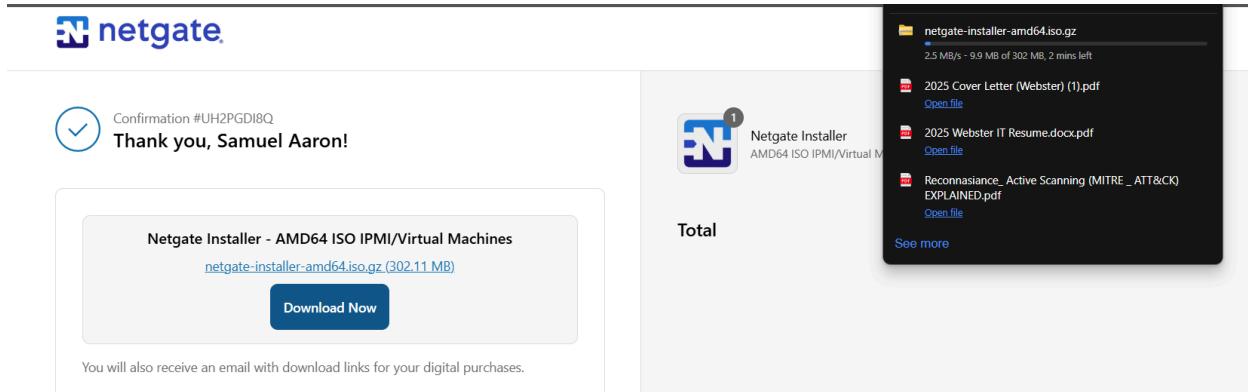
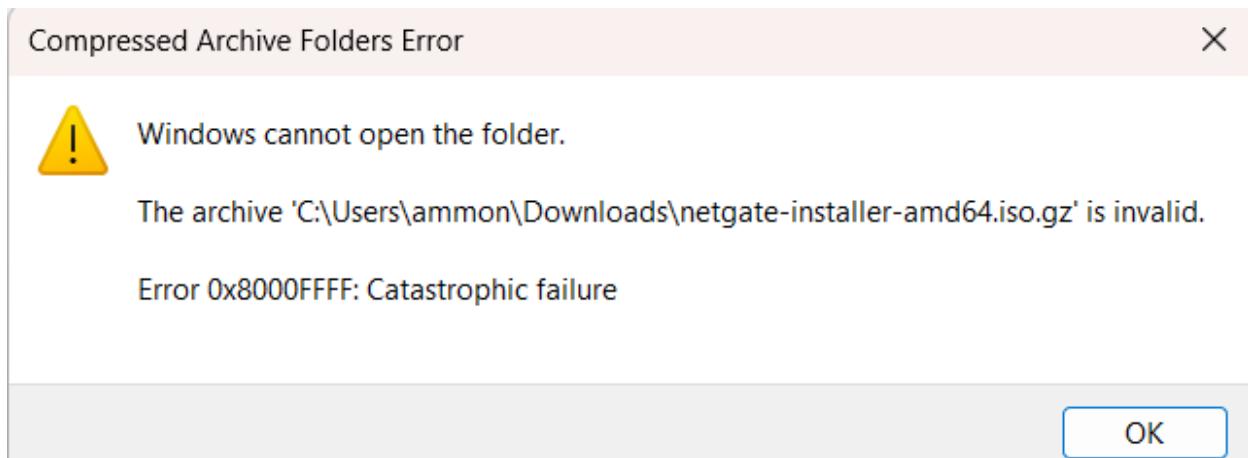


# pfSense

**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.

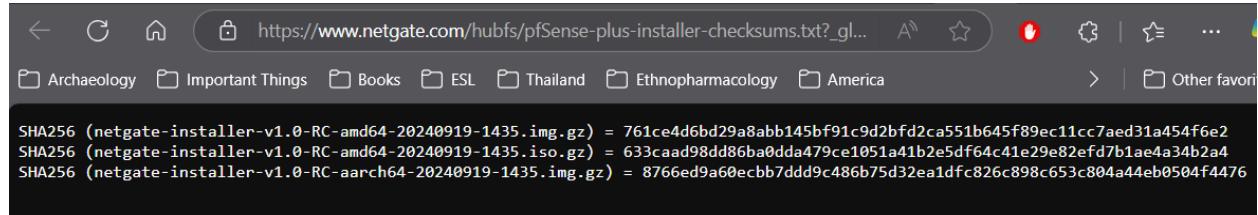
```

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], ItemNotFoundException
+ FullyQualifiedErrorId : PathNotFound,Microsoft.PowerShell.Commands.ResolvePathCommand

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

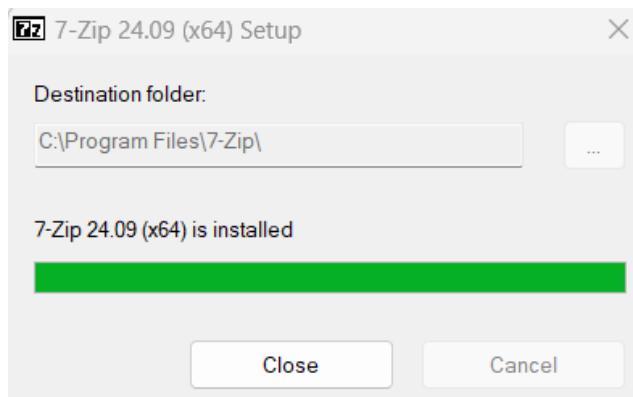
Algorithm      Hash
-----      -----
SHA256        633CAAD98DD86BA0DDA479CE1051A41B2E5DF64C41E29E82EFD7B1AE4A34B2A4
                                                               Path
                                                               -----
                                               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

```

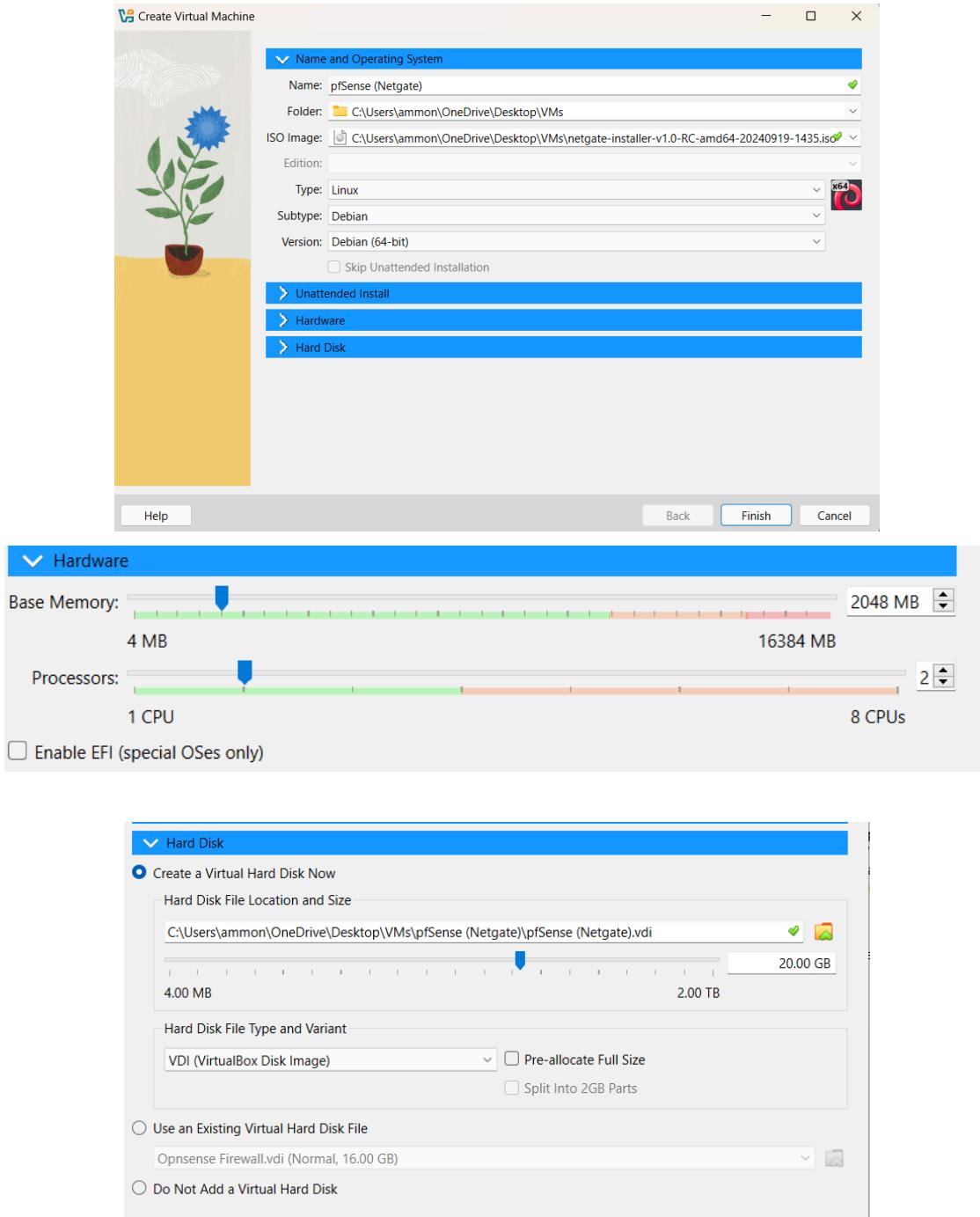


So I checked to see if the SHA256 hash of the file I downloaded matched the true SHA256 hash. They matched.

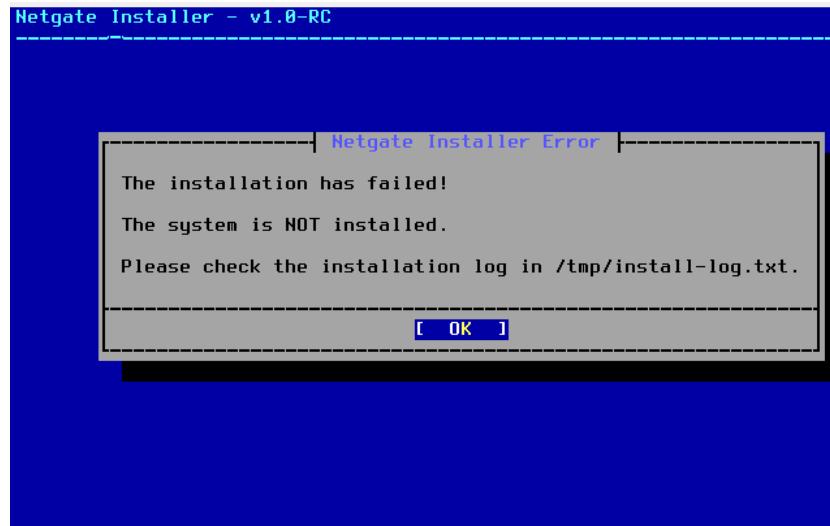
I wasn't sure how to get **pfSense** onto a virtual machine from here, so I began using the [netgate installation guide](#).



I had to download [7-Zip](#) in order to extract the *.iso* file.



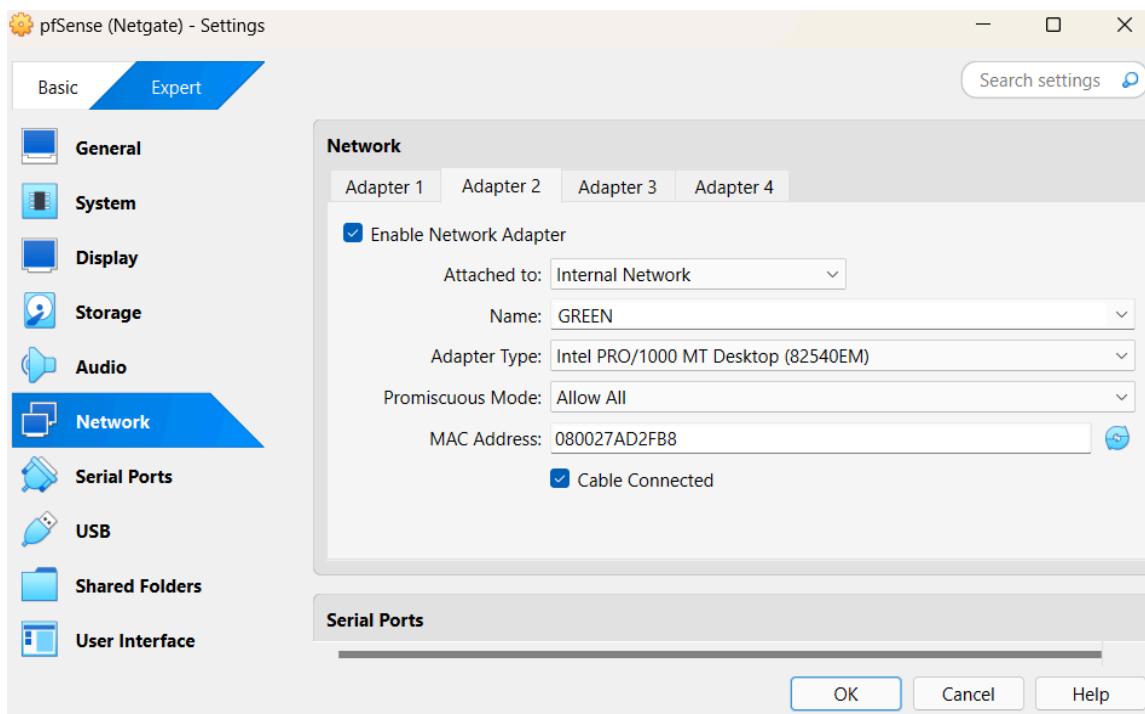
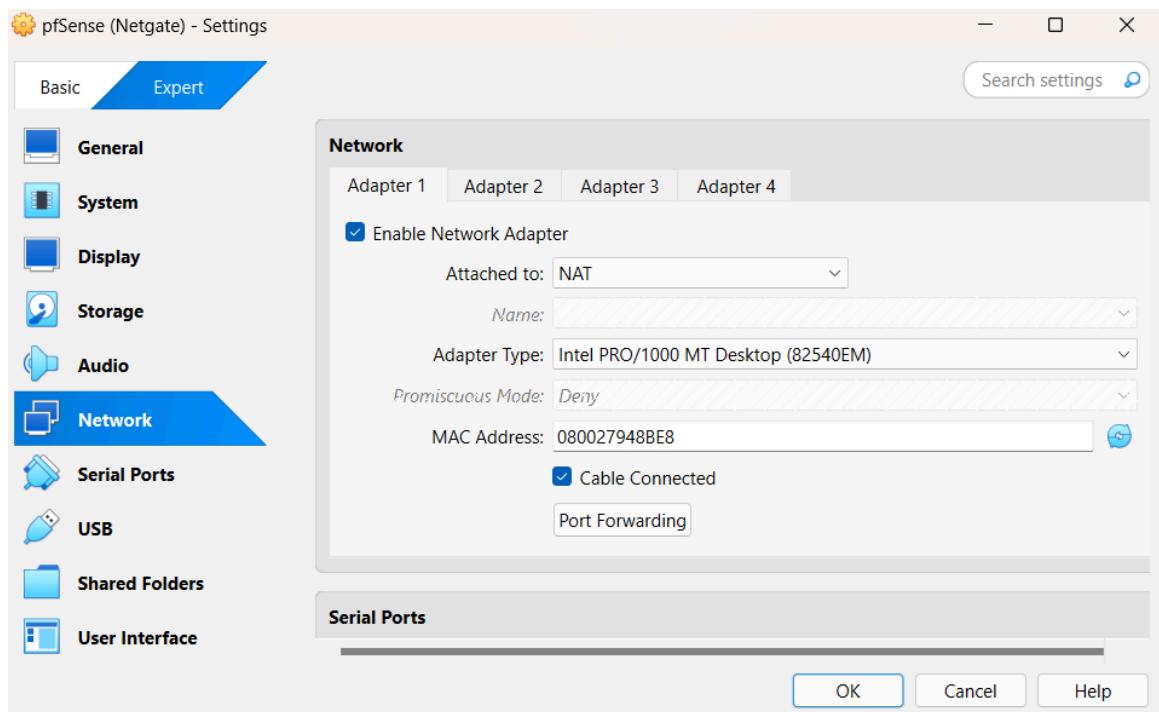
After extracting the *.iso* file using **7-Zip** I started making a VM in **VirtualBox**. It should be noted I ran into an issue later in the installation process. The issue was with this step. I should not have made the type Linux, subtype Debian, and the version Debian 64-bit.

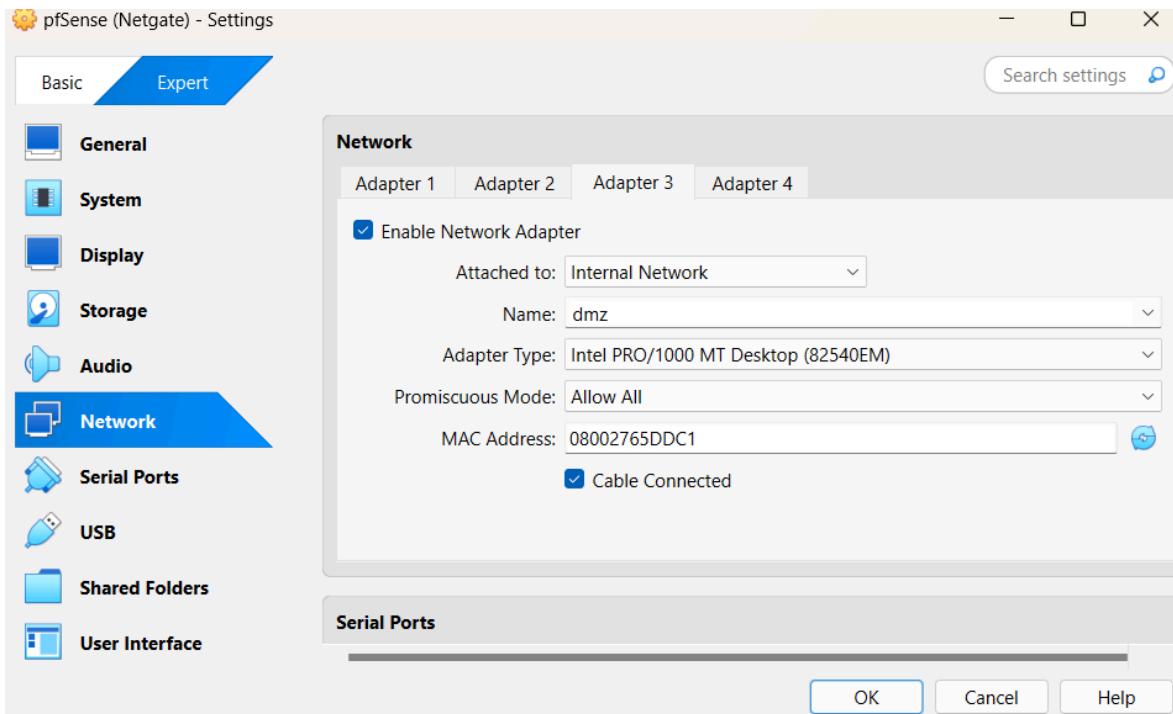


As you can see it ended up causing my installation to fail. So I had to go back and create a new VM.

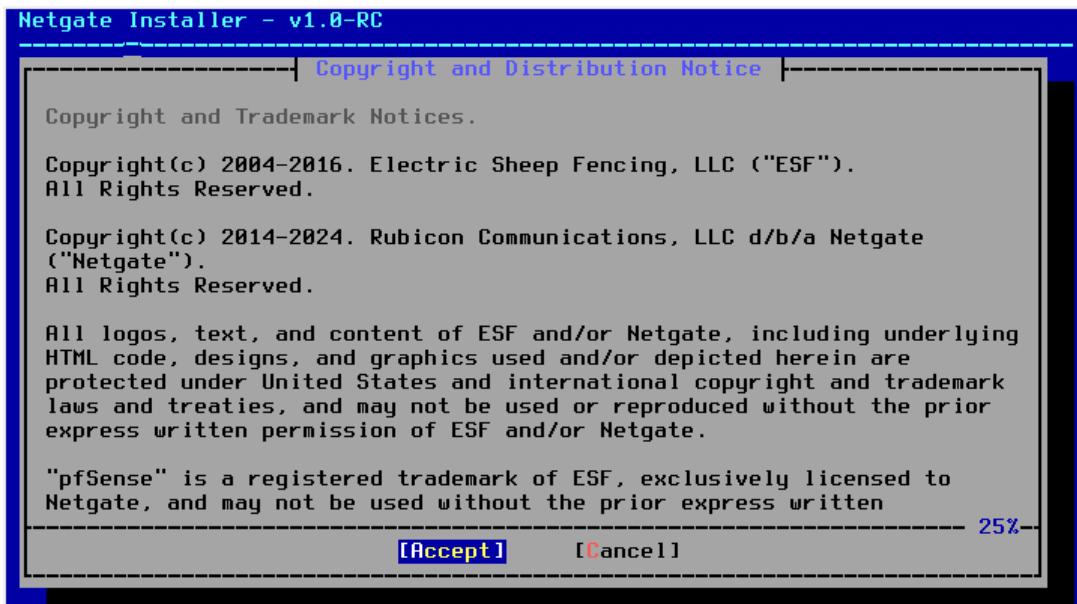
Two screenshots of the pfSense Real - Settings interface. The top screenshot shows the "General" tab under the "Basic" section. It displays the following settings: Name: pfSense Real, Type: BSD, Subtype: FreeBSD, Version: FreeBSD (64-bit). The bottom screenshot shows the "System" tab under the "Processor" section. It displays the "Base Memory" slider set to 4096 MB, with 4 MB at the bottom and 16384 MB at the top.

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.





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.

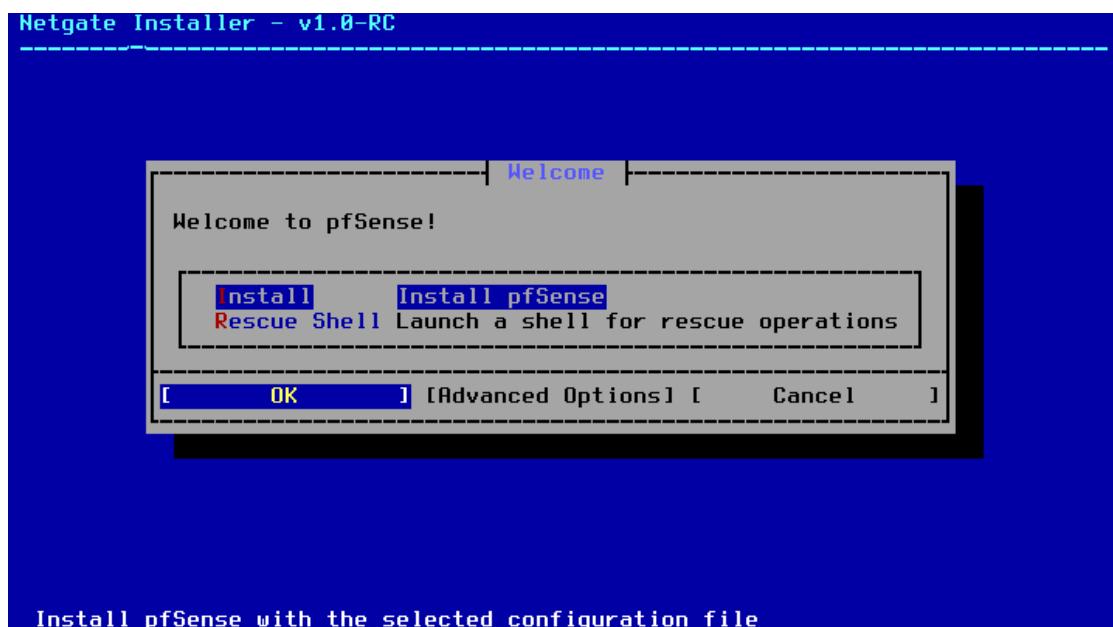
```
FreeBSD/amd64 (pfSense-install) (ttyv1)

login:

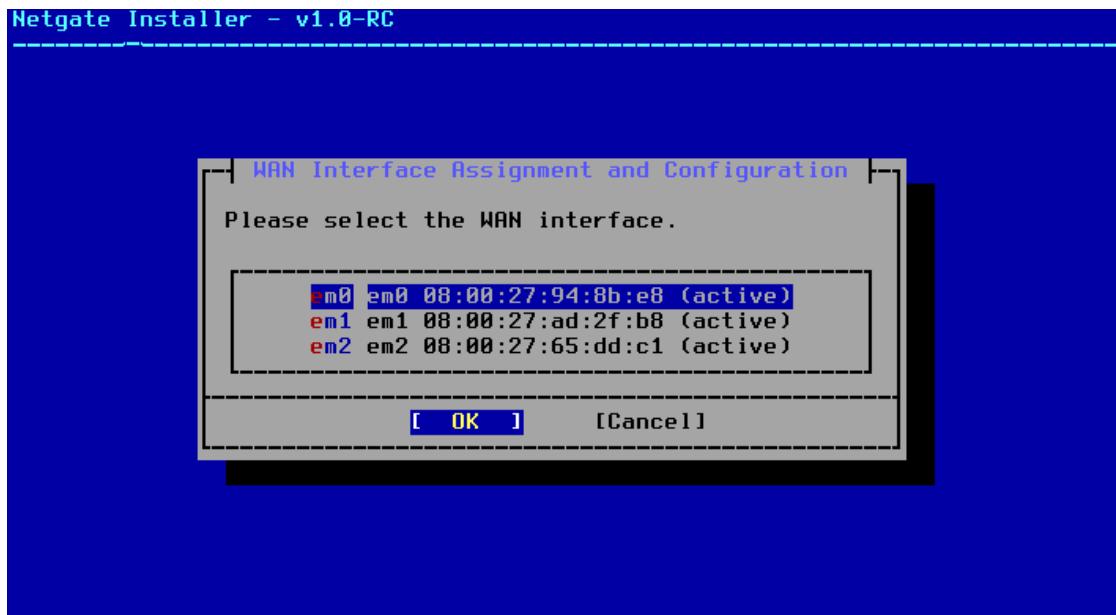
FreeBSD/amd64 (pfSense-install) (ttyv1)

login: login
Password:
Login incorrect
login: admin
Password:■
```

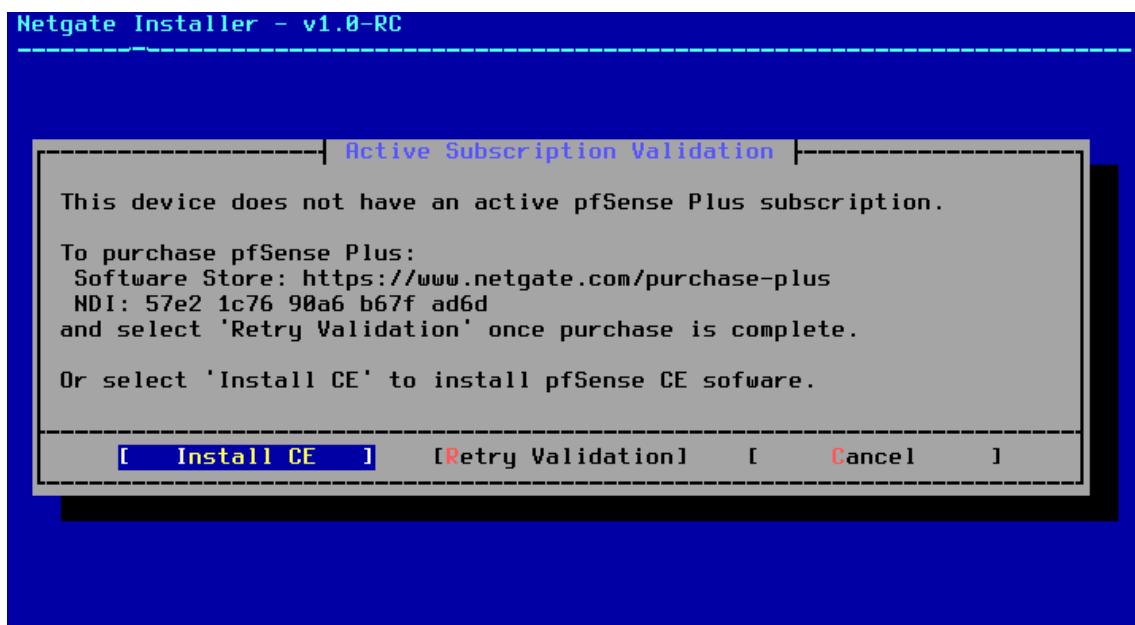
If you don't interact with the VM window for a few minutes it makes you login again.  
(Login: admin / Password: pfsense)

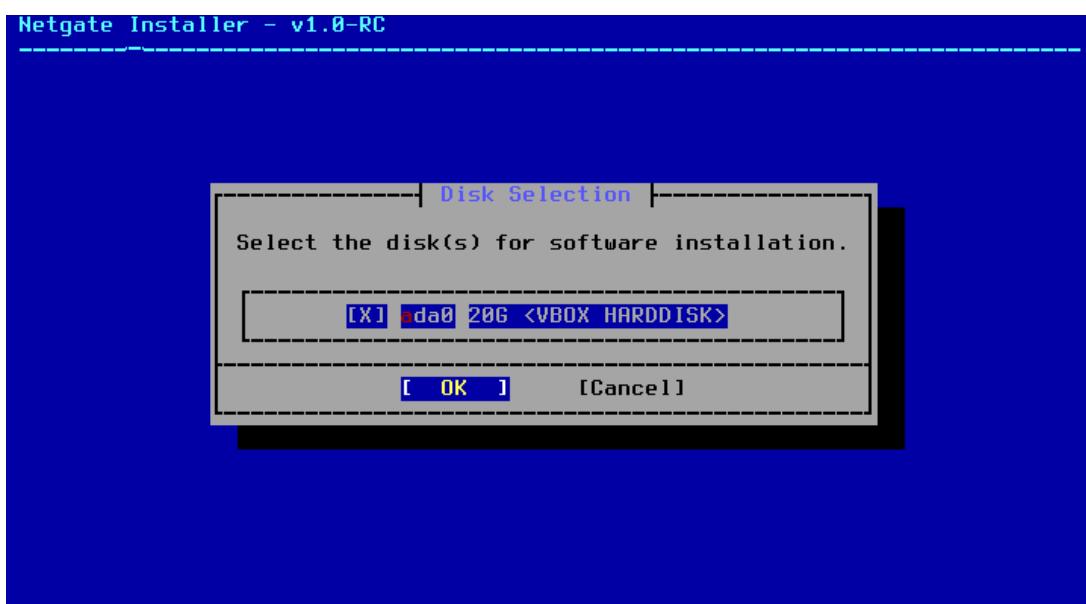
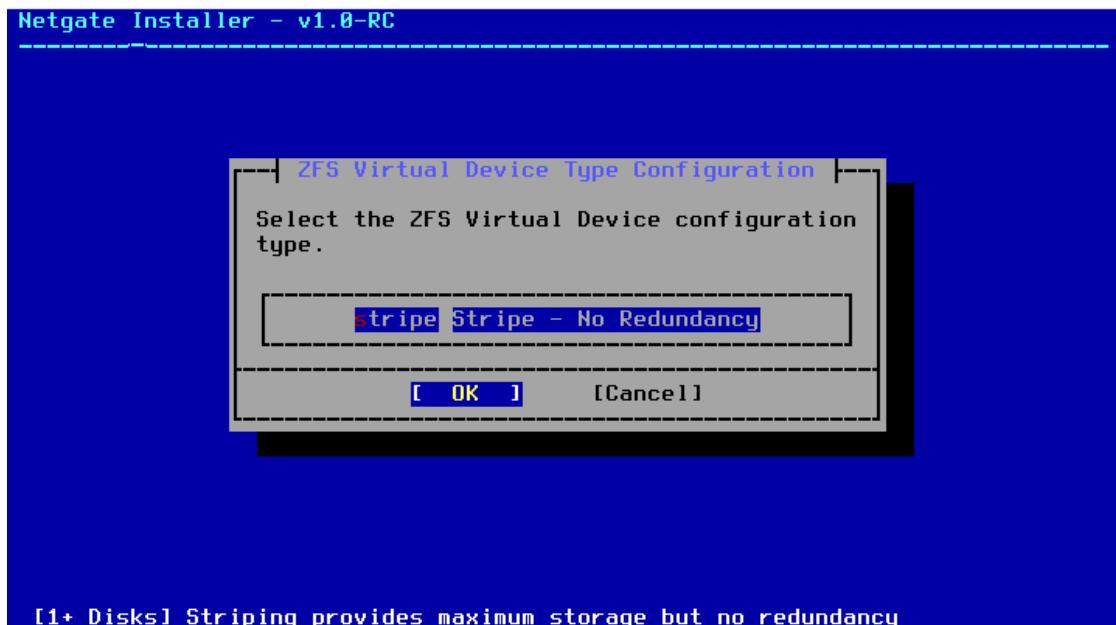


Install pfSense with the selected configuration file



I made em0 the WAN and em1 the LAN





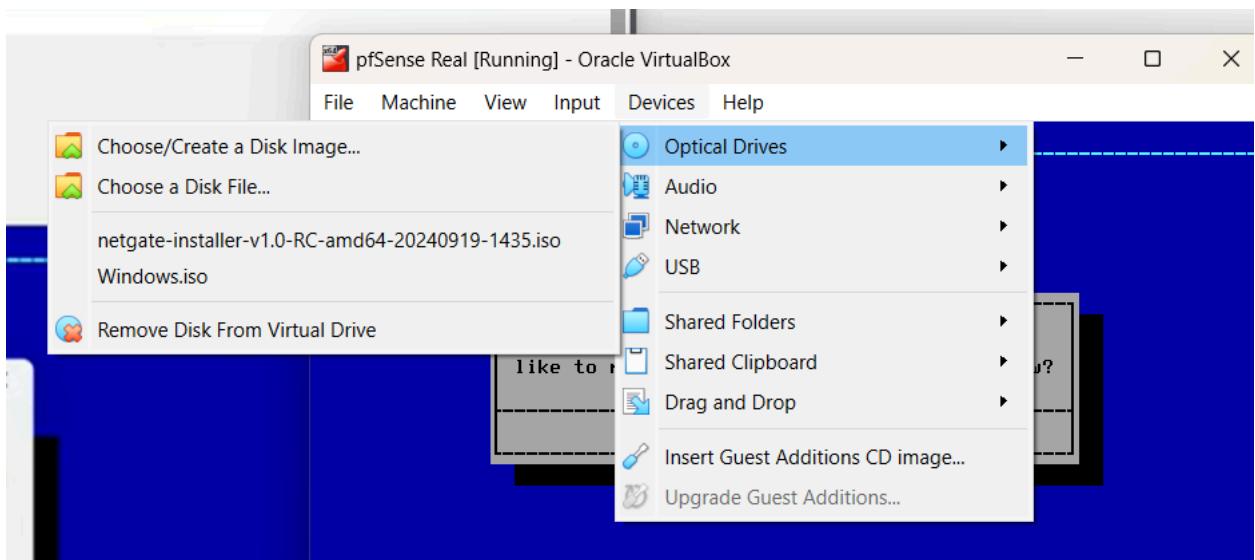
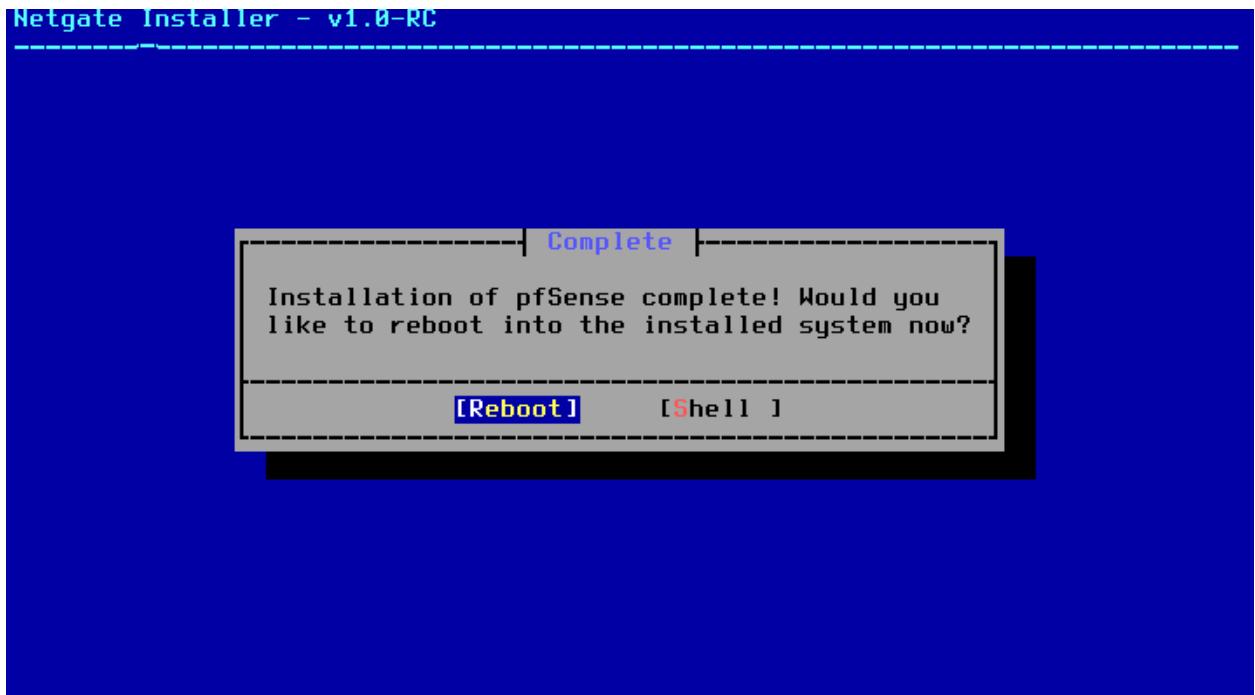
```
Number of packages to be installed: 1

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...
```

```
[6/169] Fetching filterlog-0.1_10.pkg: . done
[9/169] Fetching dpingen-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\ln]? 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\ln]? y [
```

```
Enter an option:

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
S LAN (lan)    -> em1          -> v4: 192.168.1.1/24
OPT1 (opt1)   -> em2          ->

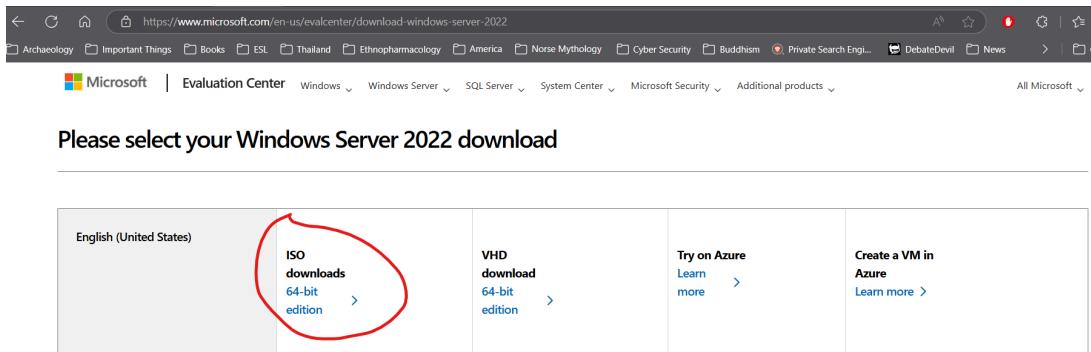
0) Logout (SSH only)           9) pfTop
1) Assign Interfaces           10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults   13) Update from console
5) Reboot system               14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

Enter an option: ■
```

After 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

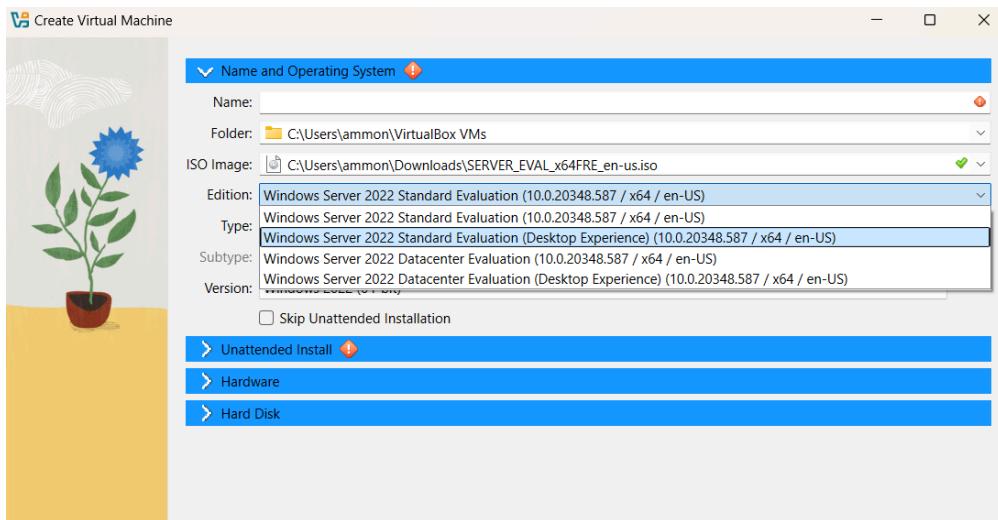
Active Directory is an important tool in SOC. It is used to manage user accounts, groups, and permissions across the entire network. It plays an important role in the Principle of Least Privilege and in Identity and Access Management. Active Directory logs every password change, login attempt, and access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



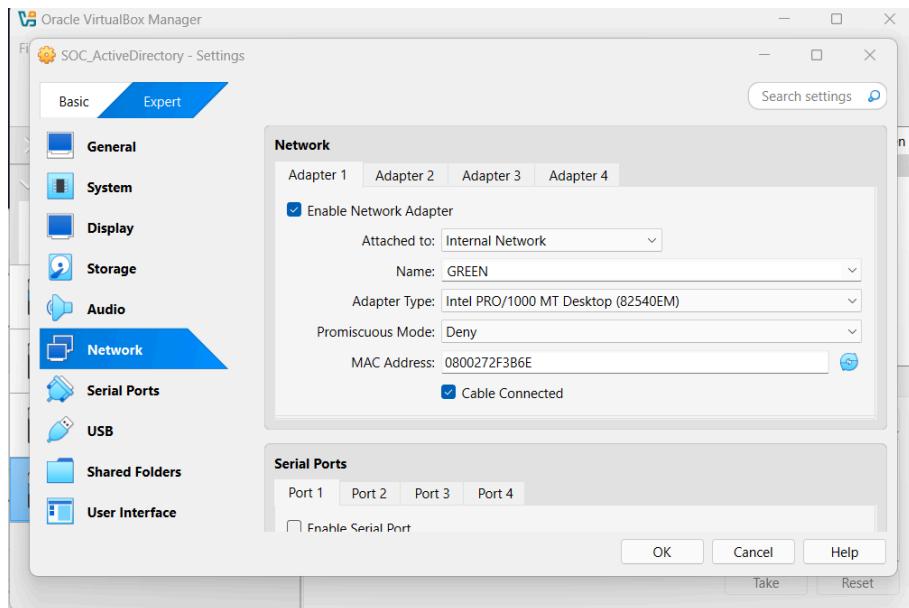
First, we downloaded Windows Server 2022 ISO file.

[Windows Server 2022 | Microsoft Evaluation Center](https://www.microsoft.com/en-us/evalcenter/download-windows-server-2022)

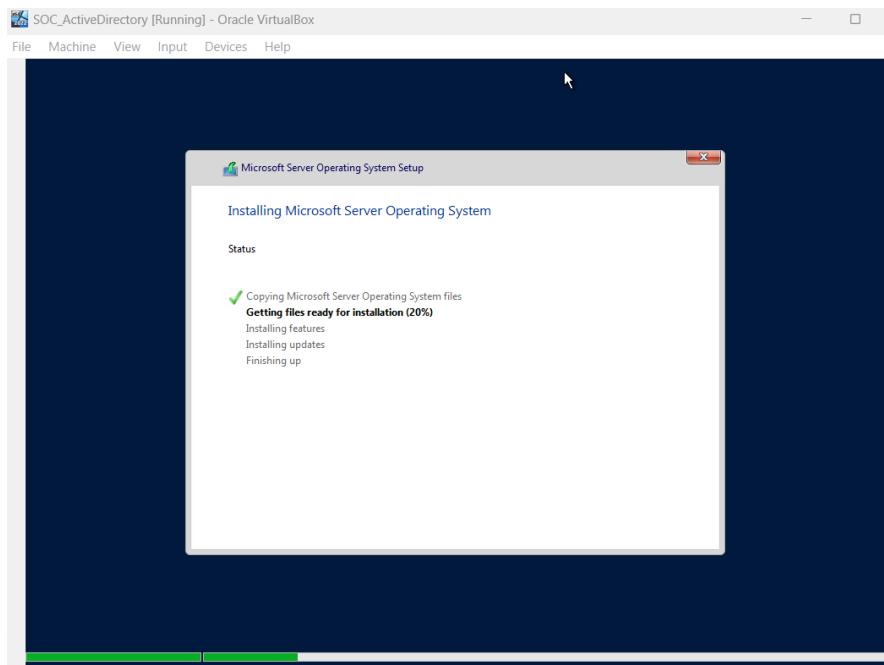
After downloading the `.iso` file I created a new machine with the file.



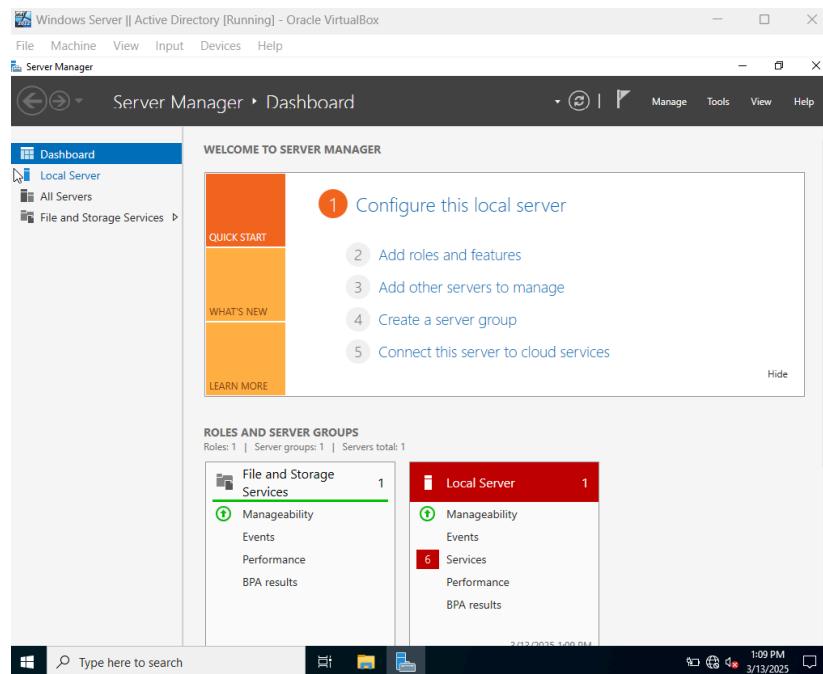
Make sure when you create the VM that you select Windows Server 2022 Standard Evaluation (Desktop Experience). I originally selected the other option and there was no GUI.



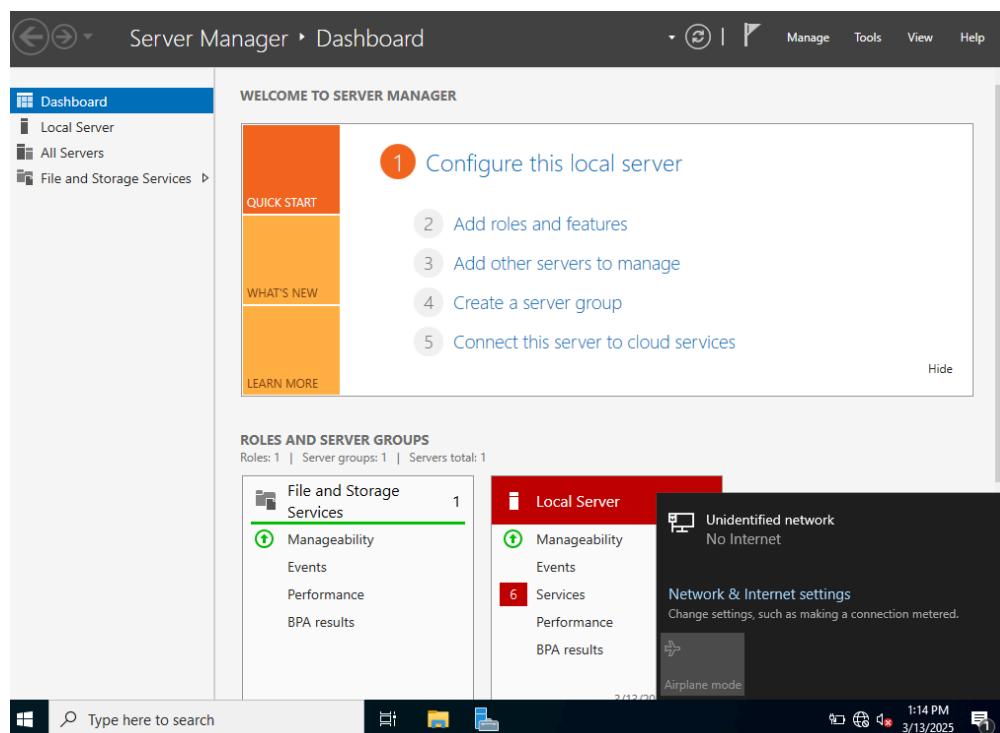
After creating it, I established one adapter attached to the Internal Network and named it Green.



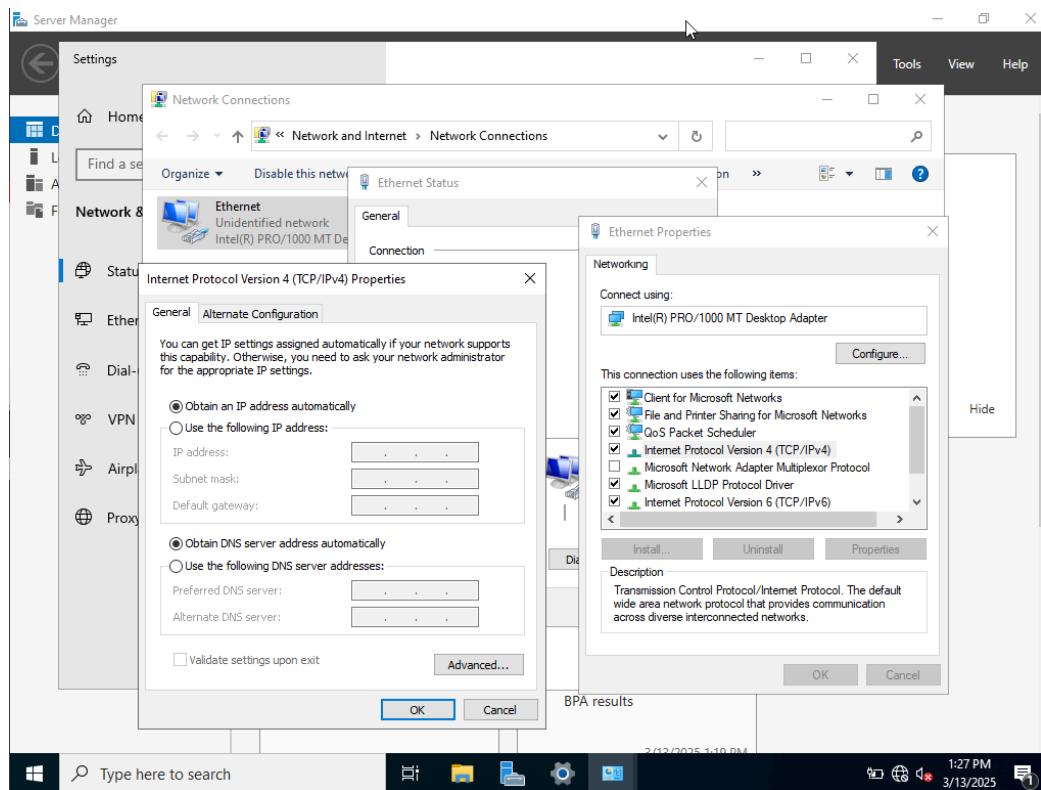
After starting the machine, the Microsoft Server OS begins to install.



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



Go to Network and Internet Settings.

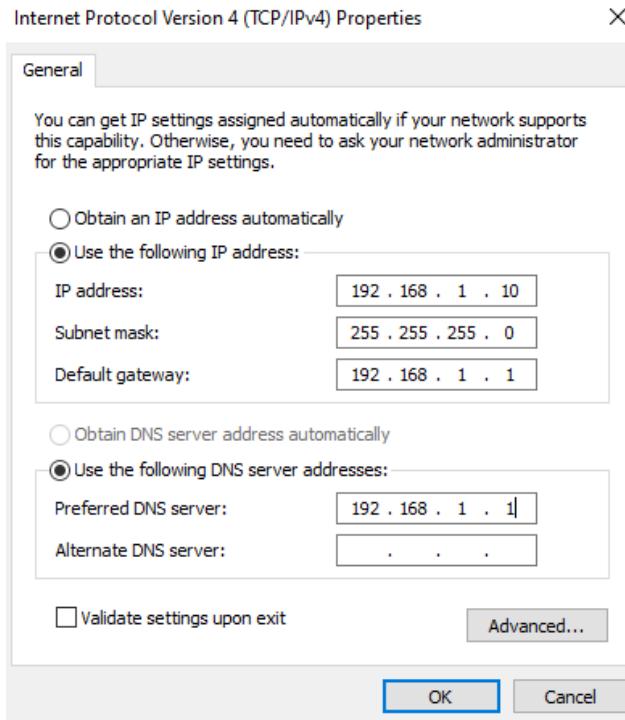


Click on Ethernet, then Ethernet Properties, then IPV 4 Properties.

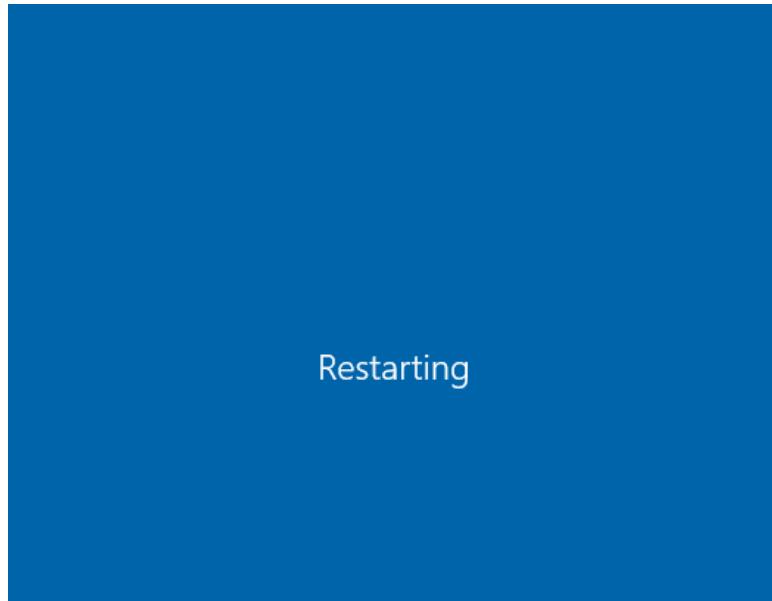
```
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

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
OPT1 (opt1)     -> em2          ->

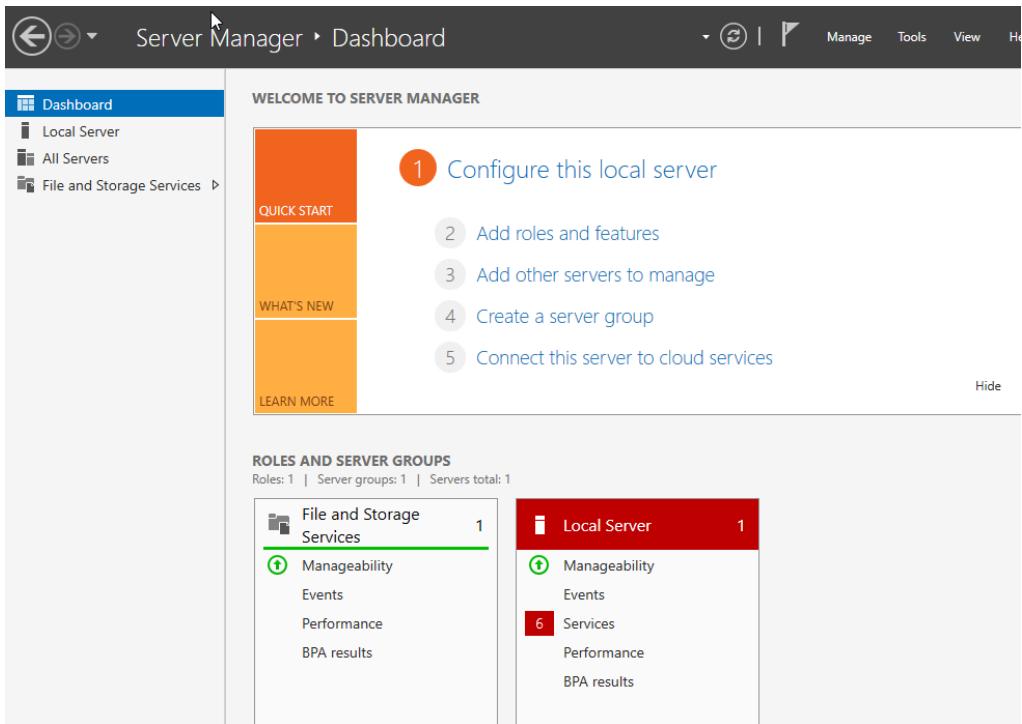
0) Logout (SSH only)   9) pfTop
```



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”.

Select installation type

DESTINATION SERVER  
WS-AD

Before You Begin

**Installation Type**

Server Selection

Server Roles

Features

Confirmation

Results

Select the installation type. You can install roles and features on a running physical computer or virtual machine, or on an offline virtual hard disk (VHD).

**Role-based or feature-based installation**  
Configure a single server by adding roles, role services, and features.

**Remote Desktop Services installation**  
Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment.

Before You Begin

**Server Selection**

Server Roles

Features

Confirmation

Results

Select a server or a virtual hard disk on which to install roles and features.

Select a server from the server pool

Select a virtual hard disk

Server Pool

Name	IP Address	Operating System
WS-AD	192.168.1.10	Microsoft Windows Server 2022 Standard Evaluation

## Select server roles

DESTINATION SERVER  
WS-AD

Before You Begin

Installation Type

Server Selection

**Server Roles**

Features

Confirmation

Results

Select one or more roles to install on the selected server.

Roles

Description

- Active Directory Certificate Services
- Active Directory Domain Services**
- Active Directory Federation Services
- Active Directory Lightweight Directory Services
- Active Directory Rights Management Services
- Device Health Attestation
- DHCP Server
- DNS Server
- Fax Server
- ▷  File and Storage Services (1 of 12 installed)
  - Host Guardian Service
  - Hyper-V
  - Network Policy and Access Services
  - Print and Document Services
  - Remote Access
  - Remote Desktop Services
  - Volume Activation Services
  - Web Server (IIS)
  - Windows Deployment Services
  - Windows Server Update Services

Active Directory Domain Services (AD DS) stores information about objects on the network and makes this information available to users and network administrators. AD DS uses domain controllers to give network users access to permitted resources anywhere on the network through a single logon process.

## Installation progress

DESTINATION SERVER  
WS-AD

Before You Begin

Installation Type

Server Selection

Server Roles

Features

AD DS

Confirmation

**Results**

View installation progress

 Starting installation

Active Directory Domain Services

Group Policy Management

Remote Server Administration Tools

Role Administration Tools

    AD DS and AD LDS Tools

        Active Directory module for Windows PowerShell

    AD DS Tools

        Active Directory Administrative Center

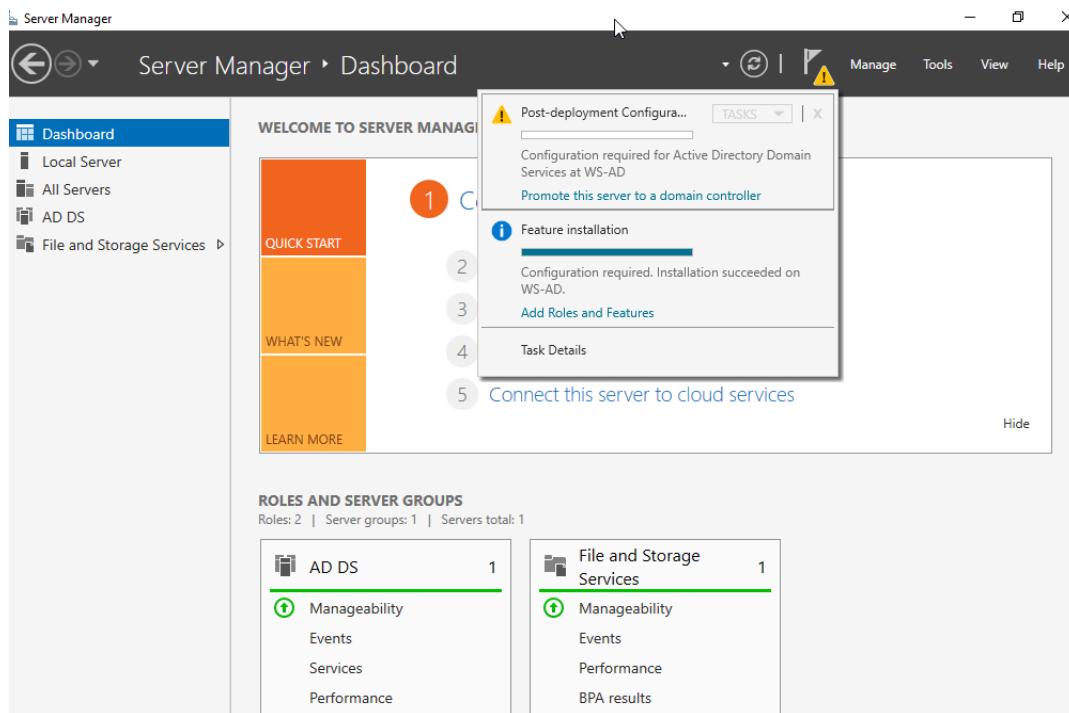
        AD DS Snap-Ins and Command-Line Tools



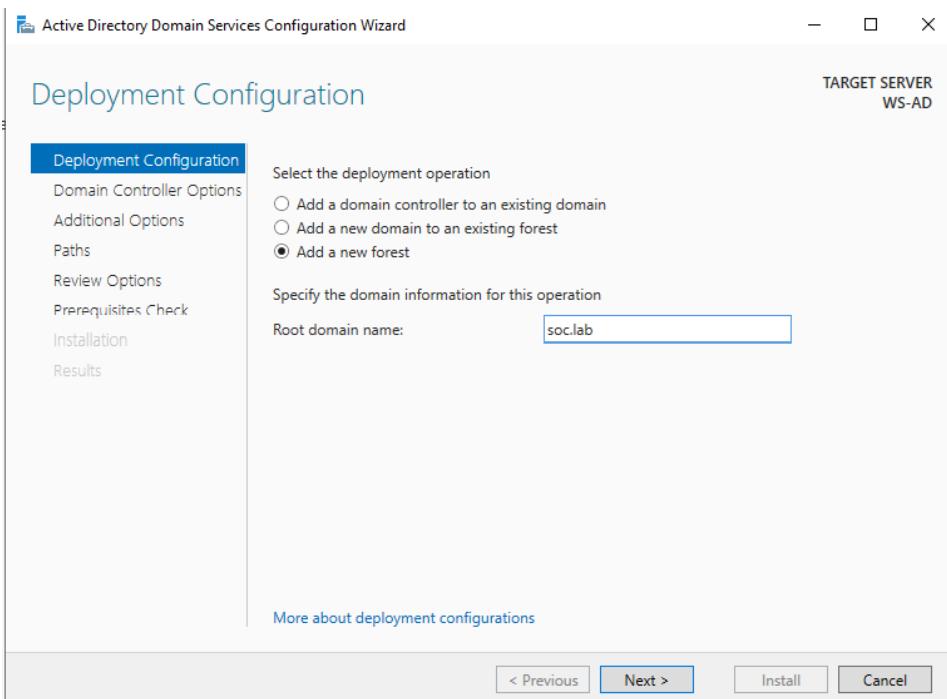
You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.

[Export configuration settings](#)

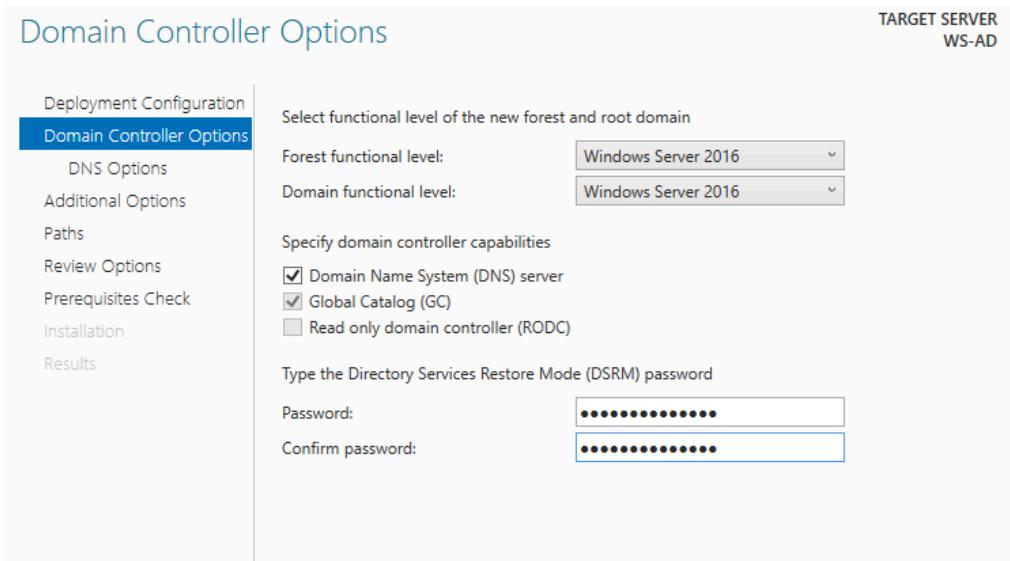
Follow all of the above steps to successfully install **Active Directory**.



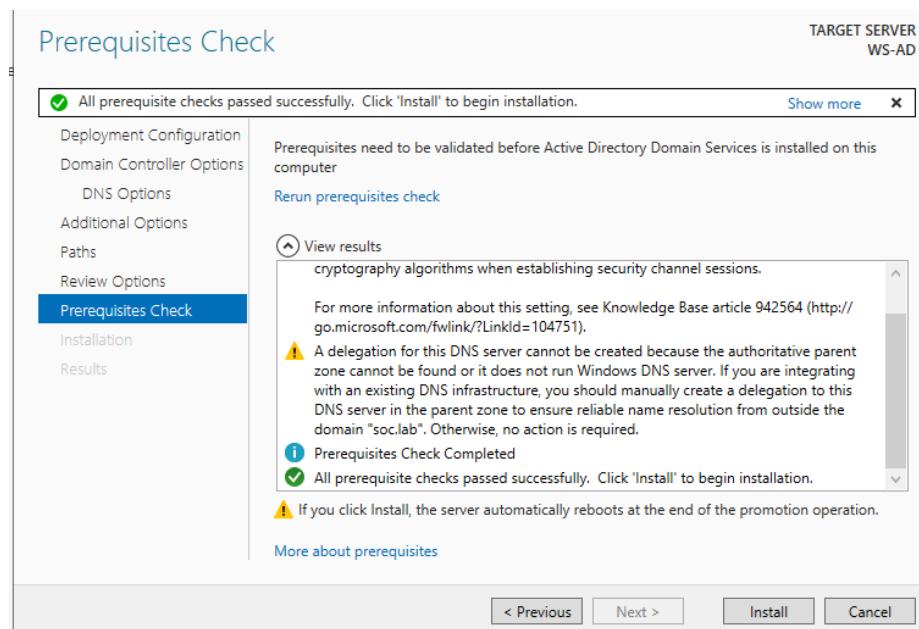
Next, we click “Promote this server to a domain controller”.



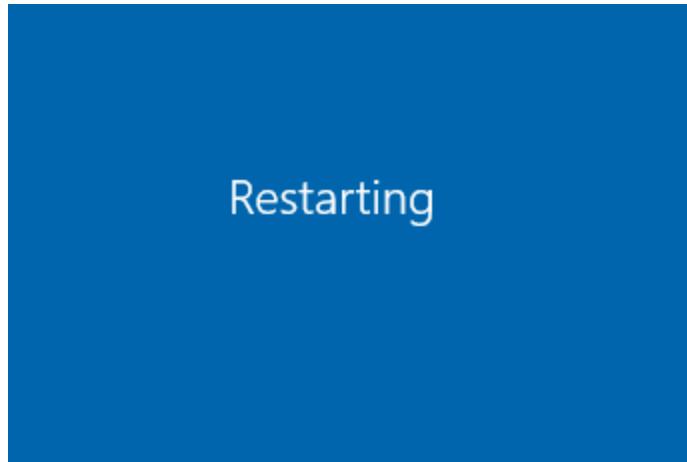
Then we “Add a new forest” and name the Root domain name.



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.

The screenshot shows a GitHub repository page for 'BadBlood' by davidprowe. The repository is public and has 5 issues, 4 pull requests, and 280 forks. The 'About' section provides a detailed description of the tool's purpose:

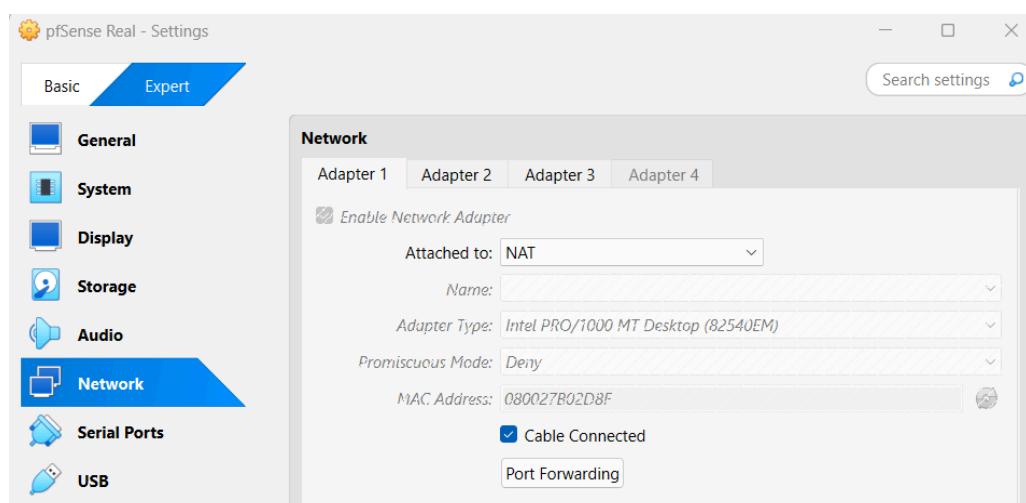
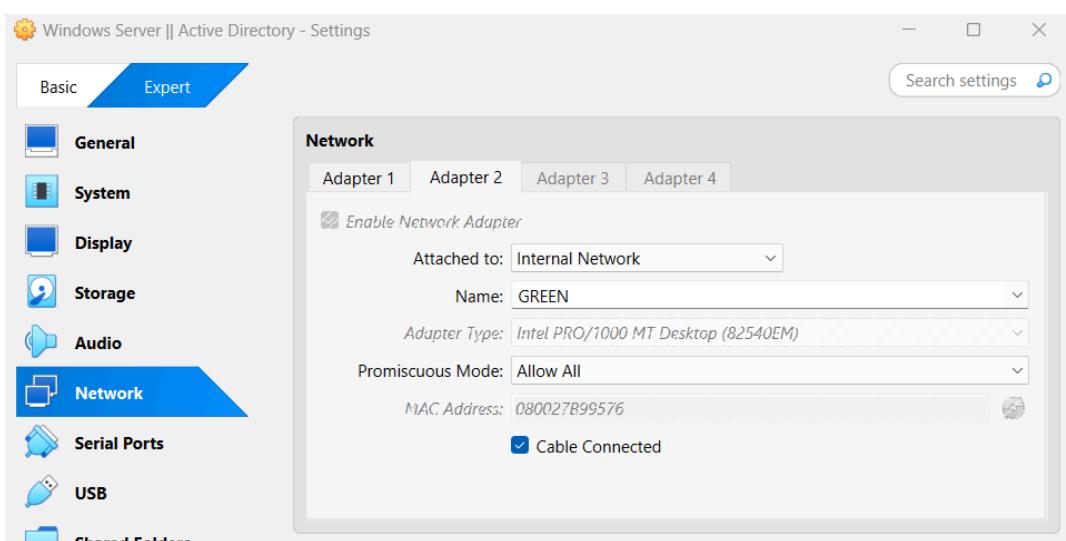
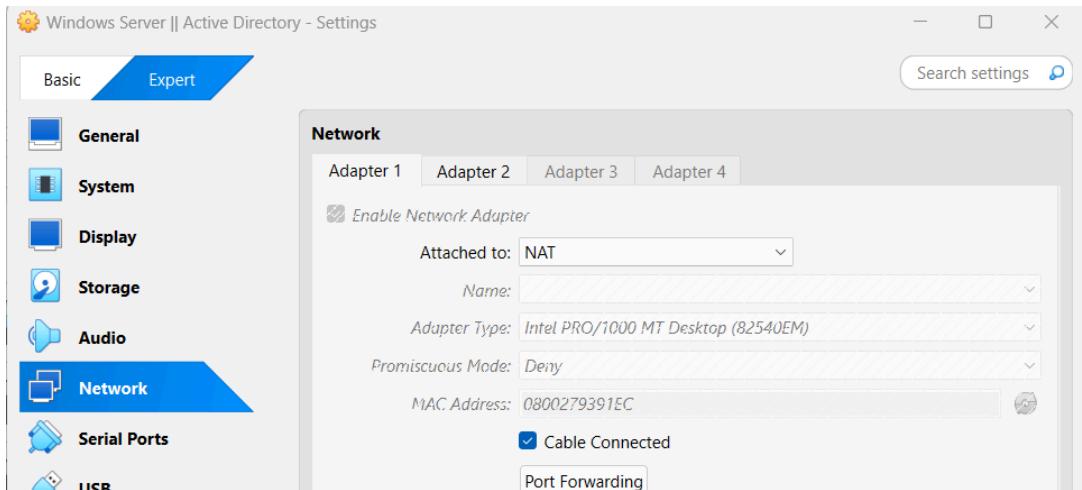
BadBlood by @davidprowe, Secframe.com, fills a Microsoft Active Directory Domain with a structure and thousands of objects. The output of the tool is a domain similar to a domain in the real world. After BadBlood is ran on a domain, security analysts and engineers can practice using tools to gain an understanding and prescribe to securing Active...

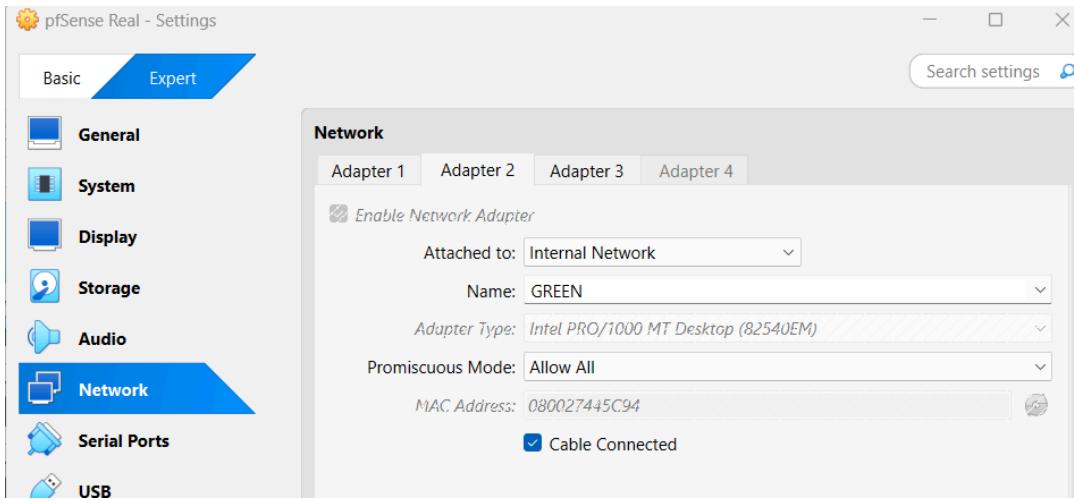
[www.secframe.com/badblood](http://www.secframe.com/badblood)

Commit	Description	Date
davidprowe Merge pull request #23 from benpatin/master	Create FUNDING.yml	b3c6325 · 2 years ago
.github	added some organization around th...	3 years ago
AD_Attack_Vectors	added parameters for group create ...	4 years ago
AD_Computers_Create	Updating User Creation, SidHistory I...	5 years ago
AD_Groups_Create	fixed spelling on my name, and rem...	4 years ago
AD_LAPS_Install	Initial commit	6 years ago

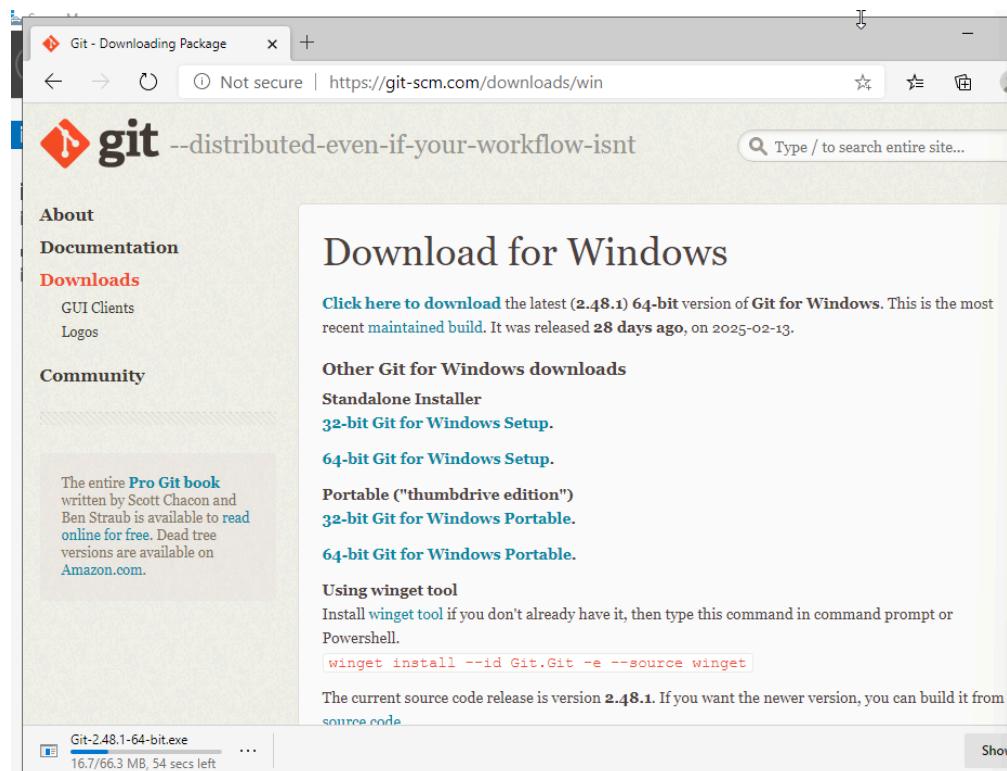
Next, we will install [BadBlood](#), which will populate Active Directory with fake users, groups, and permissions. This will be a good way to simulate a real SOC environment and practice.

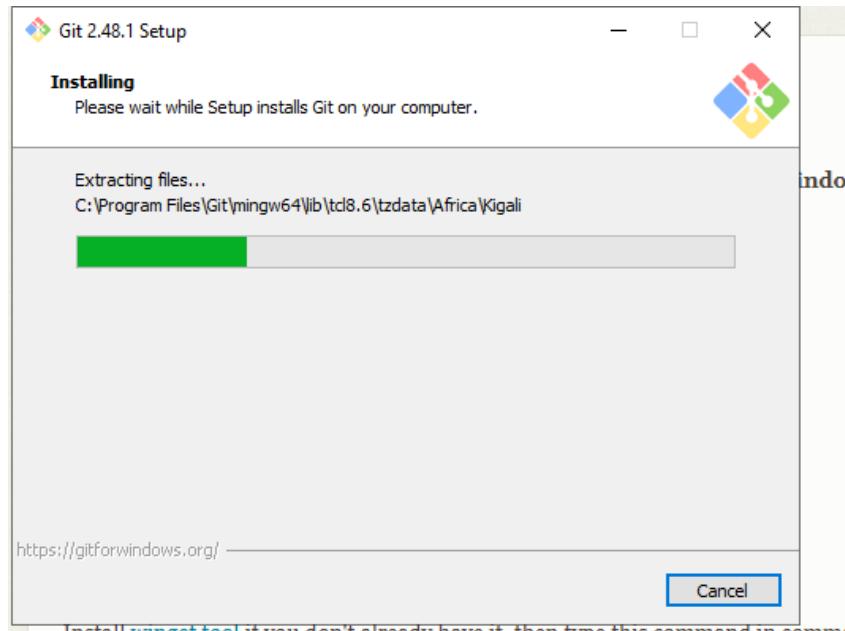
I had some issues connecting my Windows Server 2022 VM to the internet and installing Git so that I could install BadBlood. So I spent some time troubleshooting. Then I found the issue...





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.

```
PS C:\Windows\system32> git clone https://github.com/davidprowe/badblood.git
Cloning into 'badblood'...
remote: Enumerating objects: 226, done.
remote: Counting objects: 100% (132/132), done.
remote: Compressing objects: 100% (41/41), done.
remote: Total 226 (delta 103), reused 92 (delta 91), pack-reused 94 (from 1)
Receiving objects: 100% (226/226), 695.28 KiB | 1.69 MiB/s, done.
Resolving deltas: 100% (116/116), done.
PS C:\Windows\system32>
```

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:
[oooooooooooooooooooooooooooooooooooooooooooooooooooo]

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.U

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], DirectoryOperationException
+ FullyQualifiedErrorId : System.DirectoryServices.Protocols.DirectoryOperationException,AdmPwd.PS.D
rSelfPermission

Creating Tiered OU Structure
Creating Users on Domain
-
```

```
Administrator: Windows PowerShell
+ CategoryInfo          : NotSpecified: (:) [Set-AdmPwdComputerSelfPermission], DirectoryOperationException
+ FullyQualifiedErrorId : System.DirectoryServices.Protocols.DirectoryOperationException,AdmPwd.PS.D

Random Stuff into A domain - Adding Stuff to Stuff and Things
Progress:
[oooooooooooooooooooooooooooooooooooooooooooooooooooo

True
True
Creating Groups on Domain
Exception calling "Substring" with "2" argument(s): "Index and length must refer to a location within the
Parameter name: length"
At C:\Windows\system32\BadBlood\AD_Groups_Create\CreateGroup.ps1:112 char:110
+ ... 0,9)} catch{(get-content($groupscriptPath + '\hotmail.txt')|get-rando ...
+
+ CategoryInfo          : NotSpecified: (:) [], MethodInvocationException
+ FullyQualifiedErrorId : ArgumentOutOfRangeException

Exception calling "Substring" with "2" argument(s): "Index and length must refer to a location within the
Parameter name: length"
At C:\Windows\system32\BadBlood\AD_Groups_Create\CreateGroup.ps1:112 char:110
+ ... 0,9)} catch{(get-content($groupscriptPath + '\hotmail.txt')|get-rando ...
+
+ CategoryInfo          : NotSpecified: (:) [], MethodInvocationException
+ FullyQualifiedErrorId : ArgumentOutOfRangeException

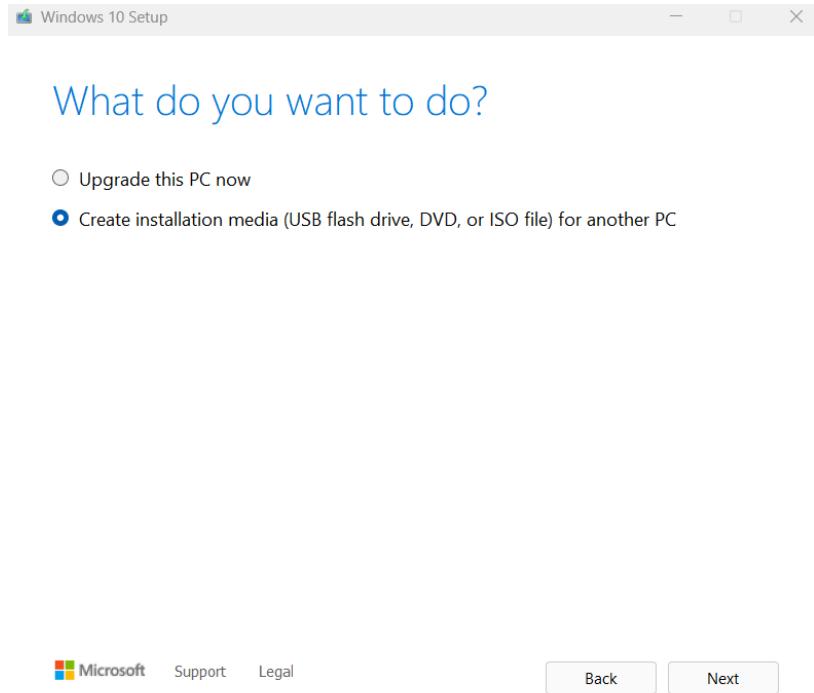
Creating Computers on Domain
Creating Permissions on Domain
Nesting objects into groups on Domain
```

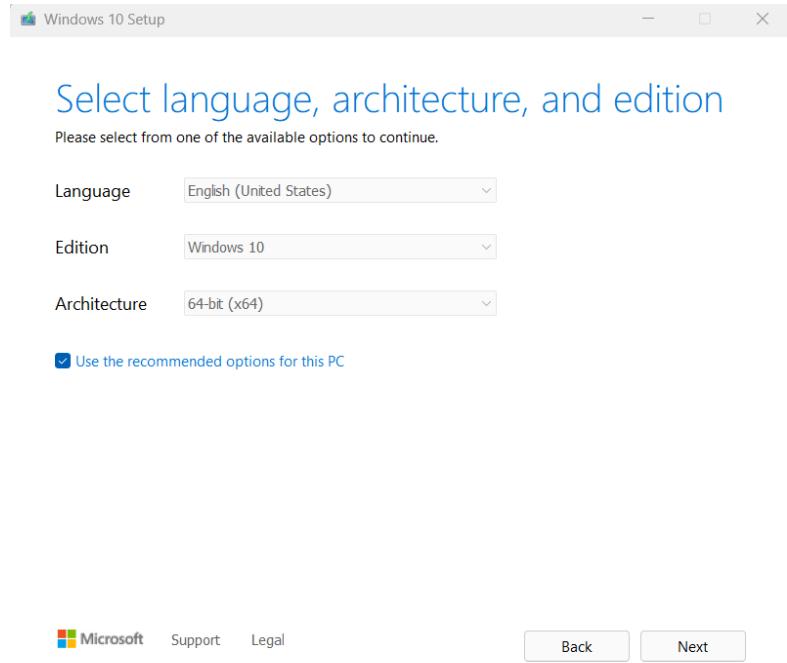
```
Creating Computers on Domain
Creating Permissions on Domain
Nesting objects into groups on Domain
Adding random SPNs to a few User and Computer Objects
Adding ASREP for a few users
PS AD:\>
PS AD:\>
PS AD:\> ■
```

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

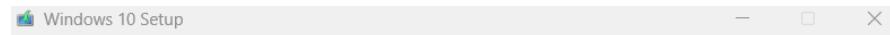
If you want to install Windows 10 on another partition, you need to create and then run the media to install it.

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.



## Burn the ISO file to a DVD

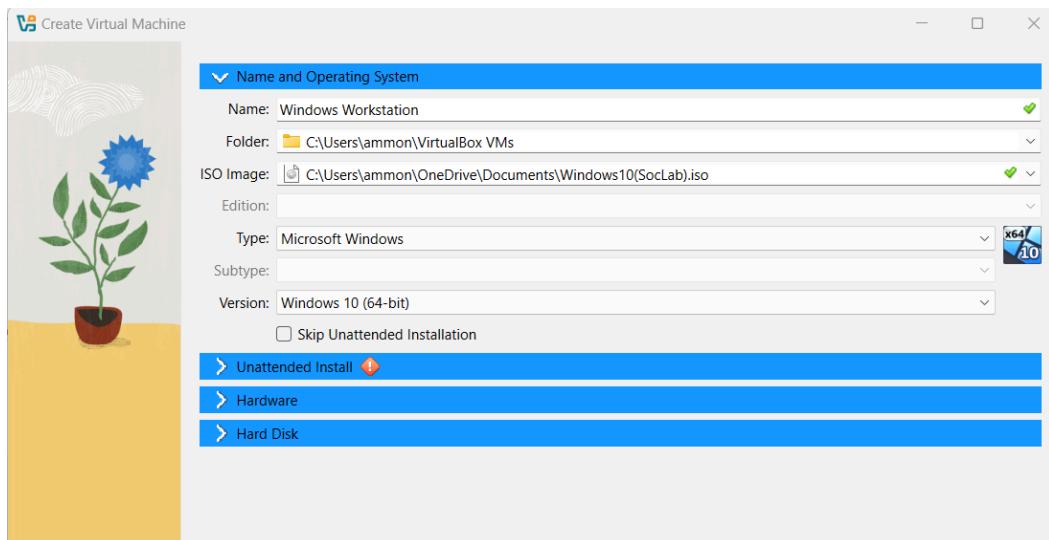
C:\Users\ammon\OneDrive\Documents\Windows10(SocLab).iso  
Open DVD burner

 Microsoft   Support   Legal

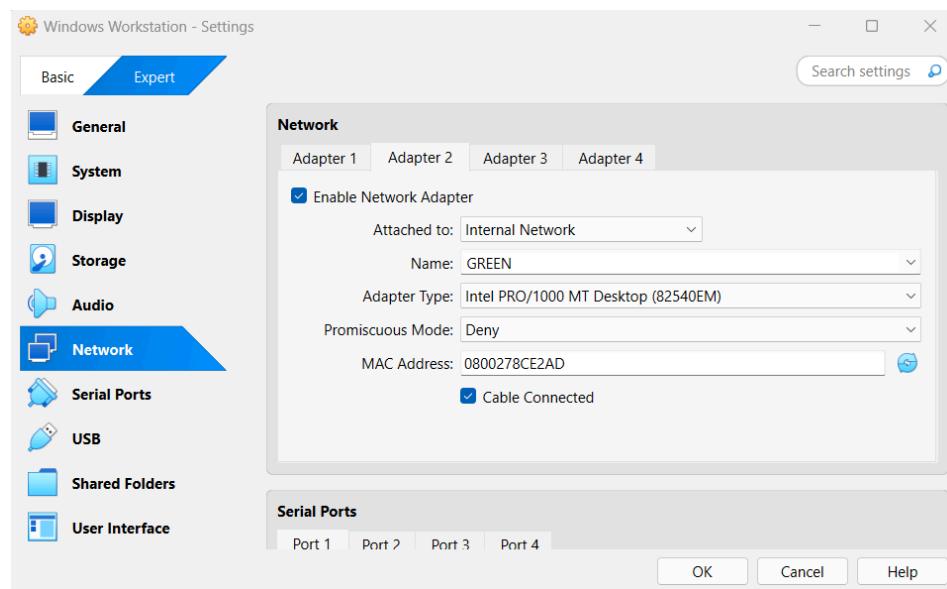
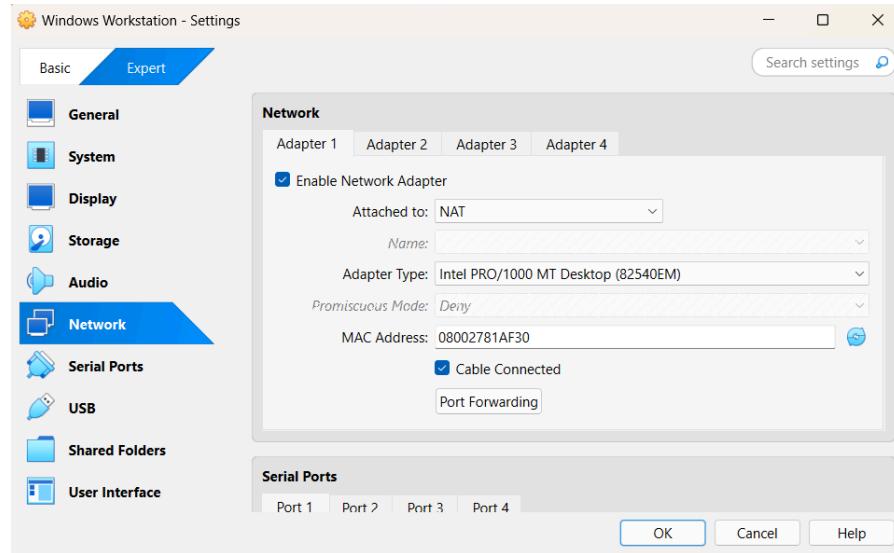
Back

Finish

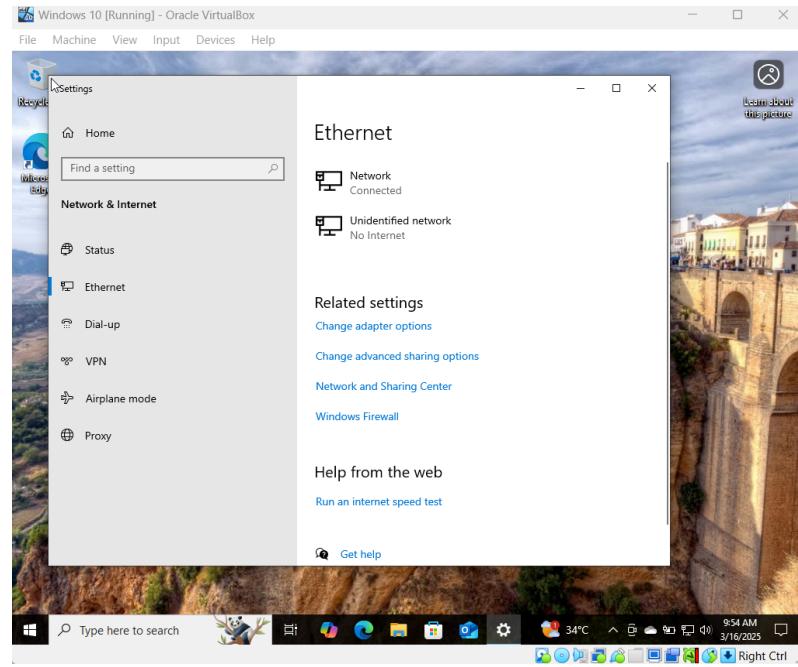
We finished creating and downloading the Windows VM.



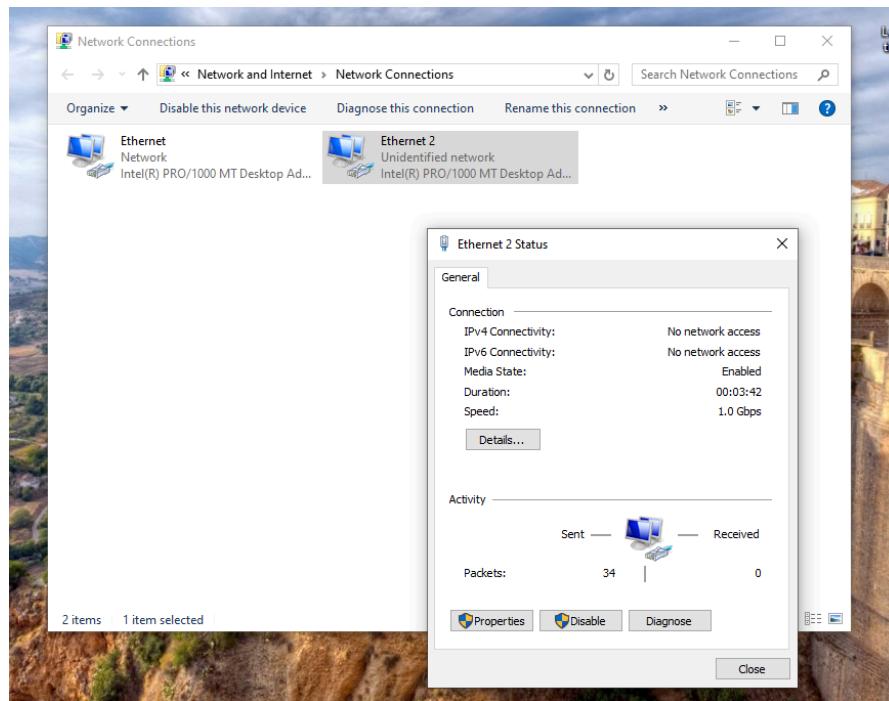
Next, we add the Windows VM we just created to VirtualBox.

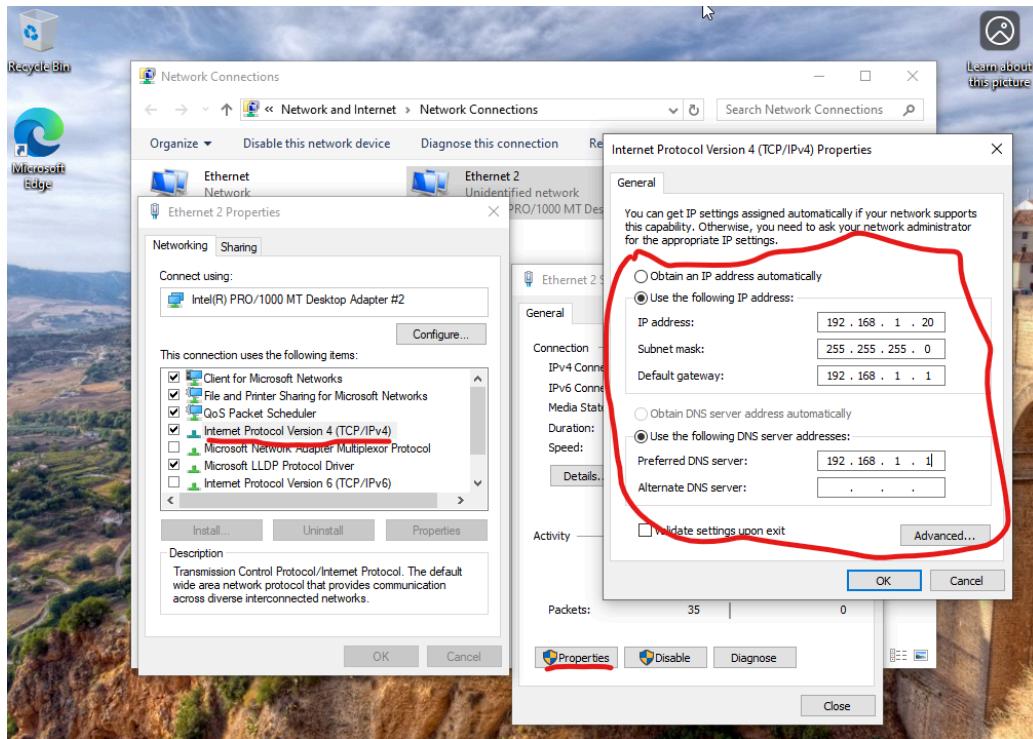


We configured the network the exact same way as the previous machine, Windows Server 2022.



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





We want this Windows Workstation to be connected to 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.

```

Administrator: Command Prompt
Microsoft Windows [Version 10.0.19045.5487]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=4ms TTL=255
Reply from 192.168.1.1: bytes=32 time=3ms TTL=255
Reply from 192.168.1.1: bytes=32 time=4ms TTL=255
Reply from 192.168.1.1: bytes=32 time=3ms TTL=255

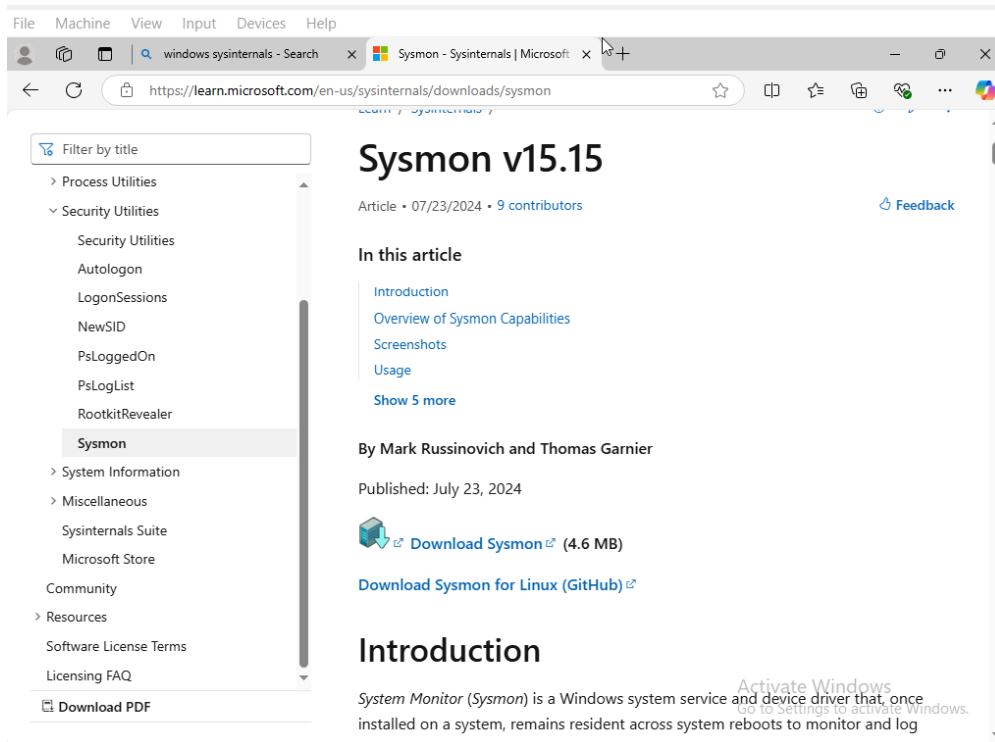
Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 3ms, Maximum = 4ms, Average = 3ms

```

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

## Sysmon

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. Sysmon 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.

Raw file content

**Download**

Jump to line

Copy path

Copy permalink

View options

Show code folding buttons

Wrap lines

Center content

## 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.lxl
-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.

```
PS C:\Users\insee\Desktop\Sysmon> .\Sysmon64.exe -accepteula -i .\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 4.90
Configuration file validated.
Sysmon64 installed.
SysmonDrv installed.
Starting SysmonDrv.
SysmonDrv started.
Starting Sysmon64..
Sysmon64 started.
PS C:\Users\insee\Desktop\Sysmon>
```

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).

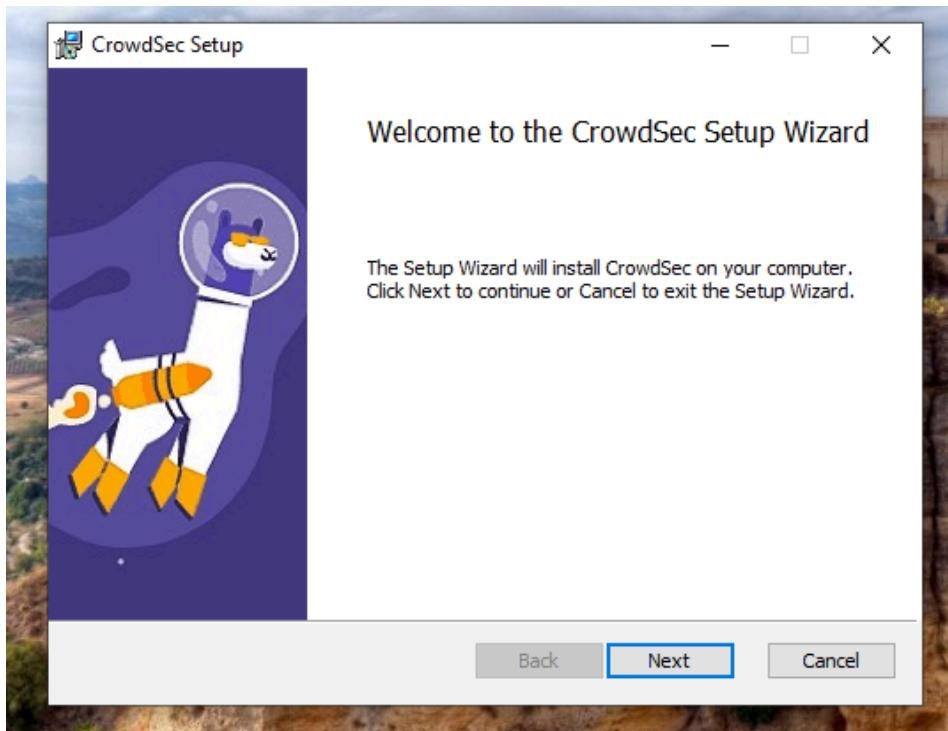


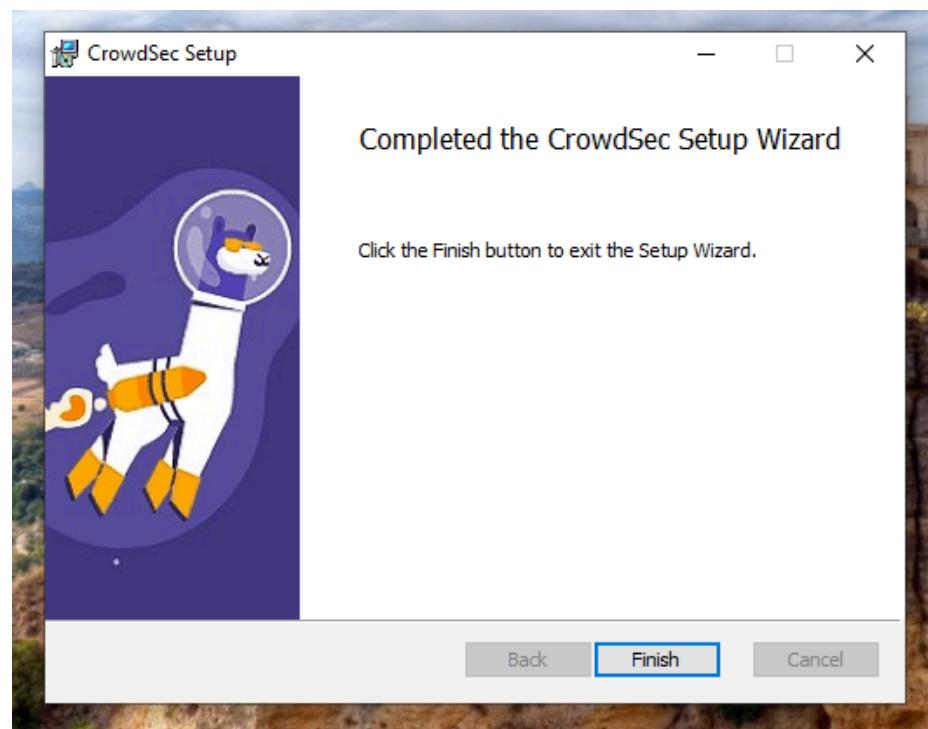
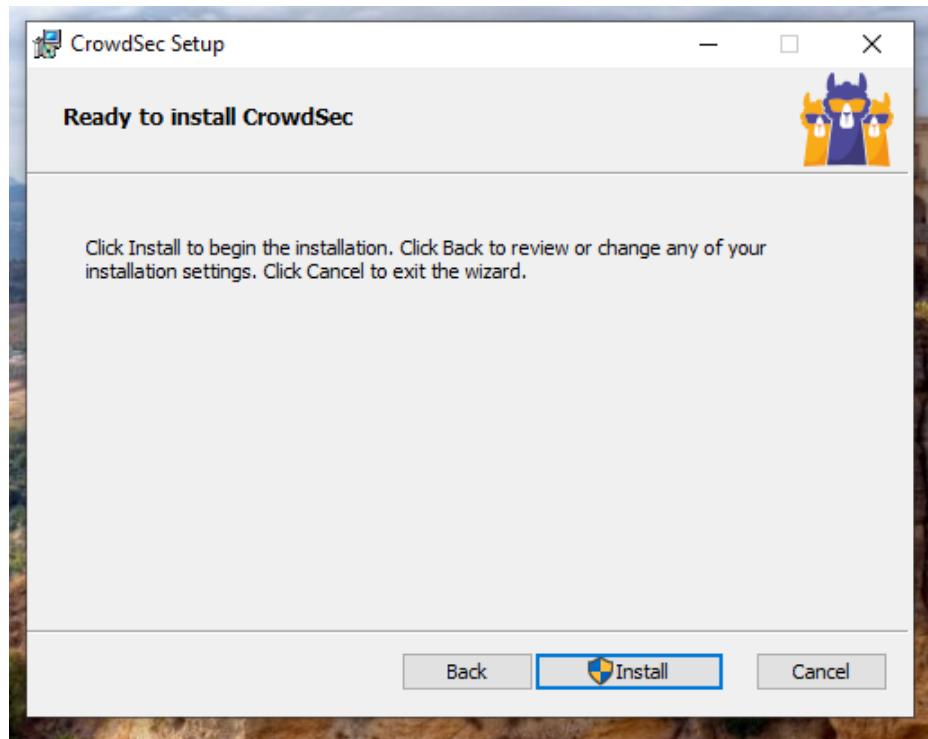
A screenshot showing two side-by-side sections of the CrowdSec platform. On the left is the "CrowdSec Console" interface, featuring a dark theme with yellow highlights. It displays three bullet points: "Unveil threats in real-time", "Secure proactively", and "Elevate your response strategy", each with a small icon and a brief description. Below these is a section with three small charts. On the right is the "Create your account" form. It has fields for "Email address" and "Password", a "Sign up" button, and a link to "Sign in". Above the form, there's a "Create your account" heading and a note: "Please fill in the details to get started." It also includes social media login buttons for Google and GitHub, and a checkbox for accepting the end user license and privacy policy.

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

The screenshot shows a web browser window with the URL <https://github.com/crowdsecurity/crowdsec/releases/tag/v1.6.5>. The page displays the release notes and assets for CrowdSec version 1.6.5. A tooltip highlights the 'crowdsec\_1.6.5.msi' file in the 'Downloads' section, which is currently being downloaded at 3.2 MB/s. Other files listed include 'sysmonconfig.xml' (removed), 'Sysmon.zip' (Open file), 'crowdsec-release.tgz', 'crowdsec-v1.6.5-vendor.tar.xz', 'crowdsec\_1.6.5.nupkg', 'crowdsec\_1.6.5.msi', 'vendor.tgz', 'Source code (zip)', and 'Source code (tar.gz)'. The bottom of the page includes standard GitHub navigation links like Terms, Privacy, Security, Status, Docs, Contact, Manage cookies, and a note about not sharing personal information.

Go to Github and [download the crowdsec .msi file](#). Then run the file.





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

