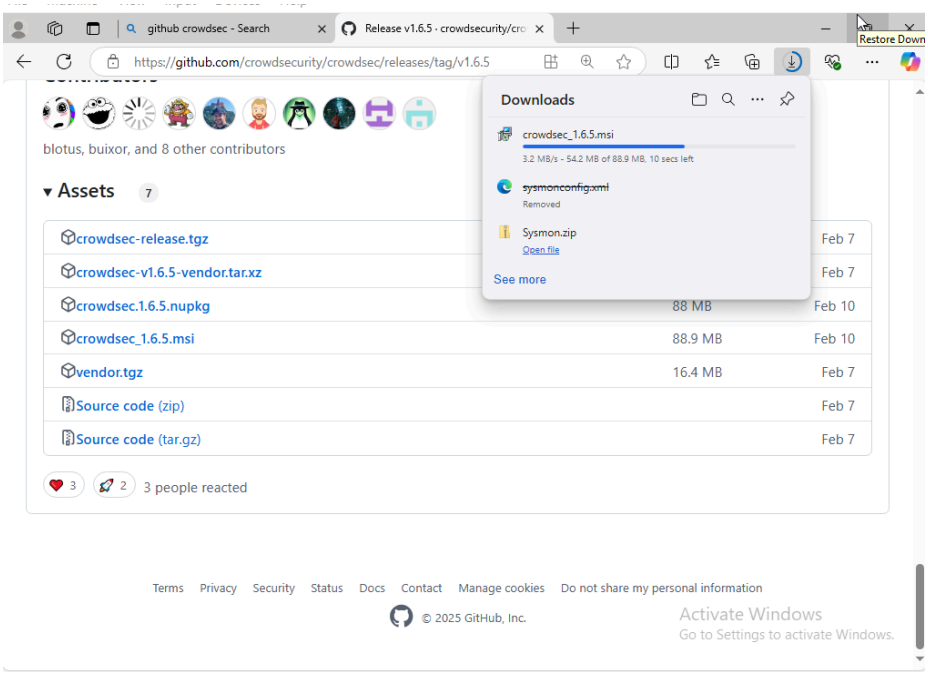
Now perform the same steps on the **Windows Server 2022** VM.

CrowdSec

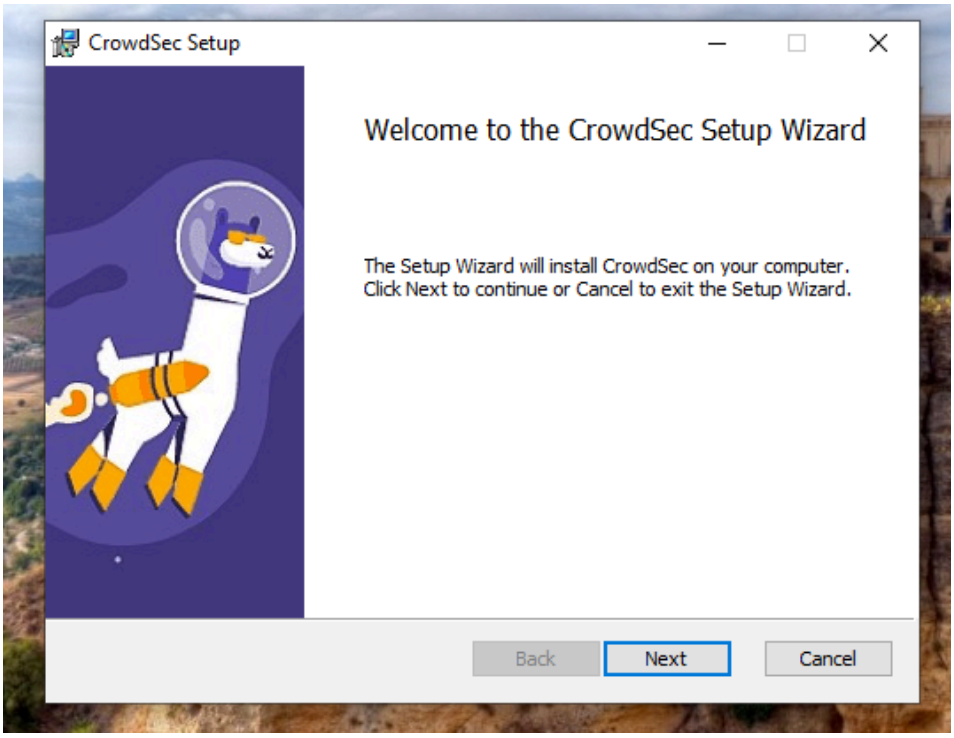
CrowdSec uses behavior-based detection, which tracks suspicious activity (failed SSH logins, port scans, etc.), and can automatically block bad IPs. We will be installing **CrowdSec** both of our Windows VMs (Workstation and Server).

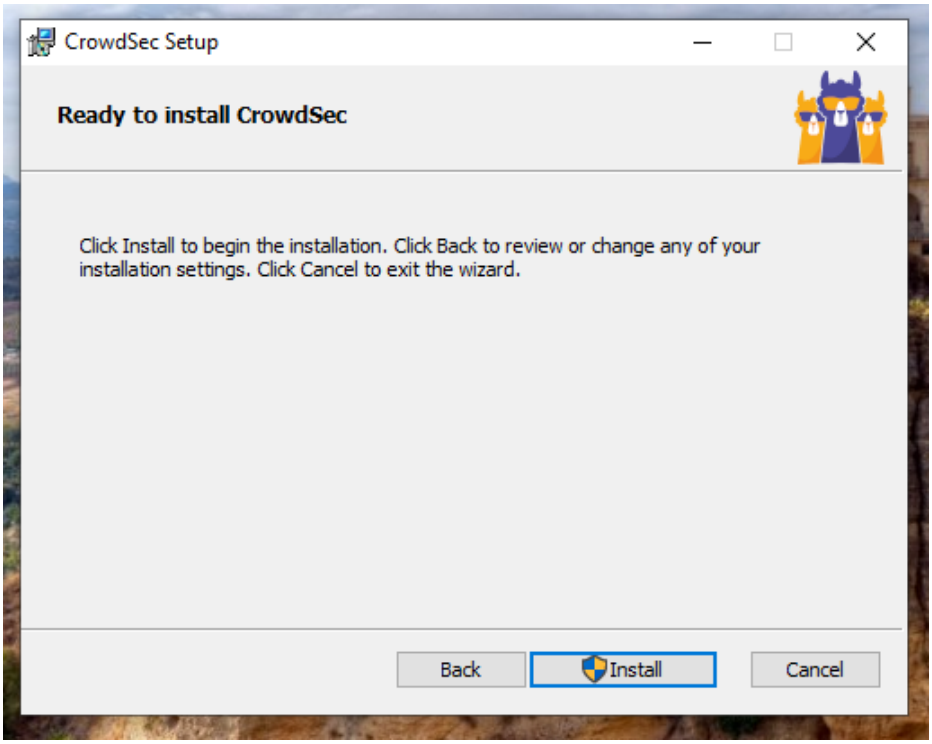


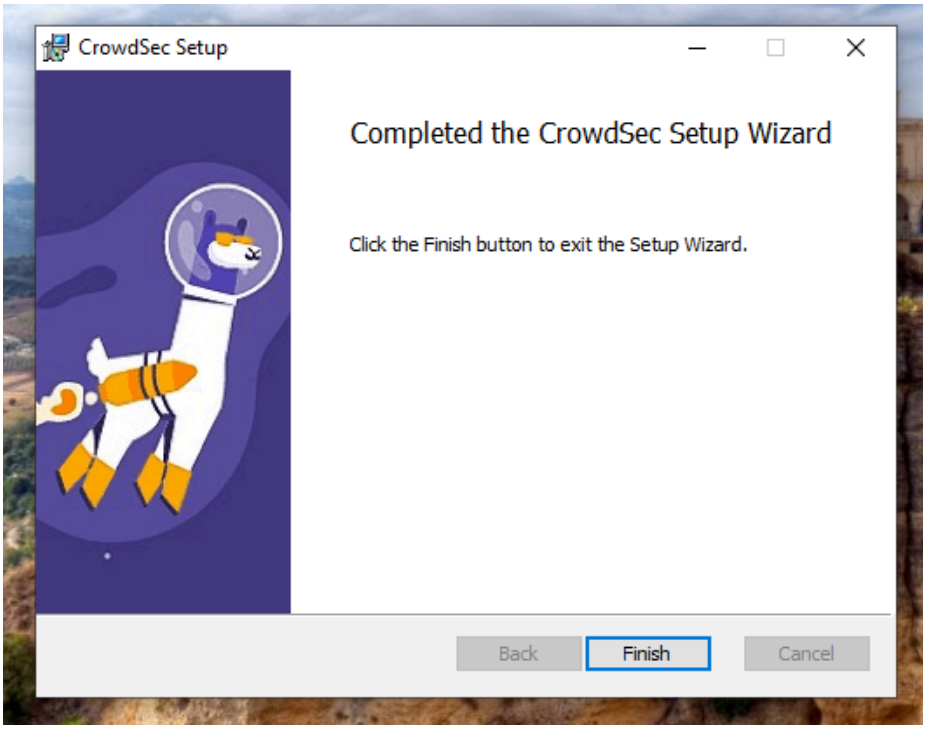
Go to the **CrowdSec** website and [create an account](#).



Go to Github and download the crowdsec .msi file. Then run the file.







Finally, download **CrowdSec** on the **Windows Workstation** VM.