How to Build a Virtual Home Lab

A Step-by-Step Guide

Benefits of a virtual cyber home lab

- Provides a safe and controlled environment to practice various cyber security scenarios
- Experiment with different configurations and setups
- Learn and practice how to setup and configure secure networks
- Gain familiarity with various security tools
- Stay up to date on latest threats and trends
- Contribute findings and projects to cybersecurity community

Project Ideas

- Create segmented networks to perform malware analysis or malware detonation
- Set up vulnerable web apps to practice web security testing
- Configured firewalls, IDS/IPS, and VPNs
- Create a honeypot
- Analyze Nmap network scan
- Simulate incidents and practice incident handling

LET’S GET STARTED!

Mandatory system requirements

- CPU: 64-bit 2.0+ GHz processor or higher based system is mandatory for this class (Important - Please Read: a 64-bit system processor is mandatory)
- BIOS/UEFI: VT-x, AMD-V, or the equivalent must be enabled in the BIOS/UEFI
- RAM: 8 GB (gigabytes) of RAM or higher is mandatory for this class (Important - Please Read: 8 GB of RAM or higher is mandatory)
- Disk: 500 - 1000 gigabytes of free disk space

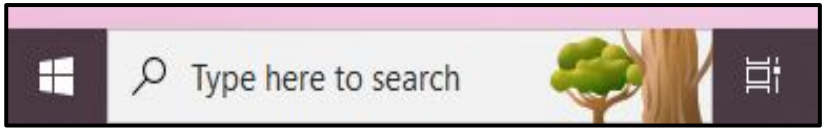
Connectivity

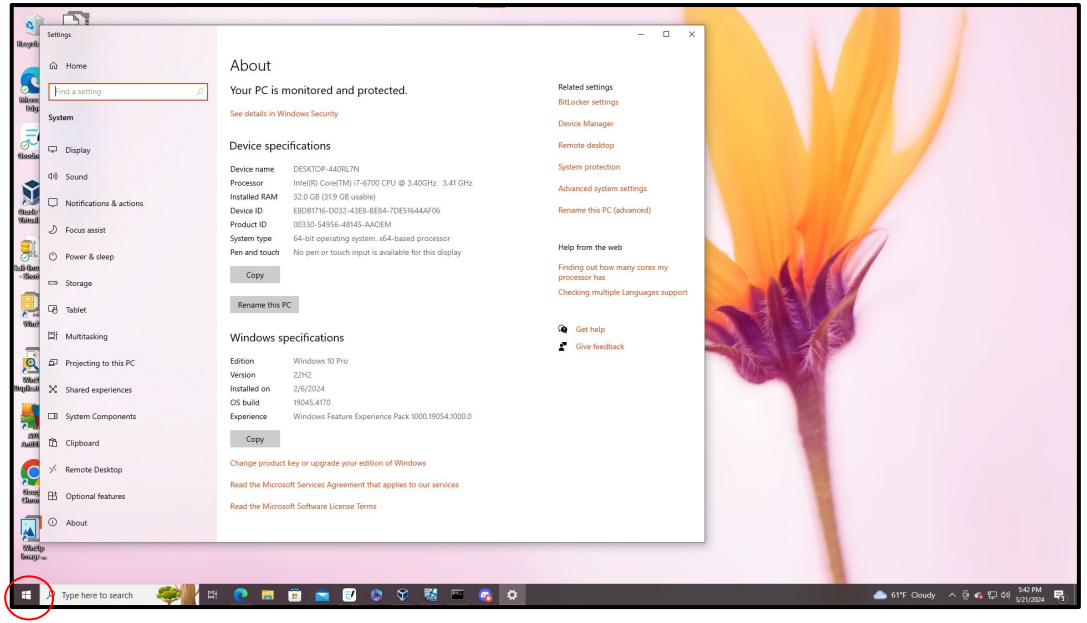
- Wireless Ethernet 802.11 B/G/N/AC USB-A ports or an adapter to use a USB-A thumb drive (version 3.0 compatibility highly recommended)

Does your system meet the requirements?

1. Right click the Windows icon in the bottom left corner of taskbar

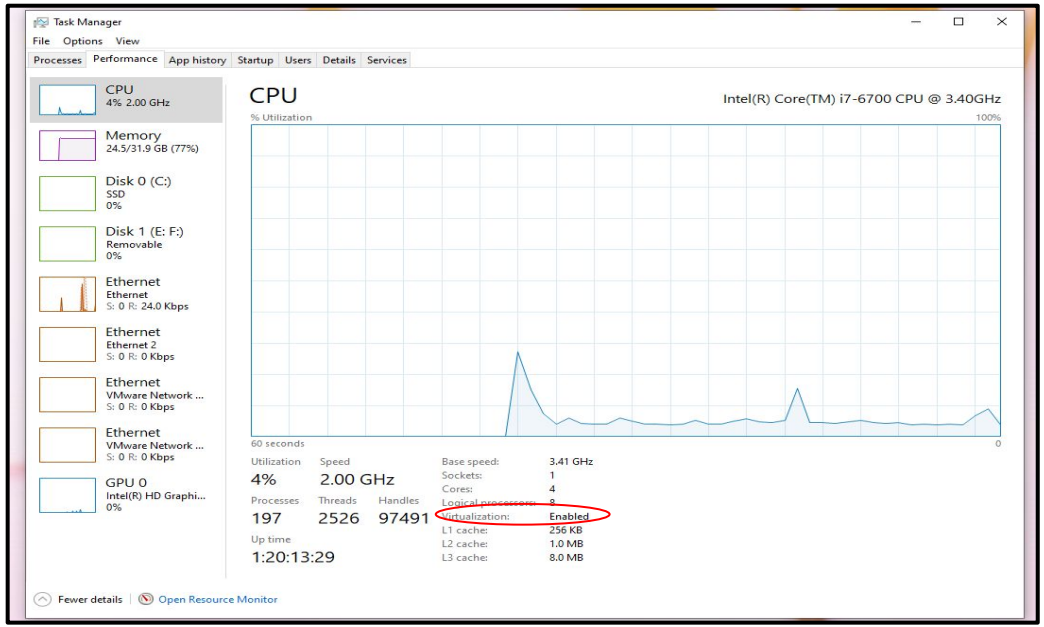
2. Select “System”





Is your system eligible for Virtualization?

- Right click windows icon
- Select Task Manager
- Verify that “Virtualization” is “Enabled”



If Virtualization is disabled, follow these steps:

Enable Virtualization in BIOS (UEFI)

1. Power off your computer.
2. Press the specific hotkey (usually **Esc**, **F2**, or **Del**) to enter the BIOS.
3. Navigate to the **Advanced** tab and select **Virtualization**.
4. Enable it and save the changes.
5. Reboot your computer.

Download files for the lab

- Download and install a Hypervisor (VirtualBox)

  https://www.virtualbox.org/wiki/Downloads

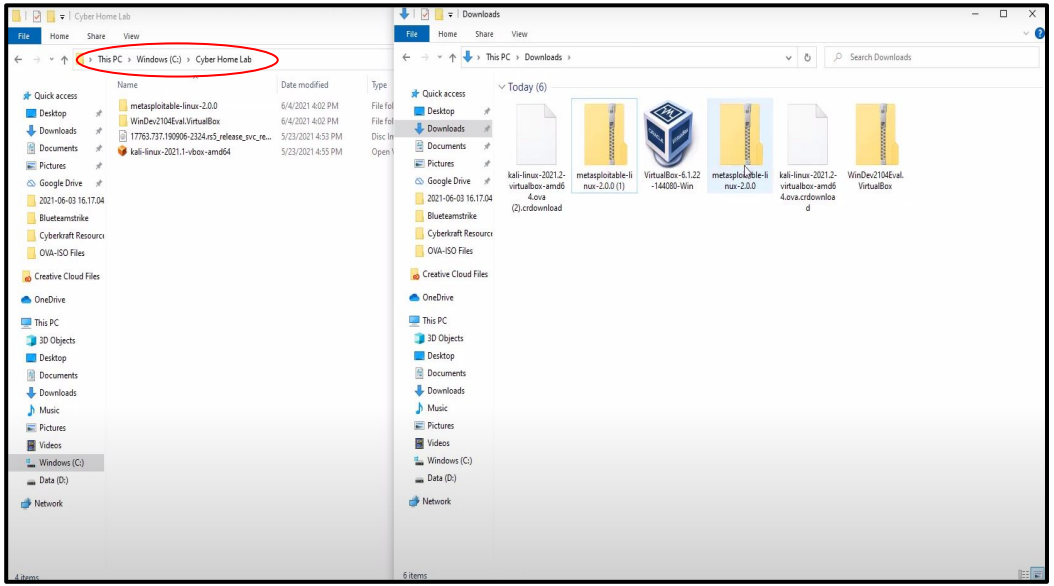
- Download OVA/ISO Files for the Lab Kali Linux - ova
  https://www.offensive-security.com/kali-linux-vm-vmware-virtualbox-image-download/#1572305786534-030ce714-cc3b
- Metasploitable-linux-2.0.0 - ova
  https://sourceforge.net/projects/metasploitable/files/Metasploitable2/metasploitable-linux-2.0.0.zip/download
- Windows 10 - ova

  https://developer.microsoft.com/en-us/windows/downloads/virtual-machines/

- Windows Server 2019 - iso
  https://www.microsoft.com/en-us/evalcenter/evaluate-windows-server-2019

Download files for the lab (cont.)

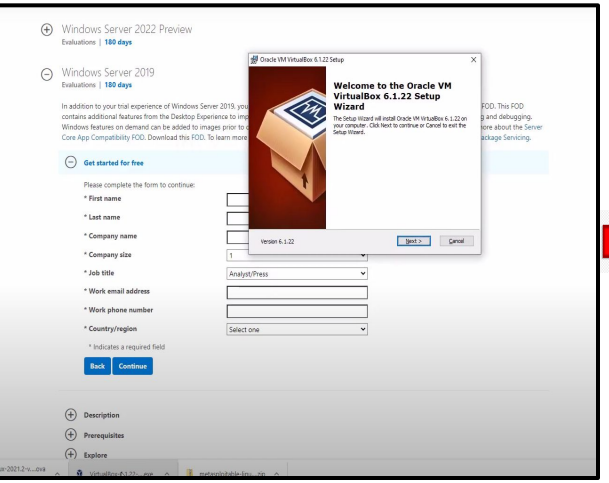
- Navigate to file explorer
- Locate C Drive
- Create folder titled “Cyber Home Lab”
- Move all downloaded files to folder for organization and ease of access
- Note that the Server 2019 and Metasploitable files will be zipped
- Right click the zipped files and select “Extract All…”
- You will then be prompted to select the location of the file you would like to extract



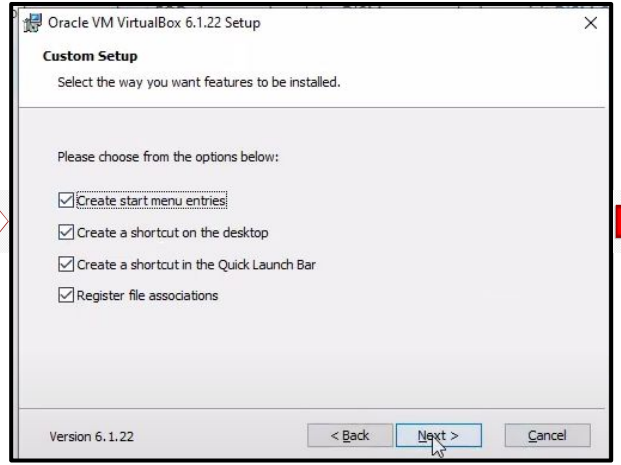
***Rename files for ease of access/organization when importing files in future steps. File names will be listed in slides that follow.**

Install and Configure

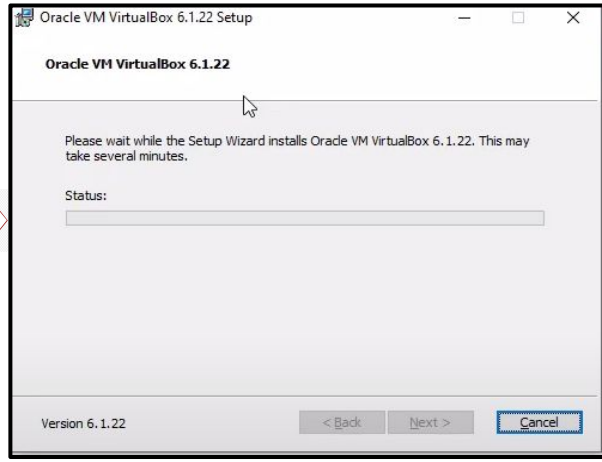
Virtualbox



- Select the Virtualbox download in bottom of screen. Once wizard displays, select “Next”. Repeat this step throughout setup process to install

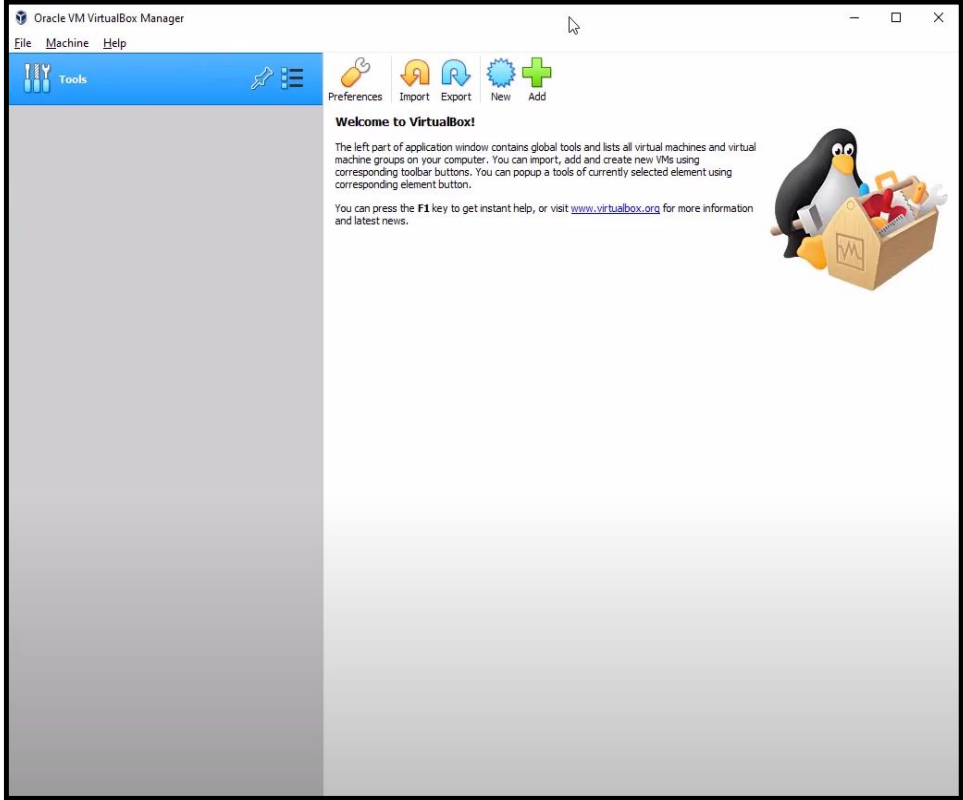


- Ensure each box is selected



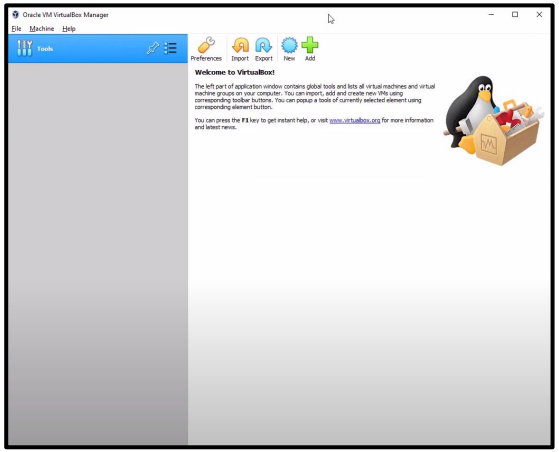
- Select “Yes” on prior pop up box to achieve this option and begin installation process. Once installed select “Finish”.

Success! Great job!

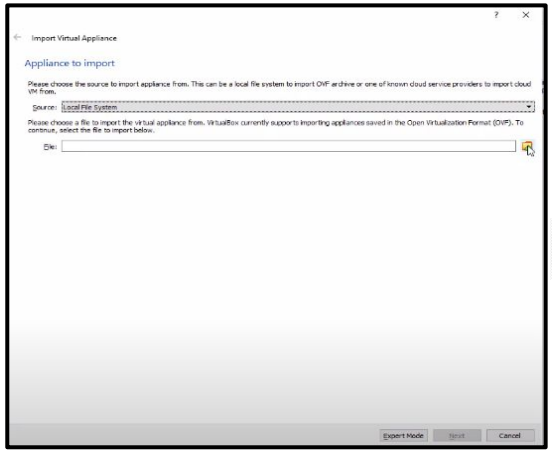


*Pin to taskbar for ease of access
(Right click icon at bottom of screen, select “pin to taskbar”)

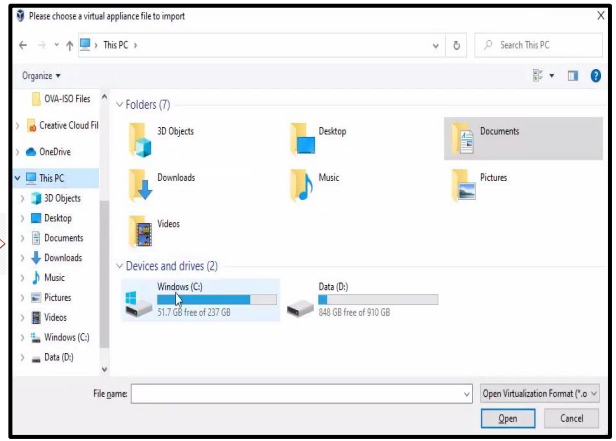
Import Kali Linux



- Select “Import”

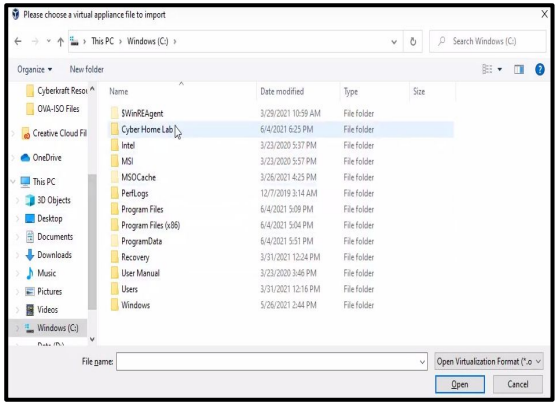


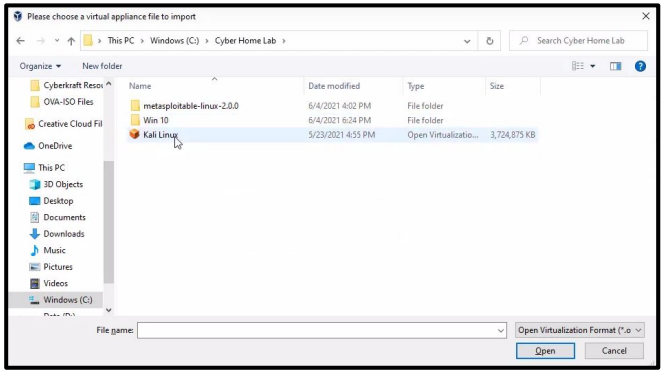
- Select yellow file icon

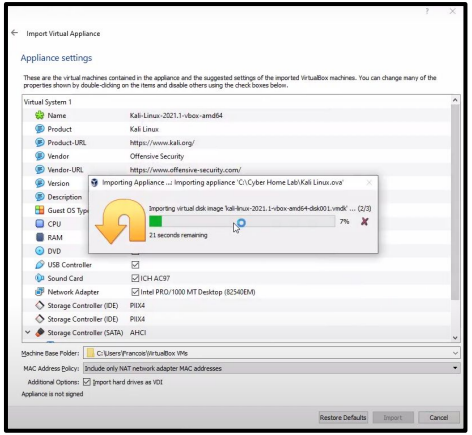


- Locate C drive

Import Kali Linux (Cont.)





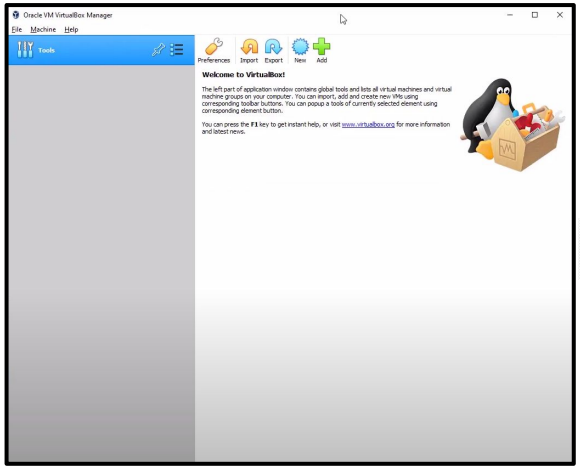


- Access “Cyber Home Lab” folder

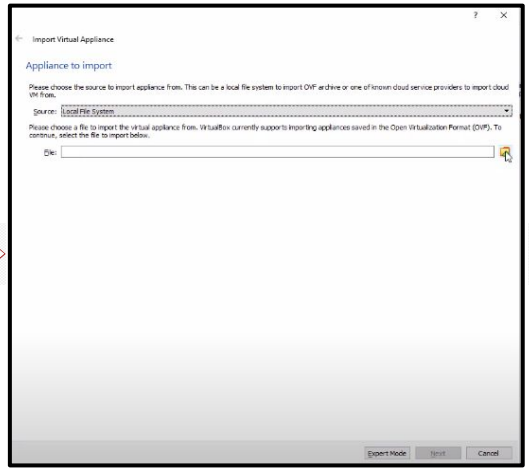
- Access Kali Linux OVA file

- Select “Next”
- Select “Import”
- Agree to terms
- Installation will begin

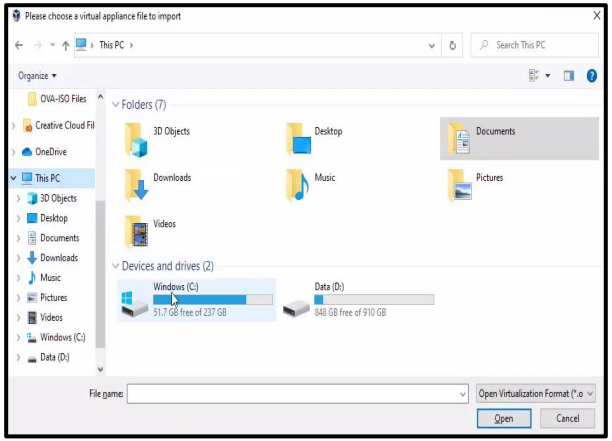
Import Windows 10 (Win10)



- Select “Add”

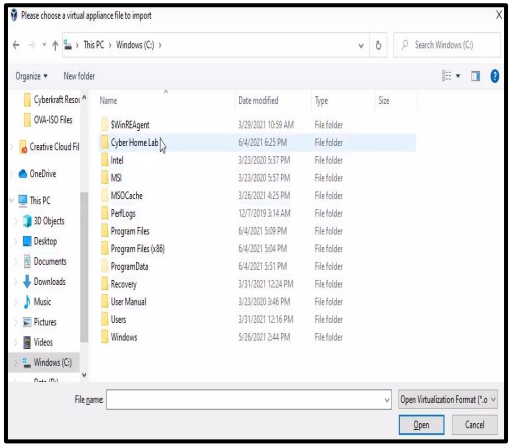


- Select yellow file icon

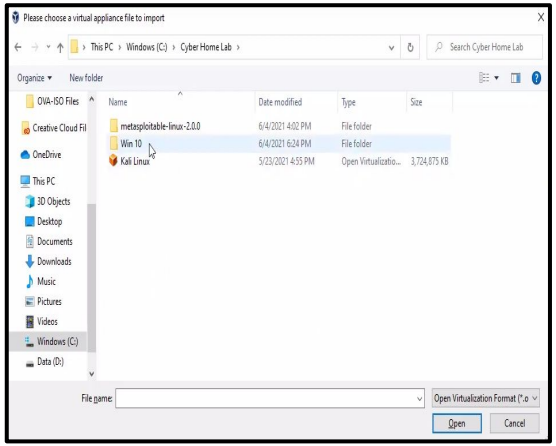


- Select Windows C drive

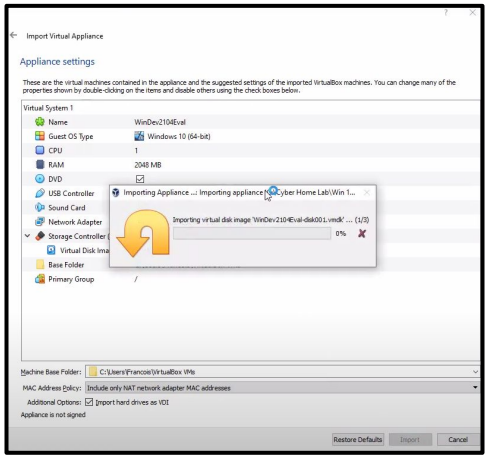
Import Windows 10 (Win10) (Cont.)



- Access “Cyber Home Lab” folder

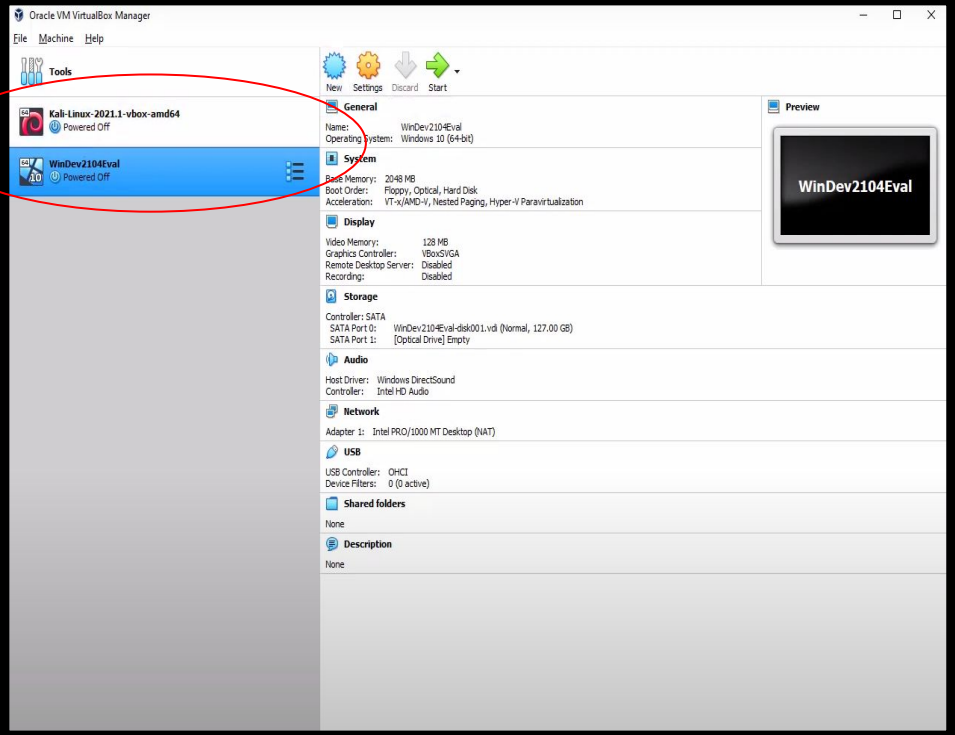


- Access Windows 10 file



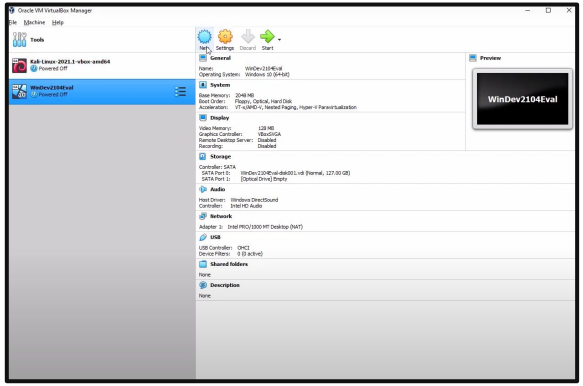
- Select “Next”
- Select “Import”
- Agree to terms
- Installation will begin

Success! Great job!

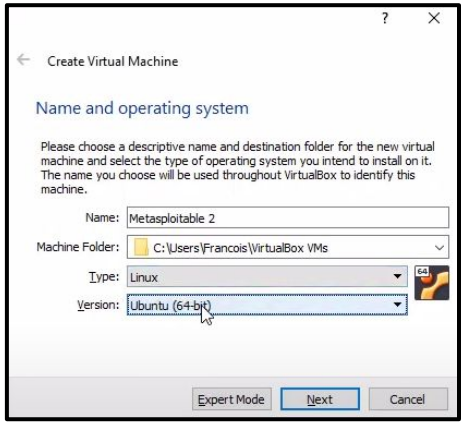


***Right click tool and access “Settings” to rename for understanding**

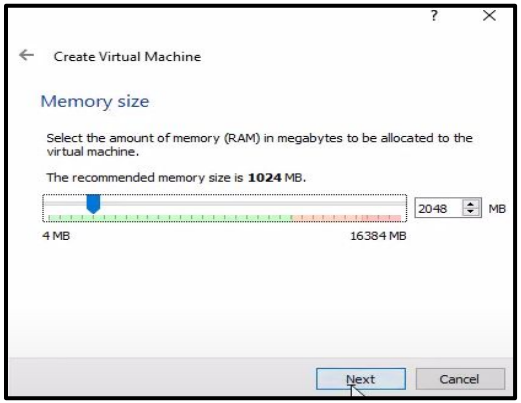
Metasploitable 2



- Select “New”

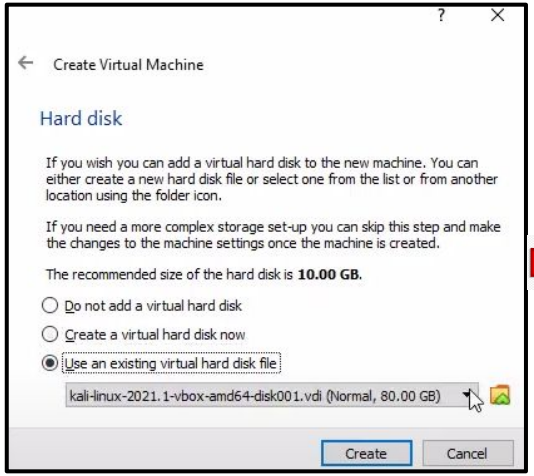


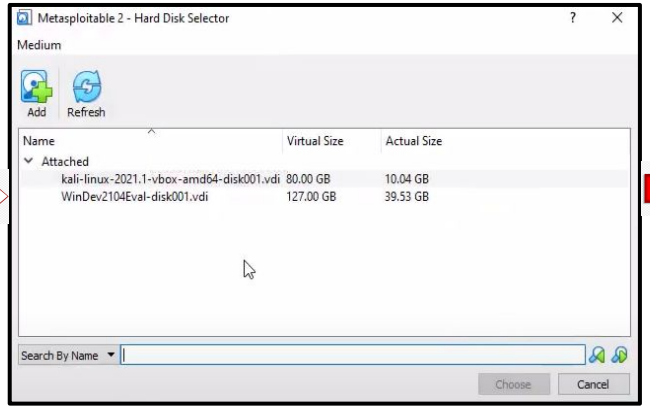
- Input “Metasploitable” in name field, “Linux” in type field, and “Ubuntu 64-bit” in version field
- Select “Next”

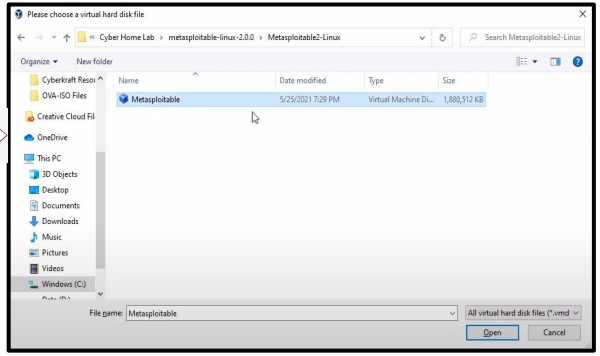


- Set memory to 2048 MB
- Select “Next”

Metasploitable 2 (Cont. 1)





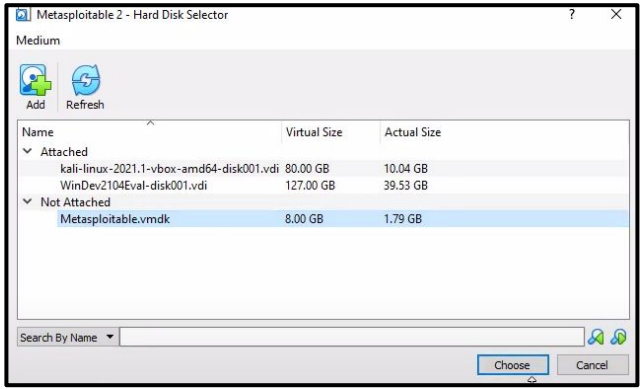


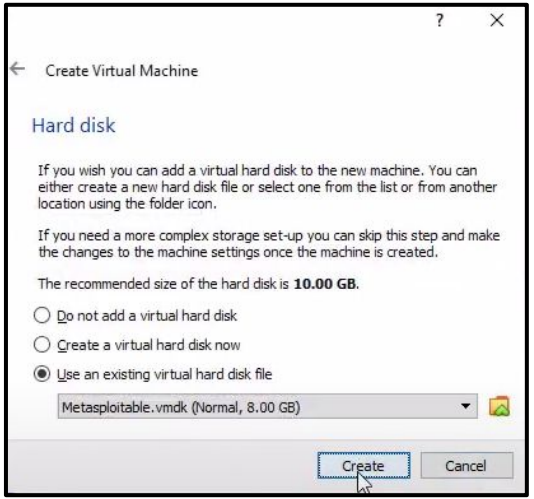
- Select “use an existing virtual hard disk file”
- Select yellow file icon

- Select “Add”
- File explorer will populate
- Locate C drive

- Select Metasploitable file

Metasploitable 2 (Cont. 2)

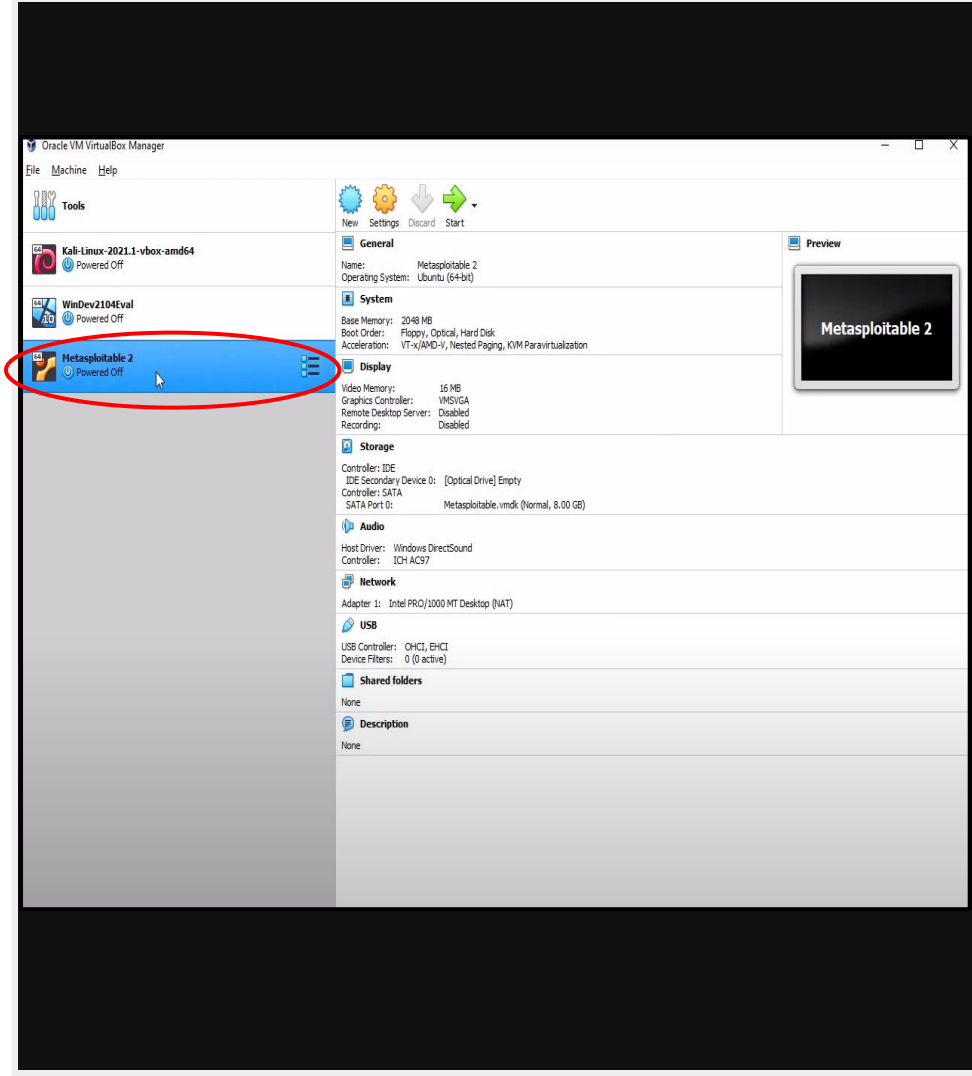




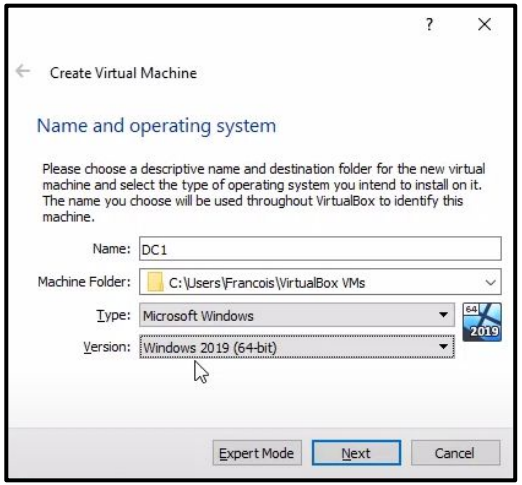
- Metasploitable will populate
- “Choose” the file

- Once attached, “Create” the file

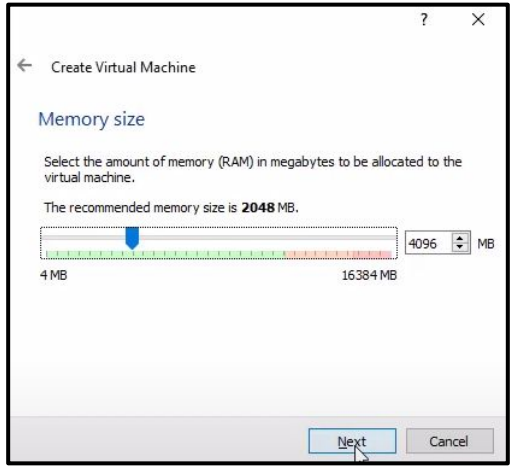
Success! Great job!



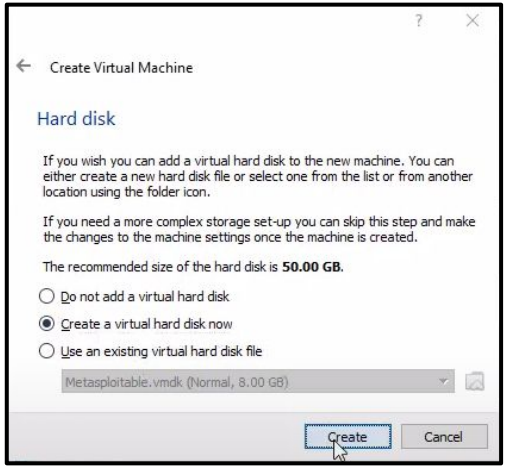
Server 2019 (DC1)



- Input “Metasploitable” in name field, “Linux” in type field, and “Ubuntu 64-bit” in version field
- Select “Next”

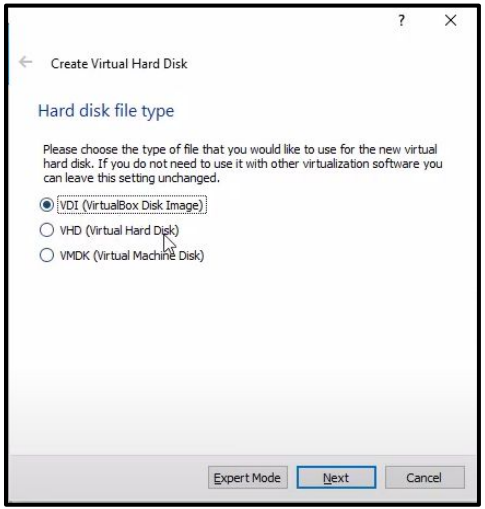


- Set memory size to 4096MB

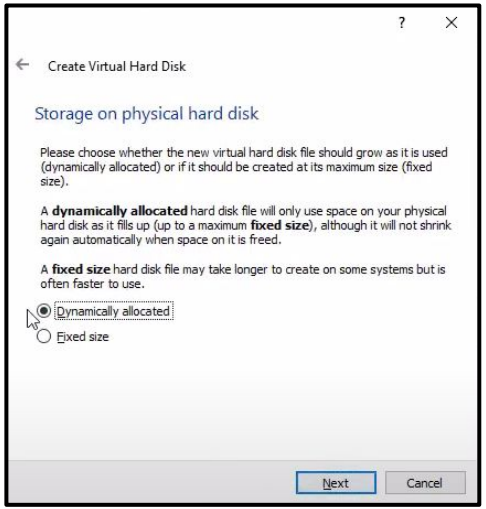


- Select “Create a virtual hard disk now”
- Select “create”

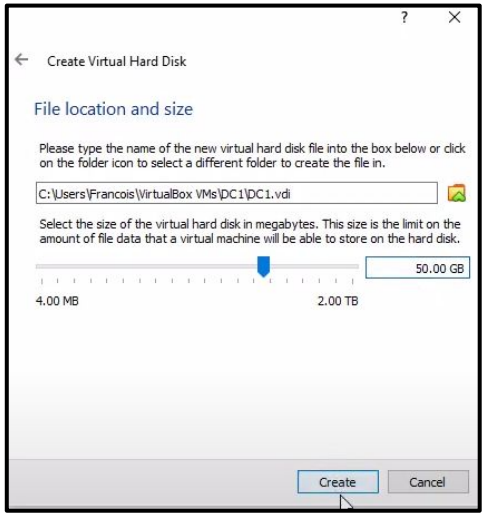
Server 2019 (DC1) (Cont. 2)



- Select “VDI (Virtual Box Image)”
- Next

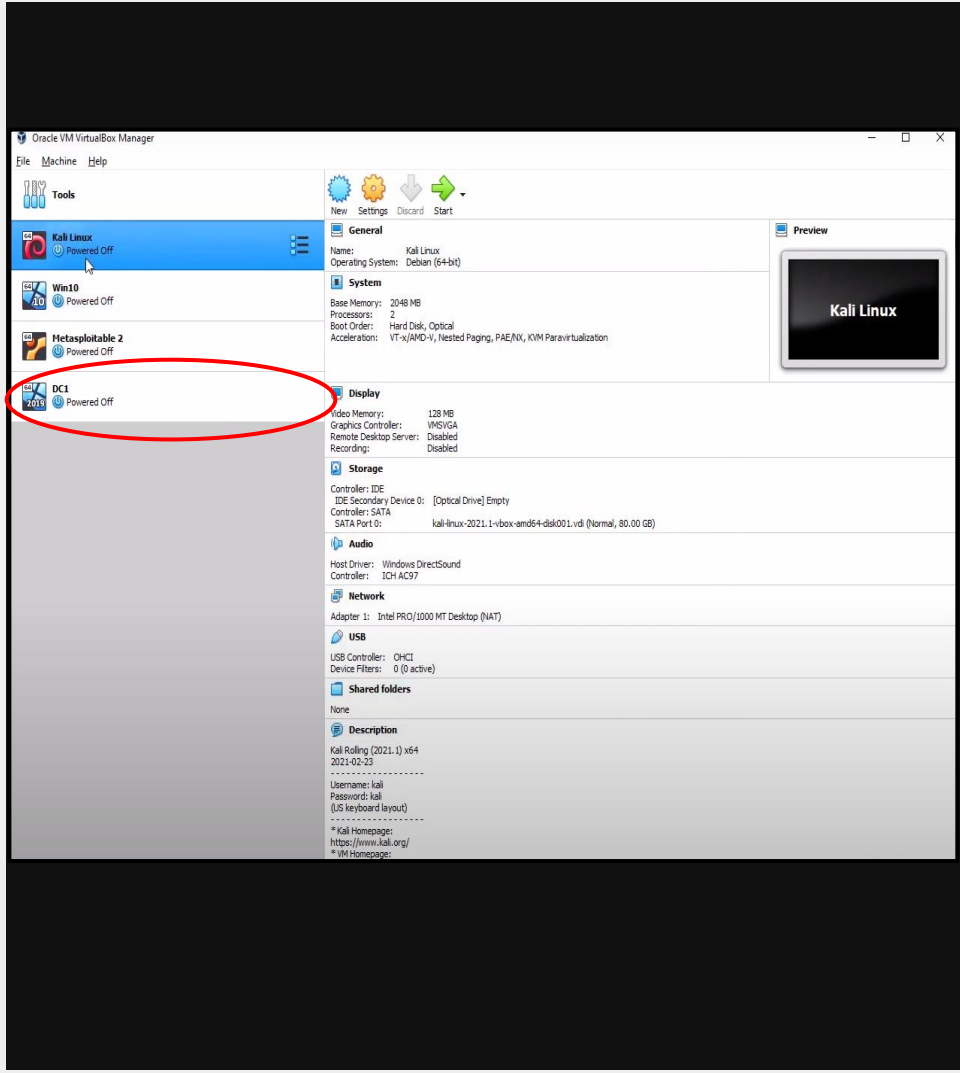


- Select “Dynamically allocated”



- Set file size to 50GB
- Create

Success! Great job!

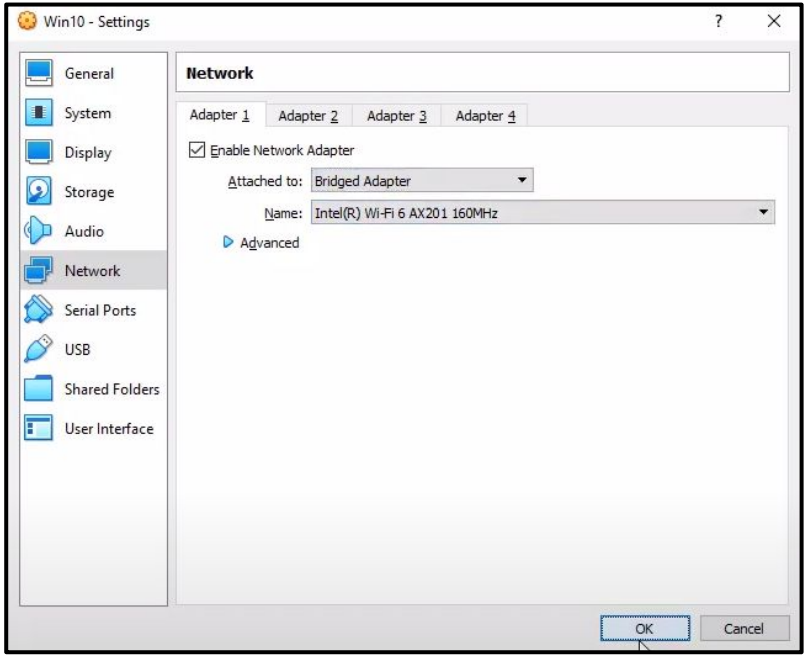


Bridged Adapter

Bridged Adapter

To allow communication and internet connectivity amongst each tool, the network must be placed on the bridged adapter option.

- Right click each tool and select the “Settings” option
- Once in settings, select the “Network” category
- Ensure the “Enable Network Adapter” option is checked
- In the “Attached To” field. Select “Bridged Adapter”



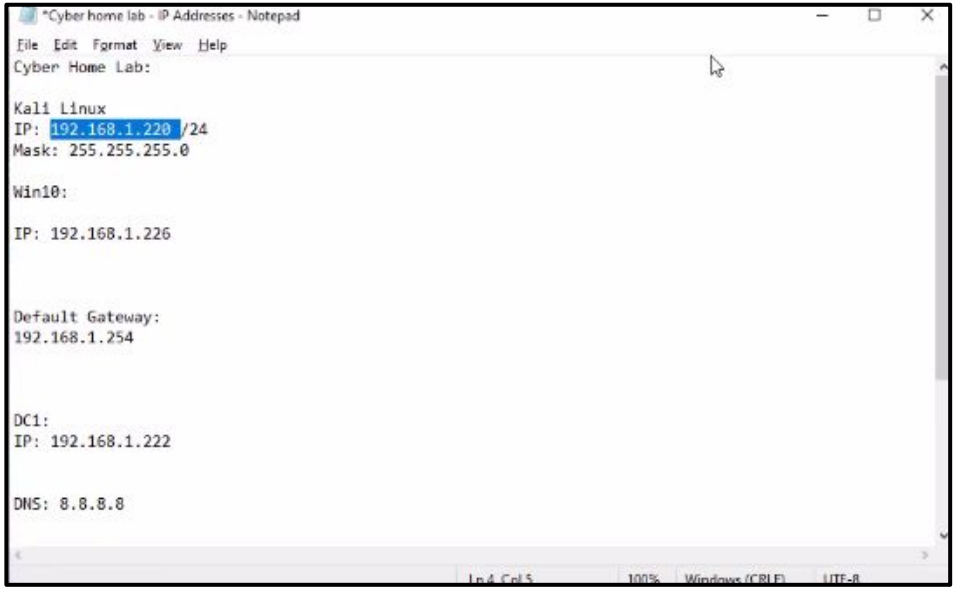
***Complete this step for each tool in Virtualbox**

Success! Great job!

Let’s Start the Machines!

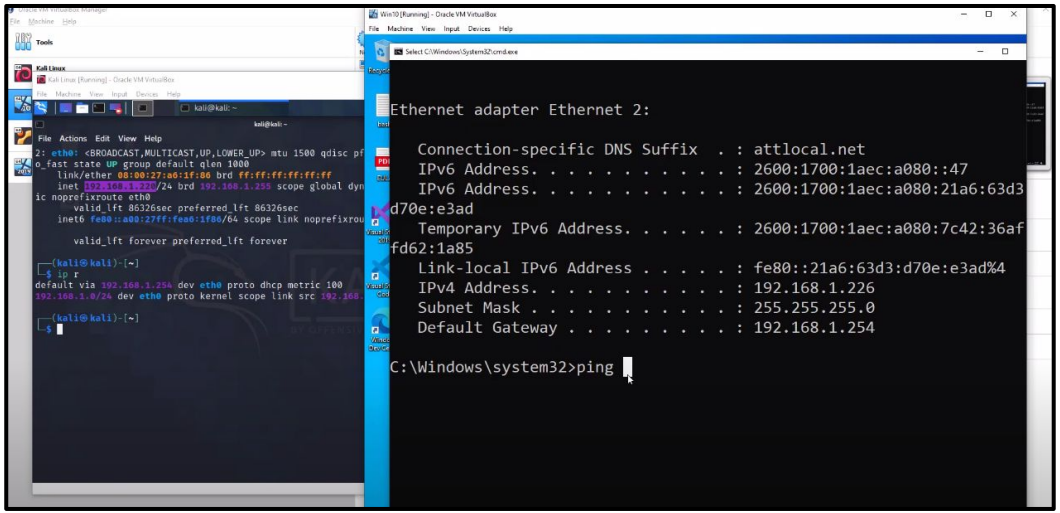
Verify that the machines will start

- Highlight the kali linux machine and select start
- Sign into the machine with the username: kali and password kali
- Once the machine has launched access the terminal in the top left corner and note the machine's ip (Ifconfig)
- Repeat this step for Win 10 (Ipconfig)



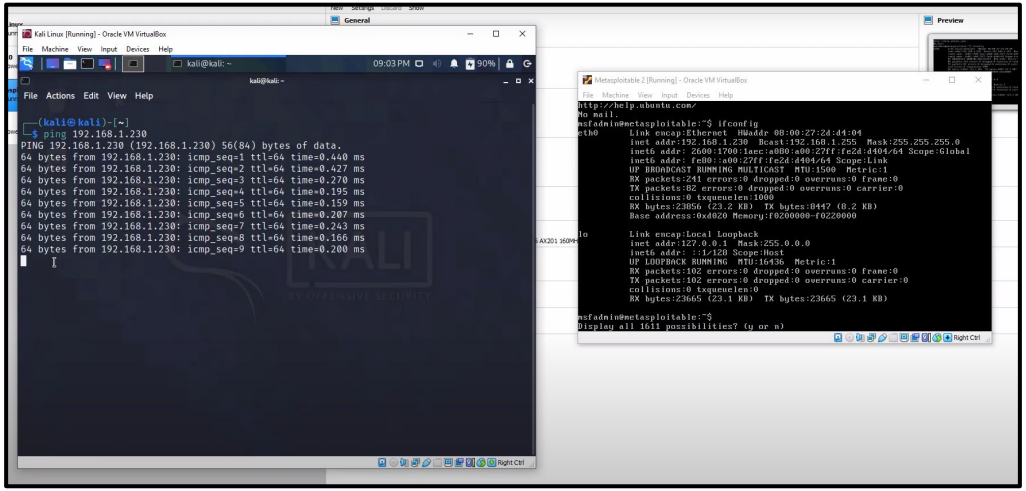
Ping It!

- After documenting the IPs of Kali Linux and the Win 10 machines, access the “Cmd” tool in Win 10
- With Kali Linux still open, on the Win 10 machine, ping the Kali Linux IP to verify that the machine is responding



Ping It! (Cont.)

- Start the Metasploitable 2 machine and sign in with “msfadmin” phrase for the user/pass
- Type “Ifconfig” in the cmd line
- After documenting the IP, ping the address in the Kali Linux machine
- Repeat these steps to ping the Kali Linux IP in Metasploitable 2
- Once completed, power off machines

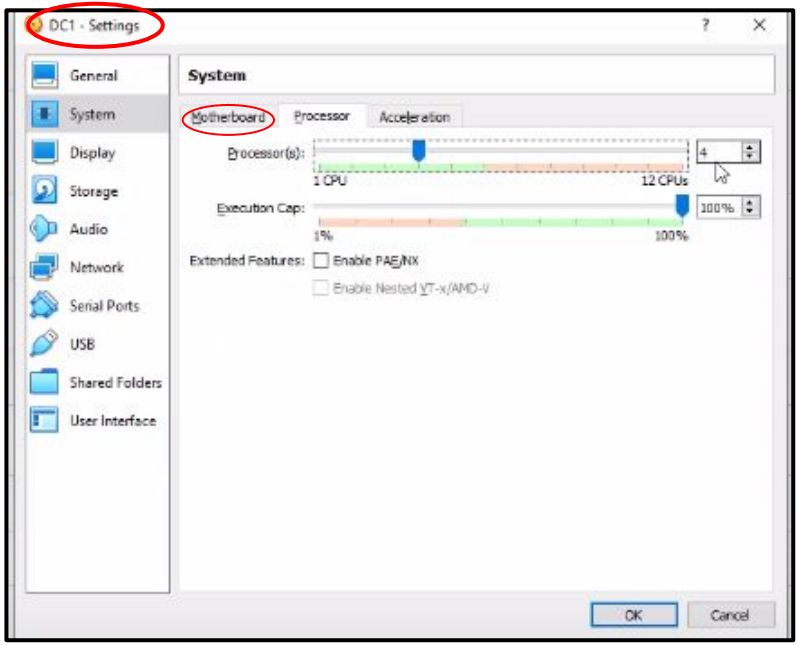


Success! Great job!

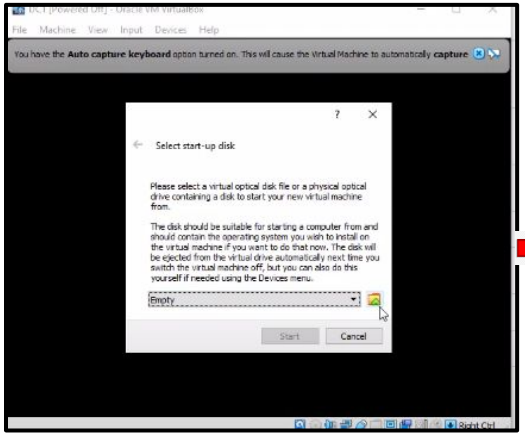
Let’s Install the DC1 Server!

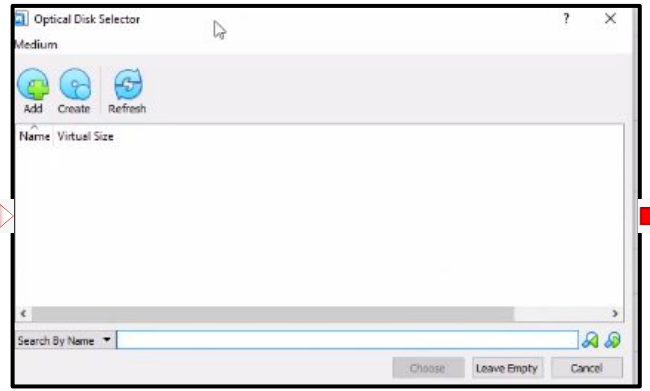
DC1

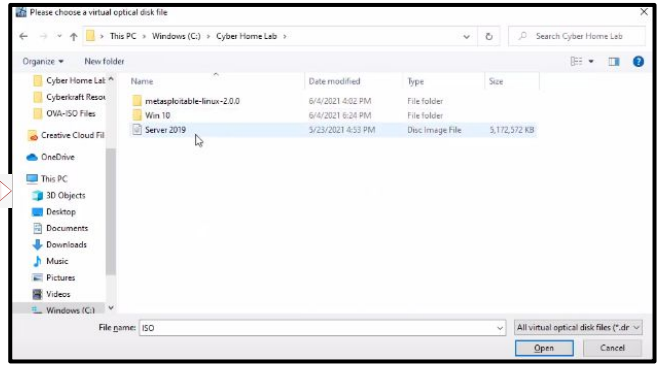
- Right click the DC1 Server machine and select settings.
- Once in settings, under the “motherboard” tab, input 8192MB. Also select the “processor” tab and set CPU to 4 for speedy installation. Select ok.
- After completing this step, start the machine



DC1 (Cont. 2)

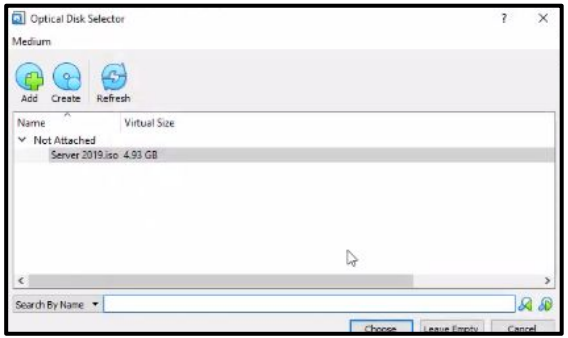


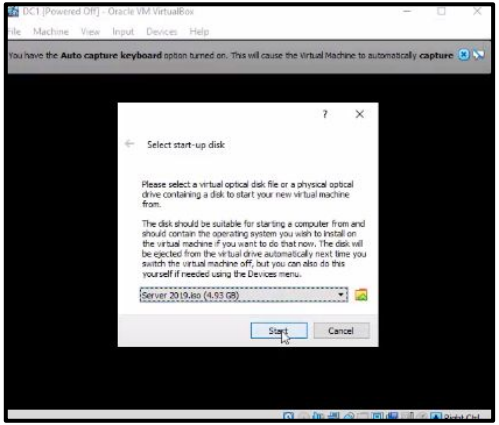


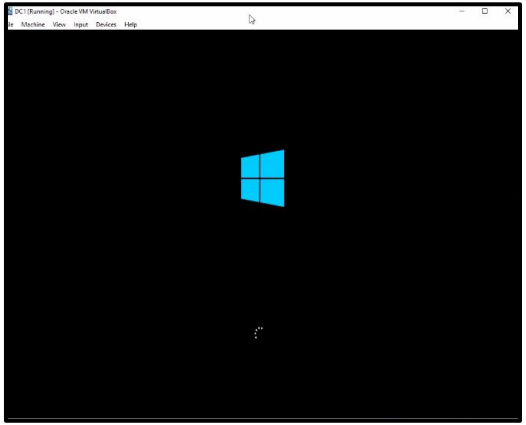


- Select yellow file icon
- Select “Add”
- Locate Windows C drive in File Explorer
- Access Cyber Home Lab folder
- Select “Server 2019” file

DC1 (Cont. 3)

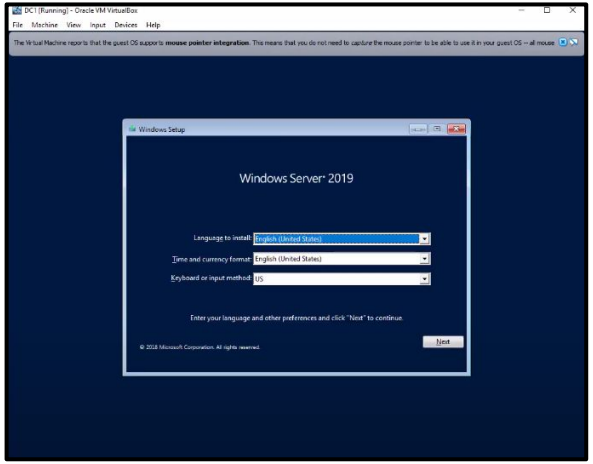




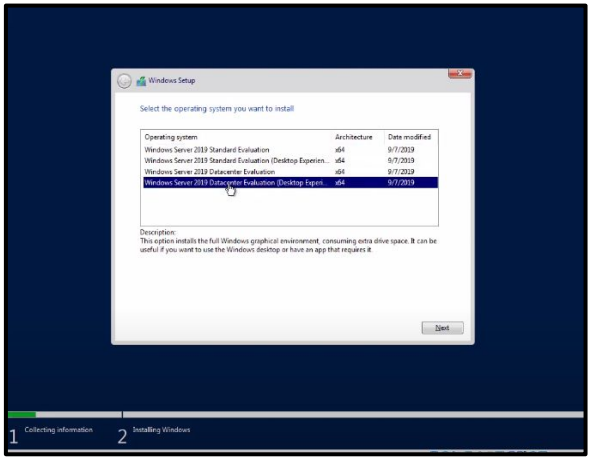


- Once the “Server 2019” file populates, select “Choose”
- Select “Start”
- Allow the server to load

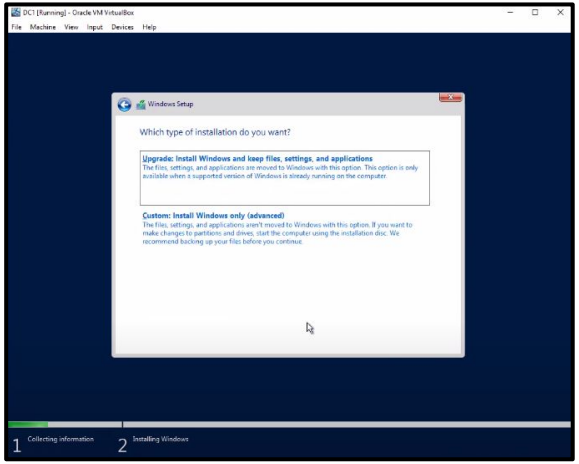
DC1 (Cont. 4)



- Select desired language



- Select “Windows Server 2019 Data Server Evaluation (Desktop Experience)”

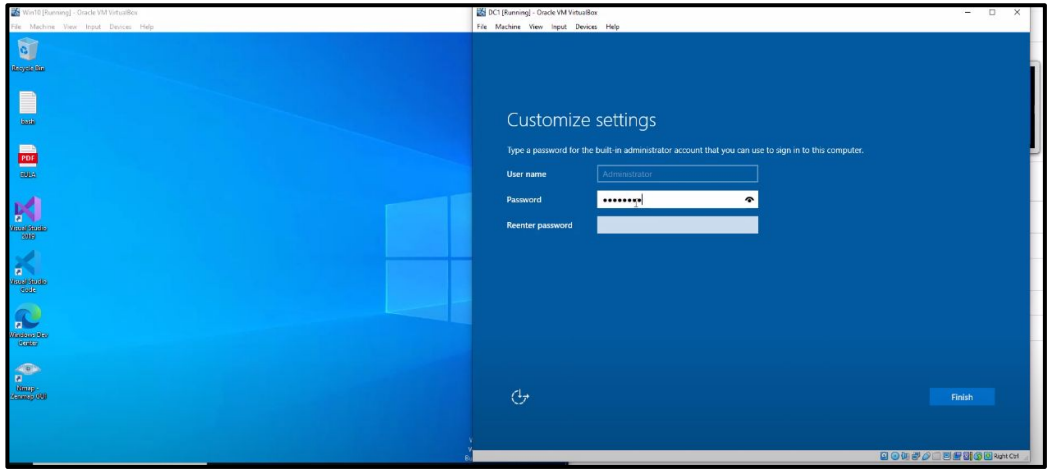


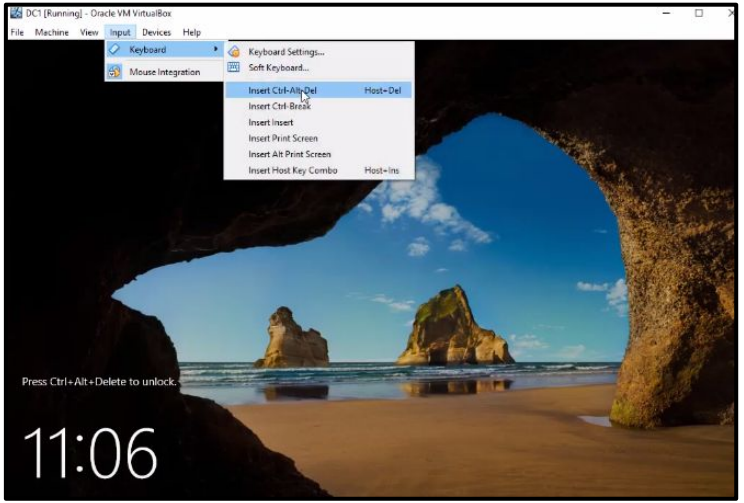
- Accept terms
- Select “Custom”
- Select “Next” without making changes
- Installation will begin

Success! Great job!

DC1

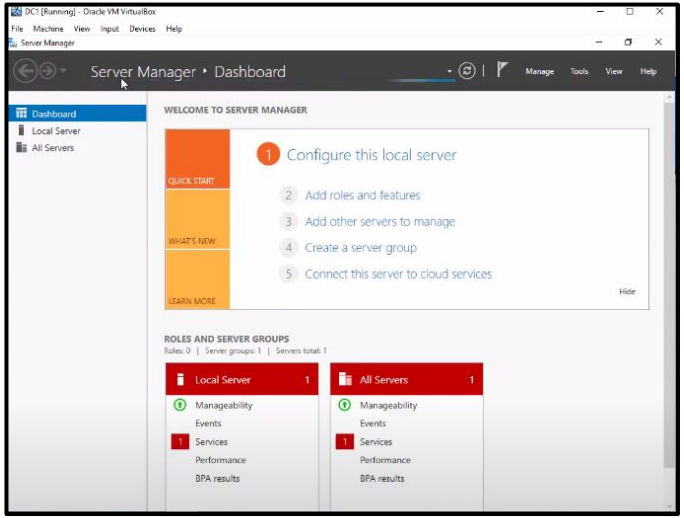
- Once the server's installation has completed, assign a password to the machine. Then select "Finish".
- You will then be directed to the Windows welcome screen
- At the top of the machine there will be a tab that reads "Input". Select that tab. Then select "keyboard"
- Once selected, search the drop down menu for the option that reads "Insert Ctrl-Alt-Delete"
- After this, you will be prompted to sign in with the password you created prior

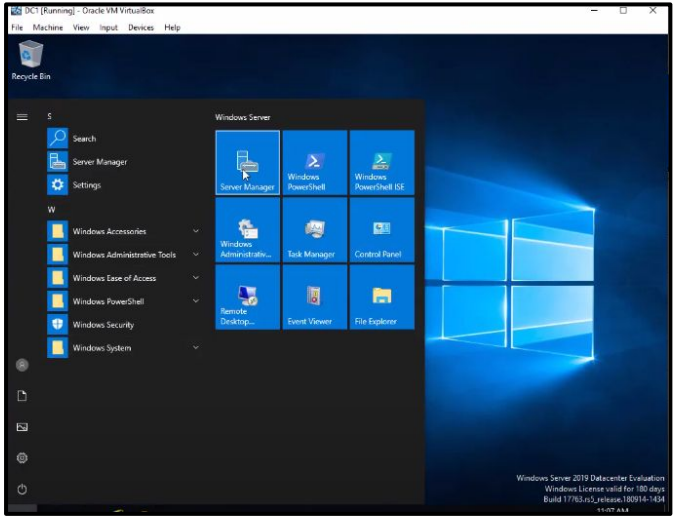




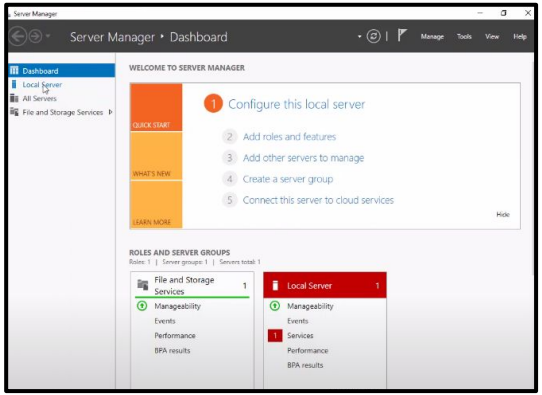
DC1 Cont.1

- Congrats! Welcome to the Windows 2019 Server.
- By default you will be directed to the Server Manager. However, if this does not auto populate, select your windows start icon and the option will be to your right.

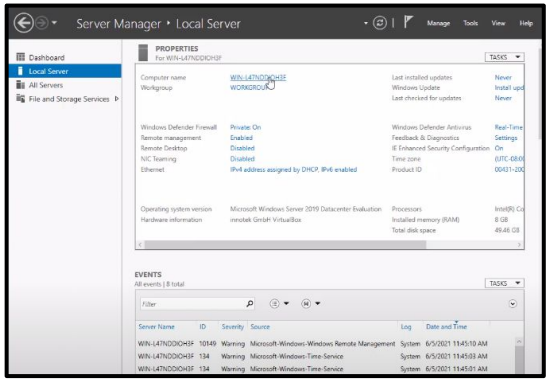




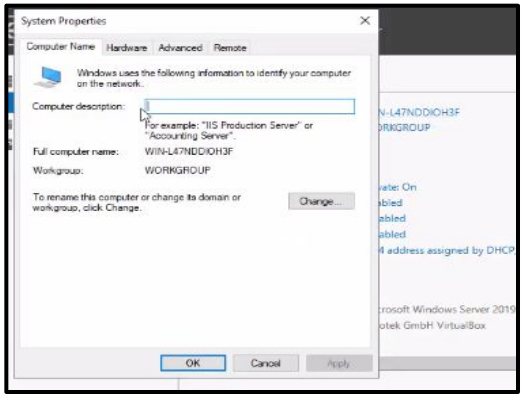
DC1 (Cont.2)



- Select “Local Server”

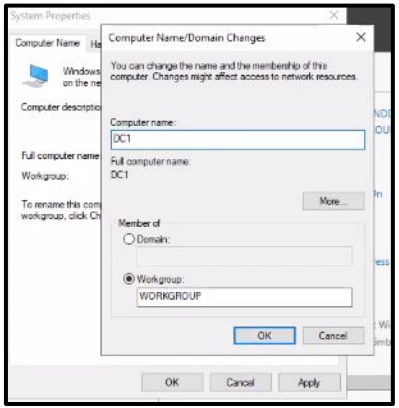


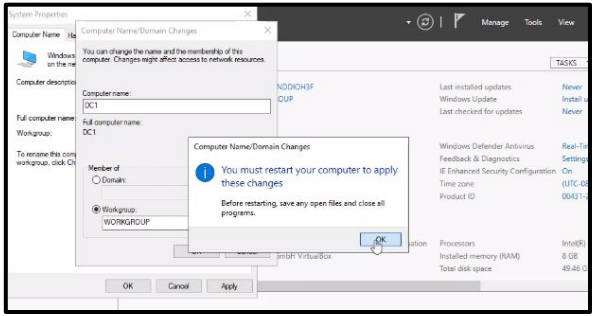
- Select highlighted computer name

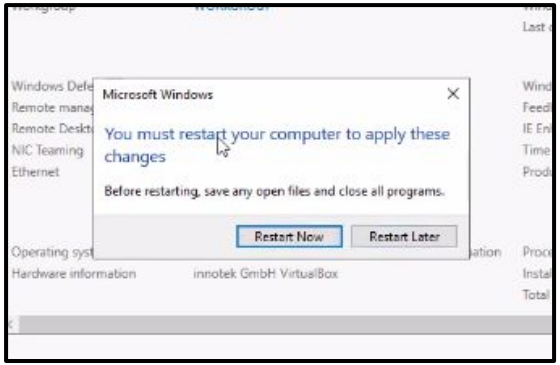


- Change “Computer description” to Server 2019. Select “change”.

DC1 (Cont.3)

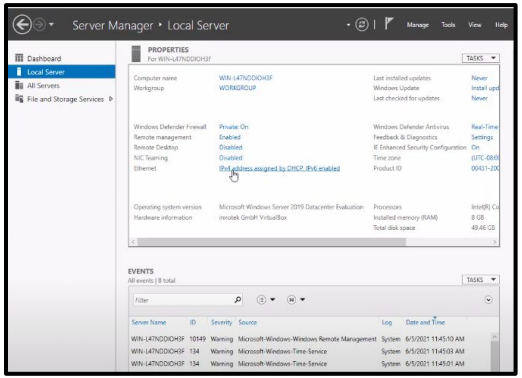


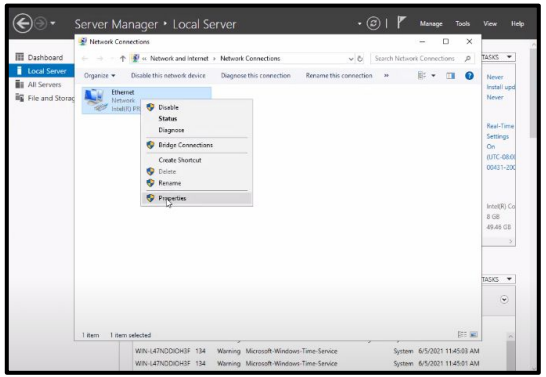


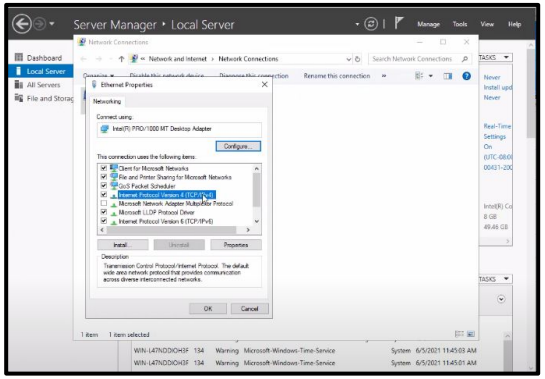


- Change “Computer name” to “DC1”
- Select “ok”, then select “apply”,
- Select “restart later”

DC1 (Cont.4)



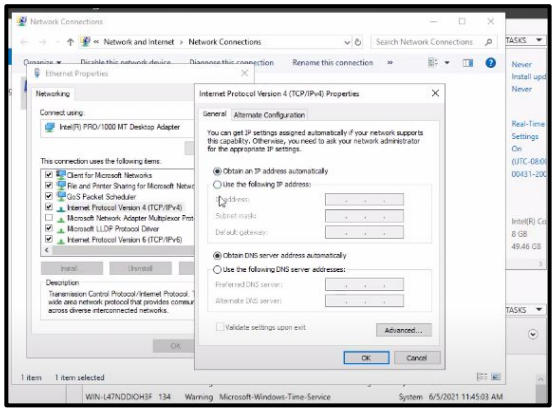


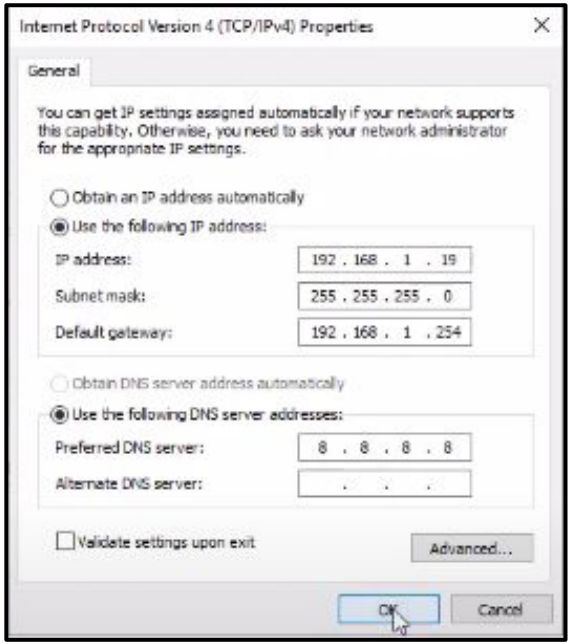


- Select the “ethernet” option
- Right click ethernet option. Select “Properties” in drop down menu
- Highlight “Internet Protocol Version 4”, then select “Properties”

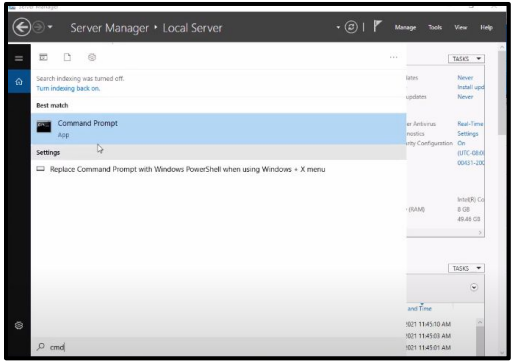
DC1 (Cont.5)

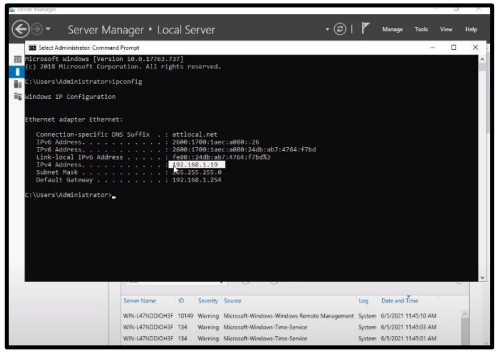
- Select “Use the following IP address”
- Select “Use the following DNS server address”
- Input the following values in each field
- The properties are found in the cmd line tool via “Ipconfig” command (reference slides 30-34)
- Select “Ok” and close ethernet window

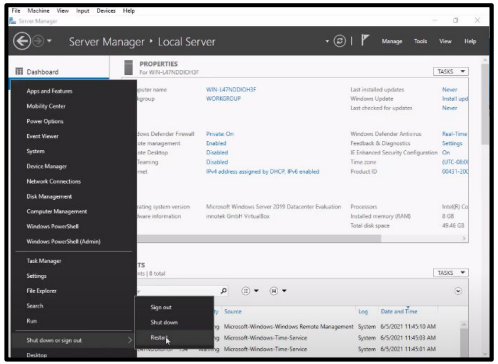




DC1 Cont.







- Access the windows command line tool

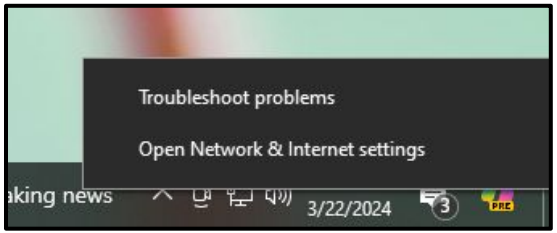
- Verify that the manual IP address that was set is being reflected in the command line tool

- After verifying the IP, right click the windows icon and restart the machine. Select “ok”

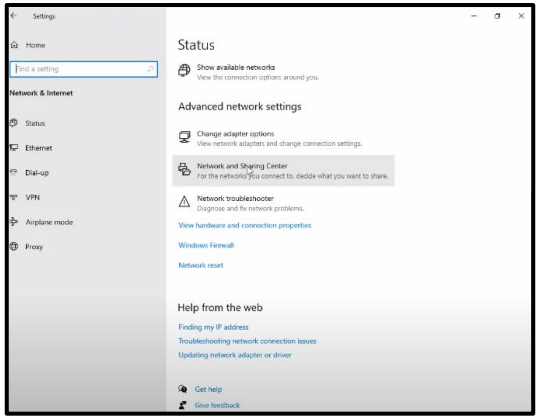
Success! Great job!

Navigate to the Win 10 machine!

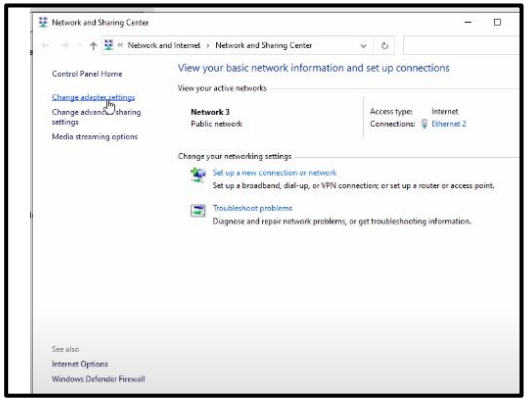
Win 10



- In the win 10 machine, right click the network icon in the bottom left corner and select “Open Network and Internet Settings”.

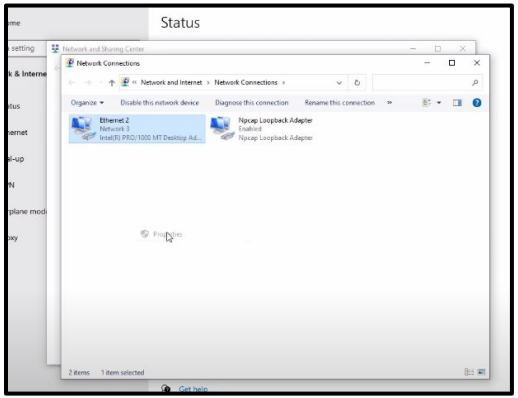


- Once in the settings access the “Network and Sharing Center”.

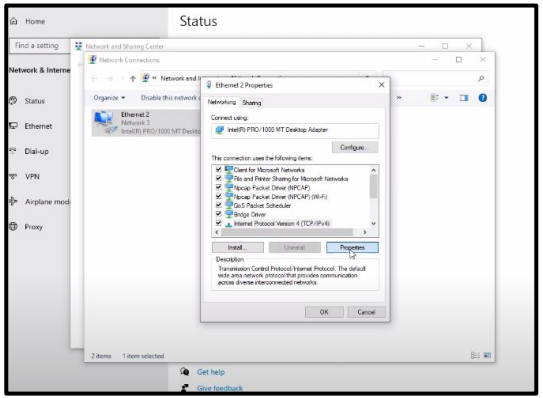


- Select “Change adapter settings”.

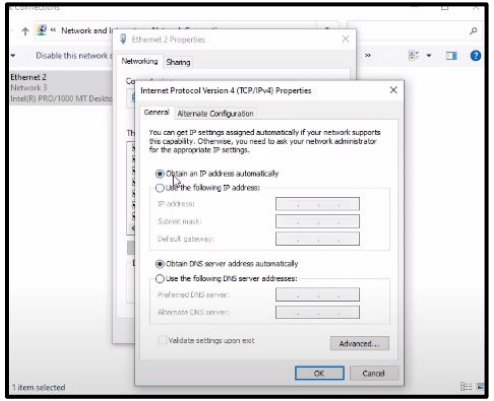
Win 10 (Cont. 1)



- Right click “Ethernet 2” box
- Select “Properties” in the drop down menu



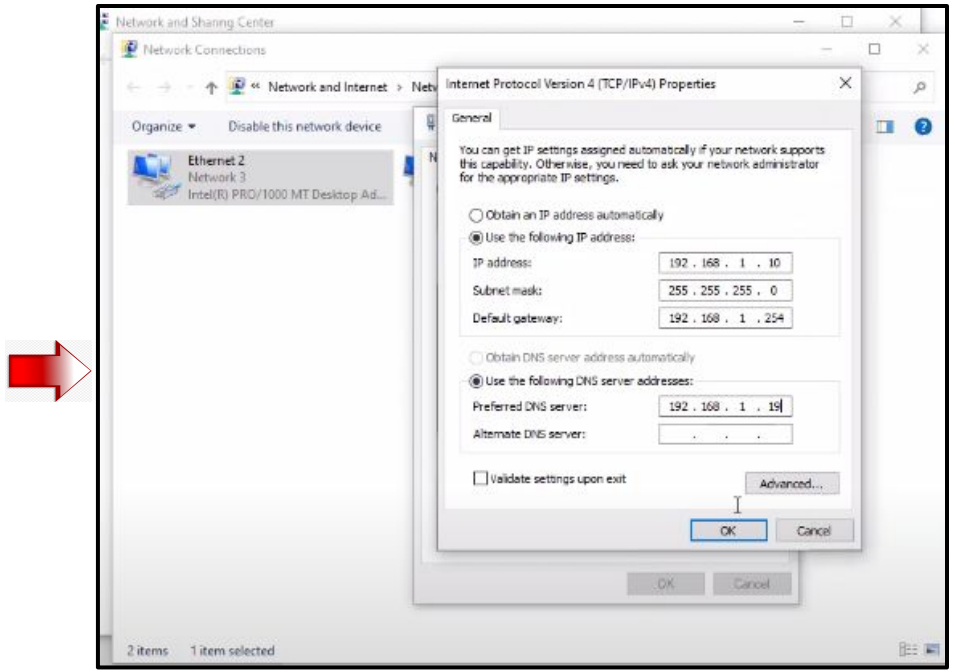
- Highlight “Internet Protocol Version 4” then select “Properties”



- Select “Use the following IP address”
- Select “Use the following DNS server address”

Win 10 (Cont. 2)

- Input the following values in each field
- Select “Ok” then close the ethernet window



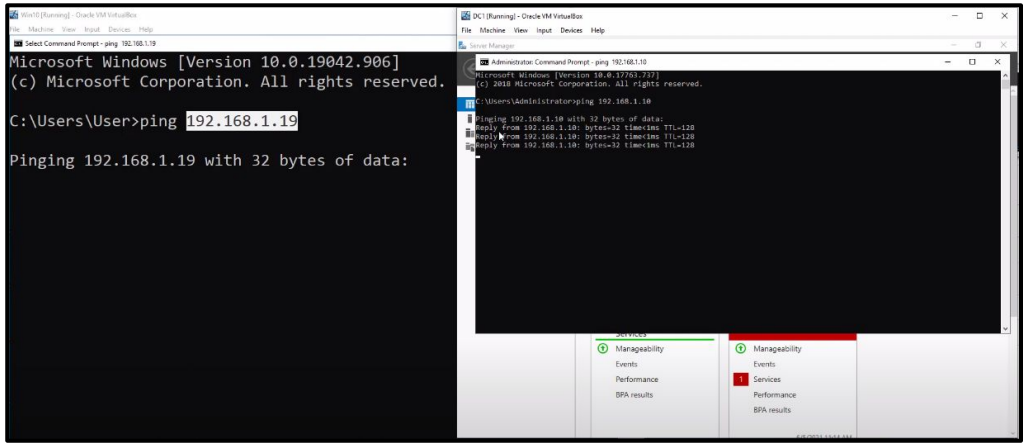
*Notice that the “Preferred DNS server” field will consist of DC1 server’s IP address

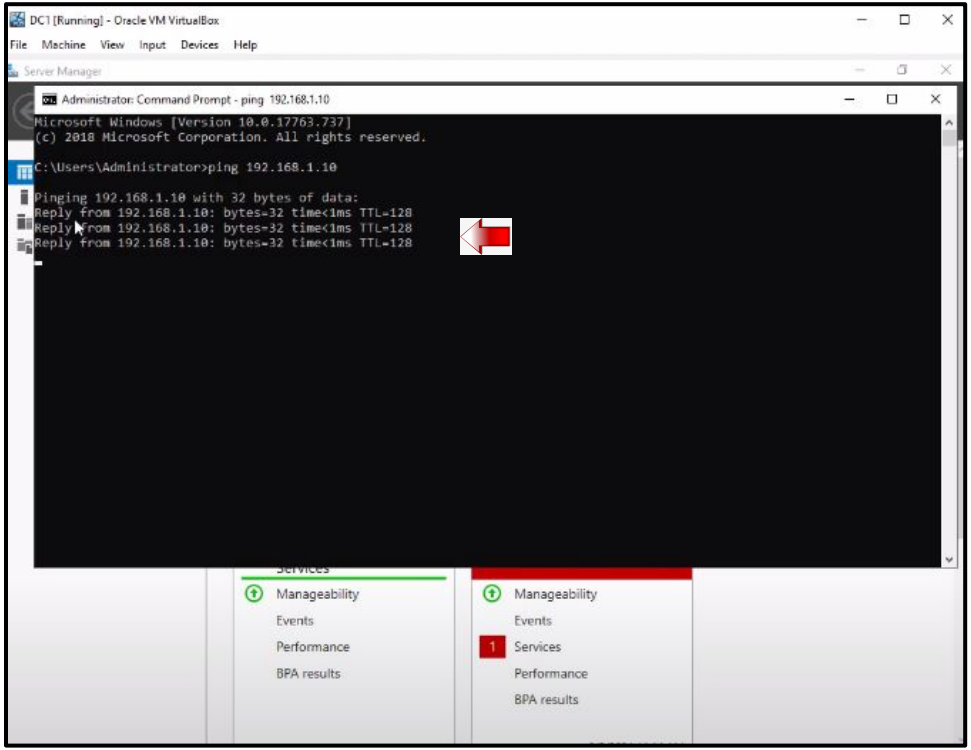
Success! Great job!

Navigate to the DC1 Server machine!

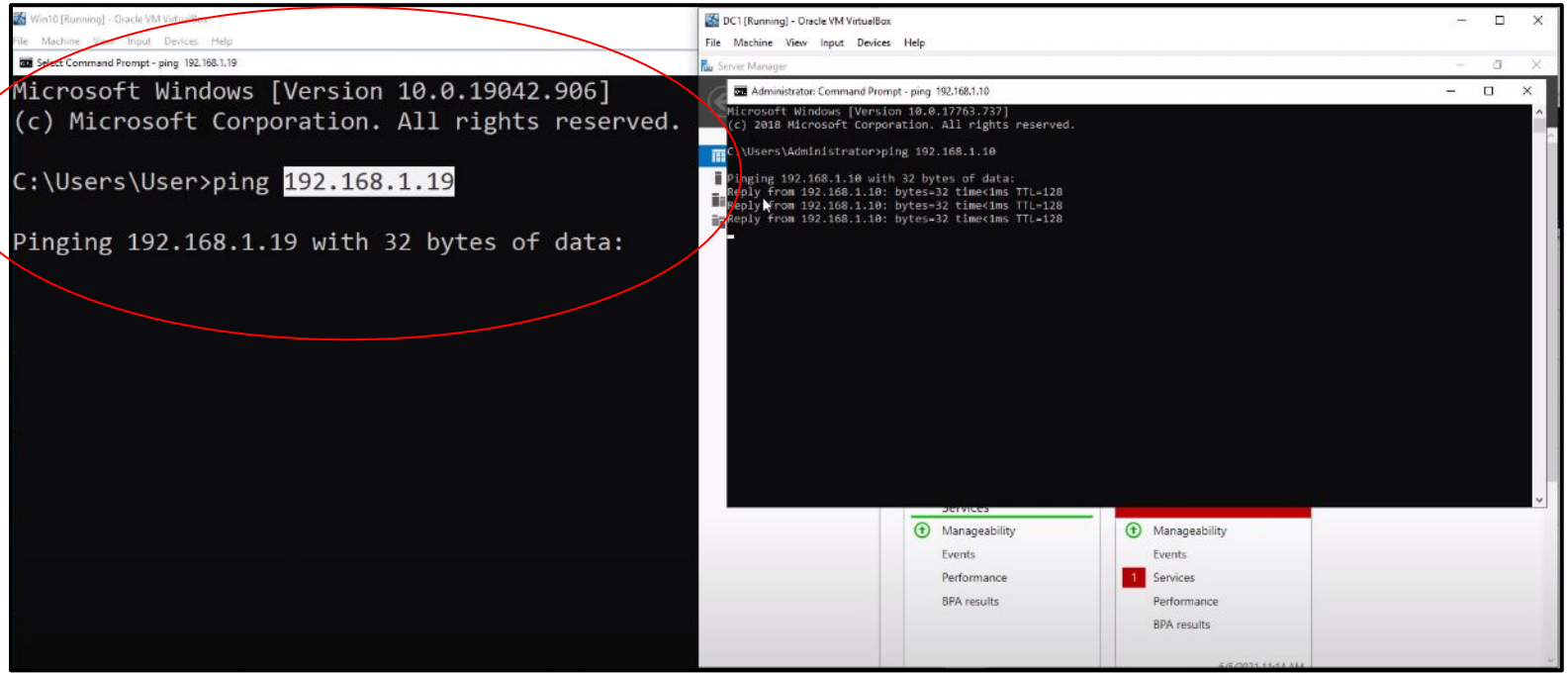
Ping It!

- In the DC1 server, access the cmd tool and ping the Win10 client using its IP address
- Likewise, in the Win10 client, access the cmd tool and ping the DC 1 server using its IP





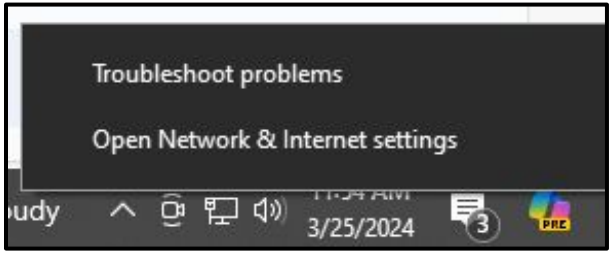
Hurray! The DC1 server is communicating with the Win 10 client!



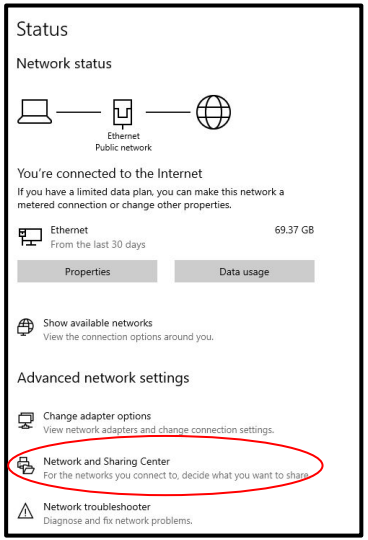
Oh no! It looks like the Win 10 client is <u>not</u> communicating with the DC1 server!

😞

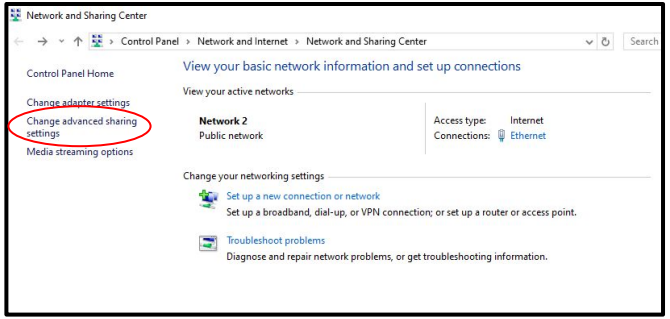
Let’s Fix It!



- Navigate to your network icon in the bottom right of screen and right click. You should see an option that reads “Open Network & Internet Settings”. Select it.



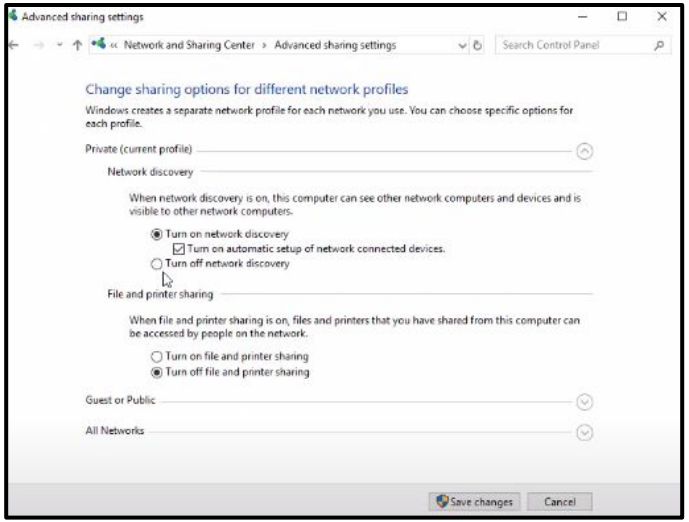
- In the status category, you will select “Network and Sharing Center”



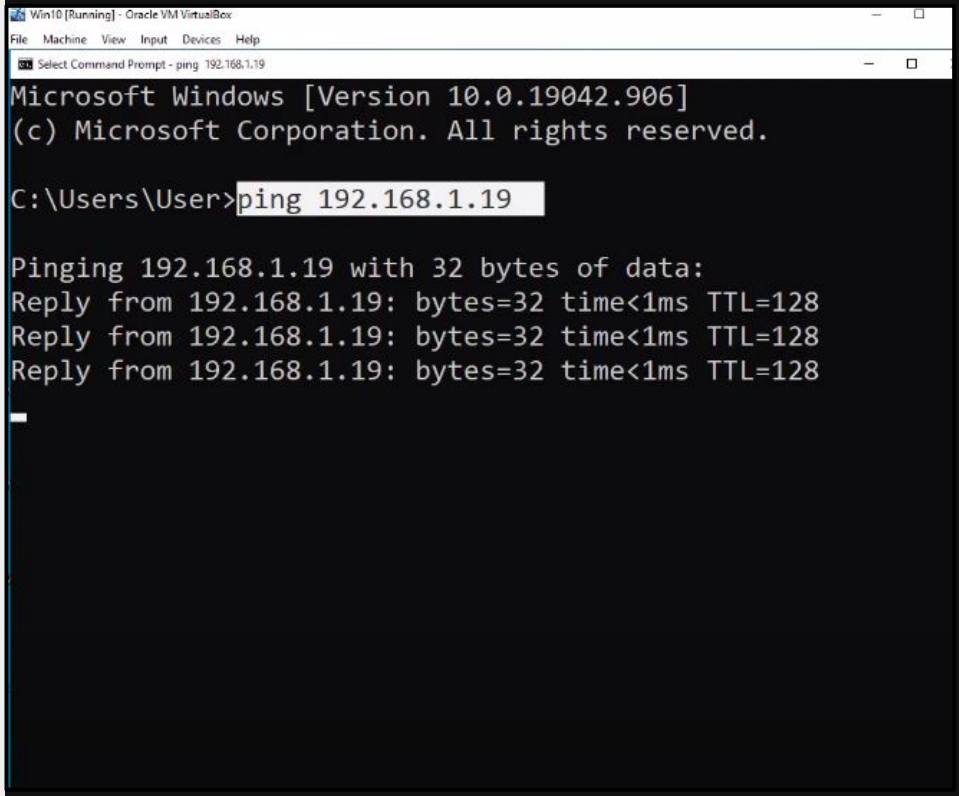
- In the popup box select “Change Advanced Sharing Settings”

Let’s Fix It (Cont. 1)

- After turning on each control, “save changes” to close the box
- Ensure that these settings are the same in both the win 10 client and the DC1 server
- Verify that the Win 10 client is now able to communicate with (ping) the Dc1 server.

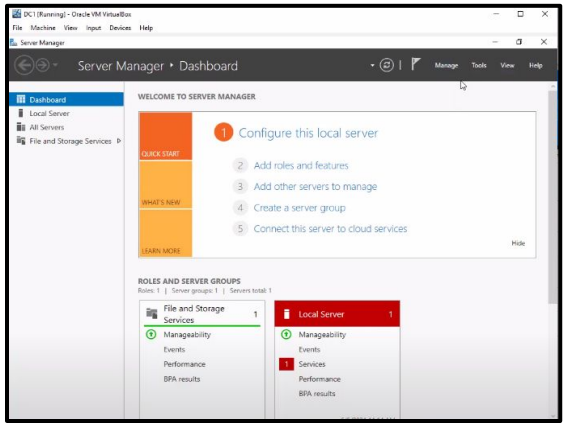


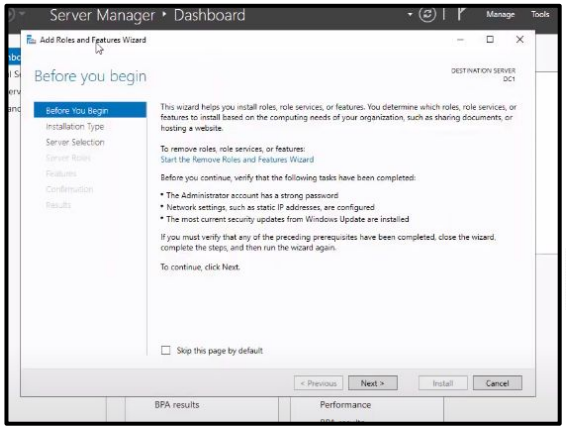
We got a ping!
Great job!

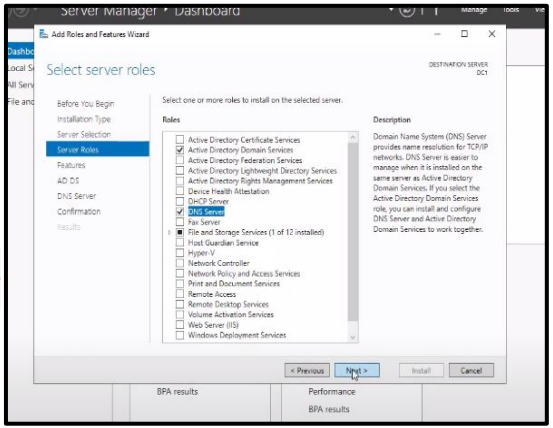


Let’s Promote DC1 into an Active Directory Server

Add Roles and Features







- Navigate to server manager in DC1 server. Select “Manage” in upper right hand corner of screen, then “Add Roles and Features”.

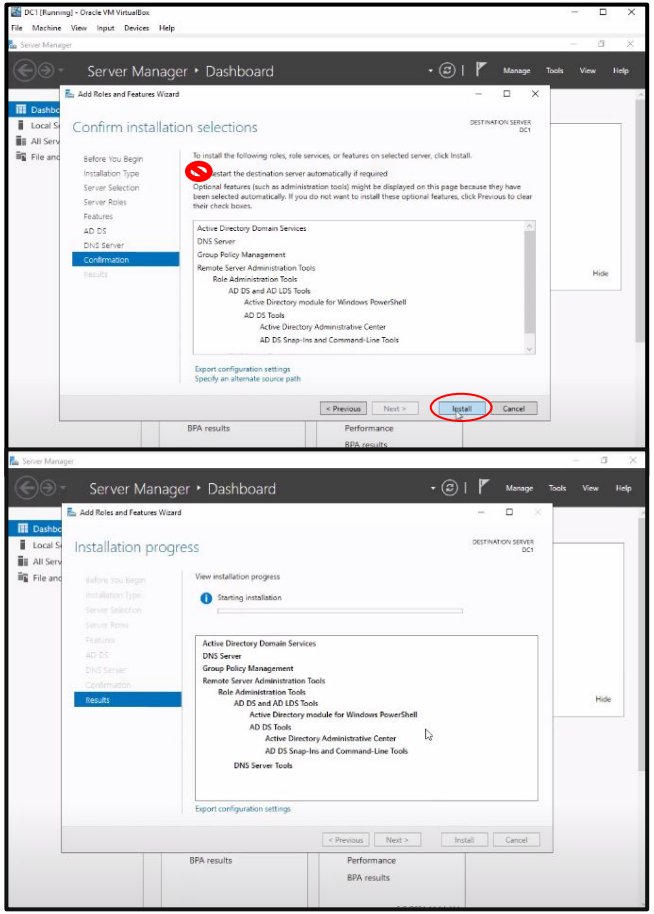
- Select “Next” in wizard until you are presented with the “Select Server Roles” options.

- Select “Active Directory Domain Service. You will be prompted to add features. Select this option. Next, select “DNS server”. Then “Continue” at the validation feature pop up. Once back at checkbox options, hit “Next”.

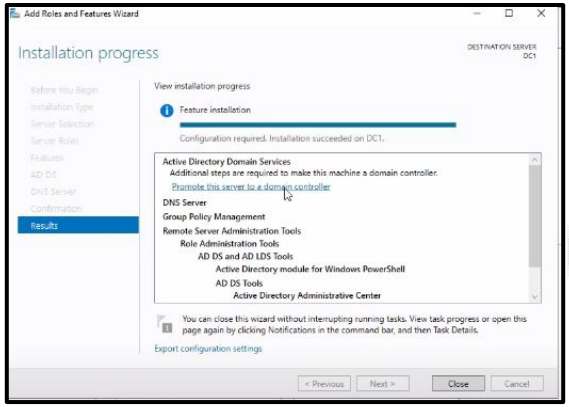
Add Roles and Features

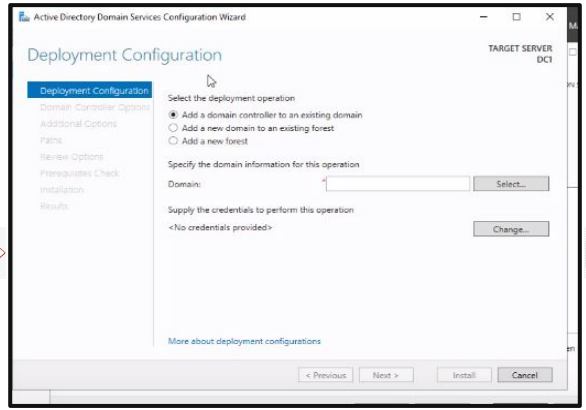
- Select “Next” until you see the prompt to “Restart the destination server automatically if required” however DO NOT SELECT THIS BOX

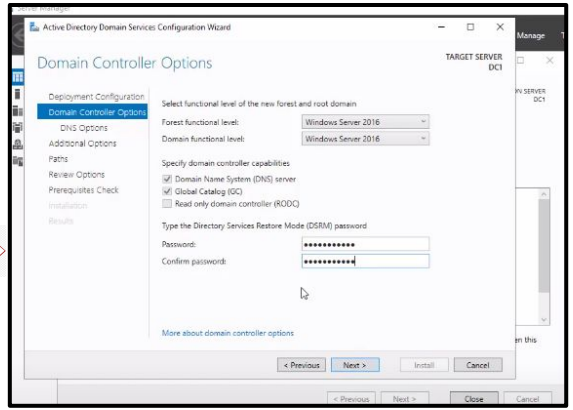
- Instead, simply select “Install” in the bottom right corner of box. Allow Installation to occur.



Add Roles and Features







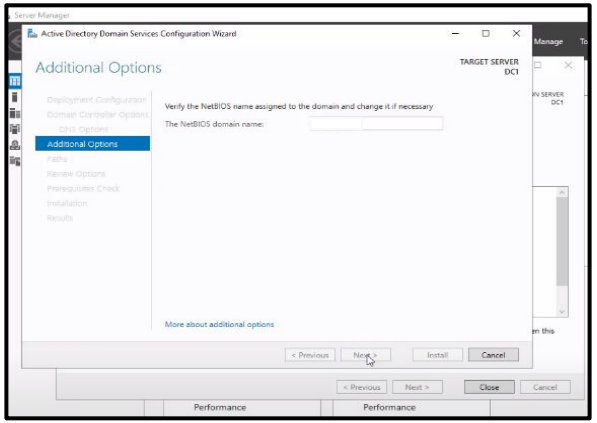
- Once the installation has completed, select the “Promote this server to a domain controller” link.

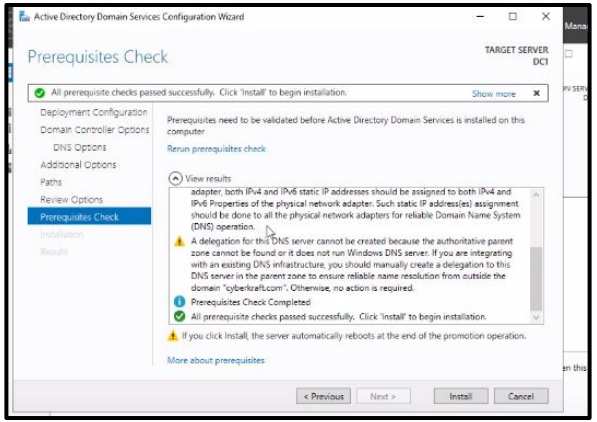
- Once at the “Deployment configuration” window, select “Add new forest” then, specify your root domain name
  Ex: smileyface.com. Once completed click “Next”.

- Provide the domain account with a password. Click “Next”.

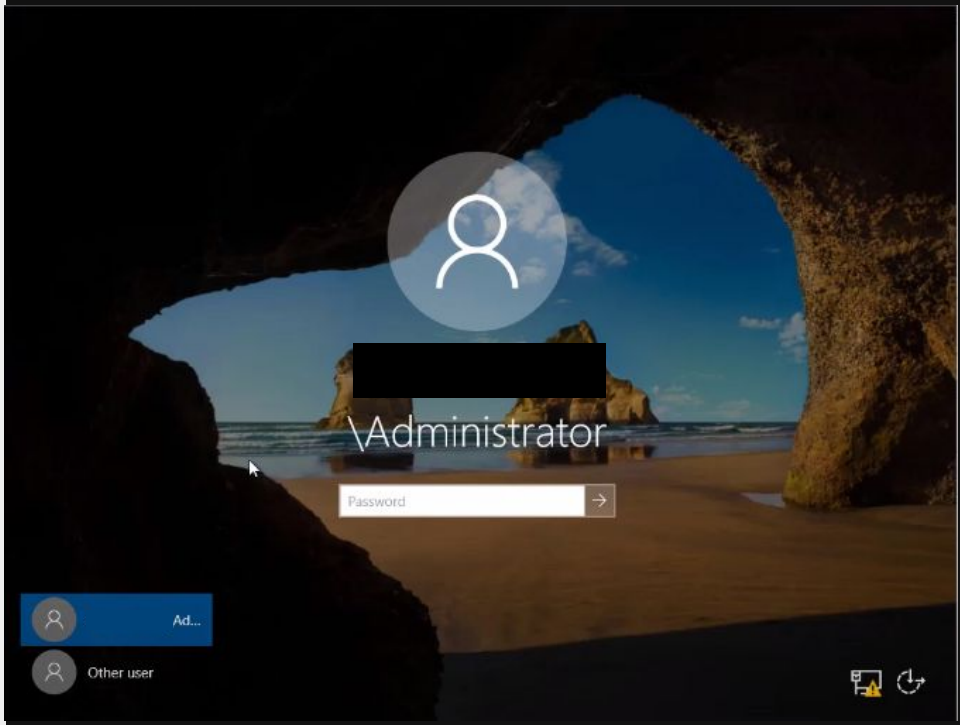
Add Roles and Features

- Once NetBIOS is verified, select “Next”.
- Allow prerequisites check to run. Once completed, select “Install”. Once completed, the server will restart automatically.





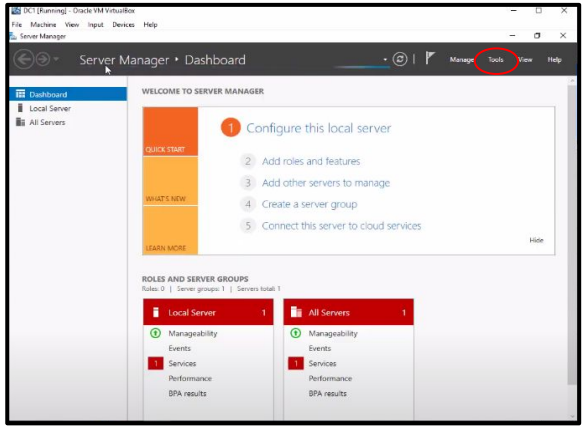
Success! Great job!

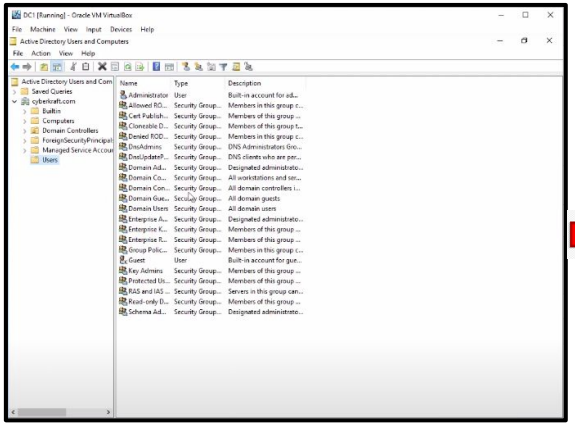


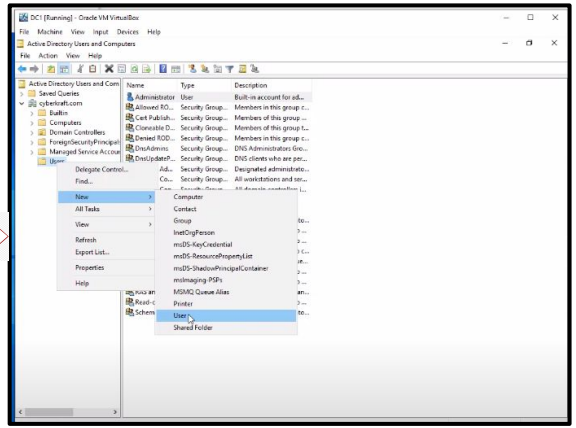
*You should now see your domain name at the Windows welcome screen upon the server's restart. Next, sign in with the password you created.

Let’s walk through adding users and groups in Active Directory

ADUC Users & Groups

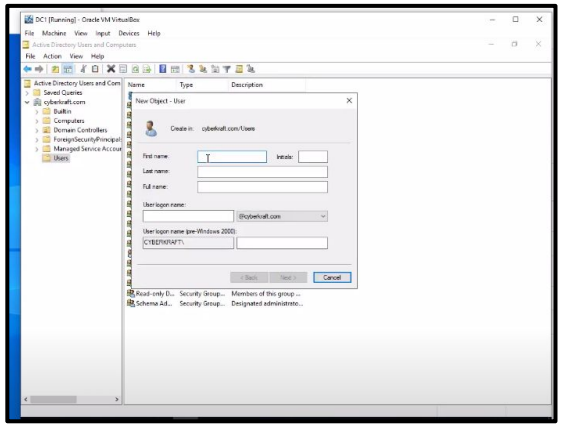




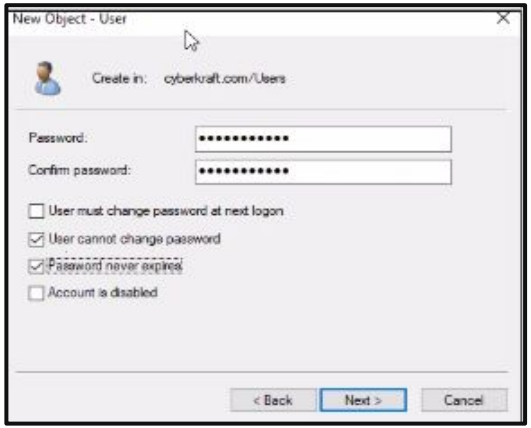


- Navigate to “Tools” at the top right corner of the server manager dashboard. Then select “Active Directory Users and Computers (ADUC).
- Expand your domain name to the left of the popup window, then expand “Users” option.
- Right click “User”, then select “New”, then “User” again.

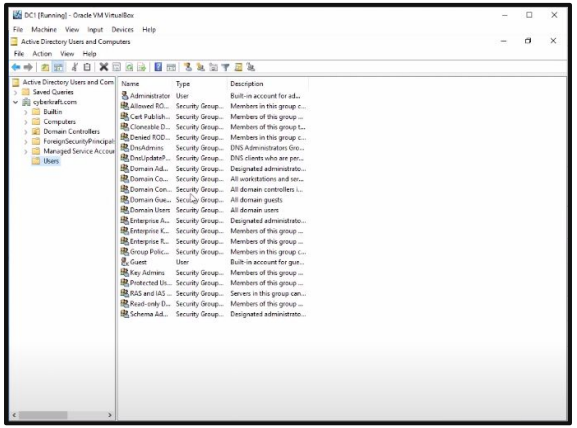
ADUC Users & Groups



- Fill in first, last, full name and user logon name. Then, select “Next”.

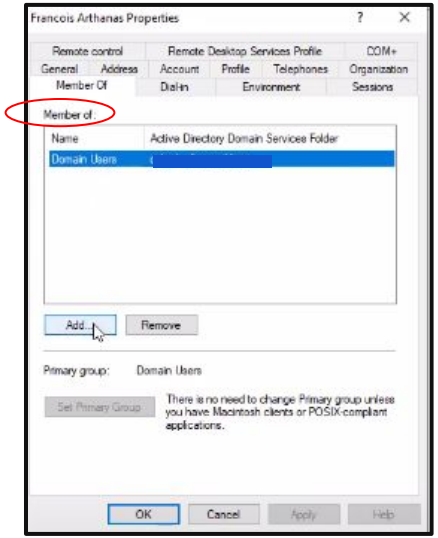


- A password must be created for the new user.
  Be sure to check “Password never expires” and “User cannot change password”. Select “Next”.

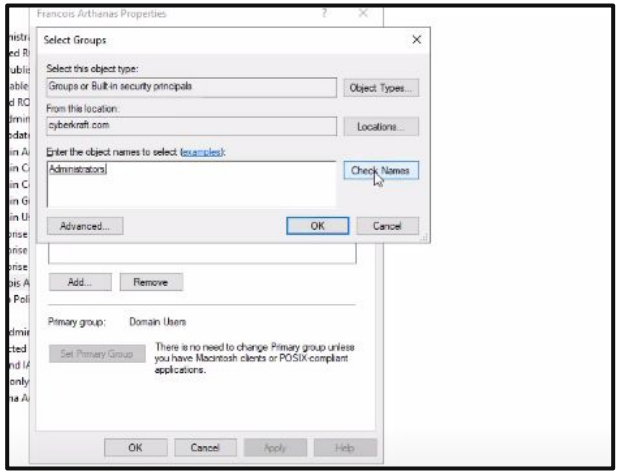


- In the expanded “Users” list, locate the user you created.

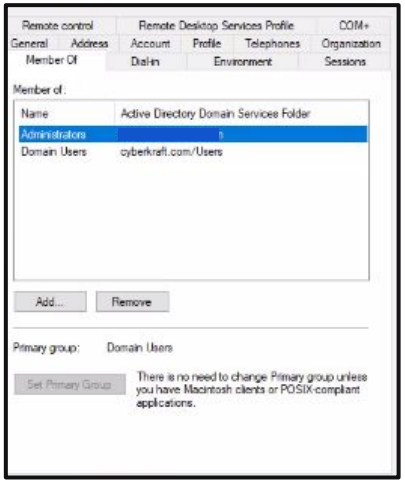
ADUC Users & Groups



- Select the “Member Of” tab in the user’s profile popup. Then select “Add”.



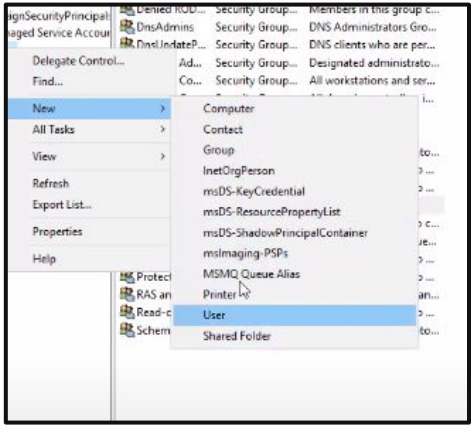
- Next, in the “Object names” field, key in “admin” then click “check names”. “Administrators” should populate. Afterwards, click “ok” until you return to the “User” menu.

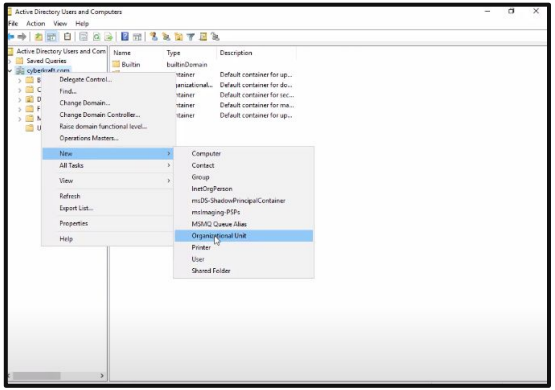


- Select the same user, you created and verify that the “Member Of” box has been updated with the new group.

ADUC Users & Groups

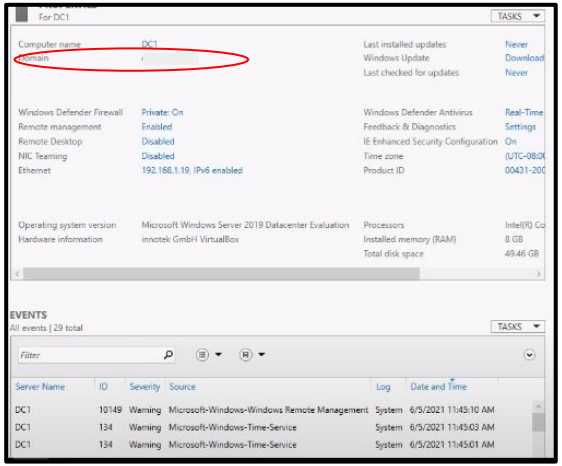
- By expanding the “Users” query, as shown by previous slides, you are able to add users, groups, etc.
- Right clicking the domain name results in the same privileges however, you can also add organizational units with this feature

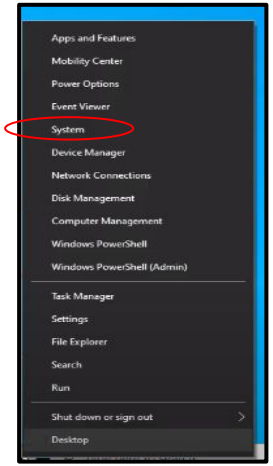


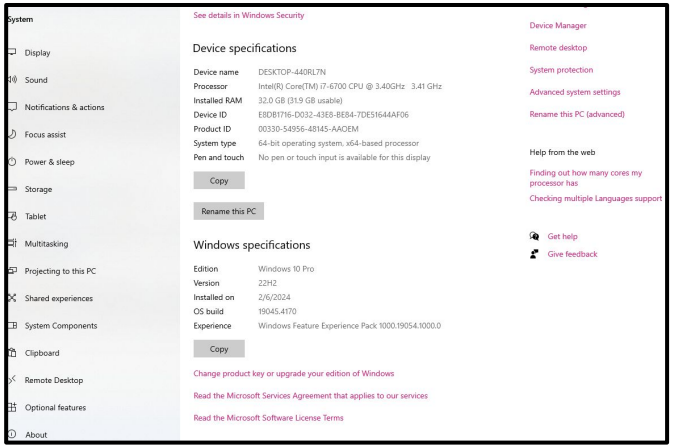


Add Win 10 client to DC1 domain

Add Computer to Domain





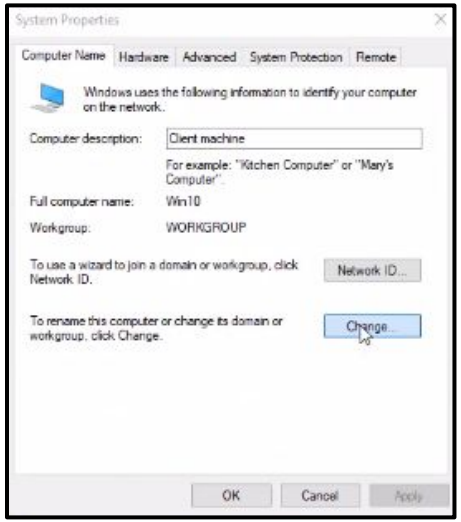


- In DC1 server verify that the domain is displaying in the server manager

- In the win10 machine, right click the windows icon and select “System”.

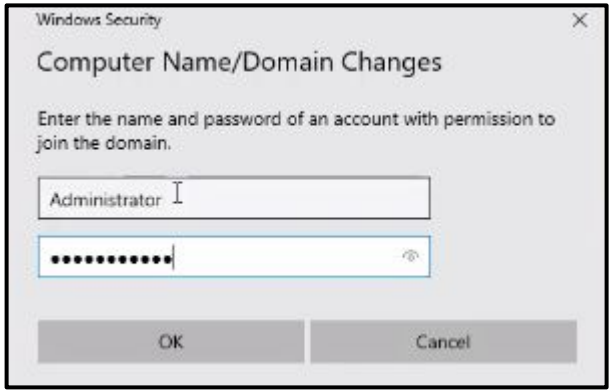
- Select “system protection”

Add Computer to Domain



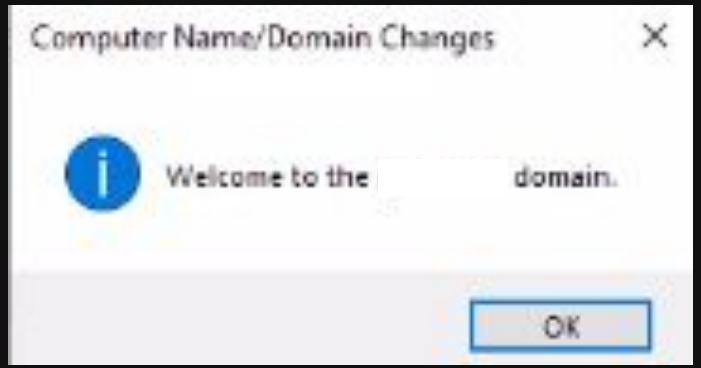
- Select the tab “Computer Name”, then select “Change”

- Select “Member of” then type domain name



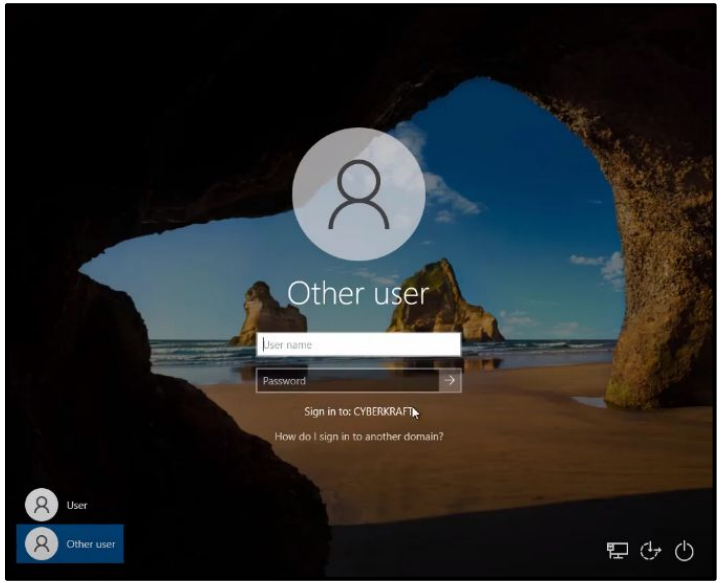
- You will then be prompted to sign in the domain’s user/pass. Select “ok”

Success! Great job!



Final Touches!

- Restart the win 10 machine.
- Once at Windows welcome screen select “Other user”
- After selecting “Other user”, sign in with user credentials created in Active Directory (ADUC).
- Once welcomed into Windows, ping the DC1 server in the cmd tool.
- Once communication is verified, power off the machines.



CONGRATS! YOU MADE IT!

Enjoy your cyber lab and make the most of it. You got this!