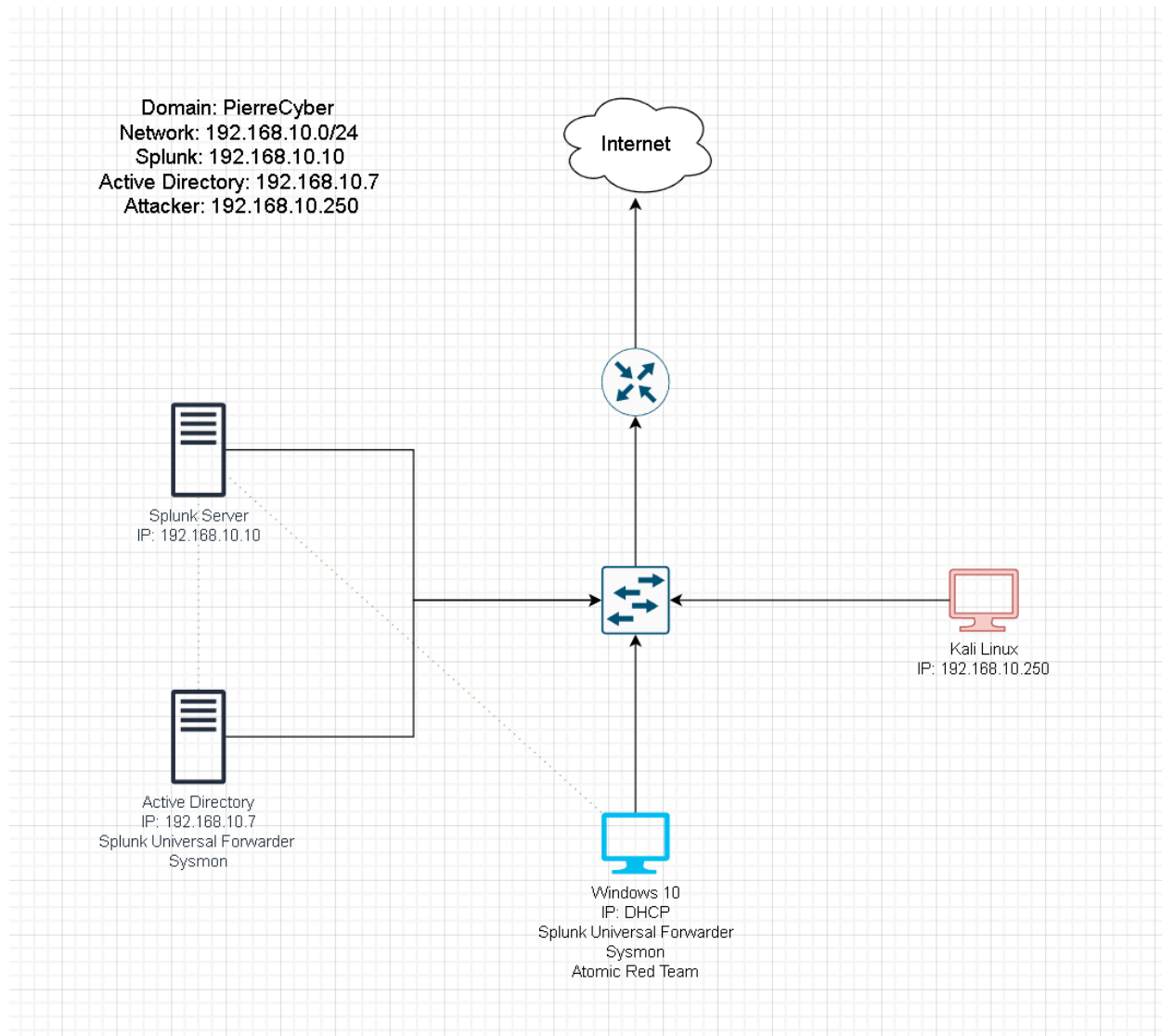
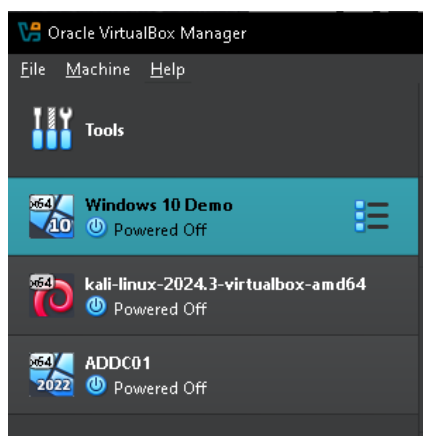


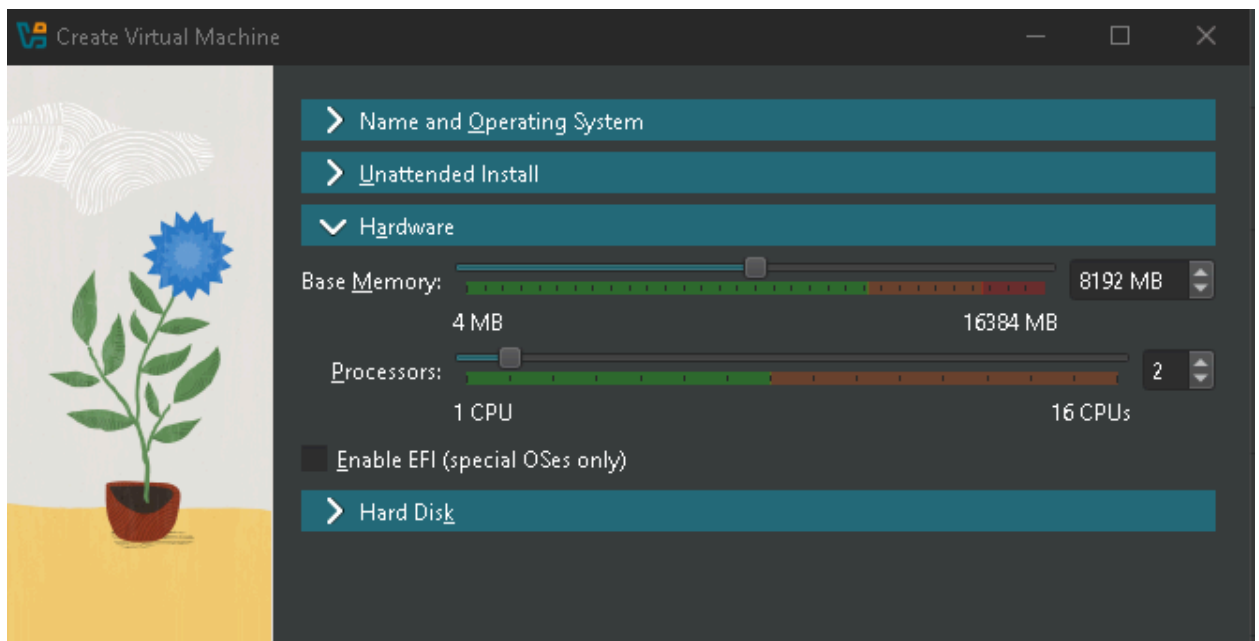
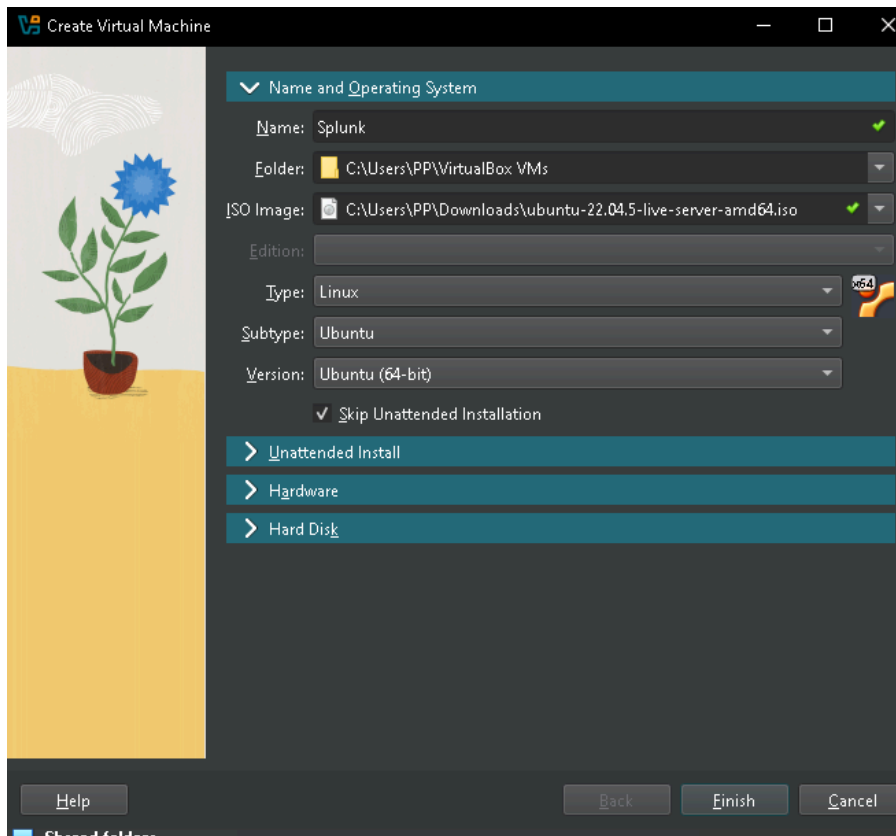
1. First, I made a logical diagram to visually map out how the lab is to be built.



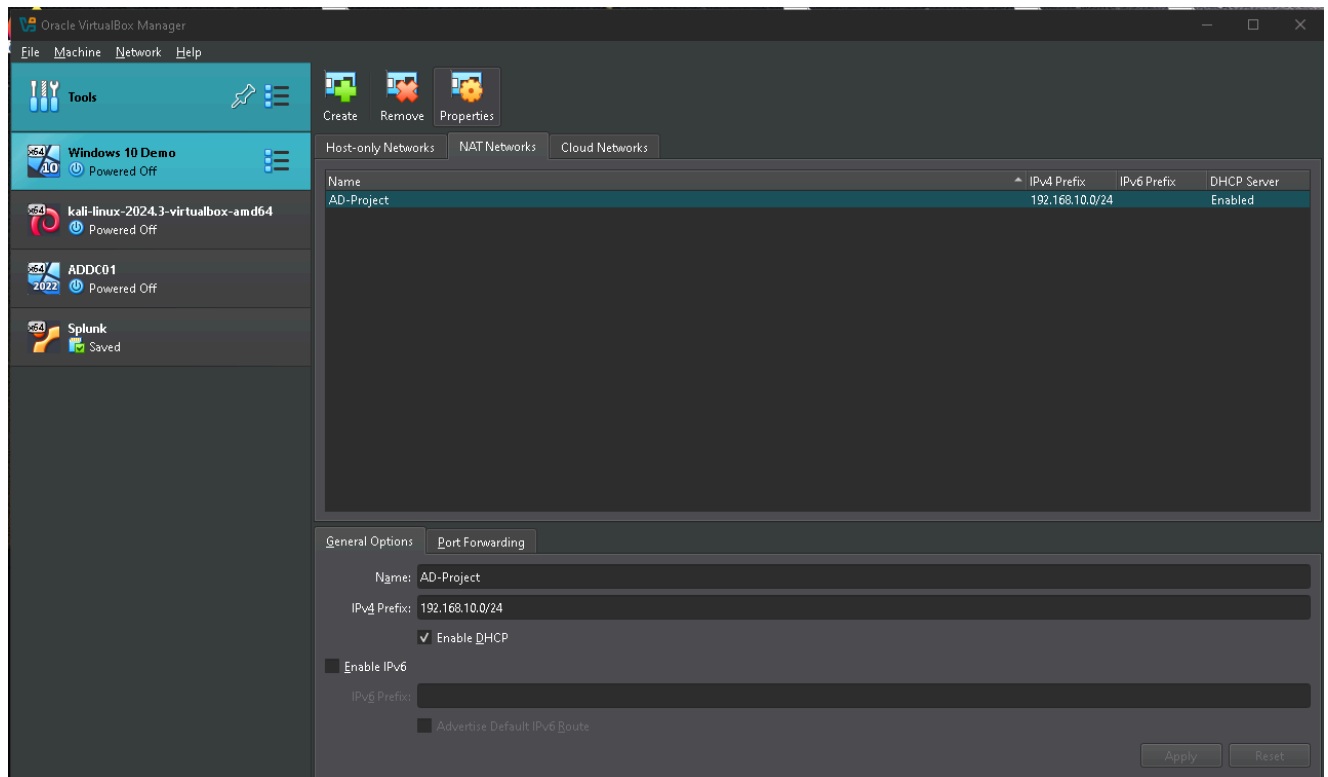
2. I used **Oracle VirtualBox** to install Windows 10, Kali Linux, and Windows server 2022 virtual machines.



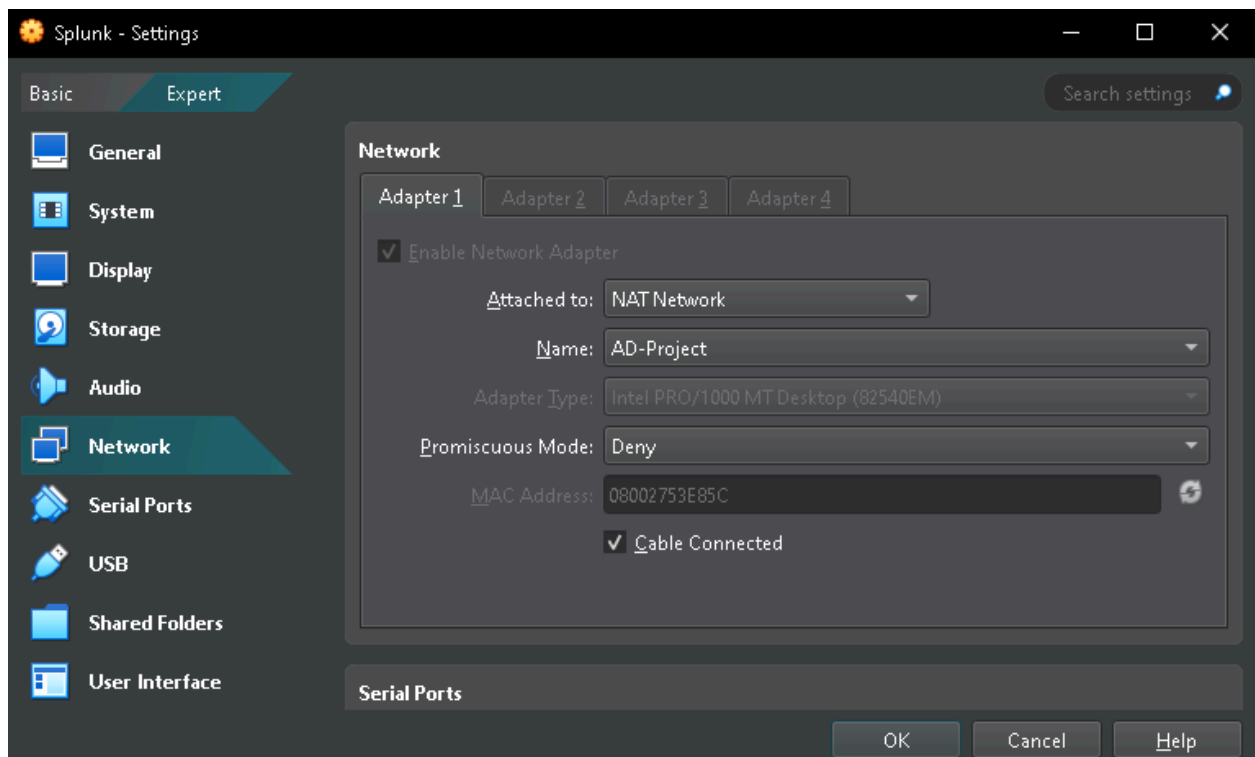
3. Then I install and configure an Ubuntu live server, which will be where the Splunk server runs. I named this server Splunk in VirtualBox and made the hardware for the machine stronger by increasing the base memory and increasing the number of processors.



- Setting all the virtual machines I created to NAT Network. This will allow all the machines to be on the same network and still have internet access. I entered 192.168.10.0/24 (Network IP from the Diagram) as the IPv4 Prefix.



I attached each virtual machine to the NAT Network that was created.



- I set a new static IP address on the splunk server by using the command

sudo nano /etc/netplan/50-cloud-init.yaml

The command will show this configuration file:

```
GNU nano 6.2 /etc/netplan/50-cloud-init.yaml
# This file is generated from information provided by the datasource.  Changes
# to it will not persist across an instance reboot.  To disable cloud-init's
# network configuration capabilities, write a file
# /etc/cloud/cloud.cfg.d/99-disable-network-config.cfg with the following:
# network: {config: disabled}
network:
  ethernets:
    enp0s3:
      dhcp4: true
  version: 2
```

I changed the Configurations to have no DHCP, added my static IP to **addresses**, I left **nameservers** blank(default), used Google's DNS for the next **addresses** line (can be any DNS), I left **routes** blank to include a default route via **192.168.10.1**(gateway).

```
GNU nano 6.2 /etc/netplan/50-cloud-init.yaml *
# This file is generated from information provided by the datasource.  Changes
# to it will not persist across an instance reboot.  To disable cloud-init's
# network configuration capabilities, write a file
# /etc/cloud/cloud.cfg.d/99-disable-network-config.cfg with the following:
# network: {config: disabled}
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
```

- I use the command **sudo netplan apply** to apply the changes of the config file.

```
pierrecyber@splunk:~$ sudo netplan apply
```

Using the command **ip a**, it shows that the IP has been changed.

```
pierrecyber@splunk:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:53:e8:5c brd ff:ff:ff:ff:ff:ff
    inet 192.168.10.10/24 brd 192.168.10.255 scope global enp0s3
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe53:e85c/64 scope link
        valid_lft forever preferred_lft forever
pierrecyber@splunk:~$ _
```

7. Next I did **ping google.com** to ensure there is a connection.

```
pierrencyber@splunk:~$ ping google.com
PING google.com (142.250.105.100) 56(84) bytes of data:
64 bytes from yt-in-f100.1e100.net (142.250.105.100): icmp_seq=1 ttl=104 time=7.54 ms
64 bytes from yt-in-f100.1e100.net (142.250.105.100): icmp_seq=2 ttl=104 time=9.56 ms
64 bytes from yt-in-f100.1e100.net (142.250.105.100): icmp_seq=3 ttl=104 time=7.22 ms
64 bytes from yt-in-f100.1e100.net (142.250.105.100): icmp_seq=4 ttl=104 time=9.64 ms
64 bytes from yt-in-f100.1e100.net (142.250.105.100): icmp_seq=5 ttl=104 time=8.45 ms
64 bytes from yt-in-f100.1e100.net (142.250.105.100): icmp_seq=6 ttl=104 time=6.91 ms
^C
--- google.com ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5012ms
rtt min/avg/max/mdev = 6.910/8.219/9.642/1.083 ms
pierrencyber@splunk:~$ _
```

8. Now I begin to install **Splunk** on my HOST machine. I installed the **.deb** Splunk installation package.

Splunk Enterprise 9.3.1

Index 500 MB/Day. Sign up and download now. After 60 days you can convert to a perpetual free license or purchase a Splunk Enterprise license to continue using the expanded functionality designed for enterprise-scale deployments.

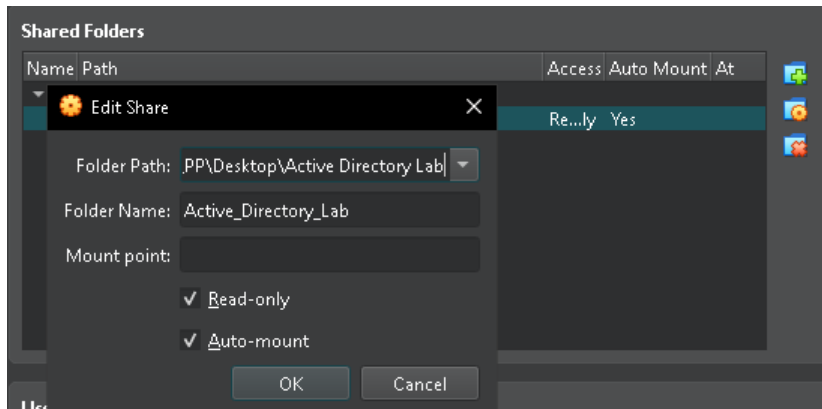
Choose Your Installation Package

Windows		Linux	Mac OS			
64-bit	4.x+, or 5.4.x kernel Linux distributions	.rpm	944.15 MB	Download Now	Copy wget link	More >
		.deb	714.76 MB	Download Now	Copy wget link	More >
		.tgz	944.3 MB	Download Now	Copy wget link	More >

9. I then installed the guest addons for virtual box on my ubuntu splunk server. Use **sudo apt-get install virtualbox** and hit tab to see all options. Then use **sudo apt-get install virtualbox-guest additions-iso**.

```
pierrencyber@splunk:~$ sudo apt-get install virtualbox
virtualbox                                virtualbox-guest-utils                    virtualbox-qt
virtualbox-dkms                           virtualbox-guest-utils-hwe                virtualbox-source
virtualbox-ext-pack                       virtualbox-guest-x11
virtualbox-guest-additions-iso            virtualbox-guest-x11-hwe
pierrencyber@splunk:~$ sudo apt-get install virtualbox-guest-additions-iso _
```

10. I created a shared folder in VirtualBox. The path will be the folder where the Splunk installer was downloaded on the host.



11. Next I add the user to the **vboxsf** group using **sudo adduser pierrecyber vboxsf**. The group will not exist yet until I install some guest utilities that VBox offers. I then used **sudo apt-get install virtualbox** and hit tab, then **sudo apt-get install virtualbox-guest-utils**.

```
pierrecyber@splunk:~$ sudo adduser pierrecyber vboxsf
[sudo] password for pierrecyber:
adduser: The group `vboxsf' does not exist.
pierrecyber@splunk:~$ sudo apt-get install virtualbox
virtualbox                                virtualbox-guest-utils                  virtualbox-qt
virtualbox-dkms                          virtualbox-guest-utils-hwe             virtualbox-source
virtualbox-ext-pack                      virtualbox-guest-x11
virtualbox-guest-additions-iso          virtualbox-guest-x11-hwe
pierrecyber@splunk:~$ sudo apt-get install virtualbox-guest-utils
```

12. I was then allowed to add user to the **vboxsf** group.

```
pierrecyber@splunk:~$ sudo adduser pierrecyber vboxsf
[sudo] password for pierrecyber:
Adding user `pierrecyber' to group `vboxsf' ...
Adding user pierrecyber to group vboxsf
Done.
pierrecyber@splunk:~$
```

13. I created the 'share' directory using **mkdir share** and **ls** shows that the directory was made.

```

pierrecyber@splunk:~$ mkdir share
pierrecyber@splunk:~$ ls
share
pierrecyber@splunk:~$ ls -l
total 4
drwxrwxr-x 2 pierrecyber pierrecyber 4096 Oct 16 14:29 share
pierrecyber@splunk:~$ ls -la
total 36
drwxr-x--- 5 pierrecyber pierrecyber 4096 Oct 16 14:29 .
drwxr-xr-x 3 root root 4096 Oct 15 22:03 ..
-rw----- 1 pierrecyber pierrecyber 231 Oct 16 14:26 .bash_history
-rw-r--r-- 1 pierrecyber pierrecyber 220 Jan 6 2022 .bash_logout
-rw-r--r-- 1 pierrecyber pierrecyber 3771 Jan 6 2022 .bashrc
drwx----- 2 pierrecyber pierrecyber 4096 Oct 15 22:05 .cache
-rw-r--r-- 1 pierrecyber pierrecyber 807 Jan 6 2022 .profile
drwxrwxr-x 2 pierrecyber pierrecyber 4096 Oct 16 14:29 share
drwx----- 2 pierrecyber pierrecyber 4096 Oct 15 22:03 .ssh
-rw-r--r-- 1 pierrecyber pierrecyber 0 Oct 15 22:06 .sudo_as_admin_successful
pierrecyber@splunk:~$ _

```

14. Next I ran the following command to mount the shared folder to the directory called "share".

```

pierrecyber@splunk:~$ sudo mount -t vboxsf -o uid=1000,gid=1000 Active_Directory_Lab share/_

```

15. I changed back to the share directory and used `ls -la`, showing that the splunk installer is in the shared folder along with other files in it.

```

pierrecyber@splunk:~/share$ ls -la
total 732412
drwxrwxrwx 1 pierrecyber pierrecyber 8192 Oct 16 14:35 .
drwxr-x--- 5 pierrecyber pierrecyber 4096 Oct 16 14:29 ..
-rwxrwxrwx 1 pierrecyber pierrecyber 28188 Oct 16 14:12 '10. splunk deb.PNG'
-rwxrwxrwx 1 pierrecyber pierrecyber 6871 Oct 16 14:14 '11. VB addons.PNG'
-rwxrwxrwx 1 pierrecyber pierrecyber 1249 Oct 16 14:24 '12. adduser vbox sf.PNG'
-rwxrwxrwx 1 pierrecyber pierrecyber 9199 Oct 16 14:26 '13. guest utils.PNG'
-rwxrwxrwx 1 pierrecyber pierrecyber 4011 Oct 16 14:28 '14. user added.PNG'
-rwxrwxrwx 1 pierrecyber pierrecyber 15594 Oct 16 14:30 '15.shared directory.PNG'
-rwxrwxrwx 1 pierrecyber pierrecyber 1933 Oct 16 14:35 '16. mount shared folder to share directory.PNG'
-rwxrwxrwx 1 pierrecyber pierrecyber 62036 Oct 2 13:47 '1.Diagram.PNG'
-rwxrwxrwx 1 pierrecyber pierrecyber 17356 Oct 7 12:23 '2. VMs Installed.PNG'
-rwxrwxrwx 1 pierrecyber pierrecyber 59529 Oct 7 12:47 '3.Beefy Splunk.PNG'
-rwxrwxrwx 1 pierrecyber pierrecyber 72757 Oct 7 12:46 '3.Splunk VB1.PNG'
-rwxrwxrwx 1 pierrecyber pierrecyber 55652 Oct 16 13:45 '4. Create NATwork.PNG'
-rwxrwxrwx 1 pierrecyber pierrecyber 49894 Oct 16 13:44 '4. NAT.PNG'
-rwxrwxrwx 1 pierrecyber pierrecyber 25553 Oct 16 13:47 '5. Splunk NAT.PNG'
-rwxrwxrwx 1 pierrecyber pierrecyber 11186 Oct 16 14:02 '6.static ip 2.PNG'
-rwxrwxrwx 1 pierrecyber pierrecyber 8653 Oct 16 13:55 '6.static ip.PNG'
-rwxrwxrwx 1 pierrecyber pierrecyber 1016 Oct 16 14:03 '7. sudo net apply.PNG'
-rwxrwxrwx 1 pierrecyber pierrecyber 12983 Oct 16 14:05 '8. inet changed.PNG'
-rwxrwxrwx 1 pierrecyber pierrecyber 15162 Oct 16 14:06 '9.Ping success.PNG'
-rwxrwxrwx 1 pierrecyber pierrecyber 749476896 Oct 16 14:12 splunk-9.3.1-0b8d769cb912-linux-2.6-amd64.deb
pierrecyber@splunk:~/share$

```

16. To install the Splunk package, I ran the command:

sudo dpkg -i splunk-9.3.1-0b8d769cb912-linux-2.6-amd64.deb

```

pierrecyber@splunk:~/share$ sudo dpkg -i splunk-9.3.1-0b8d769cb912-linux-2.6-amd64.deb
Selecting previously unselected package splunk.
(Reading database ... 94818 files and directories currently installed.)
Preparing to unpack splunk-9.3.1-0b8d769cb912-linux-2.6-amd64.deb ...
Unpacking splunk (9.3.1) ...
Setting up splunk (9.3.1) ...
complete
pierrecyber@splunk:~/share$ _

```

17. After installation I am now able to change into the Splunk directory.

```

pierrecyber@splunk:~/share$ cd /opt/splunk
pierrecyber@splunk:/opt/splunk$ ls -la
total 4880
drwxr-xr-x 11 splunk splunk 4096 Oct 16 14:41 .
drwxr-xr-x 3 root root 4096 Oct 16 14:40 ..
drwxr-xr-x 4 splunk splunk 4096 Oct 16 14:41 bin
-r--r--r-- 1 splunk splunk 57 Sep 5 17:25 copyright.txt
drwxr-xr-x 17 splunk splunk 4096 Oct 16 14:41 etc
-rw-r--r-- 1 splunk splunk 426 Oct 16 14:41 ftr
drwxr-xr-x 4 splunk splunk 4096 Oct 16 14:41 include
drwxr-xr-x 9 splunk splunk 4096 Oct 16 14:41 lib
-r--r--r-- 1 splunk splunk 85405 Sep 5 17:25 license-eula.txt
-r--r--r-- 1 splunk splunk 1090 Aug 30 23:45 LICENSE.txt
drwxr-xr-x 3 splunk splunk 4096 Oct 16 14:41 openssl
drwxr-xr-x 3 splunk splunk 4096 Oct 16 14:40 opt
drwxr-xr-x 2 splunk splunk 4096 Oct 16 14:41 quarantined_files
-r--r--r-- 1 splunk splunk 529 Sep 5 17:29 README-splunk.txt
drwxr-xr-x 4 splunk splunk 4096 Oct 16 14:41 share
-r--r--r-- 1 splunk splunk 4847082 Sep 5 17:58 splunk-9.3.1-0b8d769cb912-linux-2.6-x86_64-manifest
drwxr-xr-x 2 splunk splunk 4096 Oct 16 14:41 suidtag
pierrecyber@splunk:/opt/splunk$ _

```

18. All of the user and group permissions belong to “Splunk” as seen in the above image. I changed into the user “Splunk” using **sudo -u splunk bash**.

```

pierrecyber@splunk:/opt/splunk$ sudo -u splunk bash
splunk@splunk:~$

```

19. I changed into the Splunk binaries directory with **cd bin**. I used **./splunk start** to run the installer. After accepting the agreement, it will install.

```

Starting splunk server daemon (splunkd)...
Generating a RSA private key
.....+++++
.....+++++
writing new private key to 'privKeySecure.pem'
-----
Signature ok
subject=/CN=splunk/O=SplunkUser
Getting CA Private Key
writing RSA key
PYTHONHTTPSVERIFY is set to 0 in splunk-launch.conf disabling certificate validation fo
d with the embedded Python interpreter; must be set to "1" for increased security
Done

Waiting for web server at http://127.0.0.1:8000 to be available..... Done

If you get stuck, we're here to help.
Look for answers here: http://docs.splunk.com

The Splunk web interface is at http://splunk:8000
splunk@splunk:~/bin$

```

20. Next I exited out of the user “Splunk”, changed back to the bin directory, and ran the following: **sudo ./splunk enable boot-start -user splunk**. This ensures that whenever the VM reboots, Splunk will run with the user “splunk”.


```
splunk@splunk:~/bin$ exit
exit
pierreCyber@splunk:/opt/splunk$ cd bin
pierreCyber@splunk:/opt/splunk/bin$ ./splunk enable boot-start -user splunk
Cannot write to "/opt/splunk/etc/splunk-launch.conf": Permission denied
pierreCyber@splunk:/opt/splunk/bin$ sudo ./splunk enable boot-start -user splunk
Init script installed at /etc/init.d/splunk.
Init script is configured to run at boot.
pierreCyber@splunk:/opt/splunk/bin$ _
```

21. On the target machine, the IP is set by default to 192.168.10.5

```
Select Command Prompt
Microsoft Windows [Version 10.0.19045.3803]
(c) Microsoft Corporation. All rights reserved.

C:\Users\PierreCyber>ipconfig

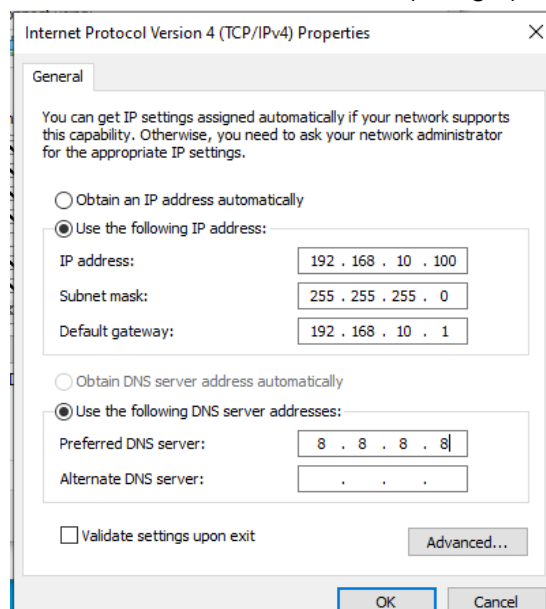
Windows IP Configuration

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . : attlocal.net
    Link-local IPv6 Address . . . . . : fe80::ebab:87db:37a4:718a%12
    IPv4 Address. . . . . : 192.168.10.5
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.10.1

C:\Users\PierreCyber>
```

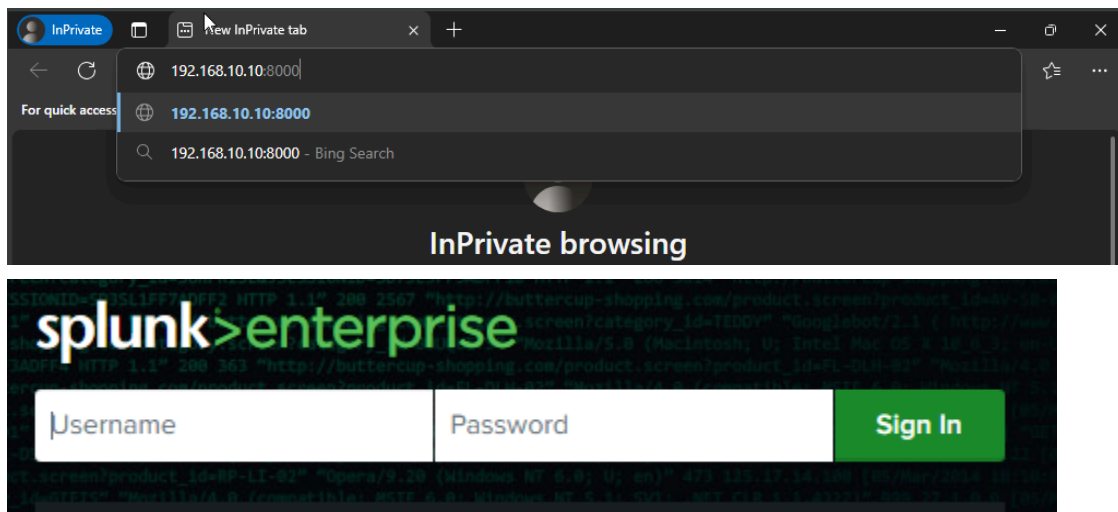
I changed this by navigating to the IPv4 Properties in the network adapter settings. I set a status IP of **192.168.10.100**, which will set the subnet to 255.255.255.0. Default gateway was set to **192.168.10.1**, and I used **8.8.8.8** (Google) for the preferred DNS.



The IP has been changed:

```
Connection-specific DNS Suffix . :  
Link-local IPv6 Address . . . . . : fe80::ebab:87db:37a4:718a%12  
IPv4 Address. . . . . : 192.168.10.100  
Subnet Mask . . . . . : 255.255.255.0  
Default Gateway . . . . . : 192.168.10.1
```

22. Visit splunk through a web browser using static IP and port **192.168.10.10:8000** and the login page should show up. I used the credentials that were created when configuring the Ubuntu LTS Splunk server.

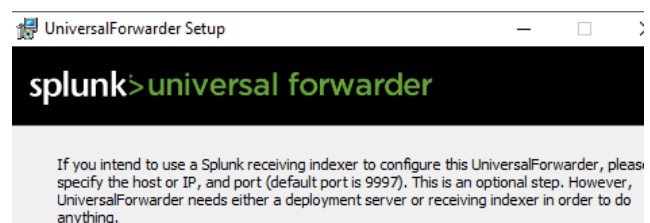
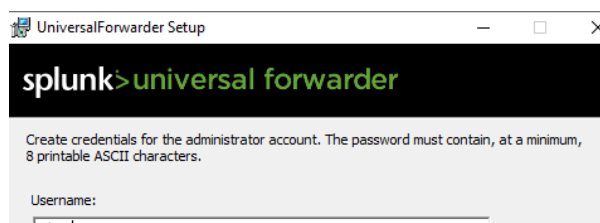
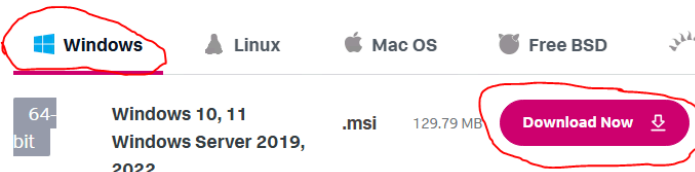


23. Next it was time to install the **Splunk Universal Forwarder 9.3.1** on the target machine from **Splunk.com**. I chose “admin” as a username and generated a random password. For the receiving indexer, I use **192.168.10.10** (Splunk Server IP) and use **9997** for the default port.

Splunk Universal Forwarder 9.3.1

Universal Forwarders provide reliable, secure data collection from remote sources and forward that data into Splunk software for indexing and consolidation. They can scale to tens of thousands of remote systems, collecting terabytes of data.

Choose Your Installation Package



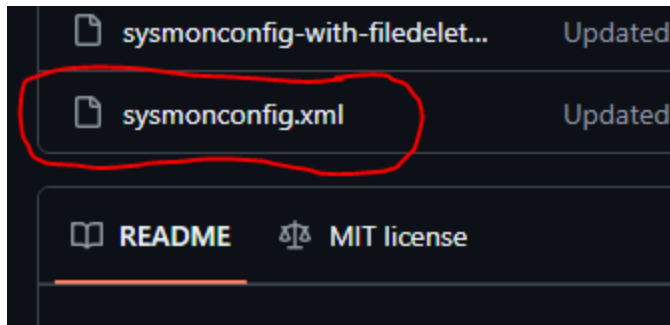
24. Then I install **Sysmon** to be able to log activity to the event log.

The screenshot shows a Microsoft Bing search interface. The search bar contains the text 'sysmon'. Below the search bar, there are navigation links: SEARCH, COPILOT, IMAGES, VIDEOS, MAPS, NEWS, and SHOP. On the left side, there is a 'Table of Contents' with links to 'Introduction', 'Overview of Sysmon...', and 'Usage'. The main search result is from Microsoft Learn, titled 'Sysmon - Sysinternals | Microsoft Learn'. The URL is 'https://learn.microsoft.com/en-us/sysinternals/downloads/sysmon'. The description states: 'Sysmon is a **Windows** service and driver that logs and monitors system activity to the event log. It provides detailed information about process creations, network connections, file creation time changes, ... See more'. On the right side, there is a section for the article 'Sysmon v15.15', dated '07/23/2024', with '10 contributors'. Below this, there is a list of links: 'Introduction', 'Overview of Sysmon Capabilities', 'Screenshots', 'Usage', and 'Show 5 more'. At the bottom right, it says 'By Mark Russinovich and Thomas Garnier', 'Published: July 23, 2024', and a download button for 'Download Sysmon' (4.6 MB).

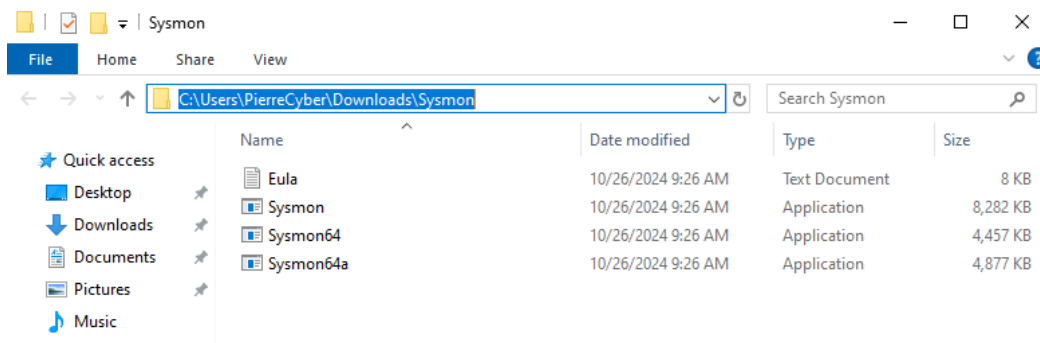
25. For Sysmon in this lab, I used Olaf's Sysmon configuration from github.

The screenshot shows a Microsoft Bing search interface. The search bar contains the text 'sysmon olaf config'. Below the search bar, there are navigation links: SEARCH, COPILOT, VIDEOS, IMAGES, MAPS, NEWS, and SHOPPING. On the left side, there is a 'Table of Contents' with links to 'Overview', 'Pre-Generated c...', and 'NOTICE: Sysmon ...'. The main search result is from GitHub, titled 'sysmon-modular | A Sysmon configuration...'. The URL is 'https://github.com/olafhartong/sysmon-modular'. The description states: 'A repository of **sysmon configuration** modules for different scenarios and purposes, such as file delete, MDE augmentation, research and more. Learn how to customize, generate and use **sysmon configs** ... See more'.

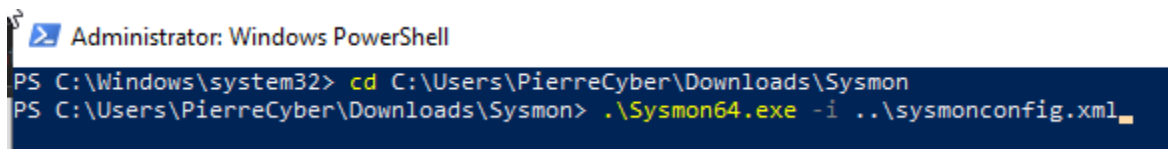
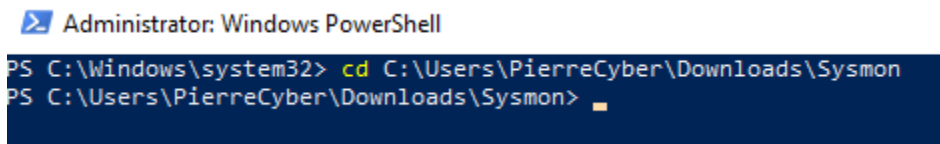
26. I scrolled down to find the **sysmonconfig.xml** file and downloaded the raw file.



27. I navigated to the downloads folder where I installed Sysmon and extracted it. Copy the path.



28. Open **Powershell** as administrator and change directory to the path that was just copied. Then I install sysmon64.exe with the configuration file from Github, using **.\Sysmon64.exe -i ..\sysmonconfig.xml**



Sysmon service should be running after installation.


Administrator: Windows PowerShell

```
PS C:\Windows\system32> cd C:\Users\PierreCyber\Downloads\Sysmon
PS C:\Users\PierreCyber\Downloads\Sysmon> .\Sysmon64.exe -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\PierreCyber\Downloads\Sysmon>
```

29. Next I navigate to this folder:

↑  C:\Program Files\SplunkUniversalForwarder\etc\system\local

Instructions are needed for the Universal Forwarder to send data to the Splunk server, so I open **Notepad** as administrator and create an Inputs.conf file with the following:

```
*Untitled - Notepad
File Edit Format View Help
[WinEventLog://Application]
index = endpoint
disabled = false

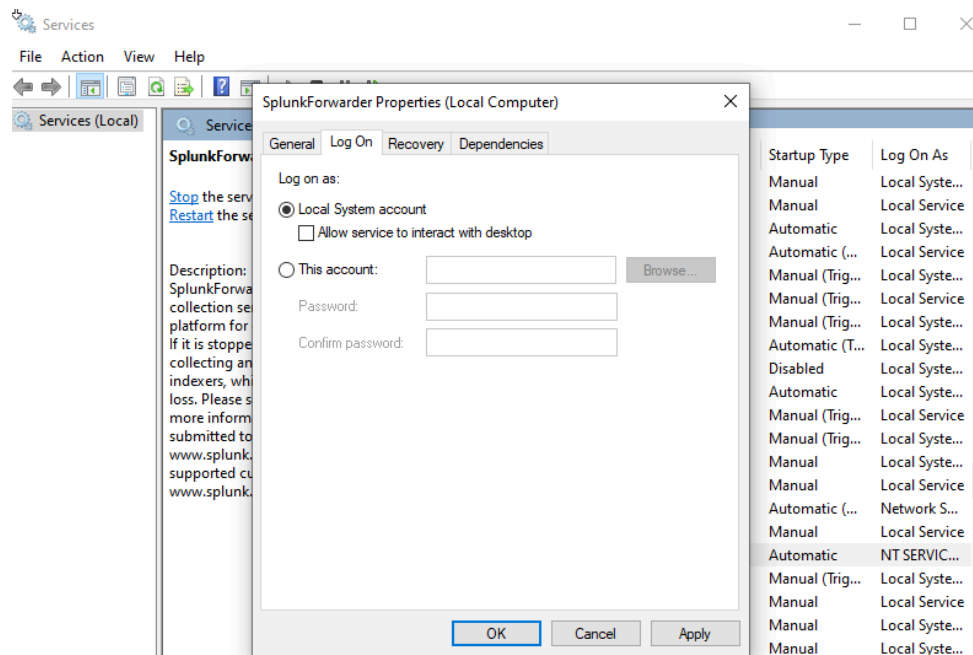
[WinEventLog://Security]
index = endpoint
disabled = false

[WinEventLog://System]
index = endpoint
disabled = false

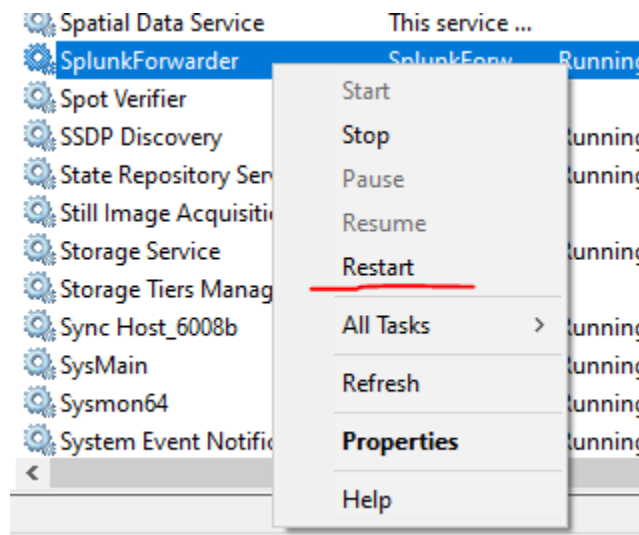
[WinEventLog://Microsoft-Windows-Sysmon/Operational]
index = endpoint
disabled = false
renderXml = true
source = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational
```

Save this file to the **local** folder from the path above.

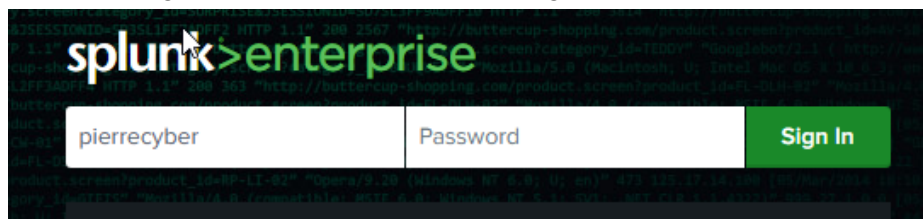
30. Open the services application from the start menu. Find the **SplunkForwarder** service and change the log on properties to **Local System Account**.



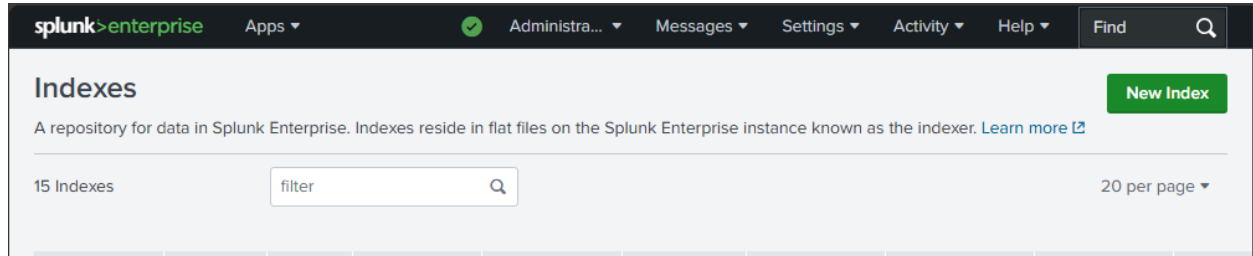
31. Because the inputs.conf file was created, the SplunkForwarder service also needs to be restarted.



32. Next I log in to the splunk server through the browser.



Navigate to **Settings**, then **Indexes**. Select **New Index**



33. Here I created an index called endpoint, which is needed because that is the index specified in the input configuration file.

New Index ×

General Settings

Index Name
Set index name (e.g., INDEX_NAME). Search using index=INDEX_NAME.

Index Data Type Events Metrics
The type of data to store (event-based or metrics).

Home Path
Hot/warm db path. Leave blank for default (\$SPLUNK_DB/INDEX_NAME/db).

Cold Path
Cold db path. Leave blank for default (\$SPLUNK_DB/INDEX_NAME/colddb).

Thawed Path
Thawed/resurrected db path. Leave blank for default (\$SPLUNK_DB/INDEX_NAME/thaweddb).

Data Integrity Check Enable Disable
Enable this if you want Splunk to compute hashes on every slice of your data for the purpose of data integrity.

Max Size of Entire Index GB

Save Cancel

34. Navigate to **Settings**, then **Forwarding and Receiving**. Select **Configure receiving**.

Forwarding and receiving

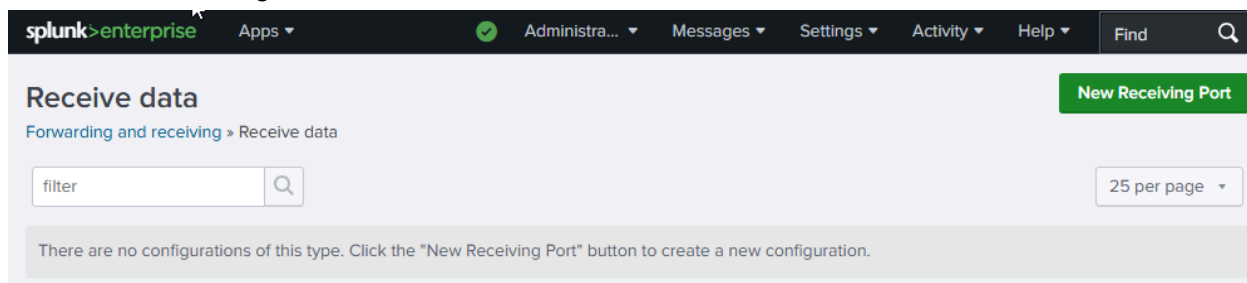
Forward data
Set up forwarding between two or more Splunk instances.

Type	Actions
Forwarding defaults	
Configure forwarding	+ Add new

Receive data
Configure this instance to receive data forwarded from other instances.

Type	Actions
Configure receiving	+ Add new

Click New Receiving Port.



35. I entered **9997** (Splunk Default) for the forwarder to listen on this port.

Configure receiving

Set up this Splunk instance to receive data from forwarder(s).

Listen on this port *

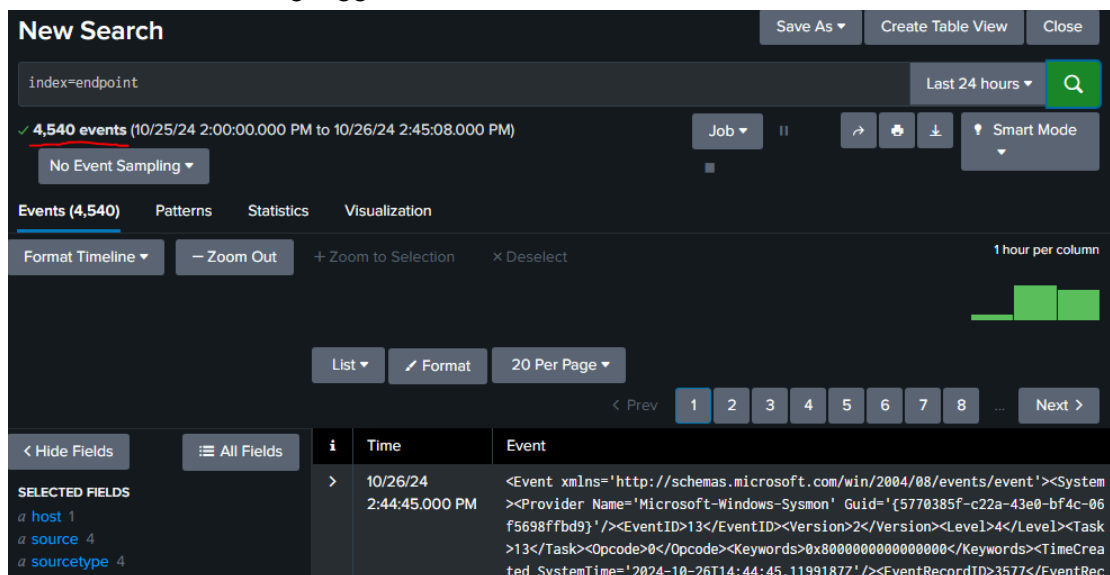
9997

For example, 9997 will receive data on TCP port 9997.

Cancel

Save

36. In the search bar, search for the endpoint index with **“index=endpoint”**. The target machine events should be being logged now.



The **Target-PC** shows under hosts, as well as the source data from the input configuration file:

< Hide Fields

All Fields

SELECTED FIELDS

a host 1

a source 4

a sourcetype 4

INTERESTING FIELDS

a ComputerName 1

EventCode 96

host

1 Value, 100% of events

Selected Yes No

Reports

Top valuesTop values by timeRare values

Events with this field

Values

Values	Count	%
TARGET-PC	4,540	100%

< Hide Fields

All Fields

SELECTED FIELDS

a host 1

a source 4

a sourcetype 4

INTERESTING FIELDS

a ComputerName 1

EventCode 96

EventType 5

source

4 Values, 100% of events

Selected Yes No

Reports

Top valuesTop values by timeRare values

Events with this field

Values

Values	Count	%
XmlWinEventLog:Microsoft-Windows-Sysmon/Operational	3,577	78.788%
WinEventLog:Security	455	10.022%
WinEventLog:System	399	8.788%
	109	2.401%

Recycle Bin

Settings

Home

Find a setting

System

Display

Sound

Notifications & actions

Focus assist

Power & sleep

Storage

Tablet

About

Your PC is monitored and protected.

See details in Windows Security

Device specifications

Device name WIN-L6N6FN1PSHB

Processor Intel(R) Core(TM) i7-10700K CPU @ 3.80GHz 3.79 GHz

Installed RAM 4.00 GB

Device ID A6B3EB58-EEA6-4F80-A382-7A51742AE524

Product ID 00454-40000-00001-AA190

System type 64-bit operating system, x64-based processor

Pen and touch No pen or touch input is available for this display

Copy

Rename this PC

Windows Server 2022 Standard Evaluation

Windows License valid for 161 days

Build 20348.1fe_release.210507-1500

7:55 AM

10/26/2024

Rename your PC

You can use a combination of letters, hyphens, and numbers.

Current PC name: WIN-L6N6FN1PSHB

ADDC01

Next

Cancel

38. Next I navigate to the **IPv4 Properties** in the network adapter settings, and use the IP address **192.168.10.7** for this machine, as previously noted in the diagram. I use the Splunk server IP **192.168.10.1** for the default gateway. **8.8.8.8** (Google) is used as the preferred DNS server.

Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

39. The new static IP has been set.


```
Connection-specific DNS Suffix . :  
Link-local IPv6 Address . . . . . : fe80::a93a:77ad:ac0b:  
IPv4 Address. . . . . : 192.168.10.7  
Subnet Mask . . . . . : 255.255.255.0  
Default Gateway . . . . . : 192.168.10.1
```


40. Next it was time to install the **Splunk Universal Forwarder** on the ADDC01 machine (windows server) from **Splunk.com**. I chose “admin” as a username and generated a random password. For the receiving indexer, I use **192.168.10.10** (Splunk Server IP) and use **9997** for the default port.


Splunk Universal Forwarder 9.3.1


Universal Forwarders provide reliable, secure data collection from remote sources and forward that data into Splunk software for indexing and consolidation. They can scale to tens of thousands of remote systems, collecting terabytes of data.


Choose Your Installation Package


 Windows

 Linux

 Mac OS

 Free BSD

 Solaris

 AIX

64-bit

Windows 10, 11
Windows Server 2019,
2022

.msi

129.79 MB

Download Now

Copy wget link

More

UniversalForwarder Setup

splunk>universal forwarder

Create credentials for the administrator account. The password must contain, at a minimum, 8 printable ASCII characters.

Username:

☒ Generate random password

Password:

Confirm password:

UniversalForwarder Setup

splunk>universal forwarder

If you intend to use a Splunk receiving indexer to configure this UniversalForwarder, please specify the host or IP, and port (default port is 9997). This is an optional step. However, UniversalForwarder needs either a deployment server or receiving indexer in order to do anything.

Receiving Indexer

Hostname or IP
 :

Enter the hostname or IP of your receiving indexer, e.g. ds.splunk.com *default is 9997*

41. Then I install **Sysmon** to be able to log activity to the event log.

Sysmon v15.15

Article • 07/23/2024 • 10 contributors

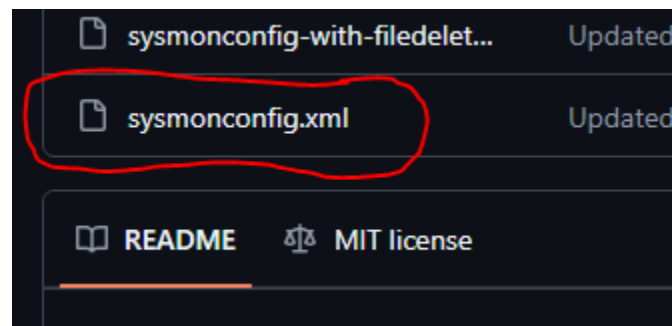
In this article

- [Introduction](#)
- [Overview of Sysmon Capabilities](#)
- [Screenshots](#)
- [Usage](#)
- [Show 5 more](#)

42. I used Olaf's Sysmon configuration By Mark Russinovich and Thomas Garnier

The screenshot shows a Microsoft Bing search interface. The search bar contains the text 'sysmon olaf config'. Below the search bar, there are navigation links for SEARCH, COPILOT, VIDEOS, IMAGES, MAPS, NEWS, and SHOPPING. The search results section displays a link to a GitHub repository: 'sysmon-modular | A Sysmon configuration...'. The repository description states: 'A repository of sysmon configuration modules for different scenarios and purposes, such as file delete, MDE augmentation, research and more. Learn how to customize, generate and use sysmon configs ... See more'. On the left side of the search results, there is a 'Table of Contents' section with links to 'Overview', 'Pre-Generated c...', and 'IOTICE: Sysmon ...'.

Download the **sysmonconfig.xml** raw file.



43. After extracting the Sysmon Zip file in the downloads folder, I opened **Powershell** as an administrator, and changed directory to the path where Sysmon was extracted. Then I install sysmon64.exe with the configuration file from Github, using:

.\Sysmon64.exe -i ..\sysmonconfig.xml

```
PS C:\Users\Administrator> cd C:\Users\Administrator\Downloads\Sysmon
PS C:\Users\Administrator\Downloads\Sysmon> .\Sysmon64.exe -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\Administrator\Downloads\Sysmon>
```

44. I navigate to the local folder in this path:

C:\Program Files\SplunkUniversalForwarder\etc\system\local					Search local	
	Name	Date modified	Type	Size		
ss	authentication.conf	10/27/2024 5:47 AM	CONF File	1 KB		
	outputs.conf	10/27/2024 5:47 AM	CONF File	1 KB		
ls	README	9/5/2024 5:40 PM	File	1 KB		
ts	server.conf	10/27/2024 5:48 AM	CONF File	1 KB		

45. Instructions are needed for the Universal Forwarder to send data to the Splunk server, so I open **Notepad** as administrator and create an Inputs.conf file (same as before) with the following:

```
*Untitled - Notepad
File Edit Format View Help
[WinEventLog://Application]
index = endpoint
disabled = false

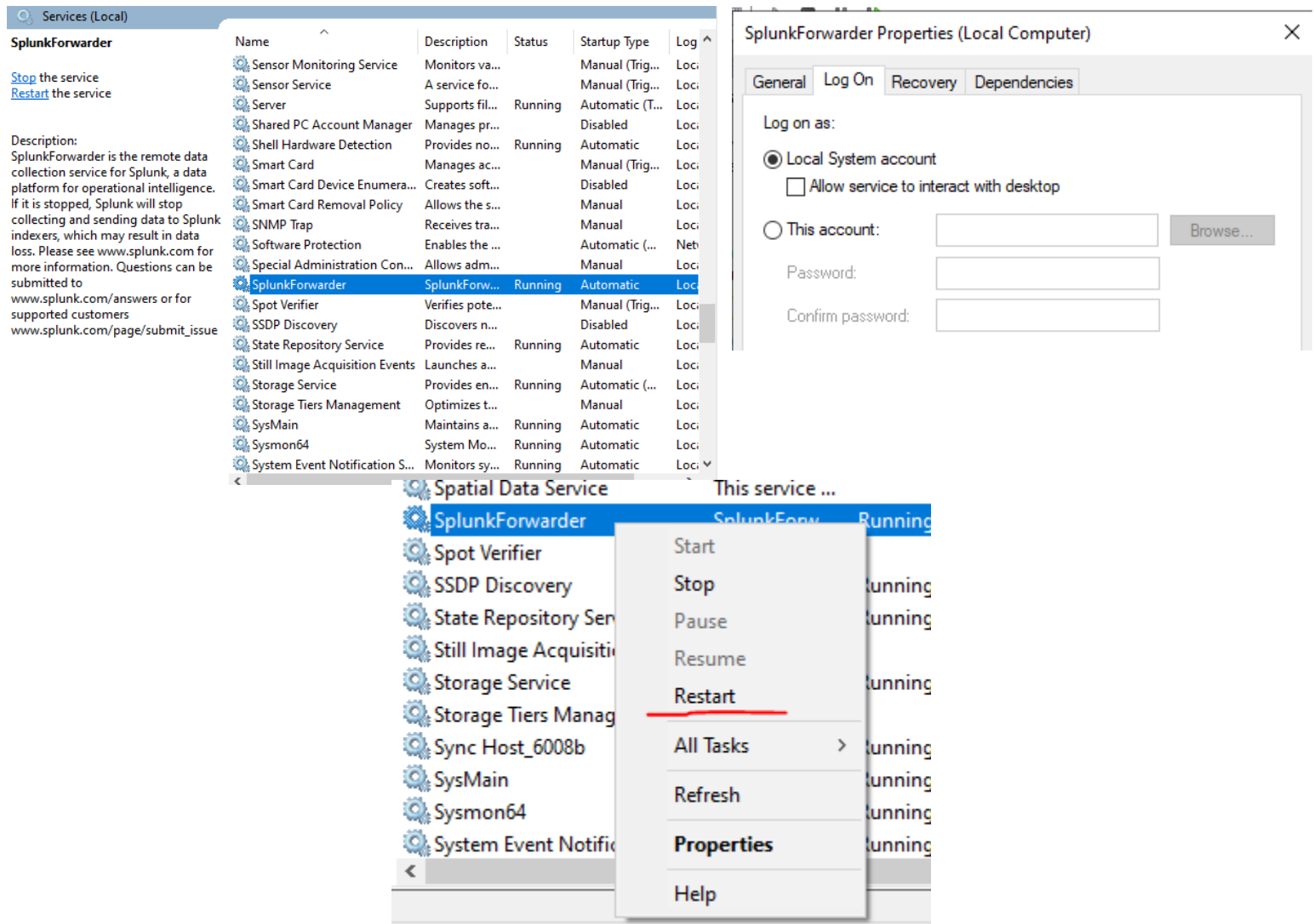
[WinEventLog://Security]
index = endpoint
disabled = false

[WinEventLog://System]
index = endpoint
disabled = false

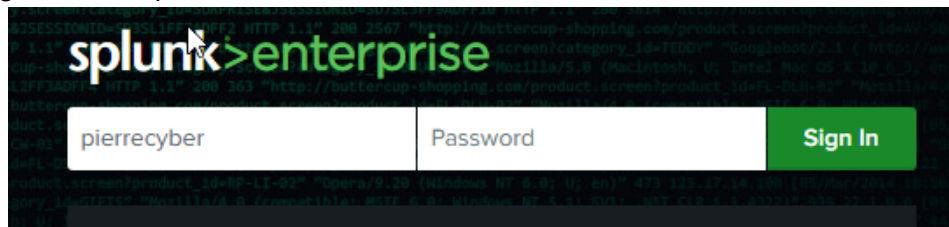
[WinEventLog://Microsoft-Windows-Sysmon/Operational]
index = endpoint
disabled = false
renderXml = true
source = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational
```

Save this file to the **local** folder from the path above.

46. Open the services application from the start menu. Find the **SplunkForwarder** service and change the log on properties to **Local System Account**.



48. Now log in to the Splunk Server from a web browser.



49. Search for “**index=endpoint**” again, and you should now see that under **hosts**, **ADDC01** is also generating logs alongside the Target PC.

The screenshot shows the Splunk Enterprise search interface. The search bar contains 'index=endpoint' and the time range is set to 'Last 24 hours'. The search results show 5,693 events. A modal window is open for the 'host' field, showing 2 values and 100% of events. The modal includes options for 'Selected' (Yes/No), 'Reports' (Top values, Top values by time, Rare values), and 'Values' (Count, %). The 'Values' section shows a table with columns for host, count, and percentage.

host	Count	%
a host 2	1	100%
a source 4	1	100%

The screenshot shows the Server Manager dashboard. The 'Manage' dropdown menu is open, showing options: 'Add Roles and Features' (highlighted with a red line), 'Remove Roles and Features', 'Add Servers', 'Create Server Group', and 'Server Manager Properties'. The dashboard includes a 'QUICK START' section with steps 1 through 5, and a 'ROLES AND SERVER GROUPS' section showing a list of roles and server groups.

QUICK START

- 1 Configure this local server
- 2 Add roles and features
- 3 Add other servers to manage
- 4 Create a server group
- 5 Connect this server to cloud services

ROLES AND SERVER GROUPS

Roles: 1 | Server groups: 1 | Servers total: 1

File and Storage Services	Local Server
Manageability	Manageability
Events	Events
Performance	Performance
BPA results	BPA results

51. I selected **Role-Based or feature-based installation**.

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.

52. Under **Server Roles**, I checked the box to install **Active Directory Domain Services**, then continued with the installation.

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

Roles

☐ 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

Installation progress

DESTINATION SERVER
ADDC01

Before You Begin

Installation Type

Server Selection

Server Roles

Features

AD DS

Confirmation

Results

View installation progress

i Feature installation

Installation started on ADDC01

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

Post-deployment Configuration

Configuration required for Active Directory Domain Services at ADDC01

Promote this server to a domain controller

i Feature installation

Configuration required. Installation succeeded on ADDC01.

Add Roles and Features

Task Details

this wizard without interrupting running tasks. View task progress or open this clicking Notifications in the command bar, and then Task Details.

settings

54. Select **add new forest** because a new domain is being created. The domain name must have a top level domain, so I added the extension to make it **pierrecyber.local**.

Active Directory Domain Services Configuration Wizard

Deployment Configuration

TARGET SERVER
ADDC01

Deployment Configuration

Domain Controller Options

Additional Options

Paths

Review Options

Prerequisites Check

Select the deployment operation

☐ Add a domain controller to an existing domain

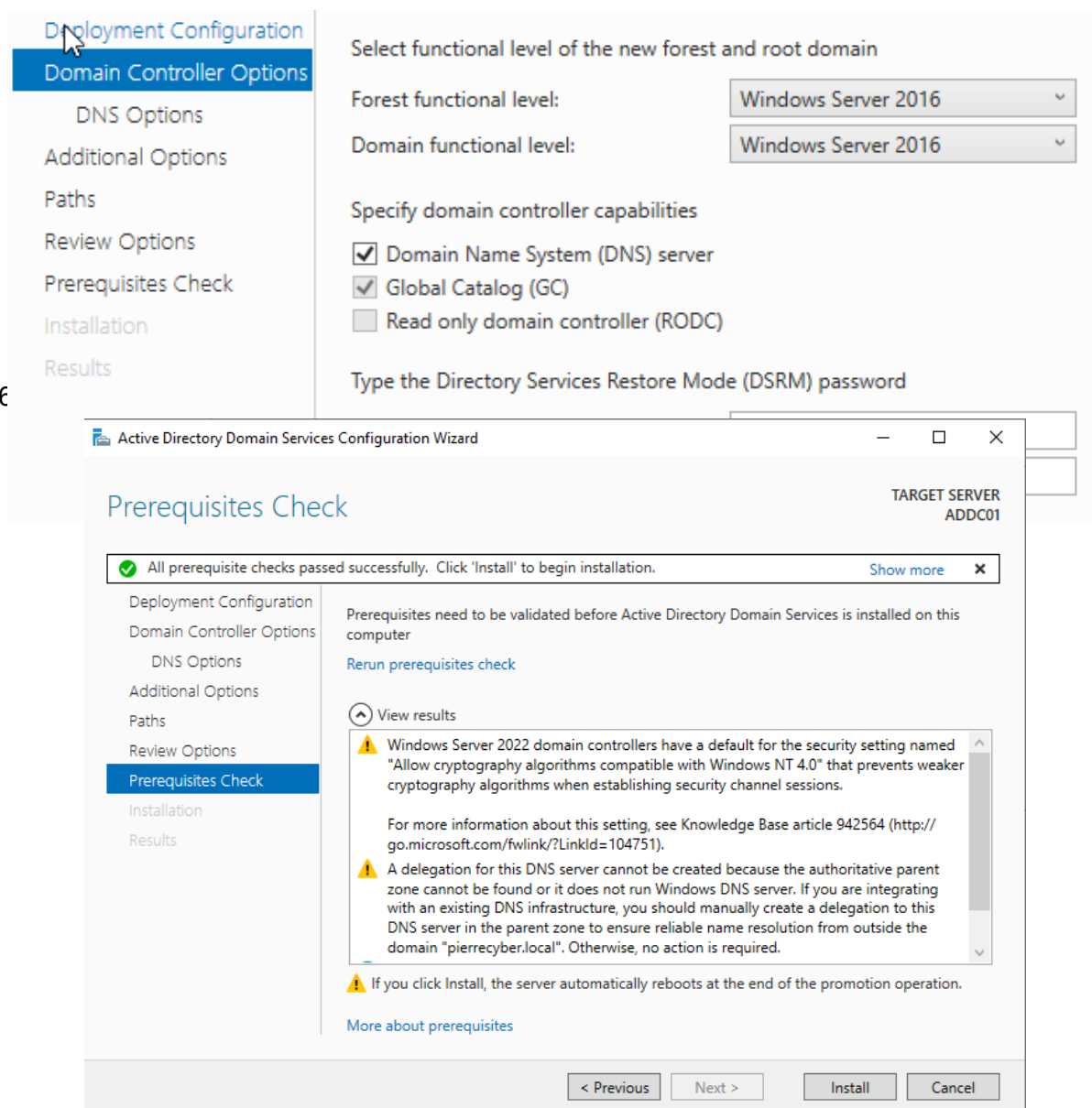
☐ Add a new domain to an existing forest

☒ **Add a new forest**

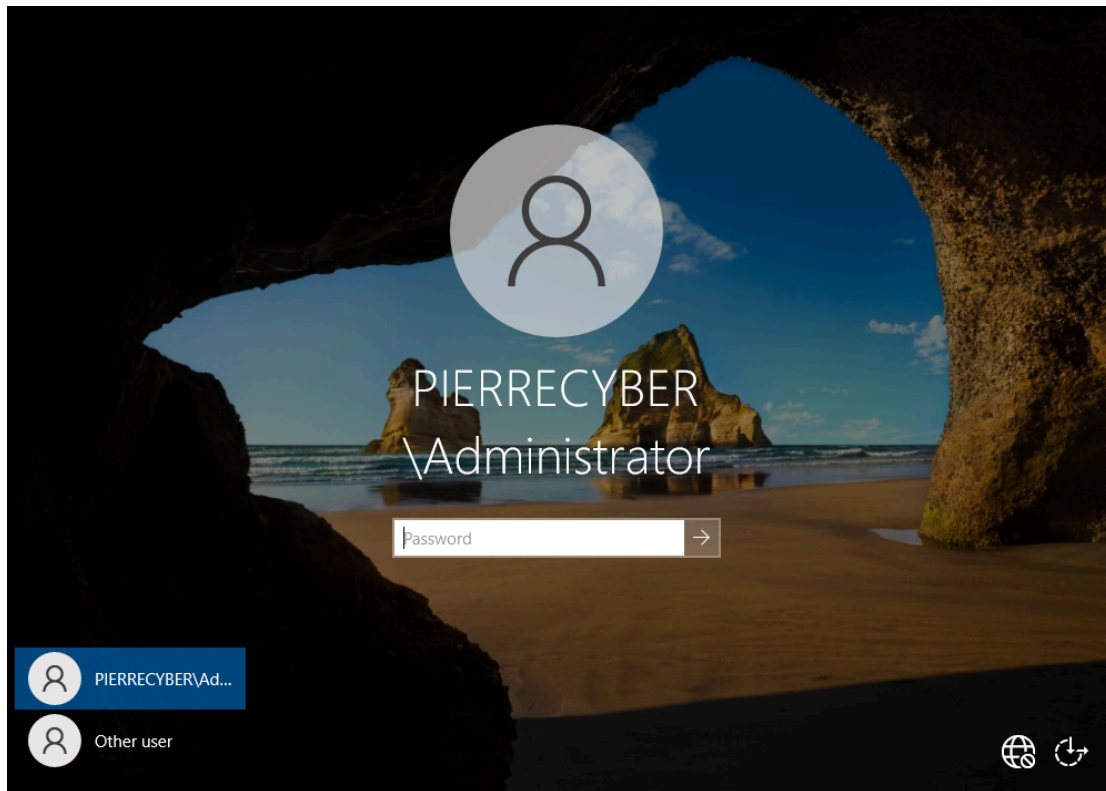
Specify the domain information for this operation

55. Under **Domain Controller Options** I created the DSRM password.

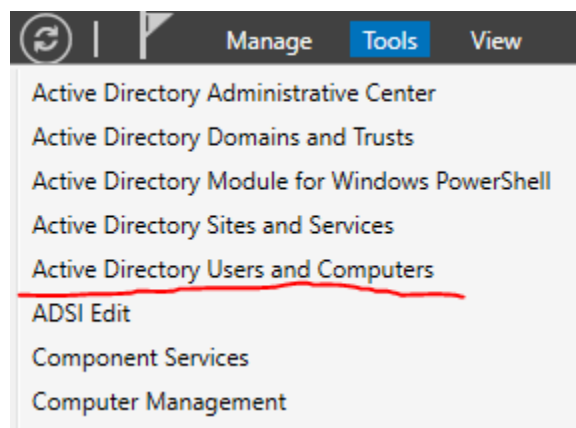
56



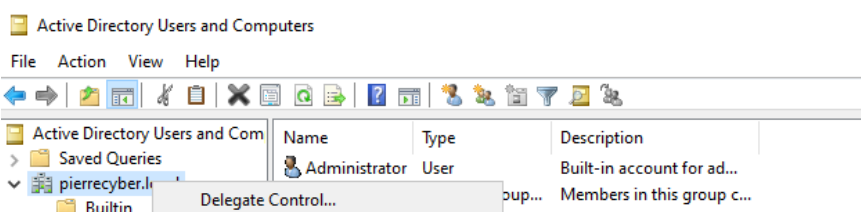
57. After restarting, the name should now include the new domain filled by a backslash, which indicates that I successfully installed Active Directory Domain Services (ADDS), and also promoted the server to a domain controller.



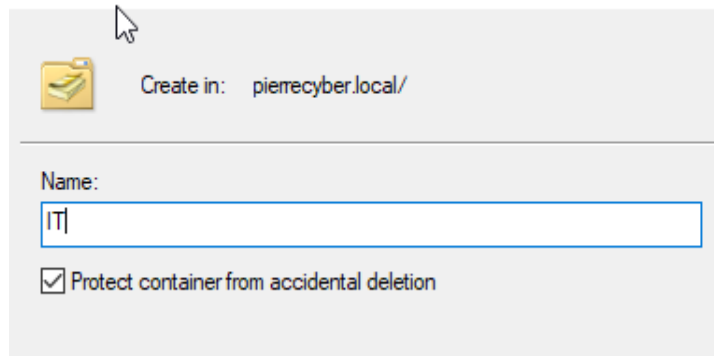
58. Then I started adding users to my domain. In the Server Manager under **Tools**, I selected **Active Directory Users and Computers**.



59. I create a new organizational unit by right clicking my domain and clicking **organizational unit**, and giving it the name "IT".

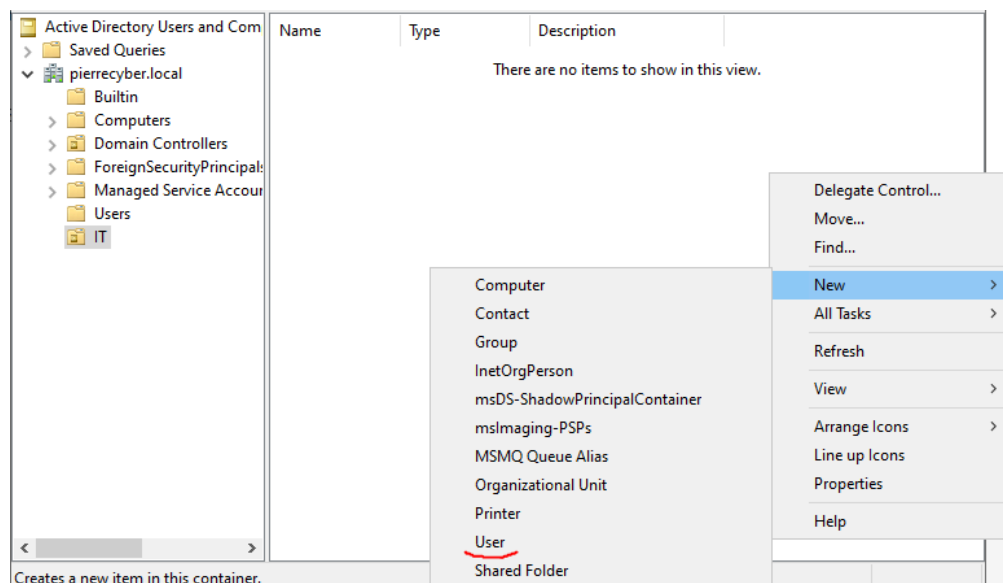


New Object - Organizational Unit

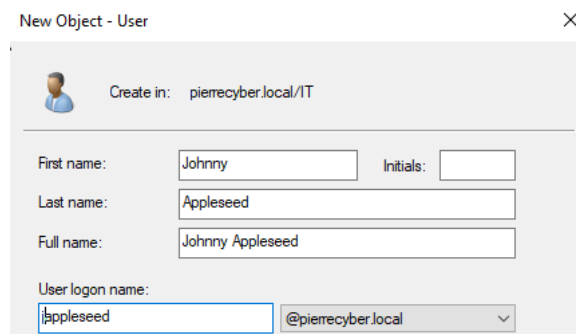


The dialog box is titled "New Object - Organizational Unit". It features a folder icon and the text "Create in: pierrecyber.local/". Below this, there is a "Name:" label followed by a text input field containing the text "IT". At the bottom, there is a checkbox labeled "Protect container from accidental deletion" which is checked.

60. Next, I started creating a new user under the “IT” organizational unit by right-clicking and selecting new user.

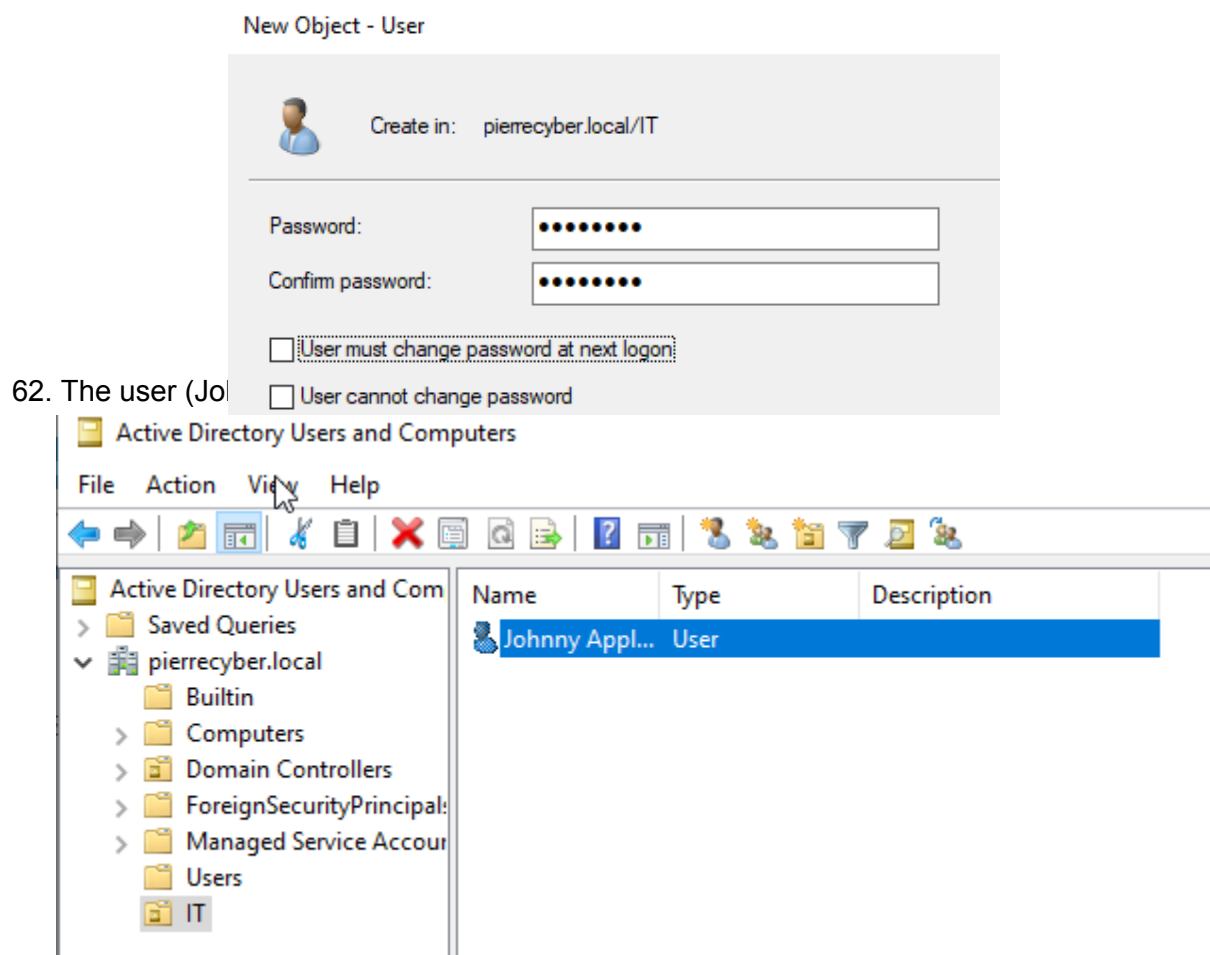


61. I input the user’s name and user logon credential.

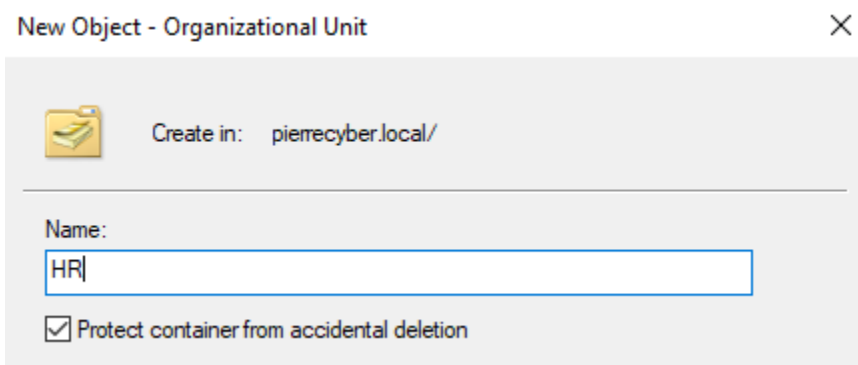


The dialog box is titled "New Object - User". It features a user icon and the text "Create in: pierrecyber.local/IT". Below this, there are input fields for "First name:" (Johnny), "Last name:" (Appleseed), and "Full name:" (Johnny Appleseed). There is also a "User logon name:" field with the text "appleseed" and a dropdown menu showing "@pierrecyber.local".

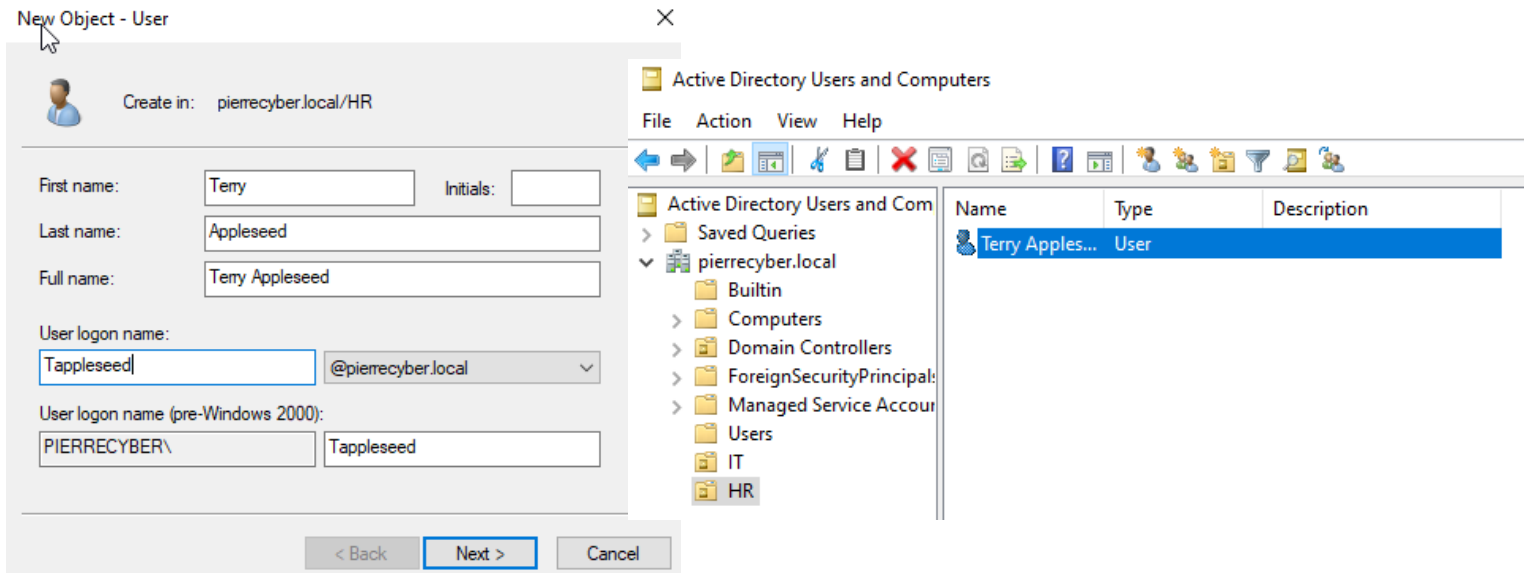
For this lab, I set a password for the user, and uncheck the box to have them change their password at next login:



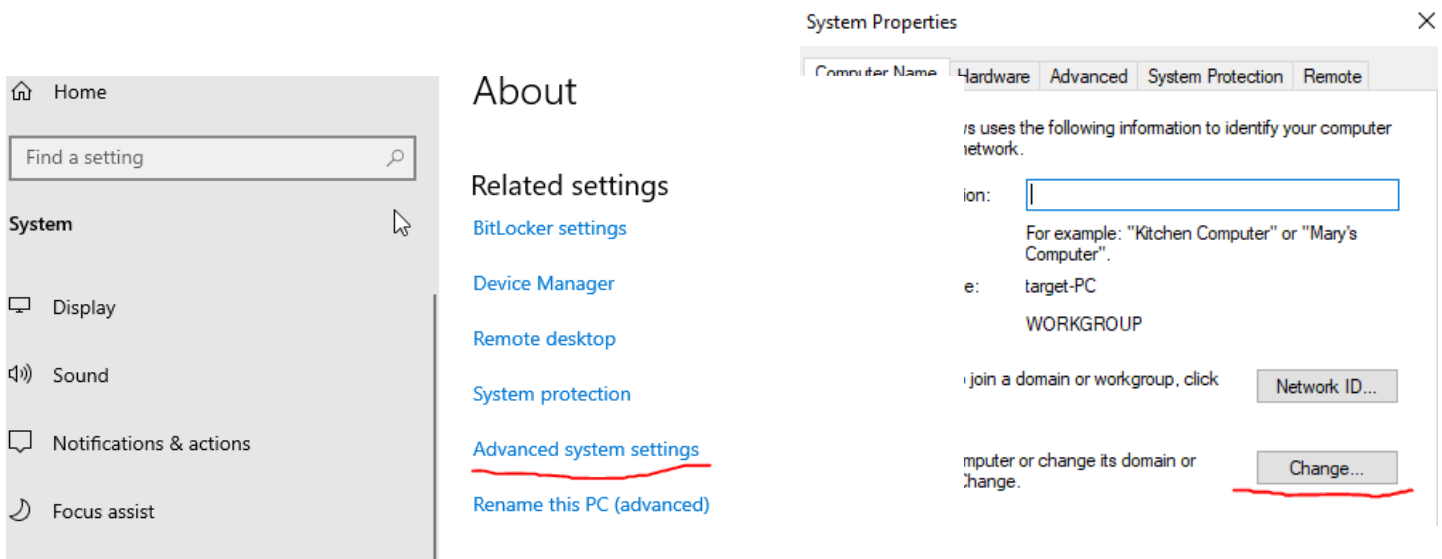
63. Next, I created another organizational unit named "HR".



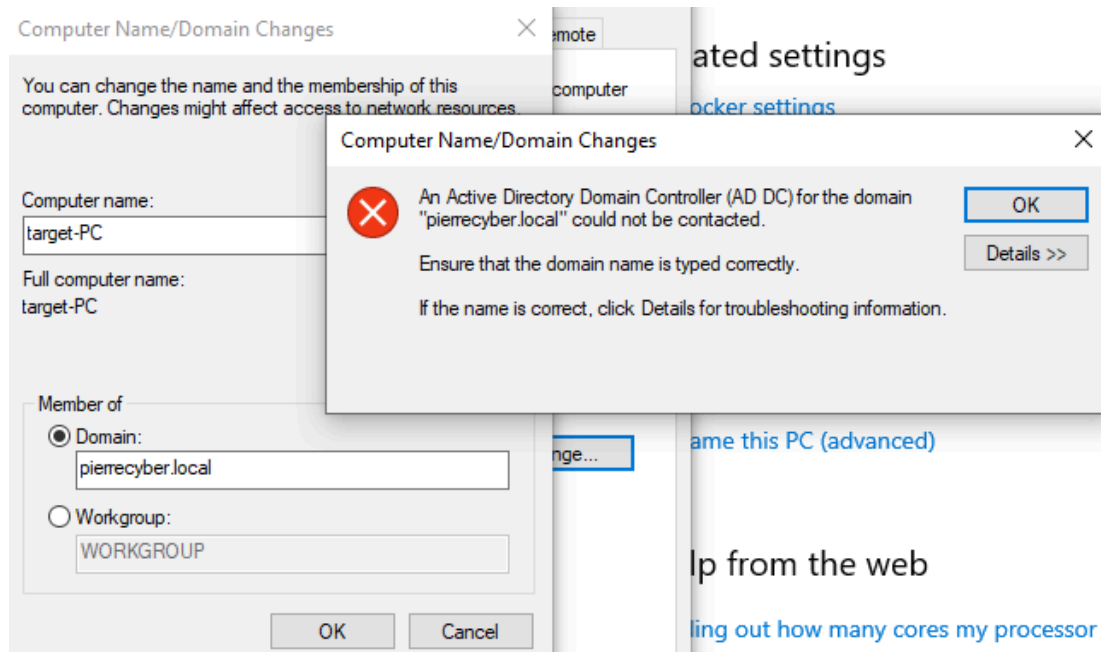
64. I created a new user under the “HR” unit named Terry Appleseed.



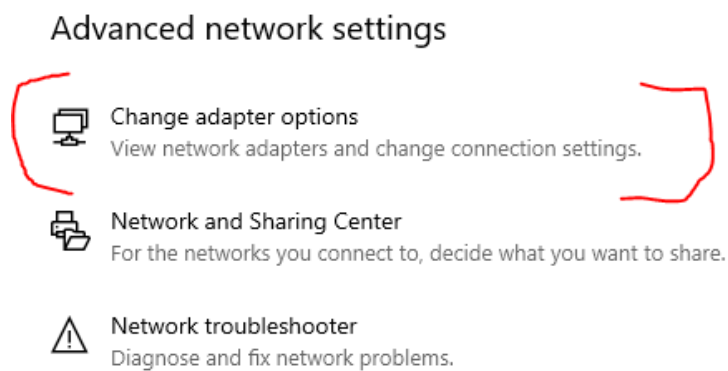
65. Now I start to add the target PC to the domain. On the **Target-PC**, I navigated to the **advanced system settings**, then **change** to update its domain.



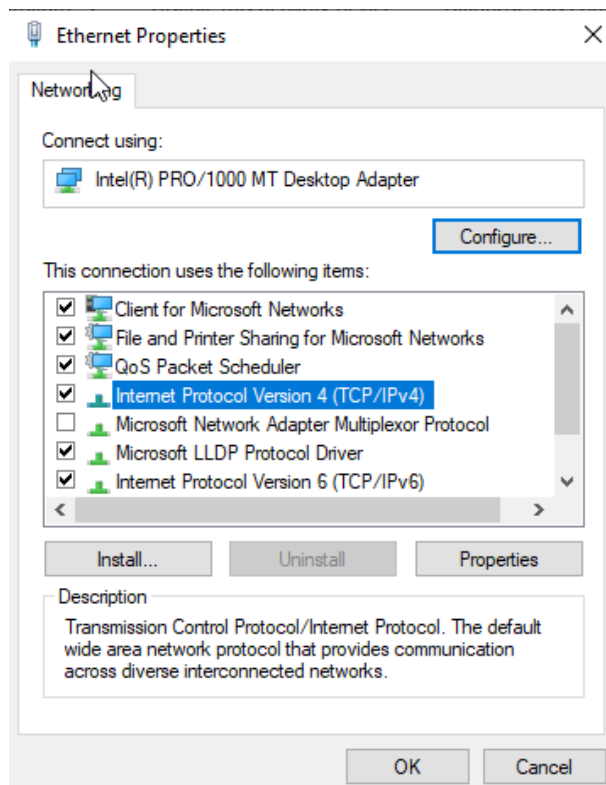
66. After typing the domain name (pierrecyber.local) and clicking “ok”, this temporary error will show up.



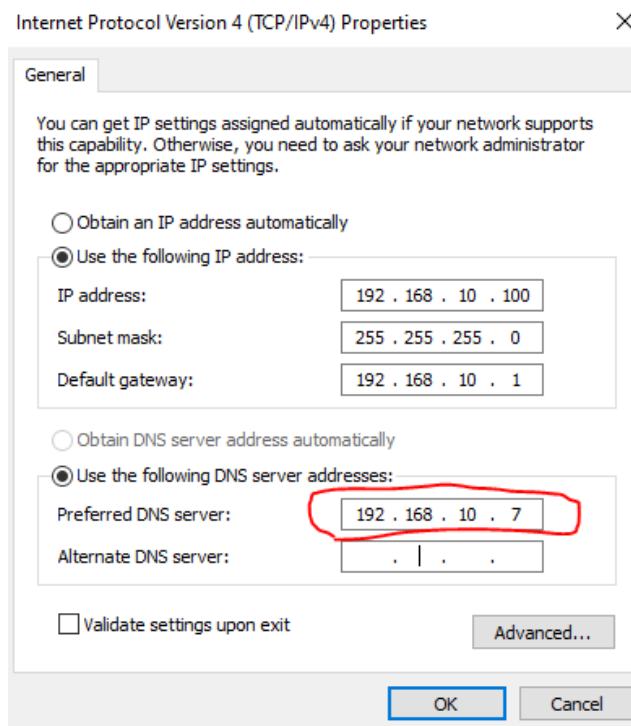
67. To fix this, I first clicked on **Change Adapter Options** in the **Advanced Network Settings**.



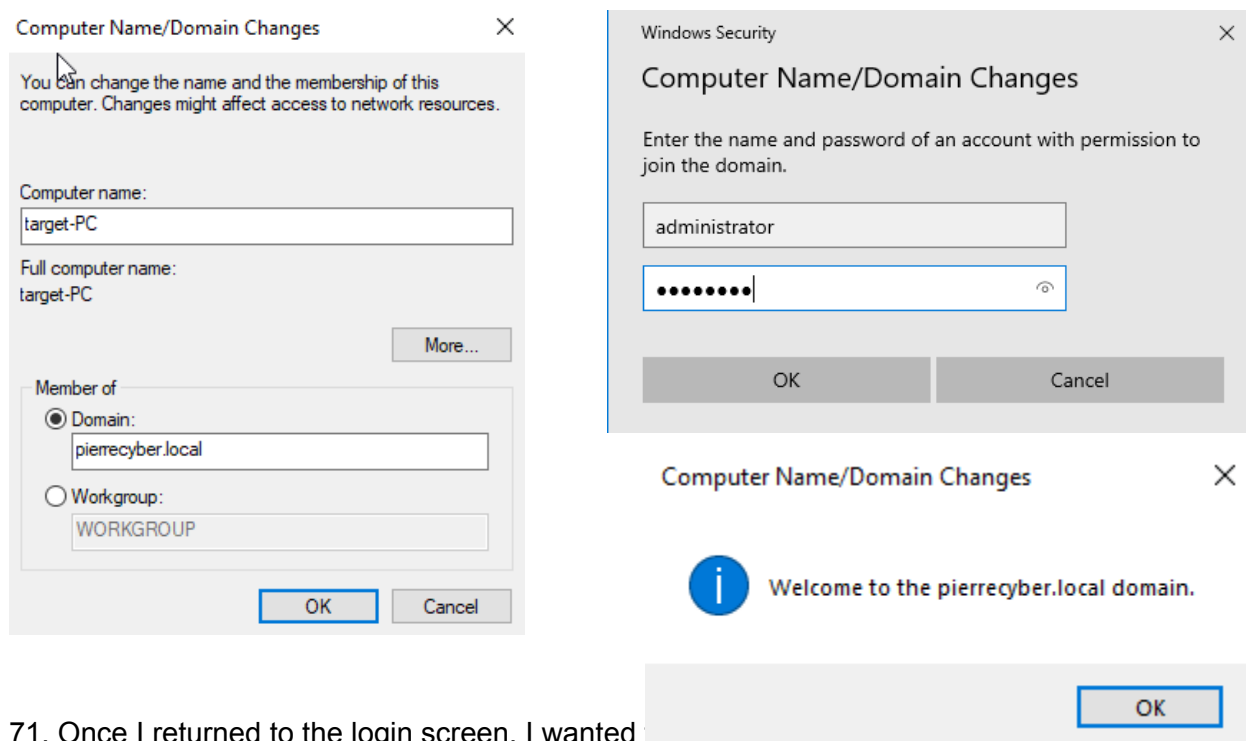
68. Under Ethernet properties, double-click **Internet Protocol Version 4**.



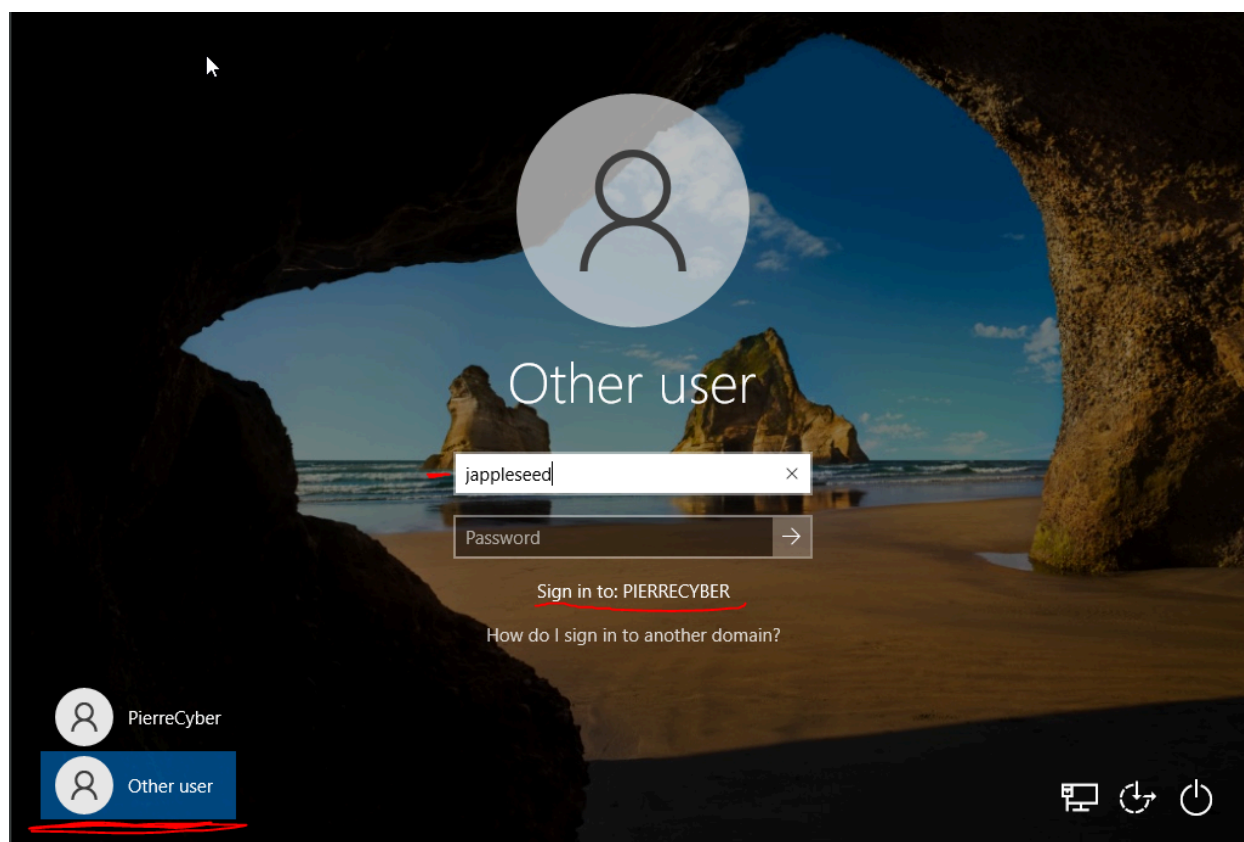
69. I changed the **preferred DNS server** from 8.8.8.8 (Google) to **192.168.10.7** (Domain Controller)



70. I went back and selected “ok” again after typing the domain (pierre cyber.local). This time I was prompted to enter the credentials for the server administrator account. The machine was added to the domain and I restarted the target PC.



71. Once I returned to the login screen, I wanted Appleseed”. I selected “Other User”, and made sure “PIERRECYBER” was the Sign in to: option. I logged in with the credentials created previously in the Server Manager.



****At this point, I have successfully created 2 new users, joined a computer to a new domain, and logged in as a domain user. In the next project, I will be using the Kali Linux machine installed here to perform a brute force attack on the new users created, granting the opportunity to view telemetry via Splunk.***