

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

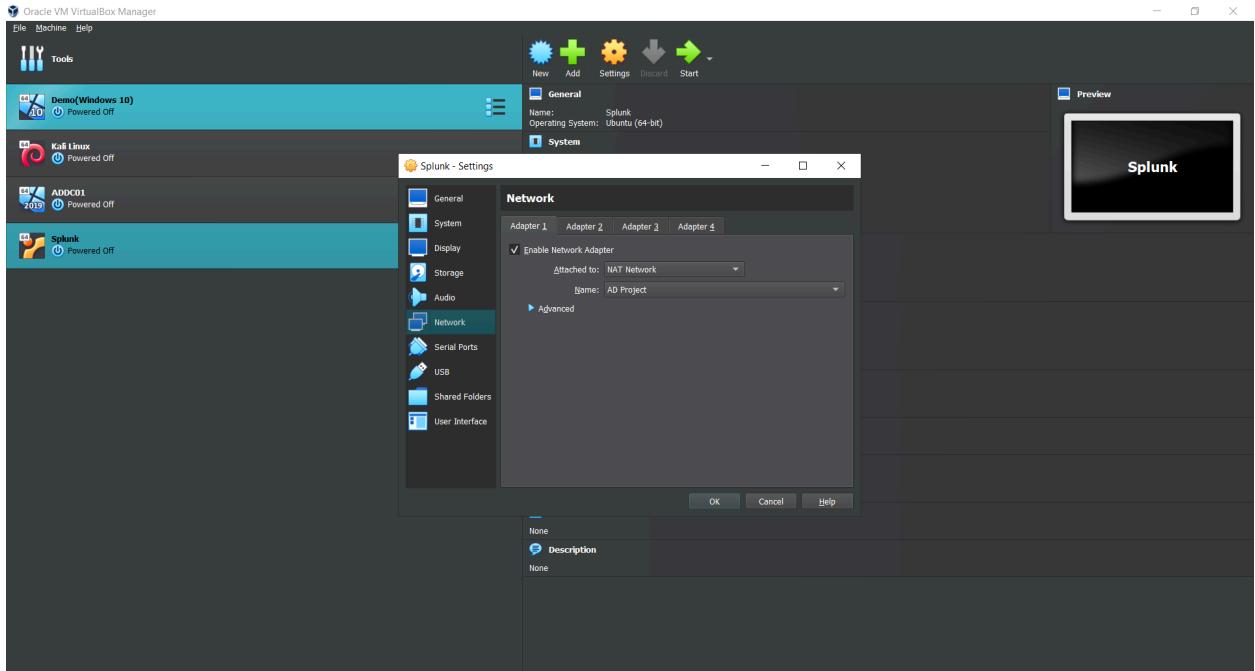
Step 6:

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

```
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 100
  link/ether 08:00:27:71:76:ab brd ff:ff:ff:ff:ff:ff
    inet 192.168.10.4/24 metric 100 brd 192.168.10.255 scope global dynamic enp0s3
      valid_lft 476sec preferred_lft 476sec
    inet6 fe80::a00:27ff:fe71:76ab/64 scope link
      valid_lft forever preferred_lft forever
fynnesse@splunk:~$ _
```

If ip's dont match, set a static ip

Navigate to **sudo nano /etc/netplan/00-installer-config.yaml**

Change default settings to:

```
GNU nano 6.2          /etc/netplan/00-installer-config.yaml *
# This is the network config written by 'subiquity'
network:
  ethernets:
    enp0s3:
      dhcp4: no
      addresses: [192.168.10.10/24]
      nameservers:
        addresses: [8.8.8.8]
    routes:
      - to: default
        via: 192.168.10.1
version: 2
```

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/>

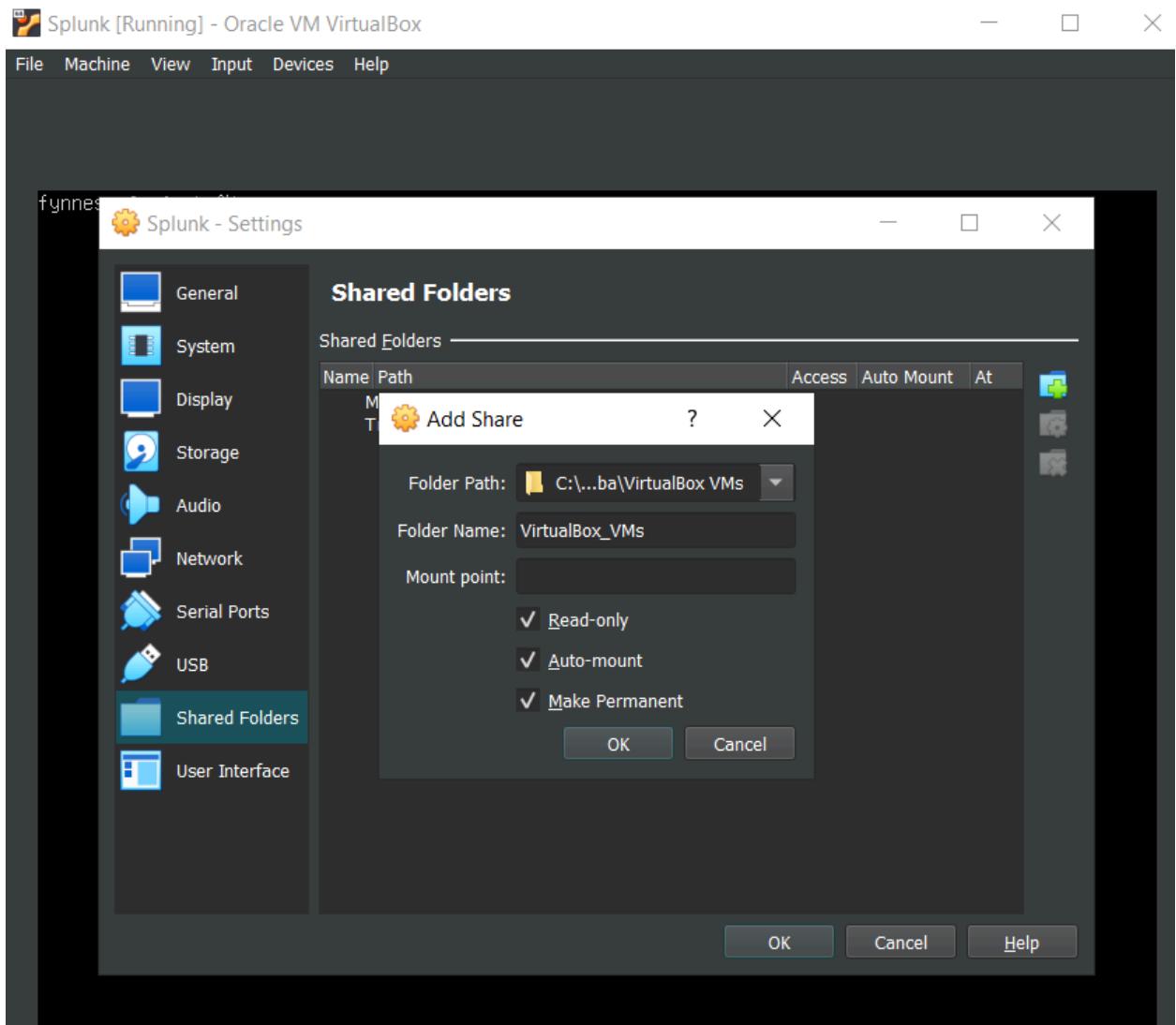
Step 10:

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**



Step 11:

Add user into vboxsf

Sudo adduser [username] vboxsf

```
Fyynnesse@splunk:~$ sudo adduser fynnesse vboxsf
[sudo] password for fynnesse:
adduser: The group `vboxsf' does not exist.
fynnesse@splunk:~$
```

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]**

```
File Machine View Input Devices Help
fynnesse@splunk:~$ cd share
fynnesse@splunk:~/share$ ls -la
total 532868
drwxrwxrwx 1 fynnesse fynnesse      0 Apr  5 13:58  .
drwxr-x--- 5 fynnesse fynnesse    4096 Apr  5 14:18  ..
drwxrwxrwx 1 fynnesse fynnesse      0 Apr  5 13:10  ADDCO1
drwxrwxrwx 1 fynnesse fynnesse      0 Apr  5 13:10  'Demo(Windows 10)'
drwxrwxrwx 1 fynnesse fynnesse      0 Apr  5 13:10  'Kali Linux'
drwxrwxrwx 1 fynnesse fynnesse      0 Apr  5 14:14  Splunk
-rw-rw-r-- 1 fynnesse fynnesse 545652596 Apr  5 13:46  splunk-9.2.1-78803f08aabb-linux-2.6-amd64.deb
fynnesse@splunk:~/share$ sudo dpkg -i splunk-9.2.1-78803f08aabb-linux-2.6-amd64.deb
Selecting previously unselected package splunk.
(Reading database ... 97440 files and directories currently installed.)
Preparing to unpack splunk-9.2.1-78803f08aabb-linux-2.6-amd64.deb ...
Unpacking splunk (9.2.1+78803f08aabb) ...
Setting up splunk (9.2.1+78803f08aabb) ...
complete
fynnesse@splunk:~/share$
```

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**

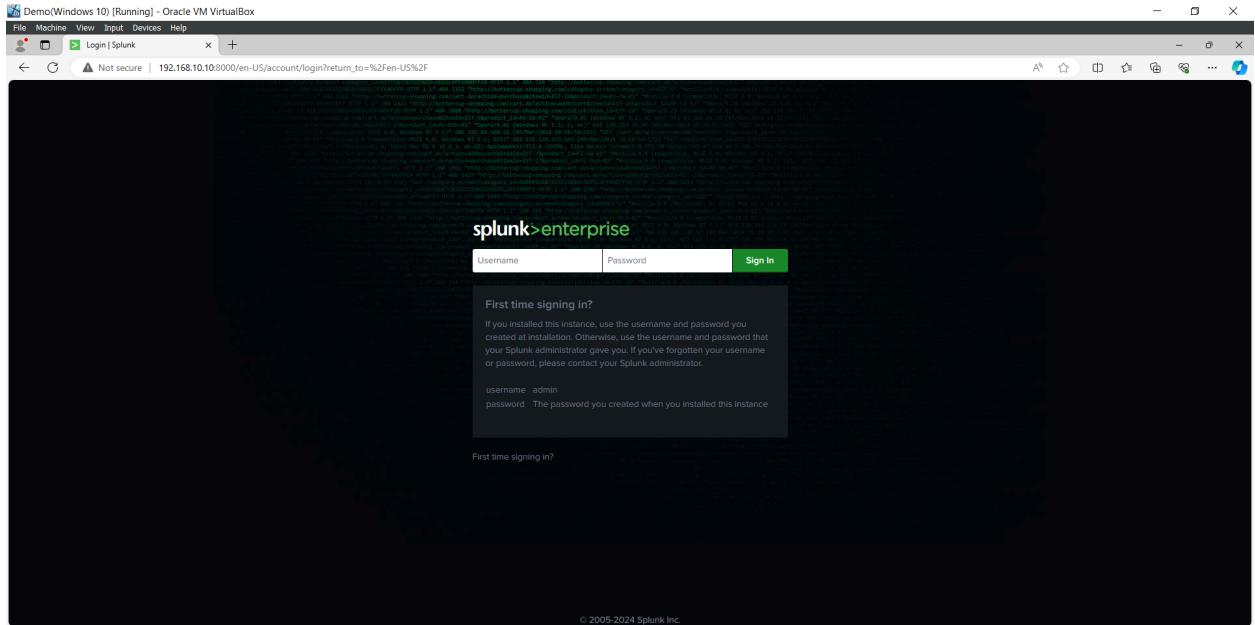
If it isn't right head to network & internet settings > change adapter options

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:

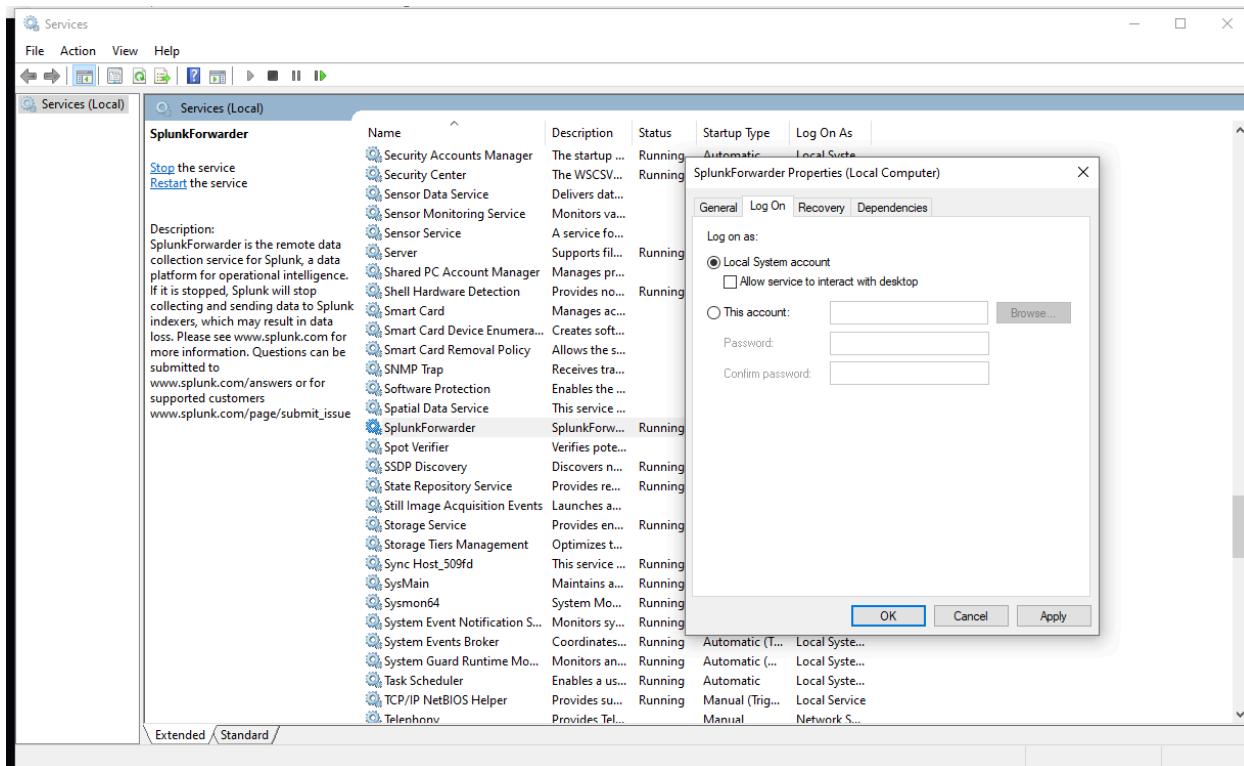
We need to instruct our splunk forwarder what we want to send to our splunk server. We must configure inputs.conf

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

The screenshot shows the Splunk interface with the following details:

- Search Bar:** index=endpoint
- Results Summary:** 5,089 events (4/4/24 6:00:00 PM to 4/5/24 6:11:08 PM) No Event Sampling
- Event Type:** Events (5,089)
- Timeline:** Format Timeline ▾ (Apr 4, 2024 6:00 PM) → (Apr 5, 2024 7:00 PM) 1 hour per column
- Host Selection:** host (Selected Yes)
- Event Details:** A large portion of the screen displays XML event data for the host 'TARGET-PC' across two time points: 6:10:56,000 PM and 4/5/24 6:10:51,000 PM. The XML includes provider information, process ID, thread ID, channel, computer name, security user ID, and various system and application data.

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

New Search

index=endpoint

6,141 events (4/4/24 7:00:00.000 PM to 4/5/24 7:16:25.000 PM) No Event Sampling Job Smart Mode

Last 24 hours

Events (6,141) Patterns Statistics Visualization

Format Timeline - Zoom Out + Zoom to Selection × Deselect 1 hour per column

host

2 Values, 100% of events Selected Yes No

Reports

Top values Top values by time Rare values

Events with this field

Values	Count	%
TARGET-PC	5,122	83.407%
ADDC01	1,019	16.593%

Type here to search 12:18 05/04/2024

Step 19:

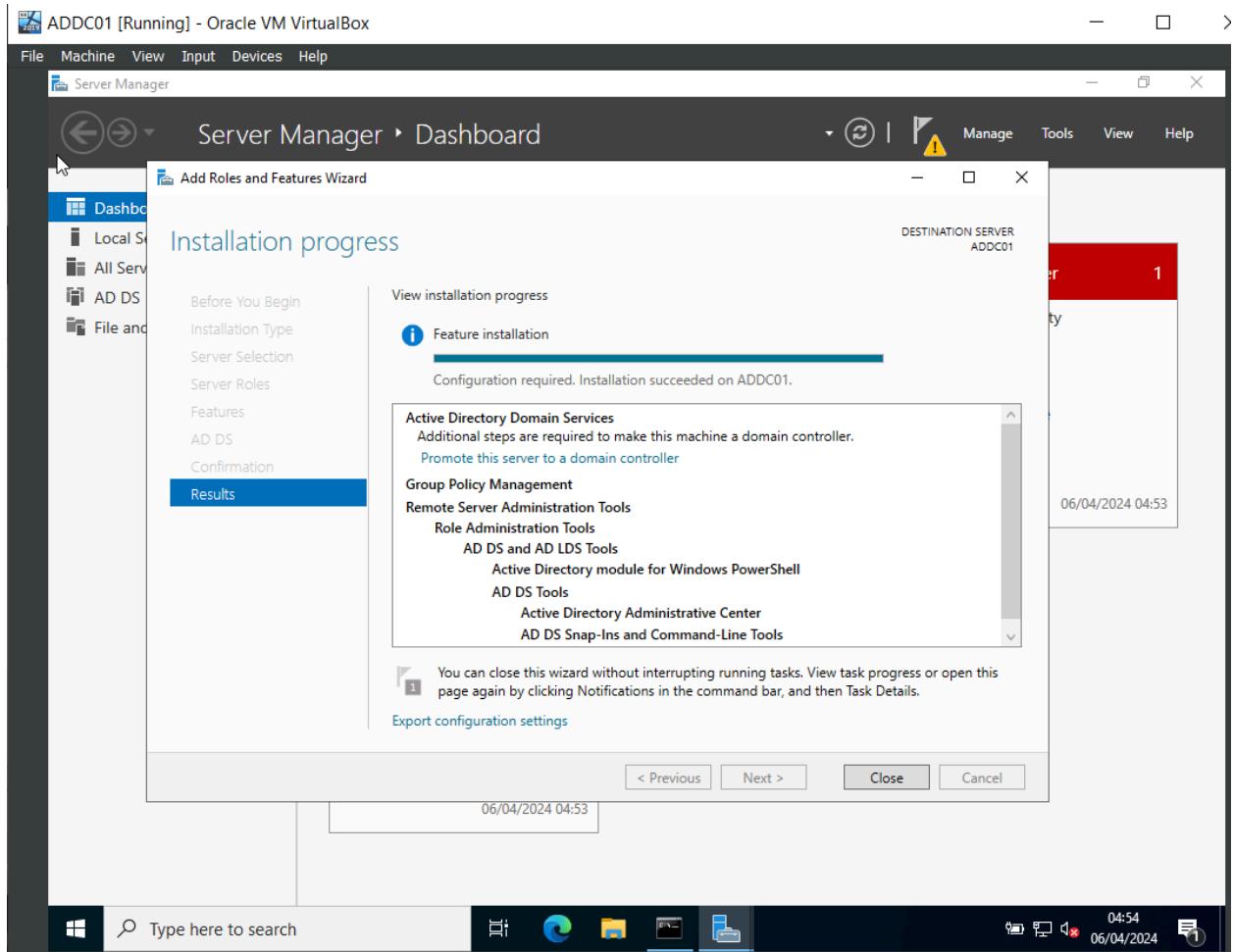
On Windows Server Machine

Open Server Manager

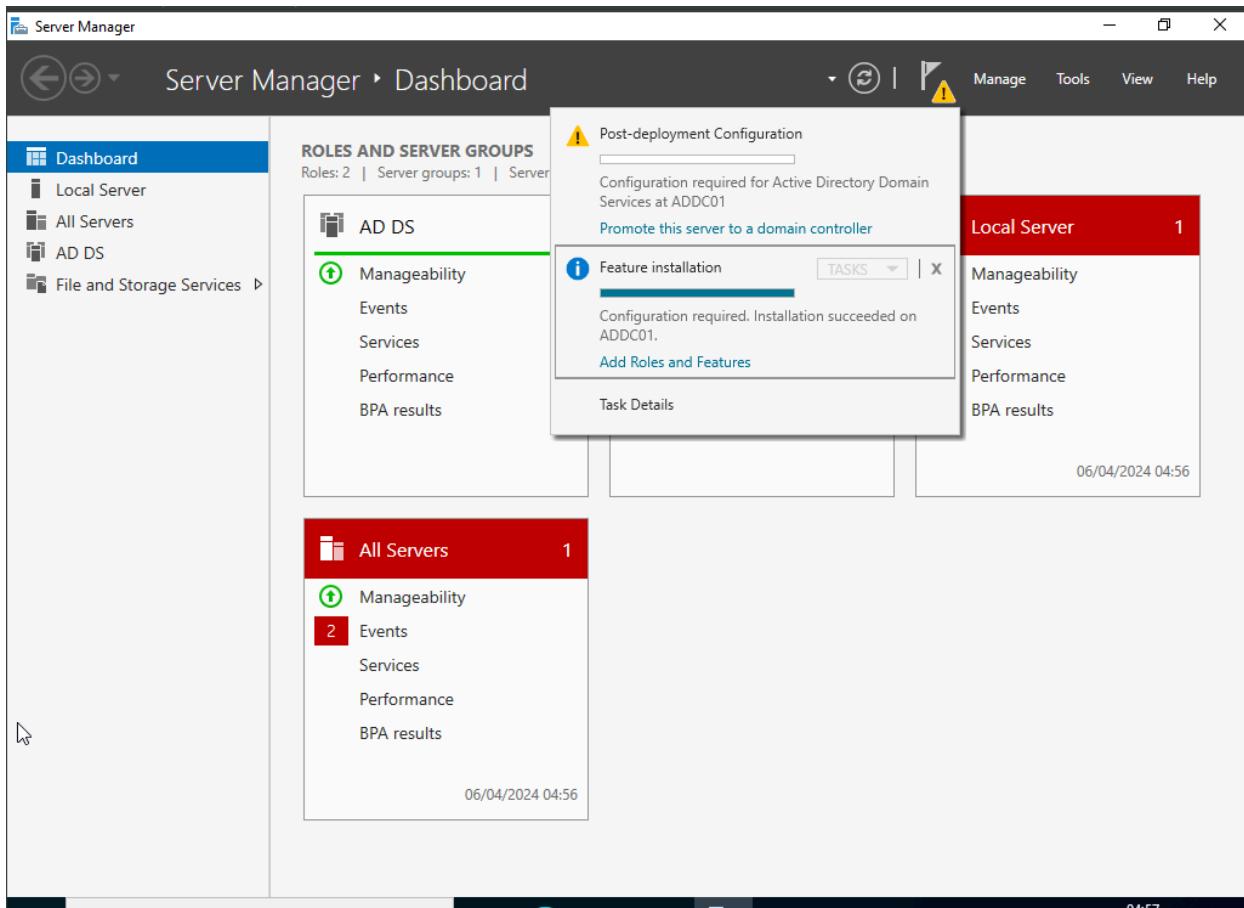
Navigate to **Manage > Add Roles and Features > Role-based or feature-based installation**

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** > **Install**

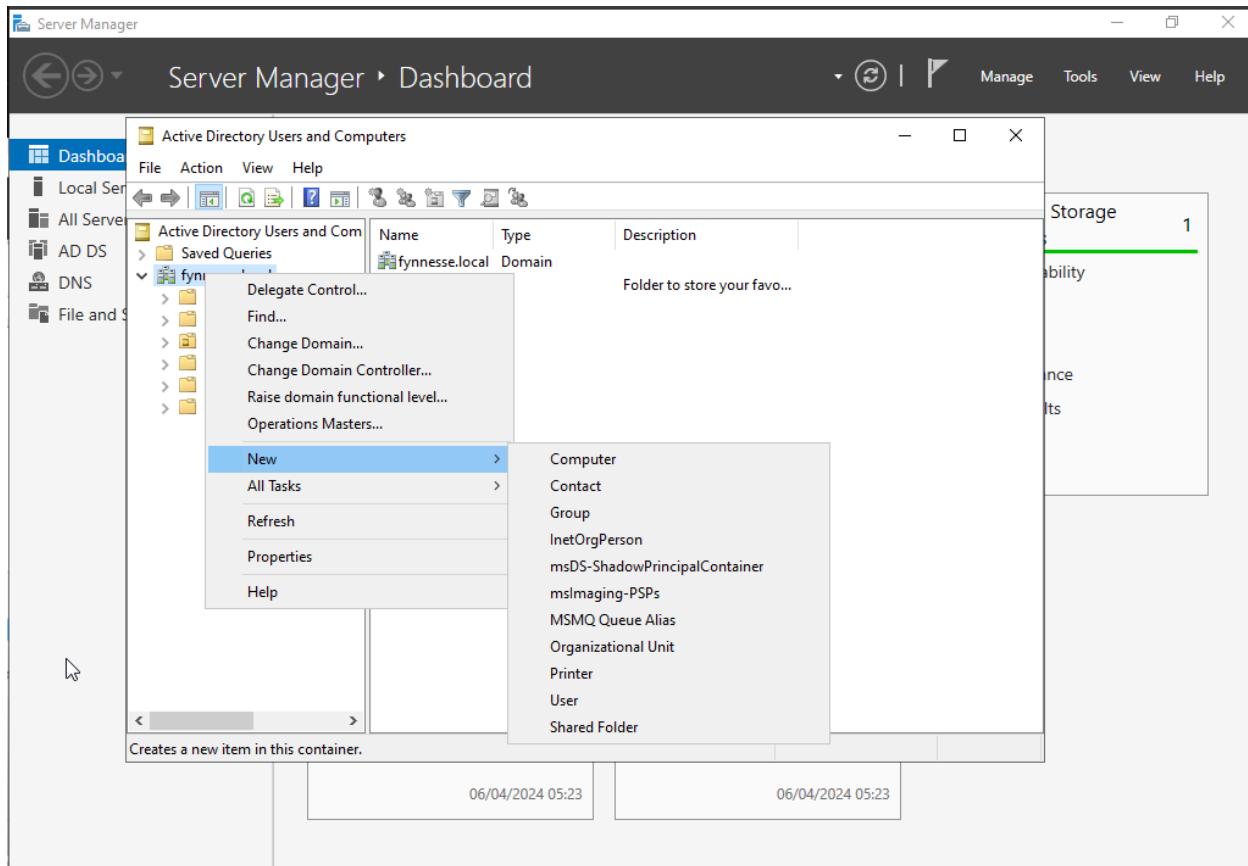
After installation Server would restart

Step 20:

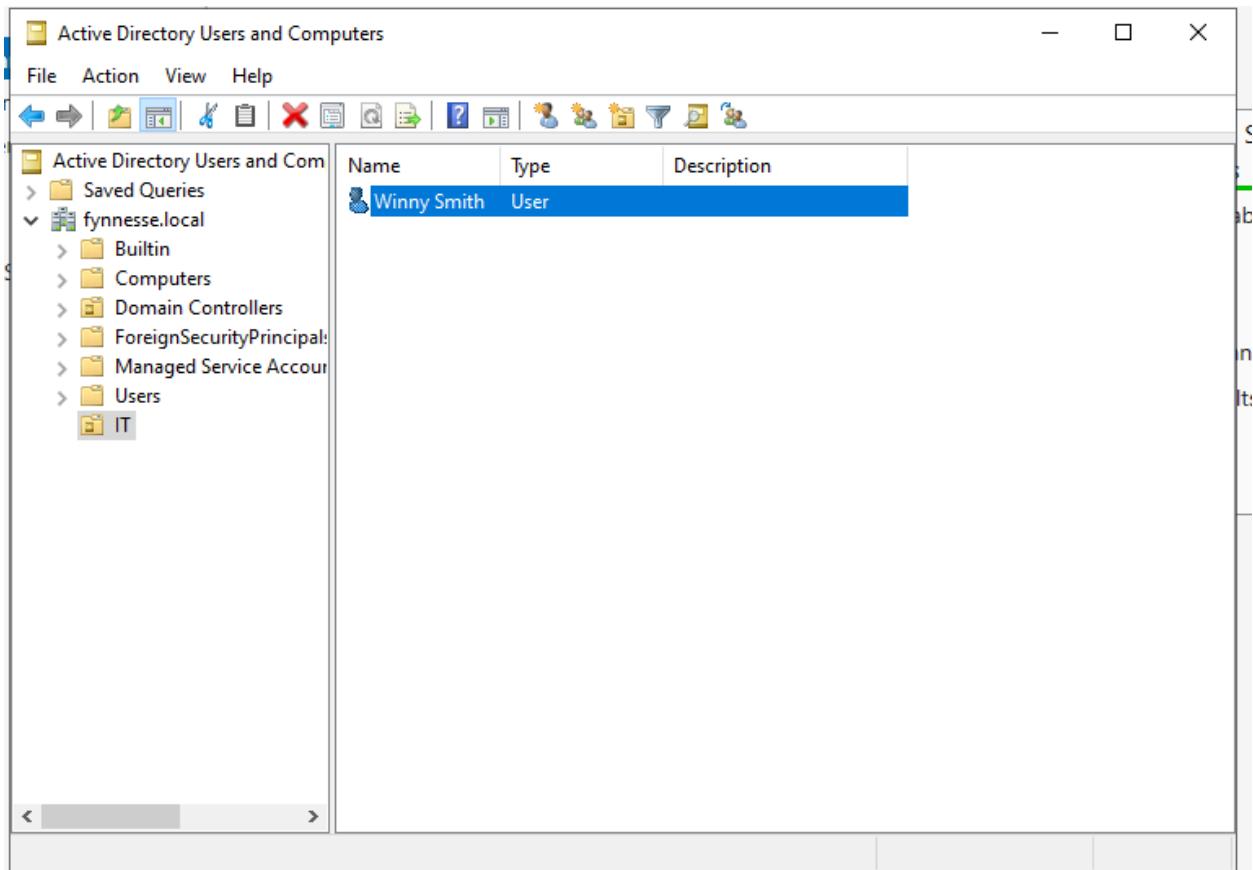
We want to create users

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:

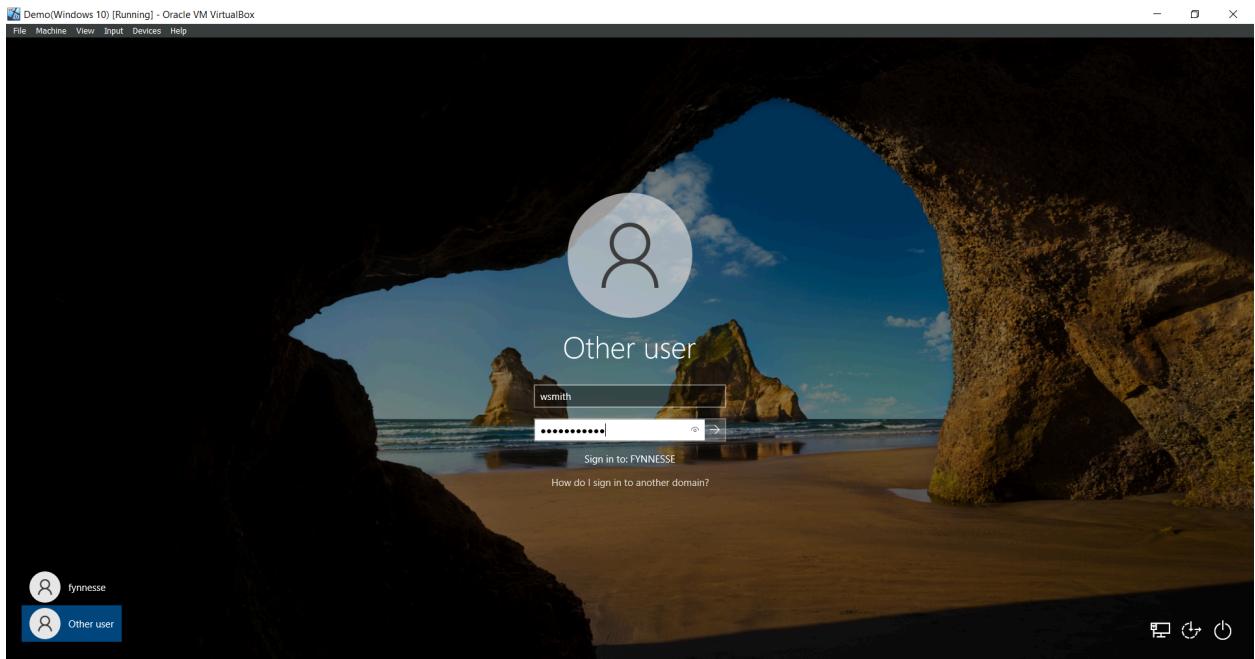
On Target Machine

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:

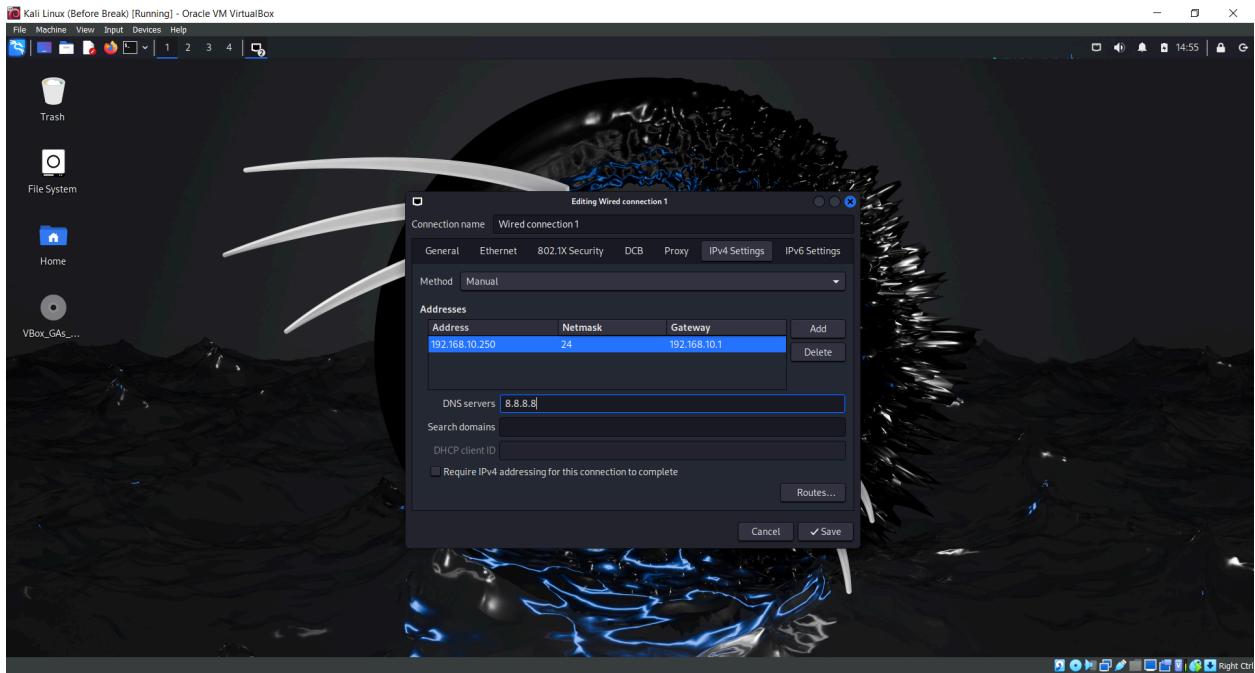
On Kali linux machine

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 **etherent icon > disconnect**

Click **etherent 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/share/wordlists/**

Sudo gunzip rockyou.txt.gz

fynnesse@kali: /usr/share/wordlists

```
(fynnesse㉿kali)-[~/Desktop/ad-project]
$ ping 192.168.10.10
PING 192.168.10.10 (192.168.10.10) 56(84) bytes of data.
64 bytes from 192.168.10.10: icmp_seq=1 ttl=64 time=0.868 ms
64 bytes from 192.168.10.10: icmp_seq=2 ttl=64 time=0.465 ms
64 bytes from 192.168.10.10: icmp_seq=3 ttl=64 time=0.378 ms
64 bytes from 192.168.10.10: icmp_seq=4 ttl=64 time=0.432 ms
^C
— 192.168.10.10 ping statistics —
4 packets transmitted, 4 received, 0% packet loss, time 3073ms
rtt min/avg/max/mdev = 0.378/0.535/0.868/0.194 ms

(fynnesse㉿kali)-[~/Desktop/ad-project]
$ cd /usr/share/wordlists

(fynnesse㉿kali)-[/usr/share/wordlists]
$ ls
amass      dnsmap.txt    john.lst     nmap.lst    wfuzz
dirb       fasttrack.txt legion      rockyou.txt wifite.txt
dirbuster  fern-wifi     metasploit  sqlmap.txt

(fynnesse㉿kali)-[/usr/share/wordlists]
$ █
```

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

```
fynnesse@kali: ~/Desktop/ad-project
File Actions Edit View Help
(fynnesse@kali)-[~/Desktop/ad-project]
$ ls -lh
total 134M
-rw-r--r-- 1 fynnesse fynnesse 134M Apr  6 15:17 rockyou.txt

(fynnesse@kali)-[~/Desktop/ad-project]
$ head -n 20 rockyou.txt > passwords.txt

(fynnesse@kali)-[~/Desktop/ad-project]
$ ls
passwords.txt  rockyou.txt

(fynnesse@kali)-[~/Desktop/ad-project]
$
```

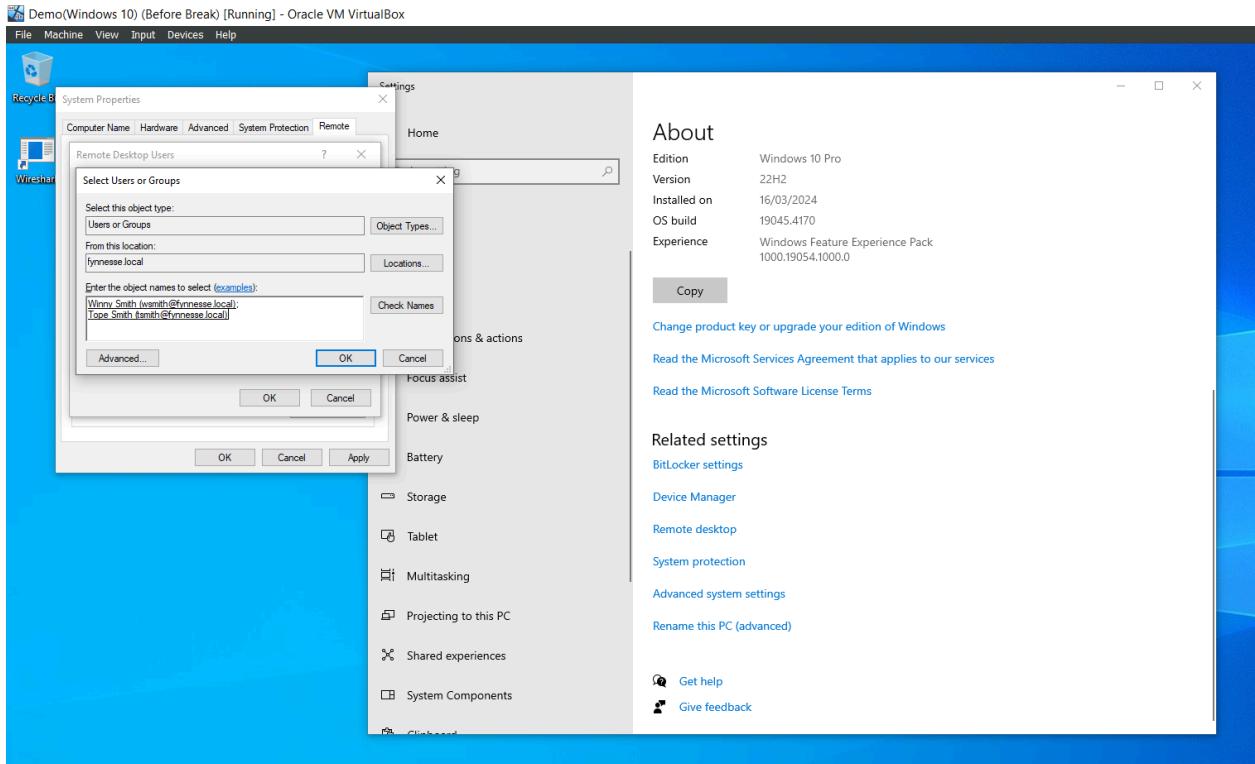
Nano passwords.txt

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

```
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> Set-ExecutionPolicy Bypass CurrentUser

Execution Policy Change
The execution policy helps protect you from scripts that you do not trust. Changing the execution policy might expose
you to the security risks described in the about_Execution_Policies help topic at
https://go.microsoft.com/fwlink/?LinkID=135170. Do you want to change the execution policy?
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "N"): Y
PS C:\Windows\system32>
```

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**

Exclusions

Add or remove items that you want to exclude from Microsoft Defender Antivirus scans.



On Powershell with Admin Priv.

Atomic Red Team Powershell Command:

IEX (IWR

**https://raw.githubusercontent.com/redcanaryco/invoke-atomicredteam/master/install-atomcredteam.ps1. -UseBasicParsing);
Install-AtomicRedTeam -getAtoms**

```
[Administrator: Windows PowerShell]
PS C:\Windows\system32> IEX (INR https://raw.githubusercontent.com/redcanaryco/invoke-atomicredteam/master/install-atomicredteam.ps1 -UseBasicParsing)
PS C:\Windows\system32> Install-AtomicRedTeam -getAtomsics
NuGet provider is required to continue
PowerShellGet requires NuGet provider version '2.8.5.201' or newer to interact with NuGet-based repositories. The
NuGet provider must be available in 'C:\Program Files\PackageManagement\ProviderAssemblies' or
Local\PackageManagement\ProviderAssemblies'. You can also install the NuGet provider by
running 'Install-PackageProvider -Name NuGet -MinimumVersion 2.8.5.201 -Force'. Do you want PowerShellGet to install
and import the NuGet provider now?
[Y] Yes [N] No [S] Suspend [?] Help (default is "Y"): Y
Installation of Invoke-AtomicRedTeam is complete. You can now use the Invoke-AtomicTest function
See Wiki at https://github.com/redcanaryco/invoke-atomicredteam/wiki for complete details
PS C:\Windows\system32>
```

Step 27:

To use Atomic red team

Invoke-AtomicTest T1059.001

```
[Administrator: Windows PowerShell]
+     $process.Start() > $null
+
+-----+
Running Atomic Tests
Progress:
[oooooooooooooooooooooooooooooooooooooooooooooooooooo]

Executing test: T1059.001-6 Invoke-AppPathBypass
Exception calling "Start" with "0" argument(s): "Access is denied"
At C:\AtomicRedTeam\invoke-atomicredteam\Private\Invoke-Process.ps1:45 char:17
+     $process.Start() > $null
+
+-----+
+ CategoryInfo          : NotSpecified: () [], MethodInvocationException
+ FullyQualifiedErrorId : Win32Exception

Exit code:
Done executing test: T1059.001-6 Invoke-AppPathBypass
Executing test: T1059.001-7 Powershell MsXml COM object - with prompt
2024-02-16T18:18:13 Download Cradle test success!
Exit code: 0
Done executing test: T1059.001-7 Powershell MsXml COM object - with prompt
Executing test: T1059.001-8 Powershell XML requests
operable program or batch file.
'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' -exec bypass -noprofile "$Xml" is not recognized as an internal
or external command,
Exit code: 255
Done executing test: T1059.001-8 Powershell XML requests
Executing test: T1059.001-9 Powershell invoke mshta.exe download
Exception calling "Start" with "0" argument(s): "Access is denied"
At C:\AtomicRedTeam\invoke-atomicredteam\Private\Invoke-Process.ps1:45 char:17
+     $process.Start() > $null
+
+-----+
+ CategoryInfo          : NotSpecified: () [], MethodInvocationException
+ FullyQualifiedErrorId : Win32Exception

Exit code:
Done executing test: T1059.001-9 Powershell invoke mshta.exe download
Executing test: T1059.001-11 PowerShell Fileless Script Execution
Exception calling "Start" with "0" argument(s): "Access is denied"
At C:\AtomicRedTeam\invoke-atomicredteam\Private\Invoke-Process.ps1:45 char:17
+     $process.Start() > $null
+
+-----+
+ CategoryInfo          : NotSpecified: () [], MethodInvocationException
+ FullyQualifiedErrorId : Win32Exception

Exit code:
Done executing test: T1059.001-11 PowerShell Fileless Script Execution
```



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

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