Tools used:
Virtualization Software(virtualbox)
Active Directory
Splunk Server
Kali linux

Step 1:
What is Active Directory?
Active Directory (AD) is a directory service developed by Microsoft for Windows domain networks. It is used for managing and storing information about network resources such as computers, users, and services, and facilitates the centralized management and security of these resources.

Step 2:
Download and install virtualbox: https://www.virtualbox.org/wiki/Downloads

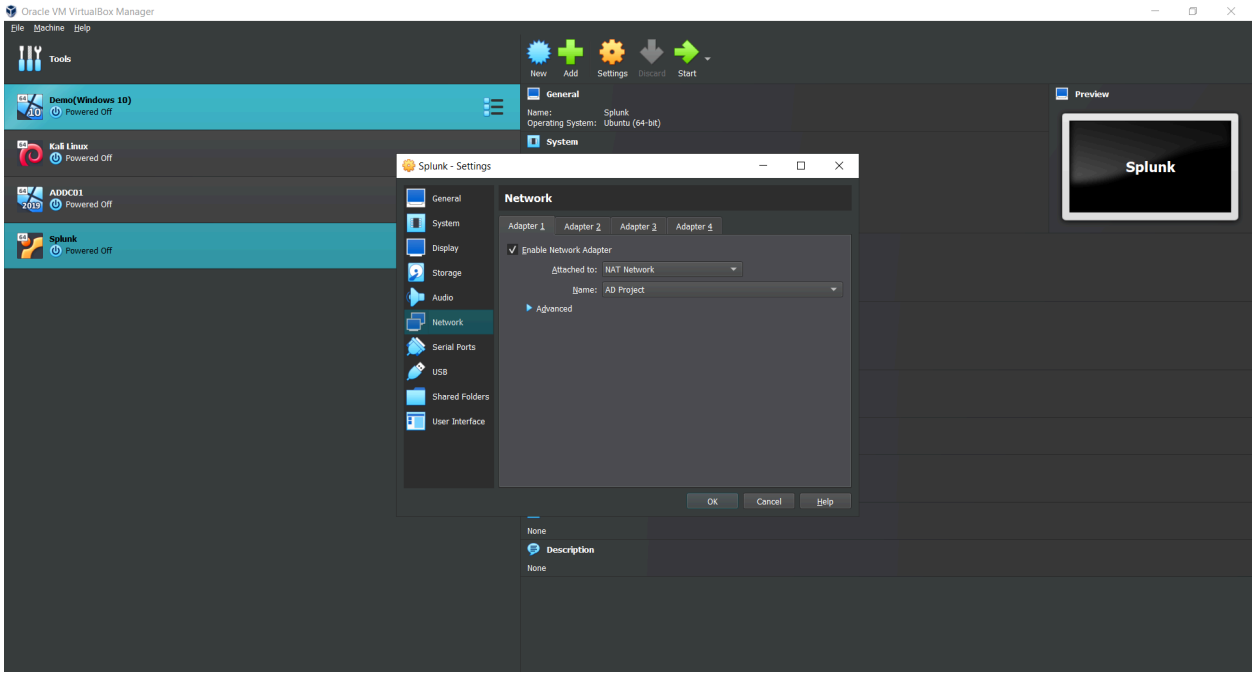
Step 3:
Download windows 10 iso file: https://www.microsoft.com/en-ca/software-download/windows10
Create a windows 10 Virtual Machine

Step 4:
Download Kali linux iso file: https://www.kali.org/get-kali/#kali-virtual-machines
Create Kali linux Virtual Machine

Step 5:
Download Windows Server 2022 Iso file:
https://www.microsoft.com/en-us/evalcenter/evaluate-windows-server-2022
Create Windows Server 2022 Virtual Machine

Step 6:
Download Ubuntu server iso file: https://ubuntu.com/download/server
Create Ubuntu server Virtual Machine
After creation, be sure to perform **sudo apt-get update && sudo apt-get upgrade -y**

Make sure virtual box network settings is on NAT-network so our vms can be on the same network and have internet access and apply settings to individual machines



Step 7
Log into Splunk machine
Perform **ip a** to see ip address to make sure its the same as the allocated ip

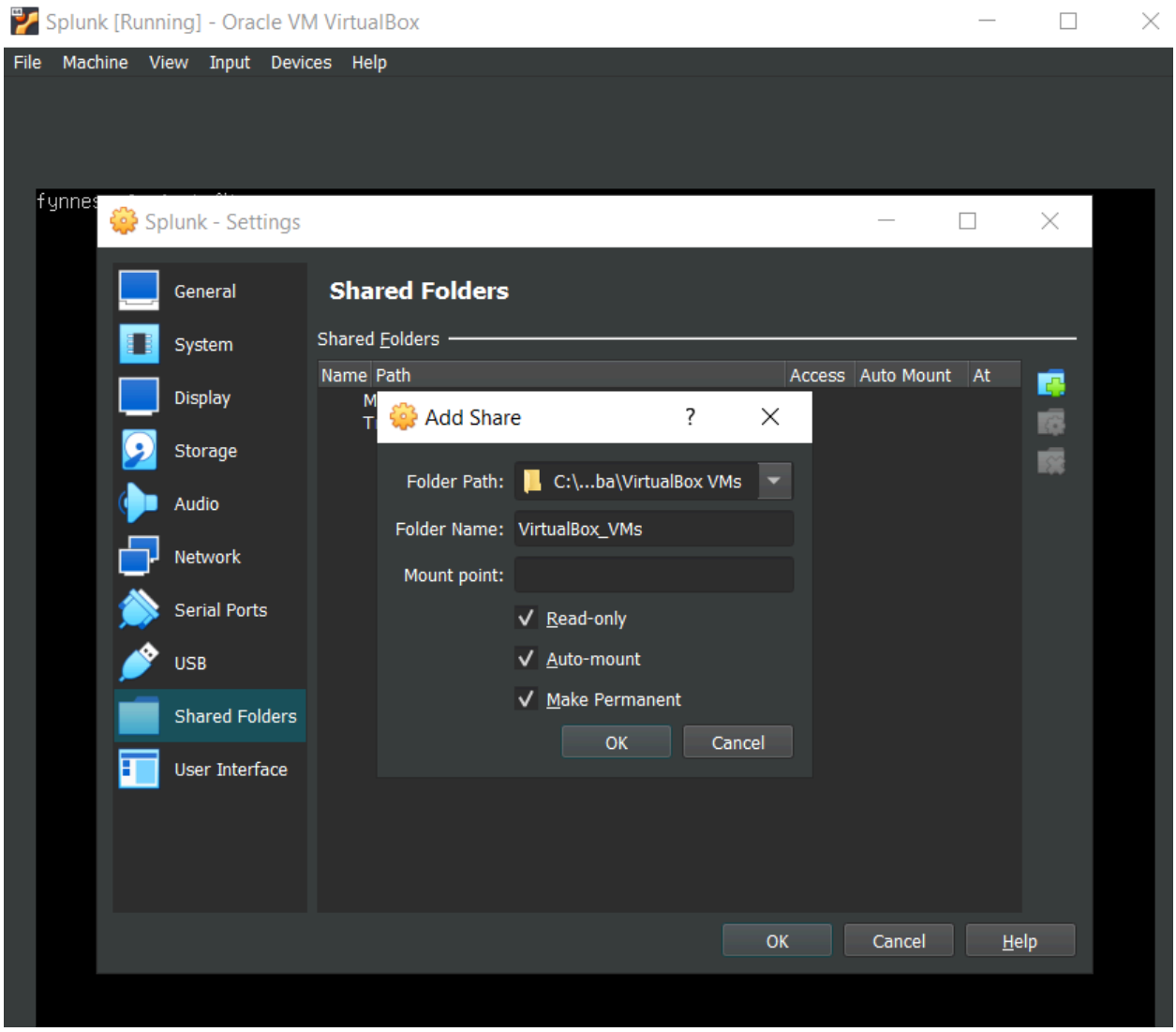
If ip's dont match, set a static ip
Navigate to **sudo nano /etc/netplan/00-installer-config.yaml**
Change default settings to:

Address would be your static ip for machine
After Settings modification run: **sudo netplan apply**
Check to make sure ip has changed: **ip a**
Check for connectivity: **ping google.com**

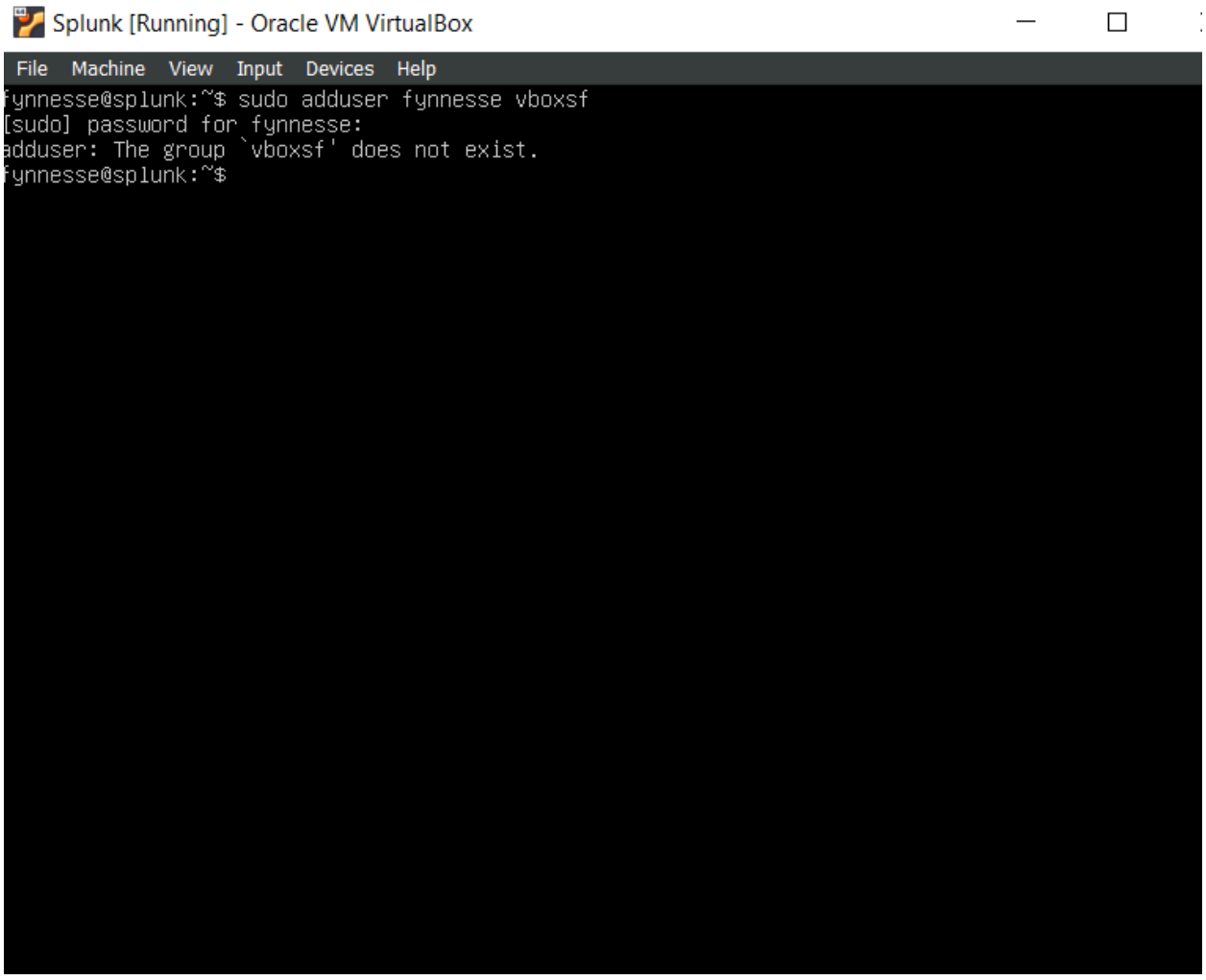
Step 8:
Install Virtual box Guest additions on ubuntu server: sudo apt-get install virtualbox-guest-additions-iso

Step 9:
On Host machine
Navigate to splunk Official site and download splunk enterprise for linux : https://www.splunk.com/

Step 10:
Configure shared folder between host machine and vm
Navigate to **devices** > **shared folders** > **shared folders settings**
Click on **add folder icon** and select the folder that contains the splunk enterprise deb file
After Creation of shared folders, Reboot system : **sudo reboot**


Splunk [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Splunk - Settings
General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
User Interface
Shared Folders
Shared Folders
Name Path Access Auto Mount At
Add Share
Folder Path: C:\...ba\VirtualBox VMs
Folder Name: VirtualBox_VMs
Mount point:
Read-only
Auto-mount
Make Permanent
OK
Cancel
OK
Cancel
Help

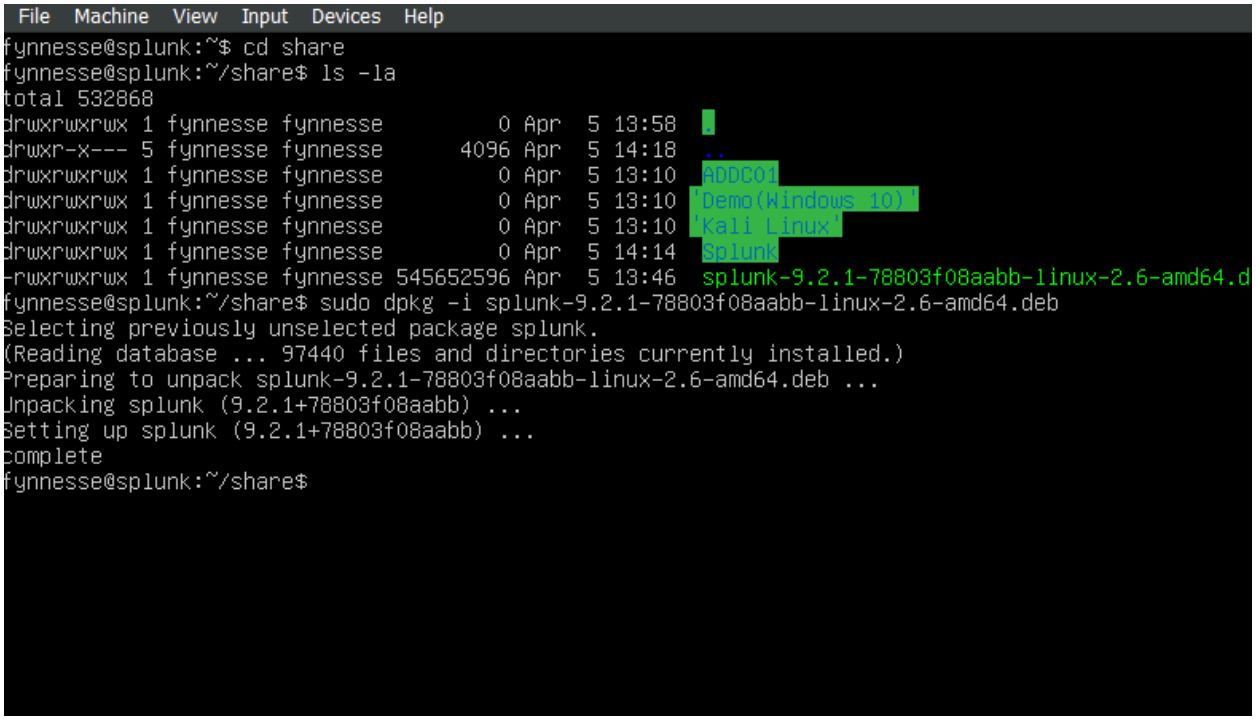
Step 11:
Add user into vboxsf
Sudo adduser [username] vboxsf



If presented with vboxsf does not exist it could mean we didnt install some additional guest installations. RUN: **sudo apt-get install virtualbox-guest-utils**
After installation Reboot: **sudo reboot**

After Reboot add user into vboxsf group again: **Sudo adduser [username] vboxsf**
Create a new directory called share: **mkdir share**
We want to mount our shared folder unto our directory called share : **sudo mount -t vboxsf -o uid=1000,gid=1000 [shared folder name] share/**

Step 12:
Install splunk : **sudo dpkg -i [Splunk installer.deb]**

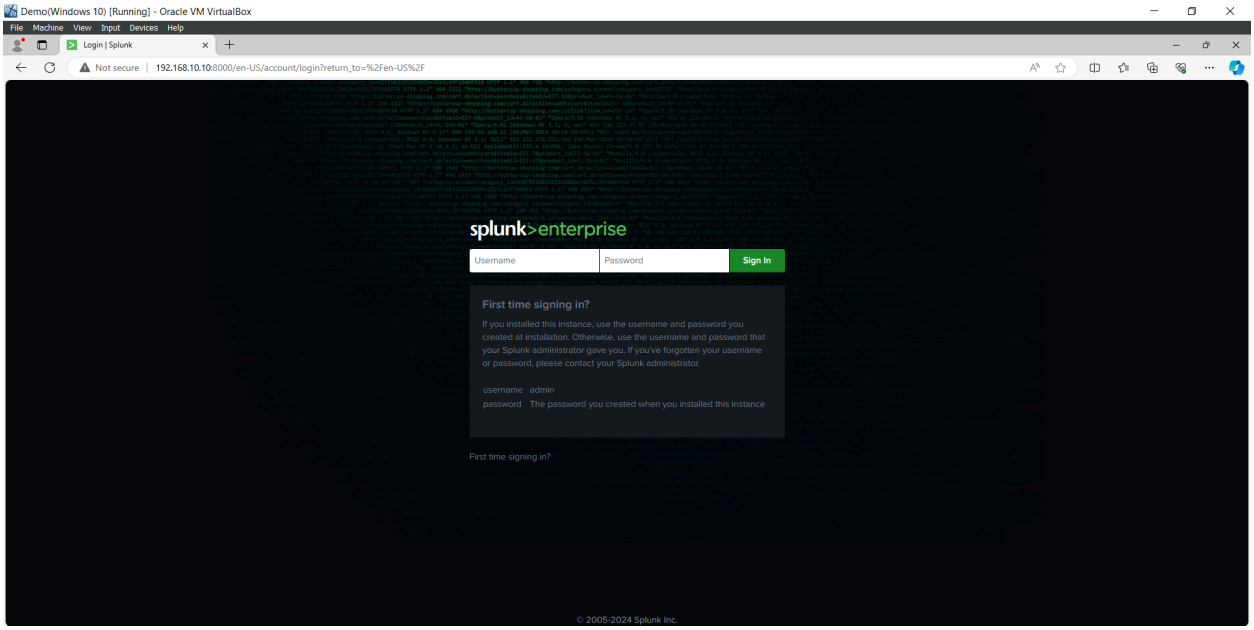


Change into the directory where splunk is located unto our server: **cd /opt/splunk**
Change into the user splunk: **sudo -u splunk bash**
Navigate to the binary files splunk can use: **Cd bin**
Run the installer: **./splunk start**
Press Q then y. Use administrator username as user name and a strong password

We want to make sure our splunk starts up everytime our VM reboots: **exit> cd bin > sudo ./splunk enable boot-start -user splunk**

Step 13:
On Target Machine
Check the ip address is the allocated ip address for the system
Open cmd and run **ipconfig**
If it isn't right head to network & internet settings > change adapter options
Right click the adapter and select properties. Select ipv4 and click properties
Set a static ip to desired IP

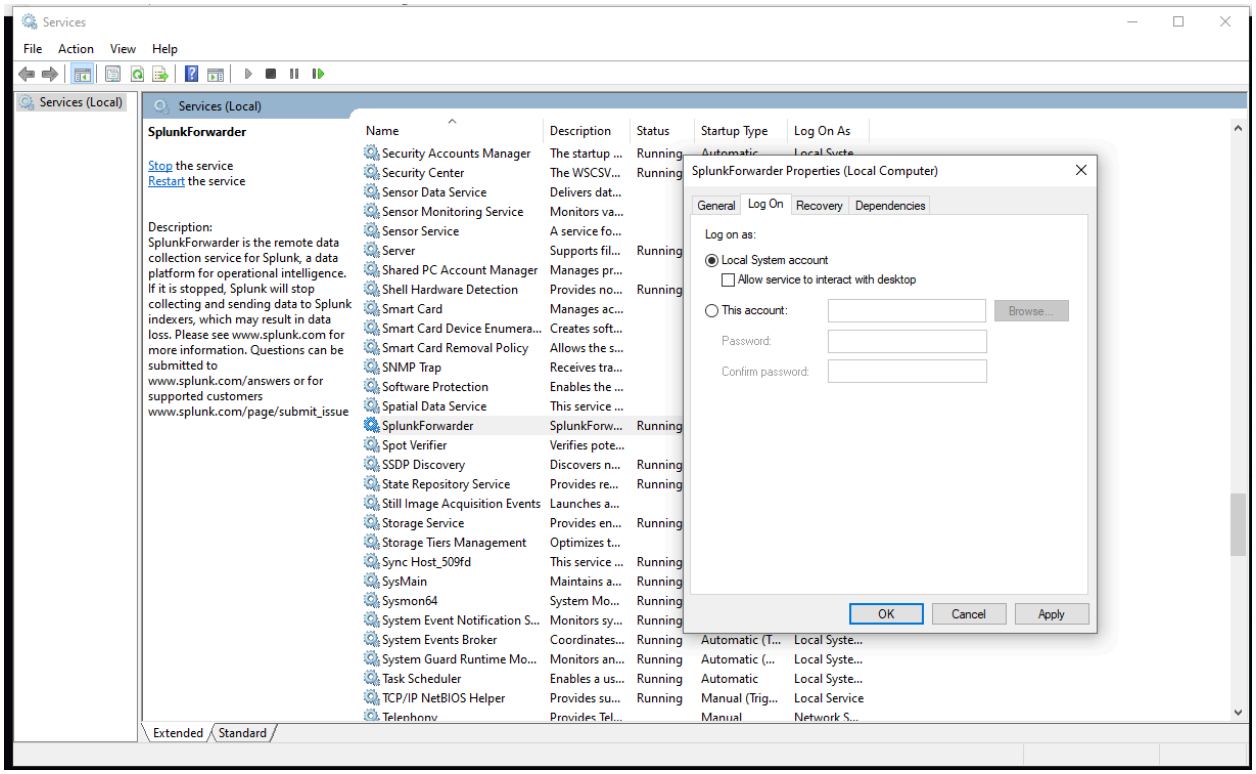
Step 14:
Head to **192.168.20.20:8000** to access splunk



Navigate to splunk.com and download universal forwarder
Navigate to sysmon official site and download sysmon
Navigate to :
https://raw.githubusercontent.com/olafhartong/sysmon-modular/master/sysmonconfig.xml and same the page as **sysmonconfig.xml**
To install sysmon: Open powershell with administrator privileges > Navigate to the folder sysmon was downloaded to and run: **.\Sysmon64.exe -i ..\sysmonconfig.xml**

Step 15:
We need to instruct our splunk forwarder what we want to send to our splunk server. We must configure inputs.conf
Navigate to **C: drive> Program files > Splunk universal forwarder > etc > system> default> input.conf**. Copy the content of input.conf and create a new file under **local** instead of default

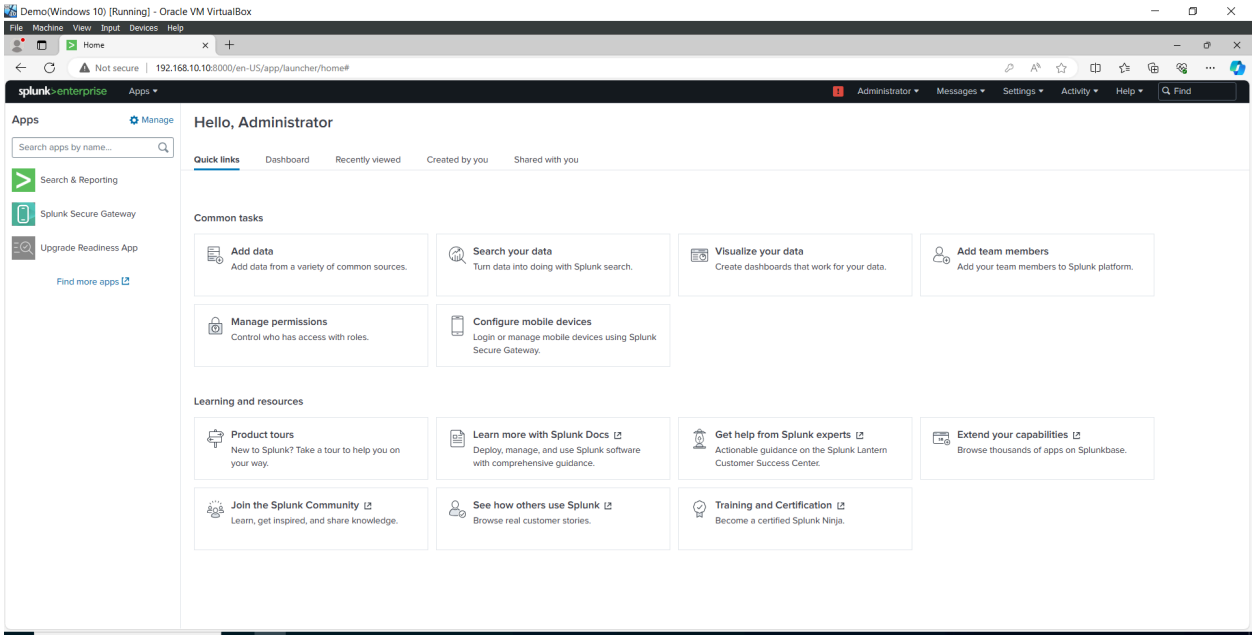
After each change to inputs.conf we must restart splunk universal forwarder
Run services as administrator
Check the log on account on that service and make sure it's on a local account. After restart, splunk forwarder.



If hit with an error that's okay, Just start the service.

Step 16:

Navigate to splunk web portal and log in with credentials created

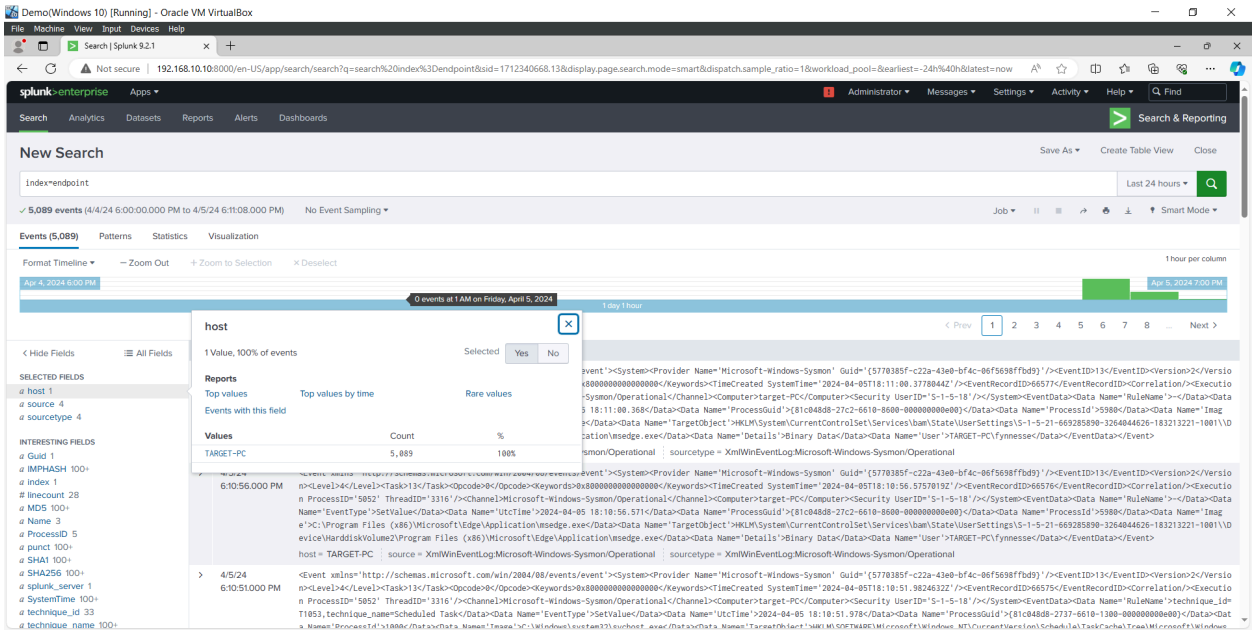


In the input.conf file all of the events are being sent to an index called “endpoint”

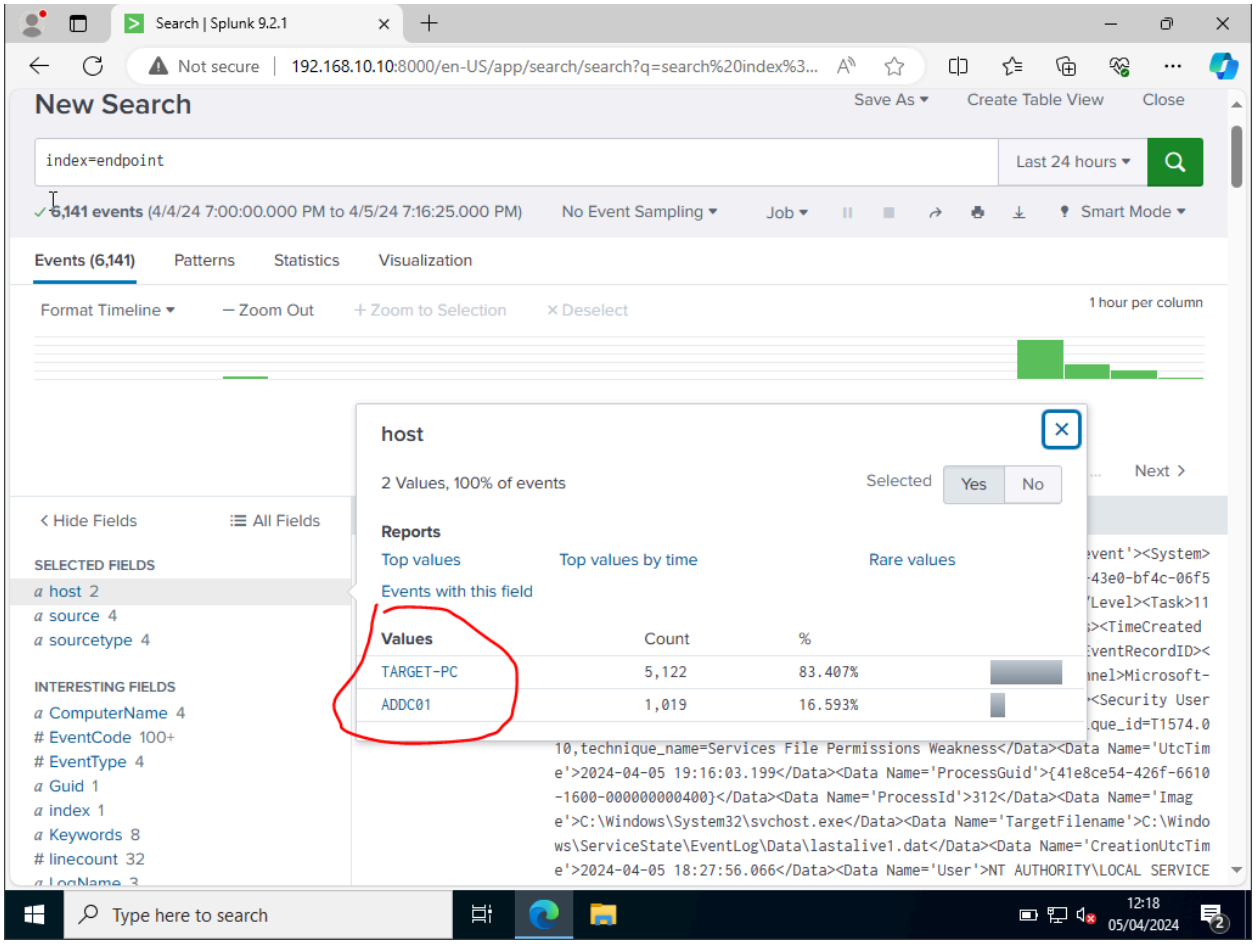
Navigate to **settings** > **indexes** > **new index** and name the index “endpoint”

We then need to enable our splunk server to receive data
Navigate to **settings** > **forwarding and receiving**. Under **Receive data** click **configure receiving** > **New receiving Port** and input default port : **9997**

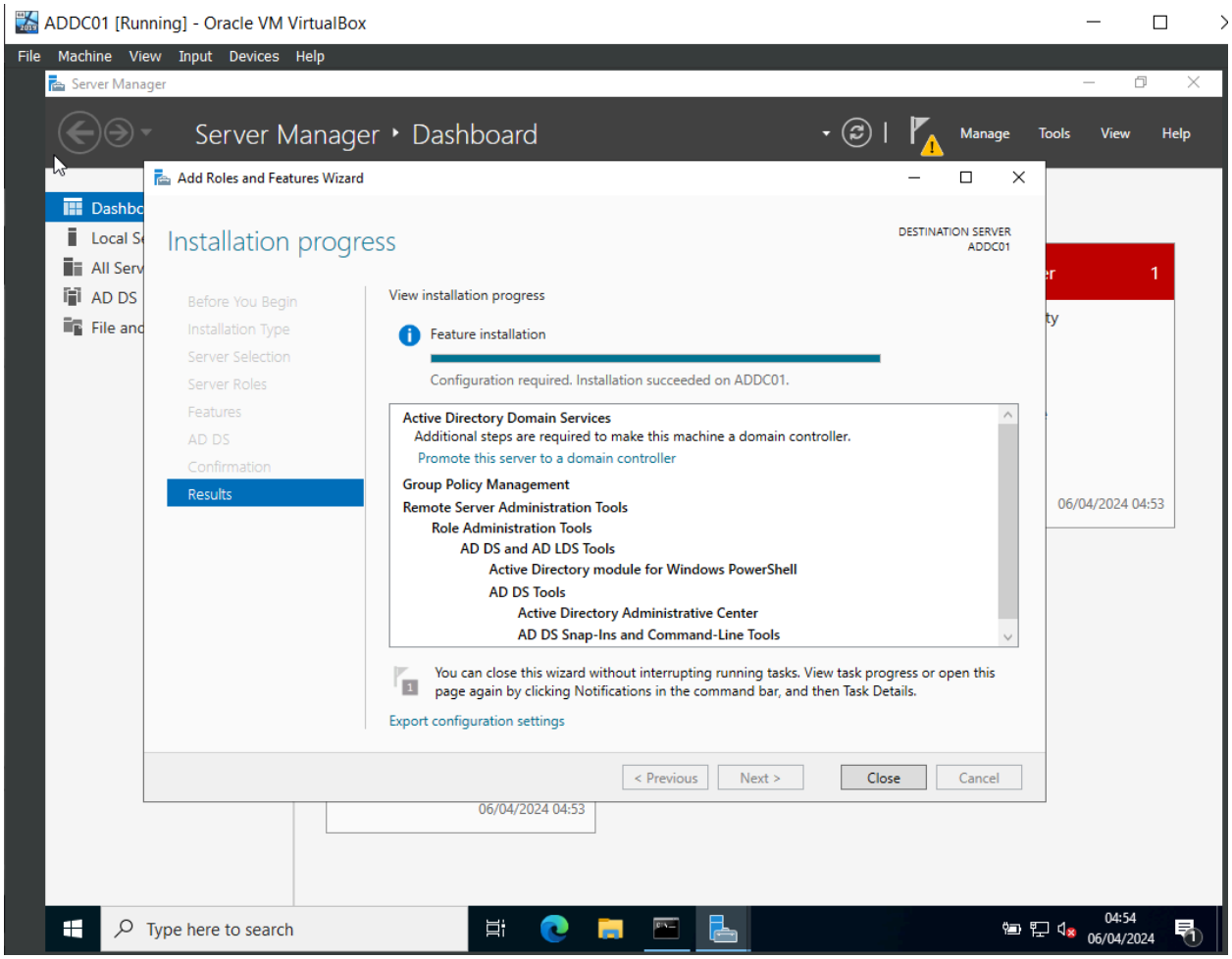
Step 17:
Navigate to **search and reporting**
Search: **index=endpoint**



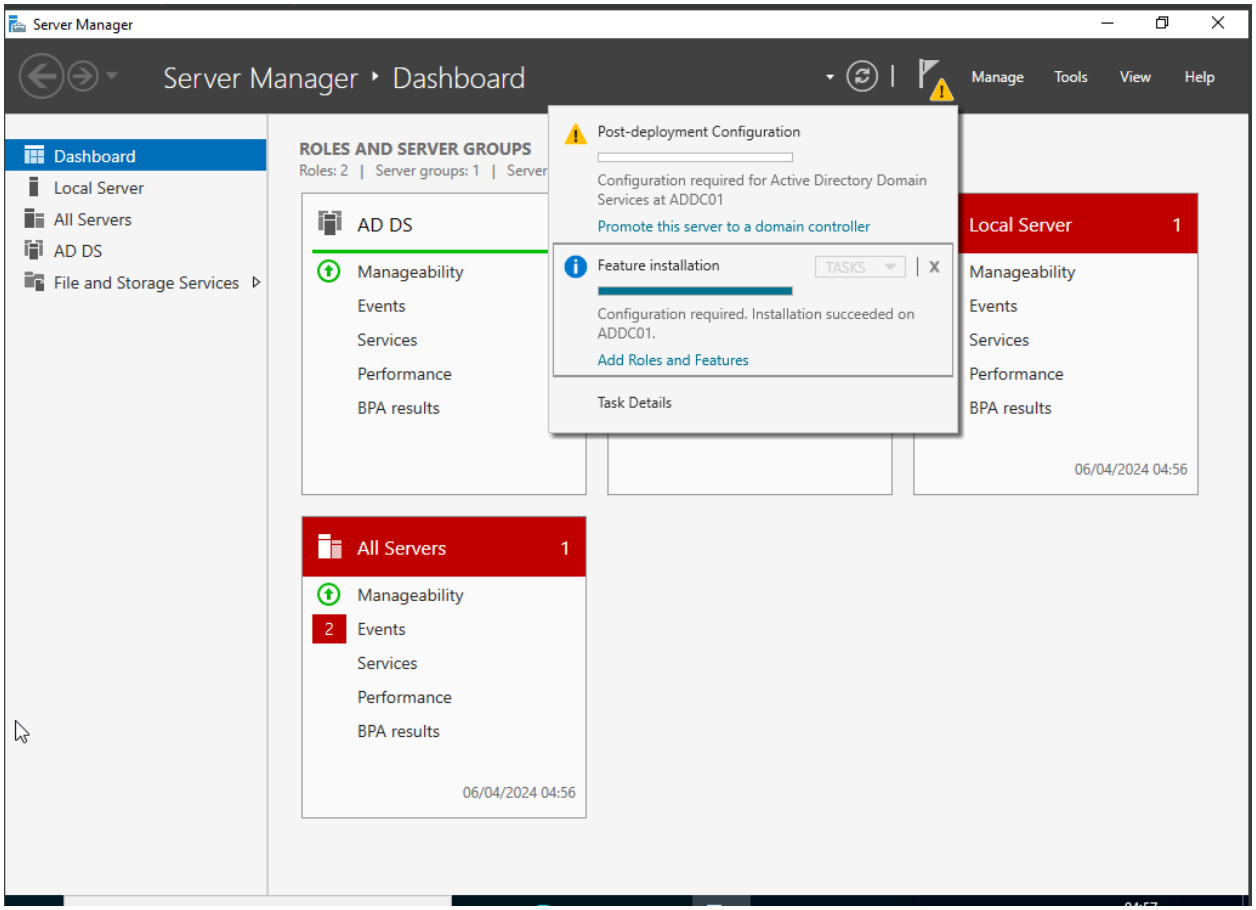
Step 18:
On windows server
Perform **step 13** to **step 15** to download install both sysmon and splunk universal forwarder



Step 19:
On Windows Server Machine
Open Server Manager
Navigate to **Manage** > **Add Roles and Features** > **Role-based or feature-based installation**
Select the **server** from **server pool** > **Select Active Directory Domain Services** > **Add Features** > **next** > **next** > **next** > **install**

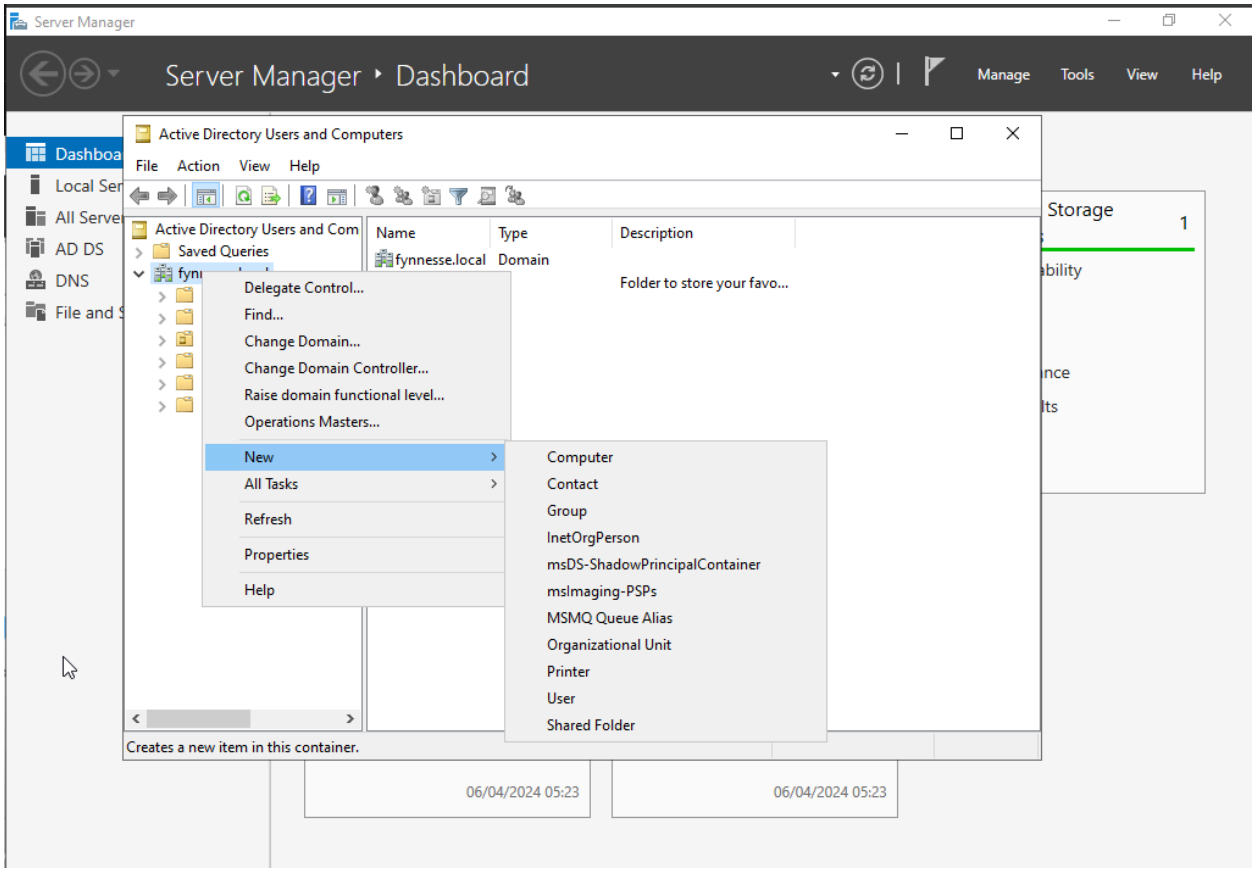


After Installation Navigate to **Notifications** > **Promote this server to a domain controller**

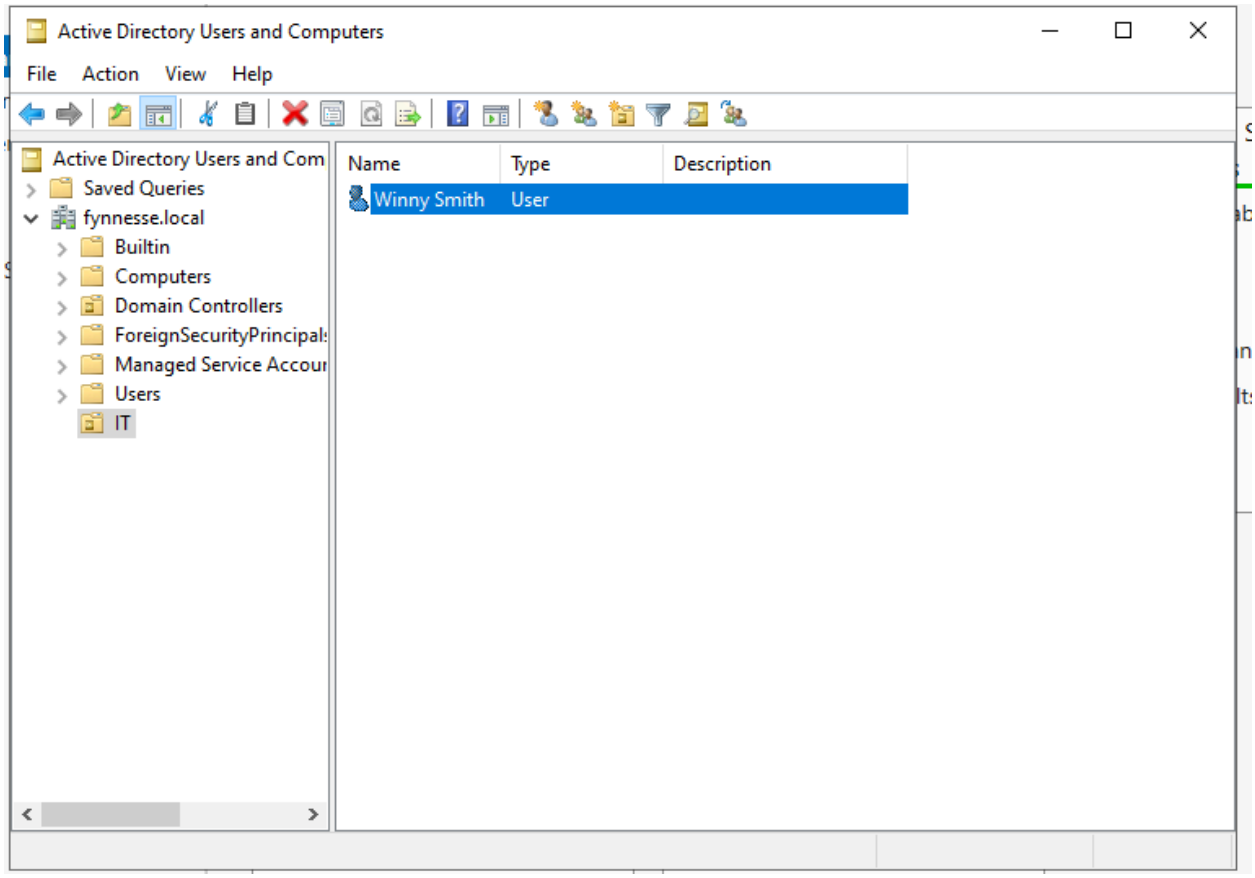


Select Add a new forest. Add a domain name with a top level domain eg [domain name].local
Click **Next** > Input Password > **Next** > **Next** > **Next** > **Next** > **Next** >**Install**
After installation Server would restart

Step 20:
We want to create users
Navigate to **Server Manager** > **Tools** > **Active Directory User and Computers**
Right click the domain > **New** > **Organizational Unit** > Name unit [Random] ie IT



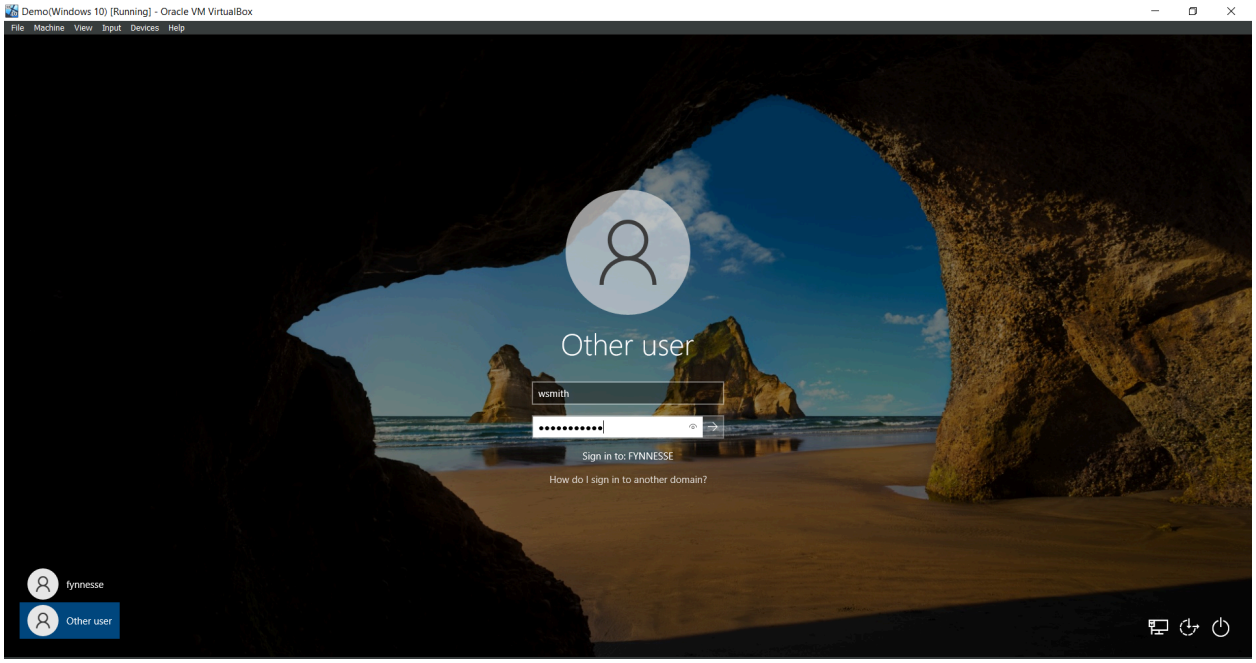
After creation > Right click it > **New** > **User** > Fill details as required > **Next** > Input Password > **Next** > **Finish.**



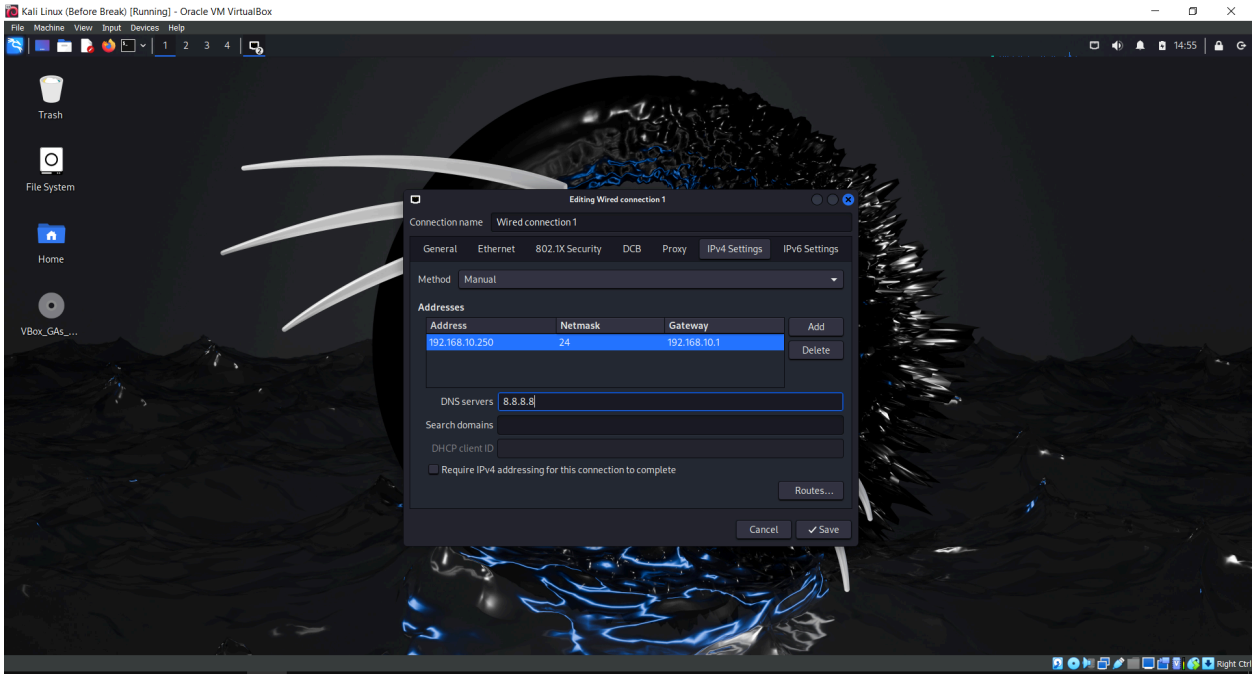
Repeat **Step 20** to create another user in another unit

Step 21:
On Target Machine
Navigate to open **Network & internet settings** > **Change adapter options** > **Right click adapter and select Properties** > **Select IPV4** > Change dns server address to domain controller
Navigate to **PC** and select **properties** > **Advanced system settings** > **Computer name** > **Change** > **Select Domain** > Input domain name from controller > **OK**
Input Username and password > **Ok**

After domain has been joined reboot system and log in with user credentials created on server



Step 22:
On Kali linux machine
We want to set up a static address as per your logical diagram.
Right click the ethernet icon at the top and select edit connections.
Select the first profile and select cog icon > **IPV4 settings**
Under the drop-down change the settings to manual > **add** > IP=192.168.10.250, netmask= /24, gateway=192.168.10.1, dns server=8.8.8.8 > Save



To reflect the changes:
Click **ethernet icon** > **disconnect**
Click **ethernet icon** > **wired connections1**

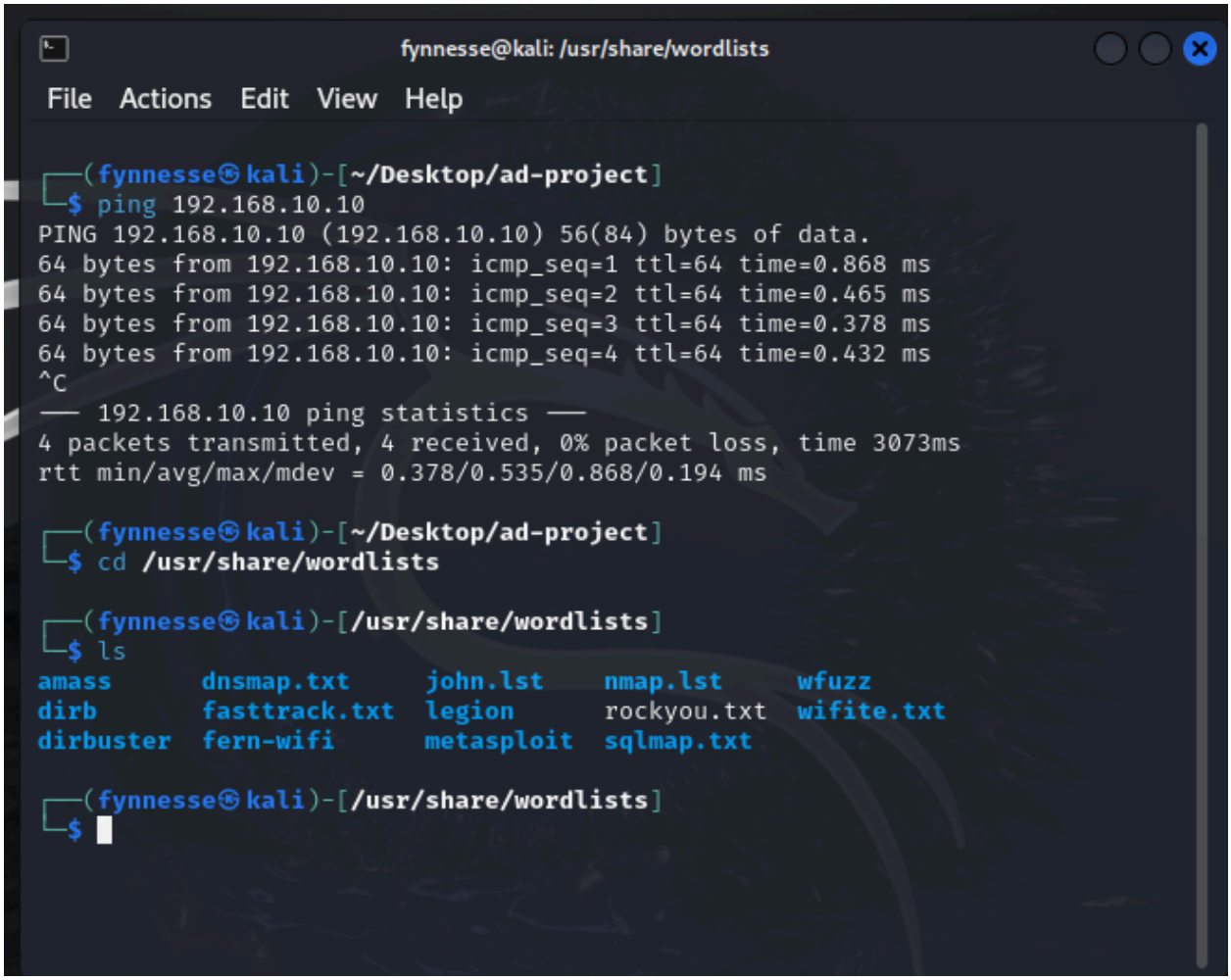
Now lets update and upgrade our repositories
Open terminal:
Sudo apt-get update && sudo apt-get upgrade -y

Attack Setup

Open terminal:
Create a new directory
Mkdir ad-project

For attack we use crowbar
Sudo apt-get install -y crowbar

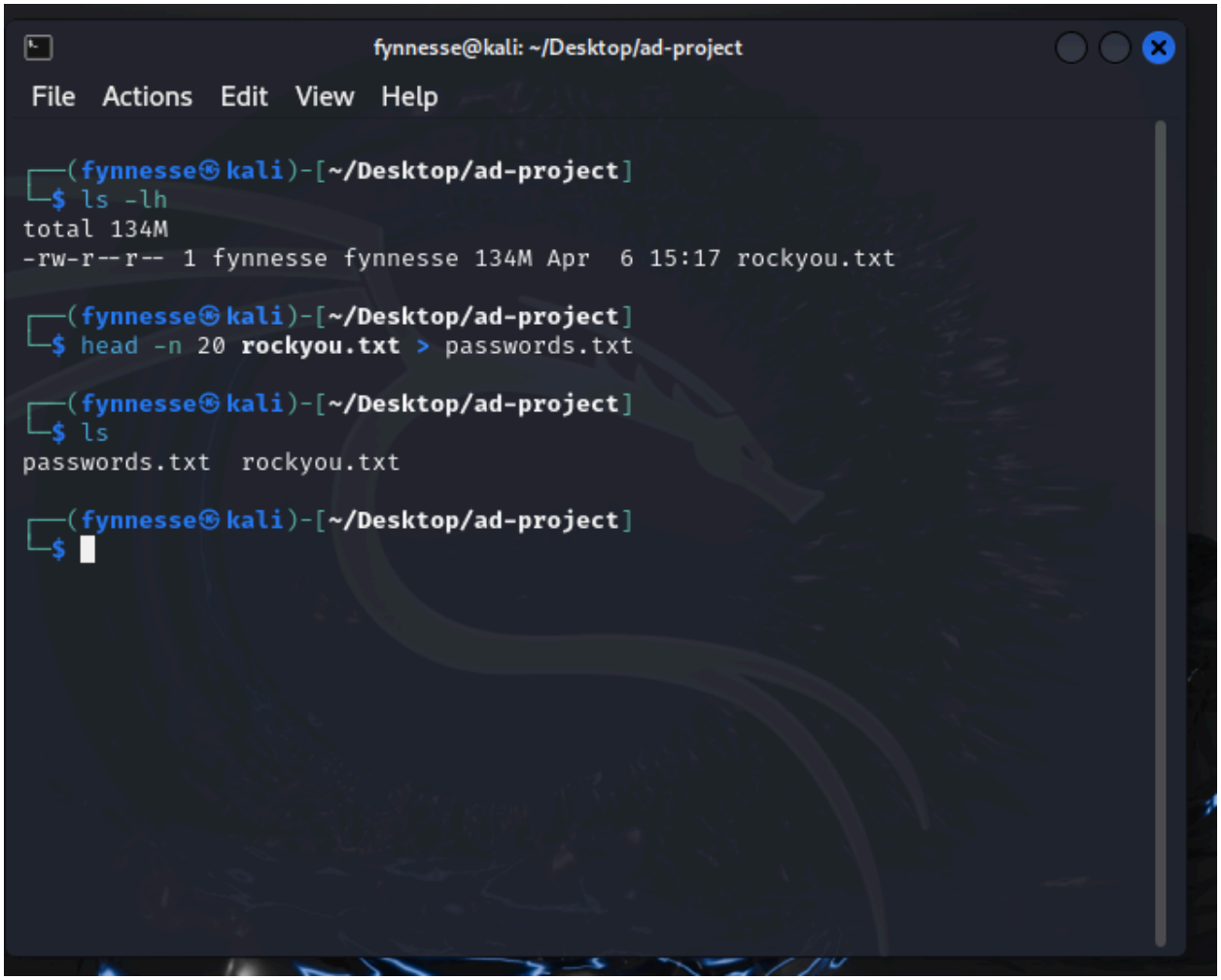
We would use rockyou for our bruteforce attack
Open terminal> **cd /usr/shar/wordlists/**
Sudo gunzip rockyou.txt.gz



Copy rockyou to ad-project directory
Cp rockyou.txt ~/Desktop/ad-project

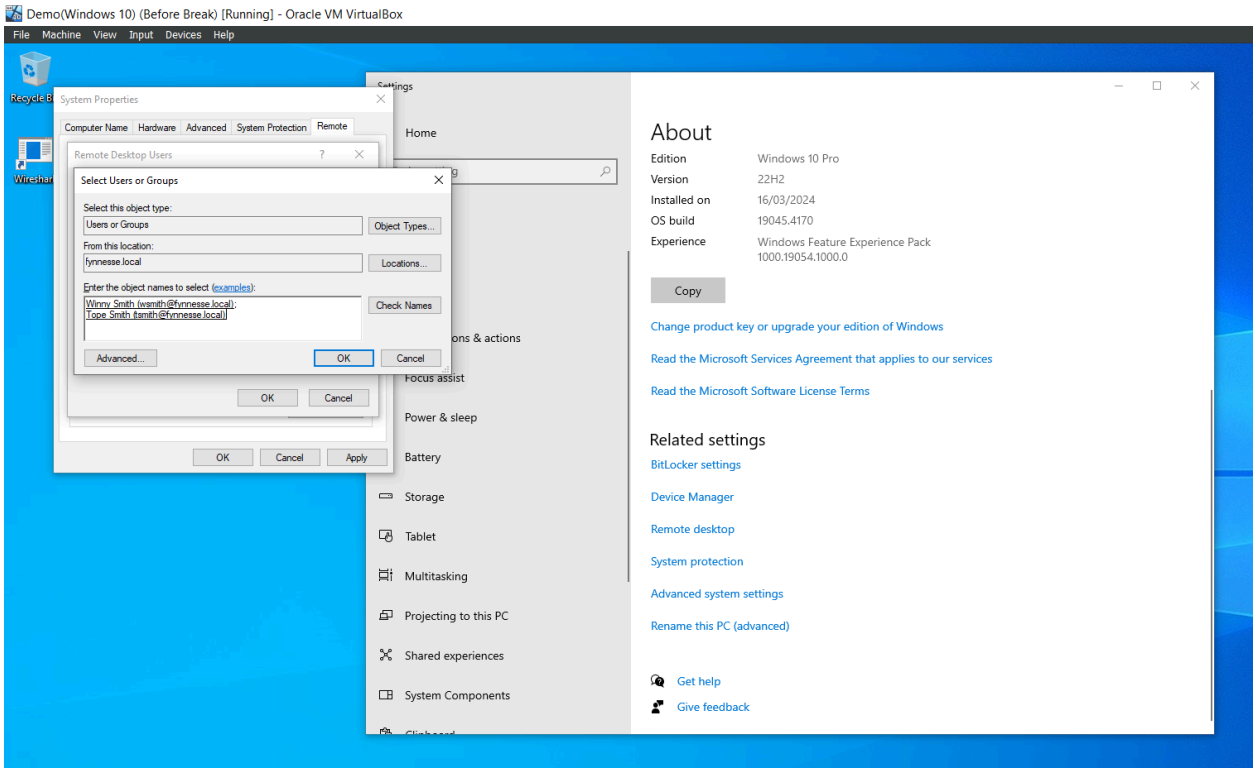
Navigate to ad-project Directory
Cd ~/Desktop/ad-project

Parse the first 20 lines from rockyou.txt to new file
Head -n 20 rockyou.txt > passwords.txt



Nano passwords.txt
At the end of the passwords.txt add the password of your windows target machine

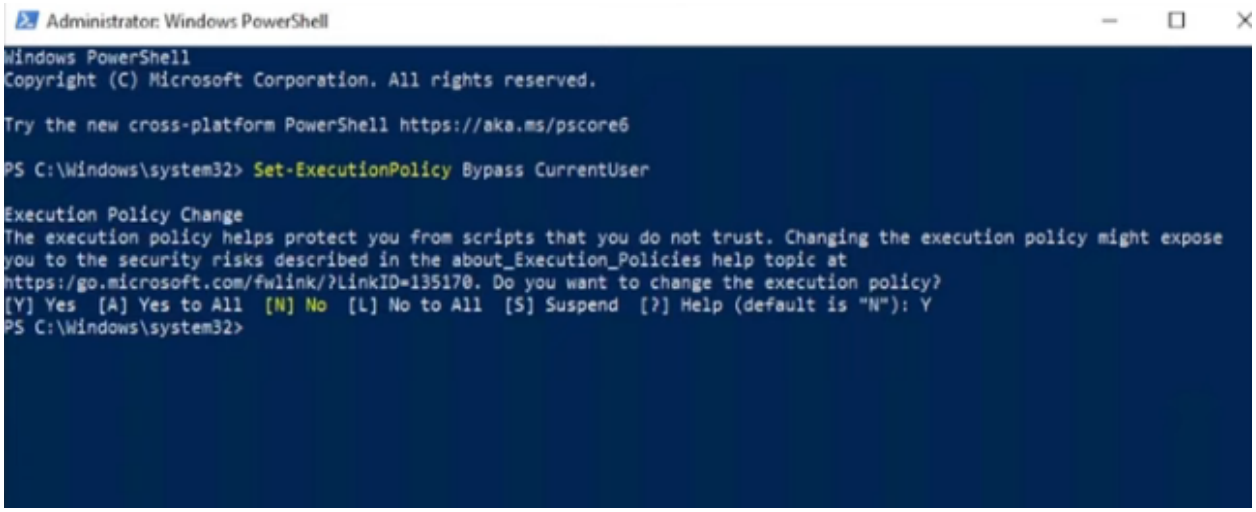
Step 23:
On Windows Target virtual machine
Search **PC** > **Properties** > **Advanced system settings** > log in with admin account > Remote> **Allow remote connections to this computer** > **users** > **add** > Add two users created to the object field > **Check Names > OK** > **OK** > **Apply** > **OK**



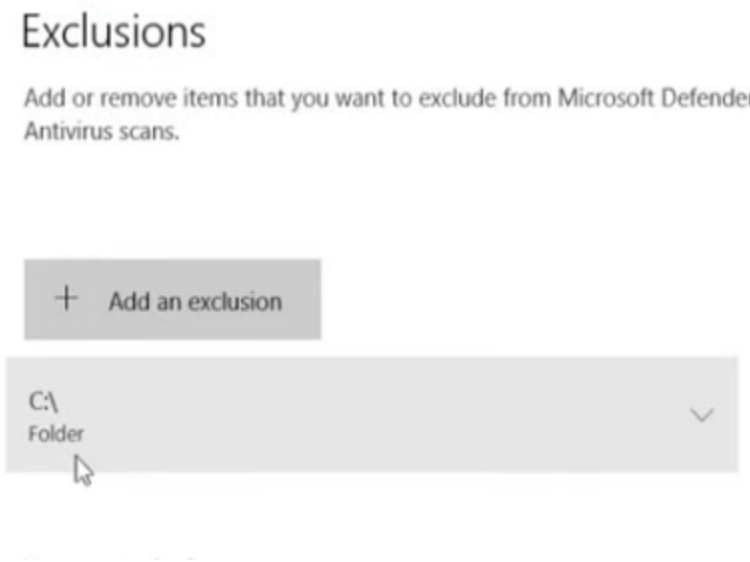
Step 24:
On Kali Linux virtual Machine
Open terminal
cd ad-project
crowbar -b rdp -u [account name] -C passwords.txt -s [Target machine ip]/32

Step 25:
Navigate to Splunk
Navigate to **Search & reporting** > "**index=endpoint**" **[Account name]** and select last 15 mins
Navigate to **Event code** > **4625**

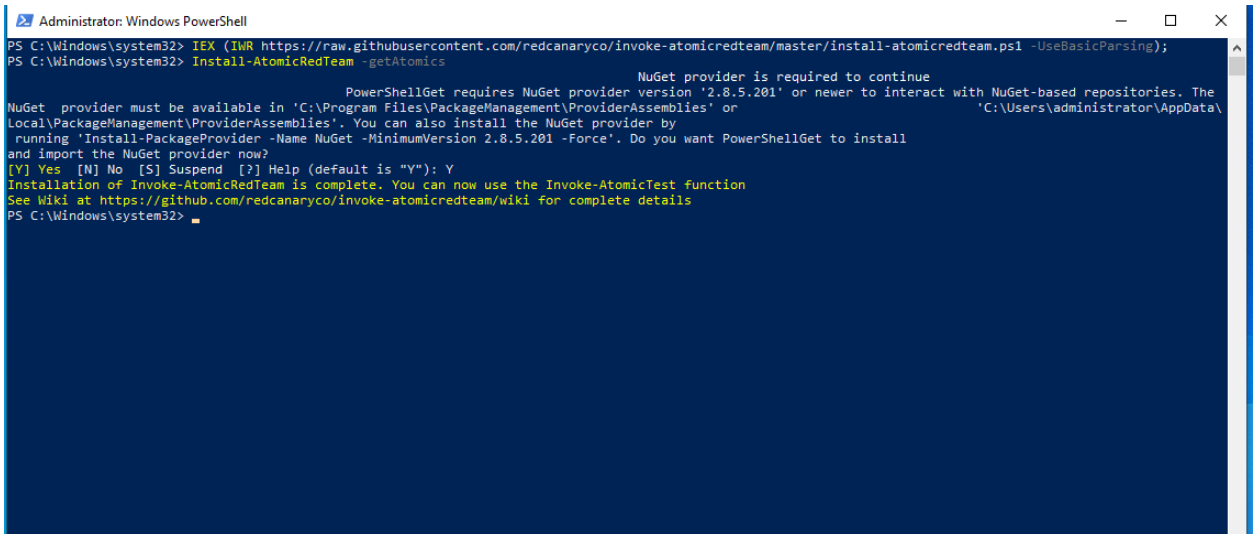
Step 26:
On target Machine
Open powershell with admin priv
Set-ExecutionPolicy Bypass CurrentUser > Y



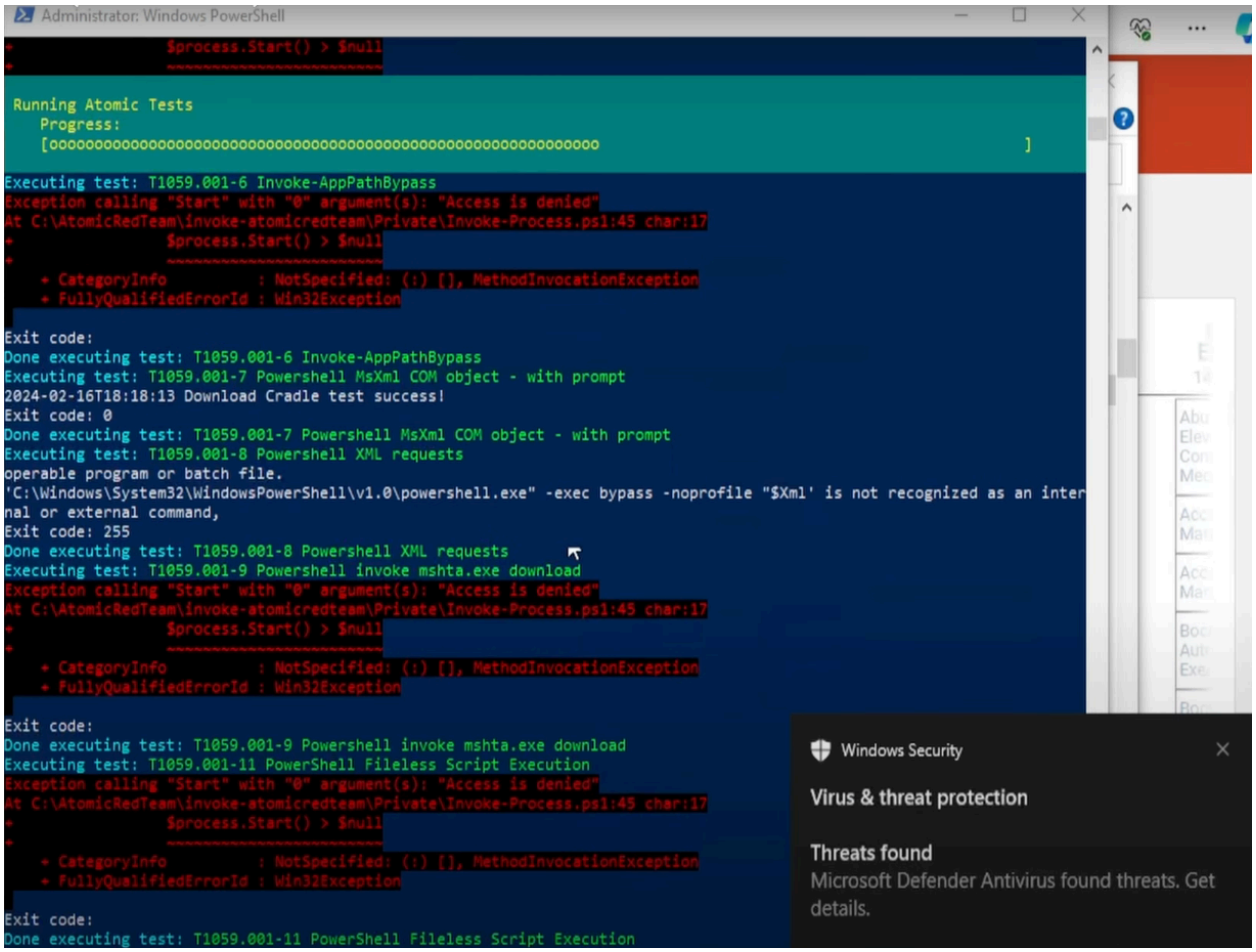
Atomic red team would be identified as a virus so we want to make an exclusion for where it would be installed
Navigate to **windows security** > **Virus & threat protection** > **Manage settings** > **Add or remove exclusions** > **Add an exclusion** > **Folder** > Select **C drive** > **Select Folder**



On Powershell with Admin Priv.
Atomic Red Team Powershell Command:
IEX (IWR https://raw.githubusercontent.com/redcanaryco/invoke-atomicredteam/master/install-atomicredteam.ps1. -UseBasicParsing);
Install-AtomicRedTeam -getAtomics

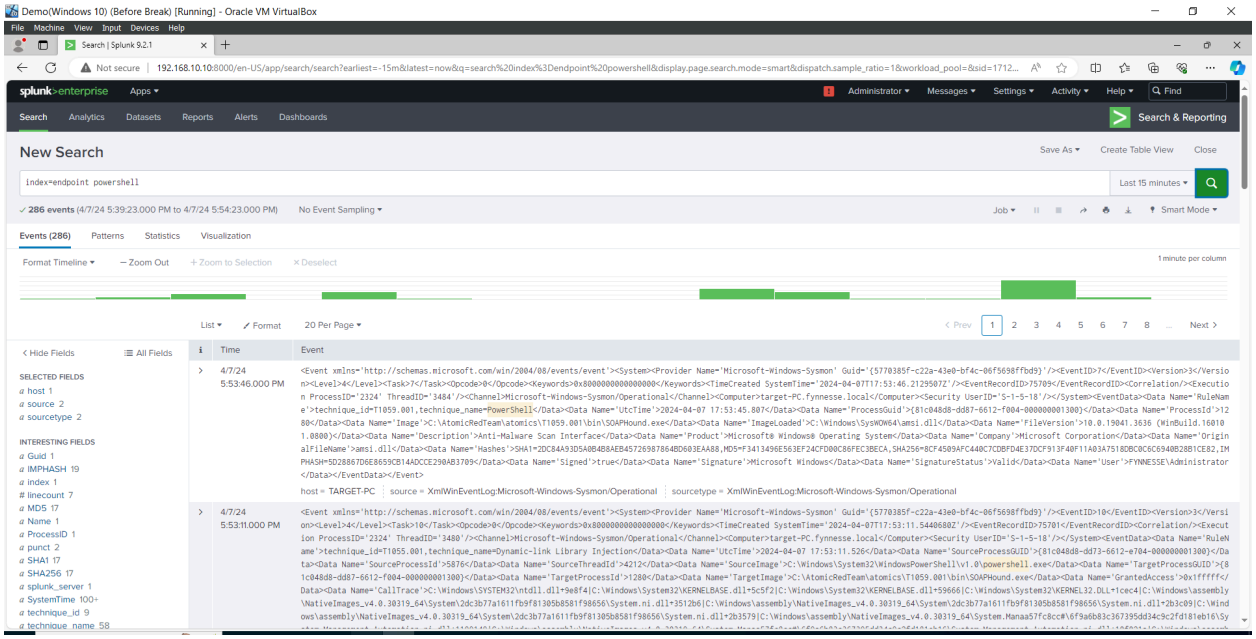


Step 27:
To use Atomic red team
Invoke-AtomicTest T1059.001



Open Splunk

Navigate to **Search & reporting** > **index=endpoint powershell**



This means we can build alerts to detect this activity in the future.