ADVANCED WIRELESS ATTACKS AGAINST ENTERPRISE NETWORKS

LAB SETUP GUIDE

VERSION 1.0.2

Gabriel Ryan

@s0lst1c3 @gdssecurity

gryan@gdssecurity.com

solstice.me

INTRODUCTION

For this workshop, we'll be using a lab that consist of five virtual machines joined to the same virtual network. Three of these virtual machines will run Windows and will be joined to one another using Active Directory. One of the three Windows machines will serve as the Domain Controller, and the other two will act as workstations. The remaining two virtual machines include a PFSense instance that will serve as a firewall between our lab and the outside world, and a Kali virtual machine that is preloaded with everything you need for this course.

The PFSense and Kali virtual machines are completely preconfigured and require no manual setup on the part of the student. Unfortunately, it was not possible to provide preconfigured Windows virtual machines due to licensing issues. That means you're going to have to download and configure your Active Directory machines yourself.

With that said, worry not. I've gone to great lengths to make the lab setup process as painless as possible by providing a set of PowerShell scripts that will do most of the legwork for you. All you have to do is download the required ISOs and Virtual Machines and use the provided scripts as described in the sections below.

Try not to get intimidated by the size of this setup guide. It's basically a giant picture book, with most of the following pages being occupied by screenshots. You should fly through the lab setup process fairly quickly once you have everything downloaded.

Regardless, I do recommend completing the lab setup process before getting to the conference. The reason for this is that you're going to have to download a couple of large files, and you probably don't want to be stuck doing this the night before over flaky conference WiFi. Windows server takes a while to install as well.

Important: if at any point you run into problems setting up the lab, please do not hesitate to email the instructor for assistance.

HARDWARE REQUIREMENTS

Wireless equipment for practice will provided at the workshop. With that said, you may want to invest in the following items so that you can practice the lab exercises at home:

1. Primary external wireless adapter.
    a. Must meet the following requirements:
        i. High gain
        ii. Atheros chipset
        iii. Supports master mode
        iv. Supports Linux
    b. Cheap, reliable option: TP-Link TL-WN722N ($13.79 on Amazon as of the time of this writing)
2. Wireless router (anything that supports OpenWRT and EAP)
3. Secondary external wireless adapter (must be Windows compatible)

STEP 1 - DOWNLOAD WINDOWS DEVELOPER VIRTUAL MACHINES

Microsoft offers free Windows virtual machines to web developers for testing website UIs within different versions of Internet Explorer. These virtual machines are made available by Microsoft for public download, giving us a means of legally obtaining a free copy of Windows 10 and Windows 8 for use in our lab.

The following steps can be used to download a Windows 10 Developer VM:

1. Navigate to the following url: https://developer.microsoft.com/en-us/microsoft-edge/tools/vms/
2. Select Microsoft Edge on Windows 10 Stable "Virtual machine" dropdown menu.
3. Select VirtualBox from the "Select platform" dropdown menu.
4. Click the grey "Download .zip" button at the bottom left in the screen.

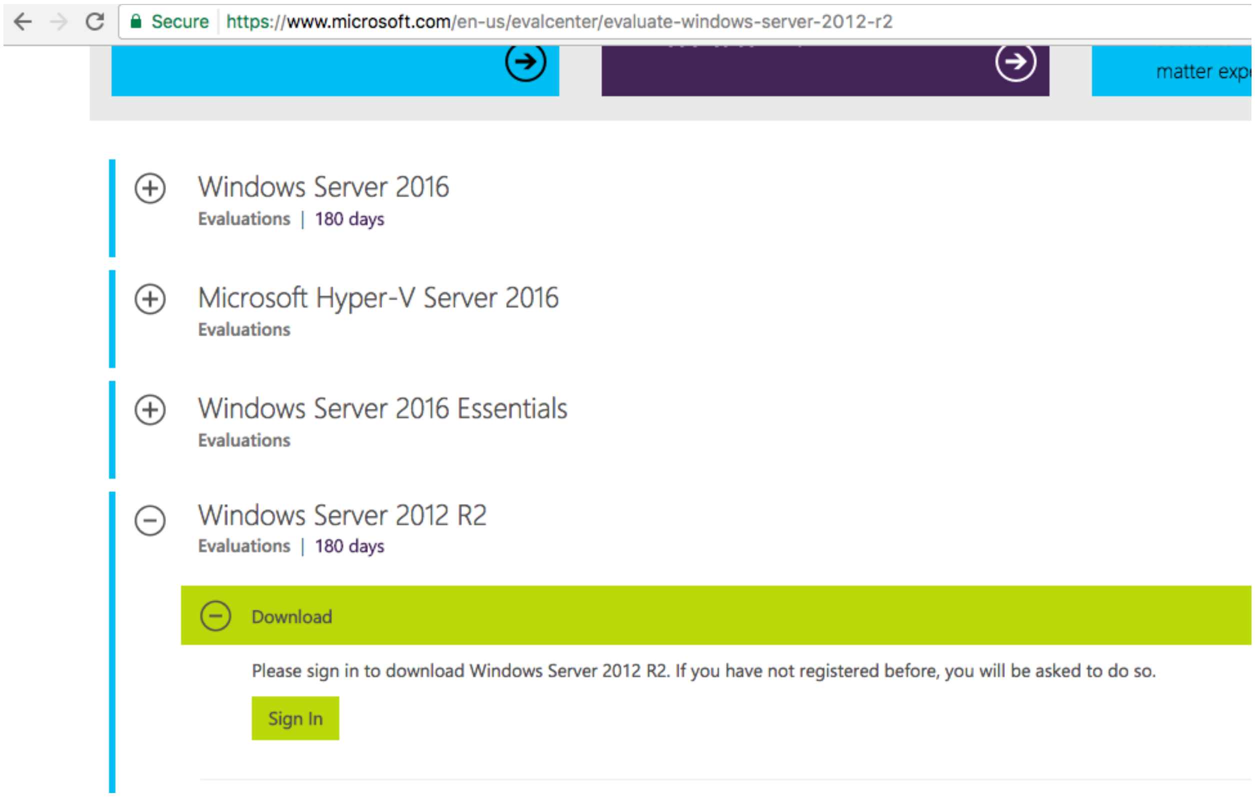
Once you've downloaded a Windows 10 virtual machine, repeat this process to obtain a Windows 8 virtual machine as well.

STEP 2 - OBTAIN WINDOWS SERVER 2012 R2 TRIAL EDITION

Next, we need to obtain a copy of Windows Server 2012 R2. Since Windows Server 2012 R2 is pretty expensive, it is recommended that you download a 180 day free trial from Microsoft.

To obtain a free Windows Server 2012 R2 trial:

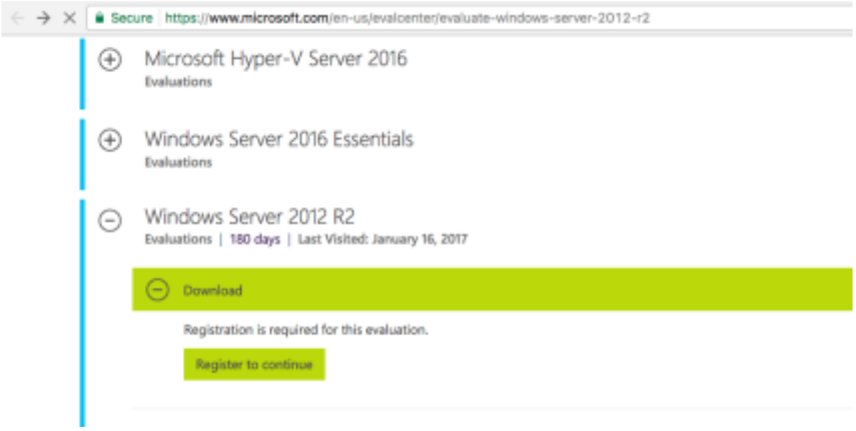
1. Navigate to the following URL: https://www.microsoft.com/en-us/evalcenter/evaluate-windows-server-2012-r2
2. In the expandable list, select Windows Server 2012 R2 → Download
3. Click the green "Sign In" button



Secure https://www.microsoft.com/en-us/evalcenter/evaluate-windows-server-2012-r2

Please sign in to download Windows Server 2012 R2. If you have not registered before, you will be asked to do so.

4. You will now be required to authenticate using a valid Microsoft or Skype account. If you don't have one, make one now.
5. After signing in, you will be redirected back to the previous page. The green "Sign In" button will have been replaced with a green button that says "Register to continue". Click the "Register to continue" button.



Secure | https://www.microsoft.com/en-us/evalcenter/evaluate-windows-server-2012-r2

Microsoft Hyper-V Server 2016
Evaluations

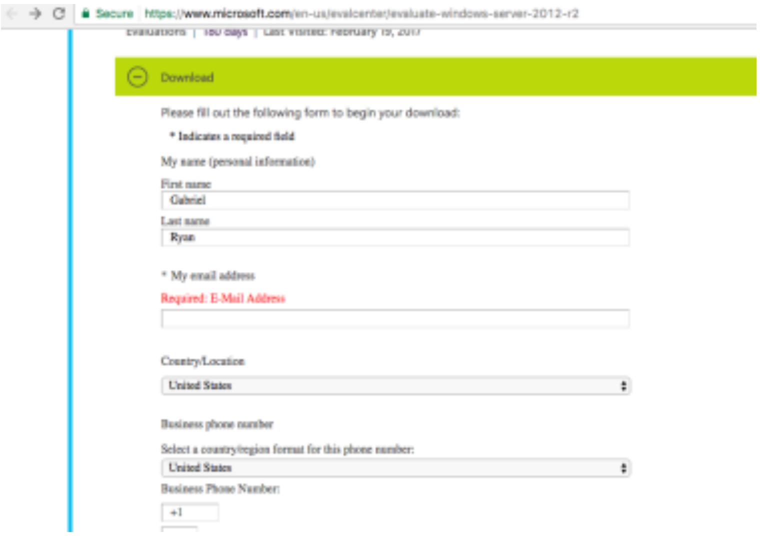
Windows Server 2016 Essentials
Evaluations

Windows Server 2012 R2
Evaluations | 180 days | Last Visited: January 16, 2017

Download

Registration is required for this evaluation.

6. Fill out registration form
7. Click “Continue”



Secure | https://www.microsoft.com/en-us/evalcenter/evaluate-windows-server-2012-r2

Evaluations | 180 days | Last Visited: February 19, 2017

Download

Please fill out the following form to begin your download:

* Indicates a required field

My name (personal information)

First name: Gabriel

Last name: Ryan

* My email address

Required: E-Mail Address

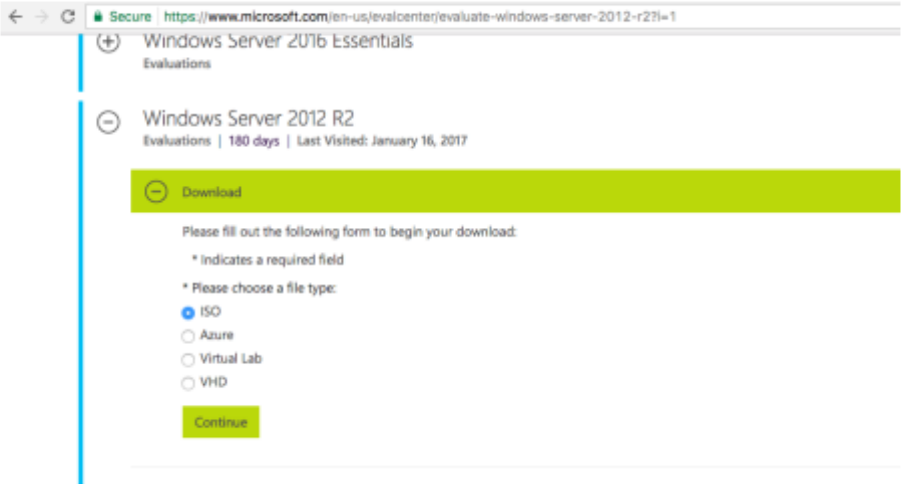
Country/Location: United States

Business phone number

Select a country/region format for this phone number: United States

Business Phone Number: +1

8. Select the “ISO” option
9. Click “Continue”



Secure https://www.microsoft.com/en-us/evalcenter/evaluate-windows-server-2012-r2?i=1

Windows Server 2016 Essentials
Evaluations

Windows Server 2012 R2
Evaluations | 180 days | Last Visited: January 16, 2017

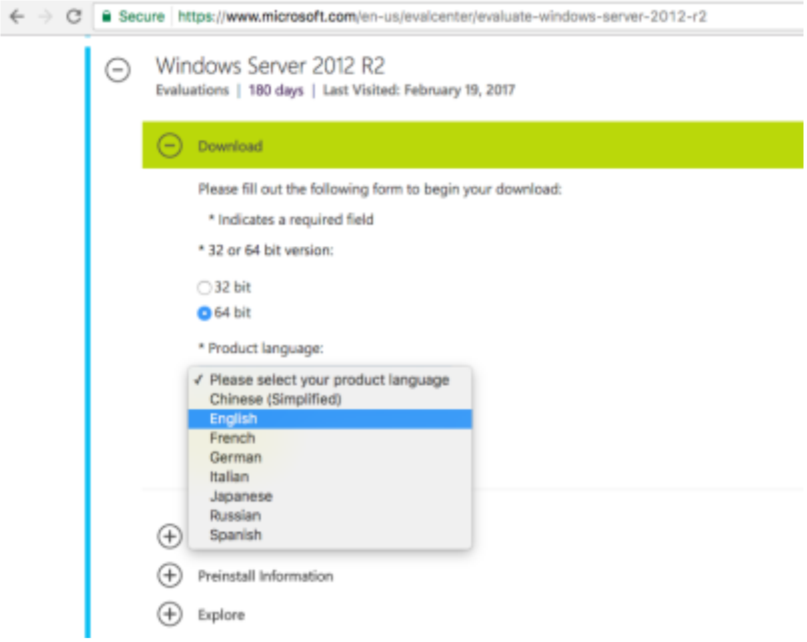
Please fill out the following form to begin your download:

* Indicates a required field

* Please choose a file type:

● ISO
○ Azure
○ Virtual Lab
○ VHD

10. Select the "64 bit" option
11. Select "English" from the "product language" dropdown menu
12. Click the green "Download" button



Secure https://www.microsoft.com/en-us/evalcenter/evaluate-windows-server-2012-r2

Windows Server 2012 R2
Evaluations | 180 days | Last Visited: February 19, 2017

Please fill out the following form to begin your download:

* Indicates a required field

* 32 or 64 bit version:

○ 32 bit
● 64 bit

* Product language:

STEP 3 - INSTALL VIRTUALBOX

Next, we need to download and install VirtualBox. This should be pretty straightforward. Just navigate to the link below and select the build that is appropriate for your operating system.

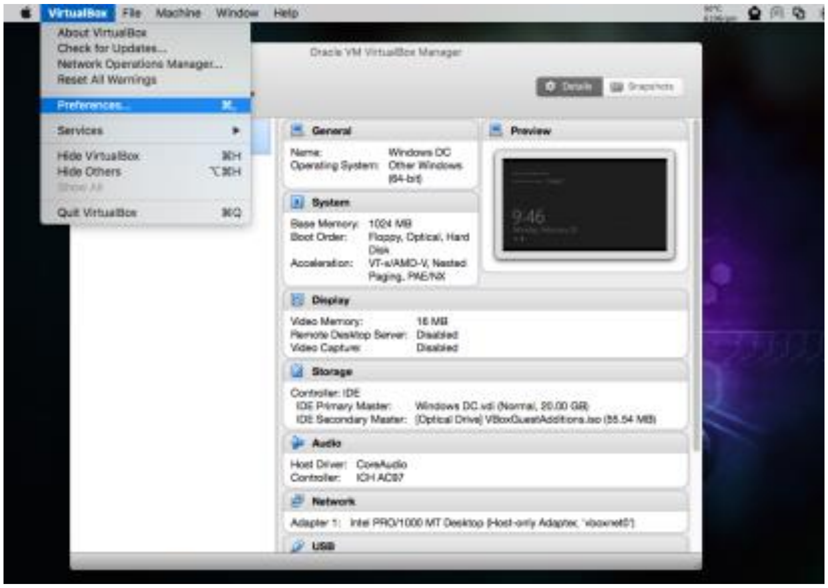
- https://www.virtualbox.org/wiki/Downloads

Once VirtualBox is downloaded, install it.

STEP 4 - CONFIGURE VIRTUAL NETWORK

Now that we have VirtualBox installed, we need to configure our virtual lab network. To do this, use the following steps:

1. Start the VirtualBox application
2. In the toolbar at the top right of the screen, select VirtualBox > Preferences



General
Name: Windows DC
Operating System: Other Windows (64-bit)

System
Base Memory: 1024 MB
Boot Order: Floppy, Optical, Hard Disk
Acceleration: VT-x/AMD-V, Nested Paging, PAE/NX

Display
Video Memory: 16 MB
Remote Desktop Server: Disabled
Video Capture: Disabled

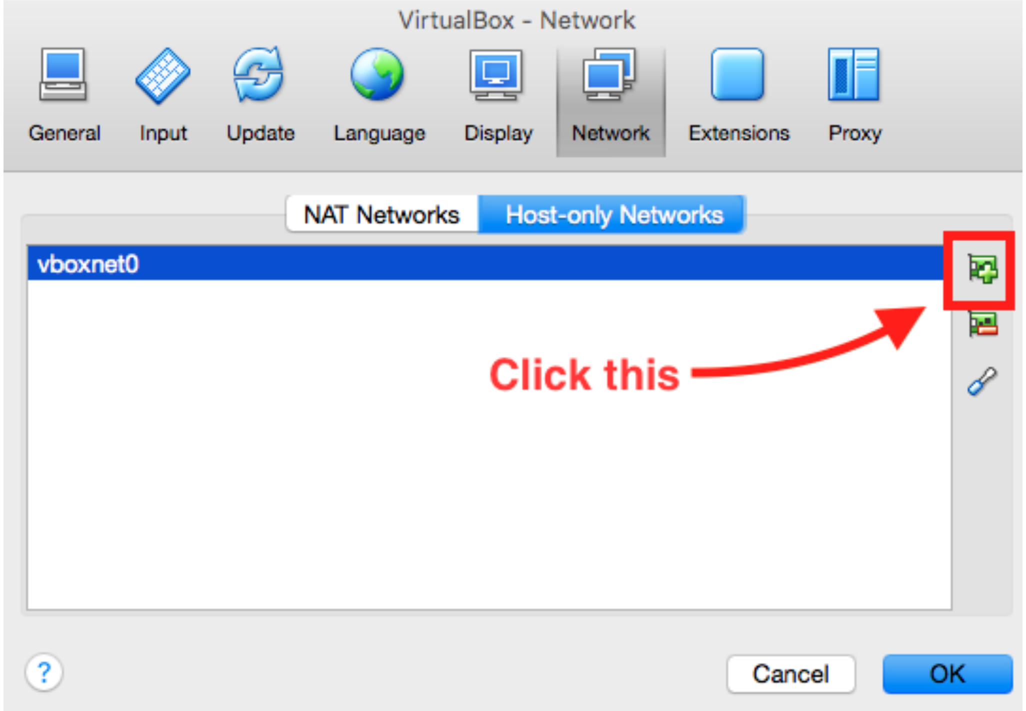
Storage
Controller: IDE
IDE Primary Master: Windows DC.vdi (Normal, 20.00 GB)
IDE Secondary Master: [Optical Drive] VBoxGuestAdditions.iso (55.54 MB)

Audio
Host Driver: CoreAudio
Controller: ICH AC97

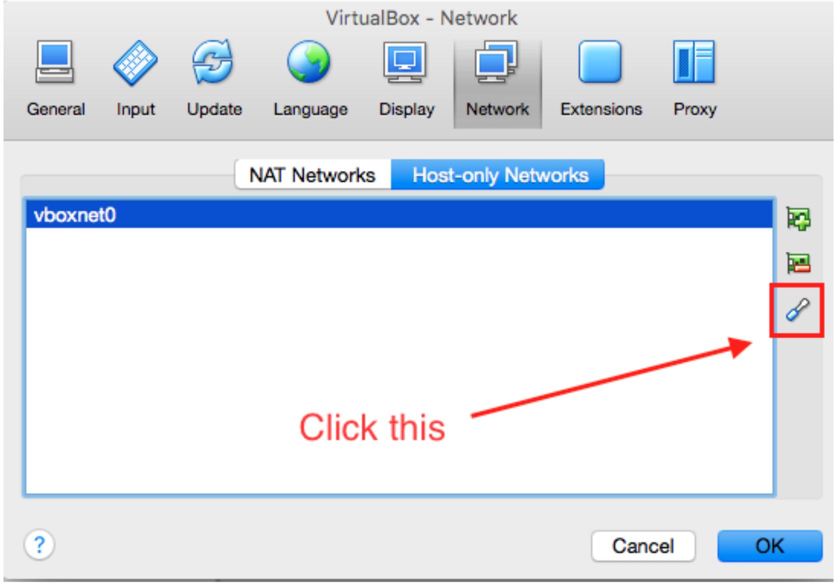
Network
Adapter 1: Intel PRO/1000 MT Desktop (Host-only Adapter, 'vboxnet0')

USB

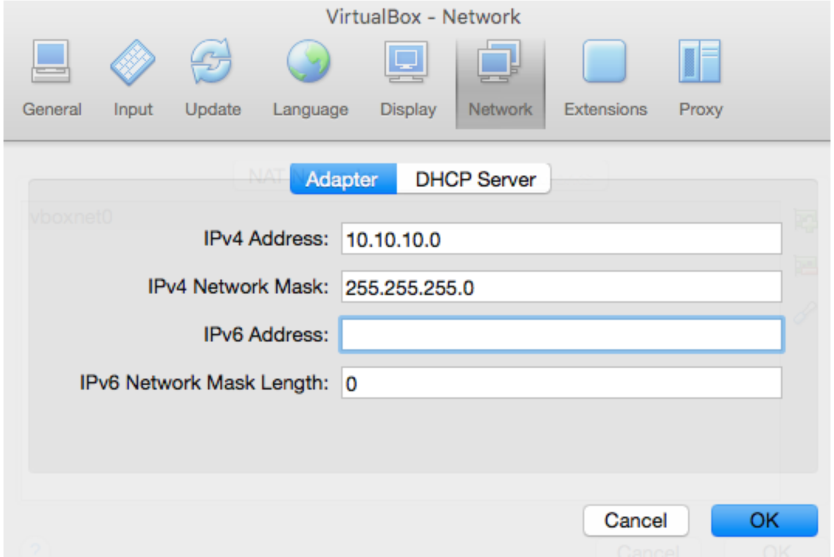
3. In Preferences, go to Network > Host-only Networks, then click the green icon to add a new Host-only network.



4. From Network > Host-only Networks, click the blue screwdriver icon to edit the network you just created

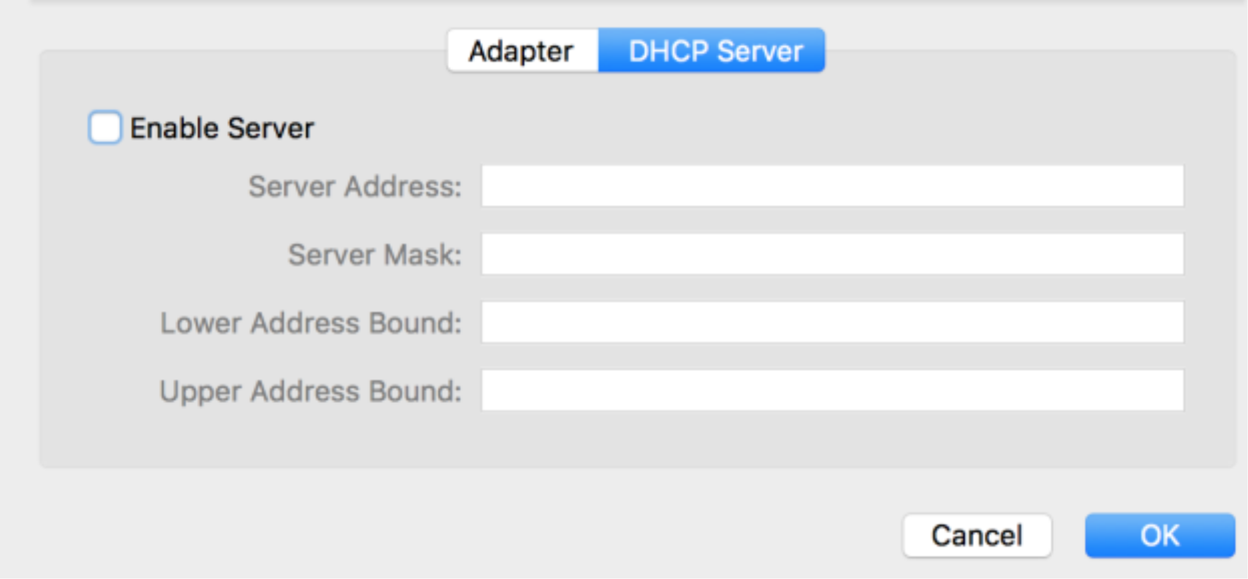


5. Configure the Host-only network so that it has the following attributes:
    a. IPv4 Address: 10.10.10.0
    b. IPv4 Network Mask: 255.255.255.0



IPv4 Address: 10.10.10.0
IPv4 Network Mask: 255.255.255.0
IPv6 Address:
IPv6 Network Mask Length: 0

6. Select the “DHCP Server” tab and uncheck the “Enable Server” option as shown in the screenshot below.



□ Enable Server

Server Address:

Server Mask:

Lower Address Bound:

Upper Address Bound:

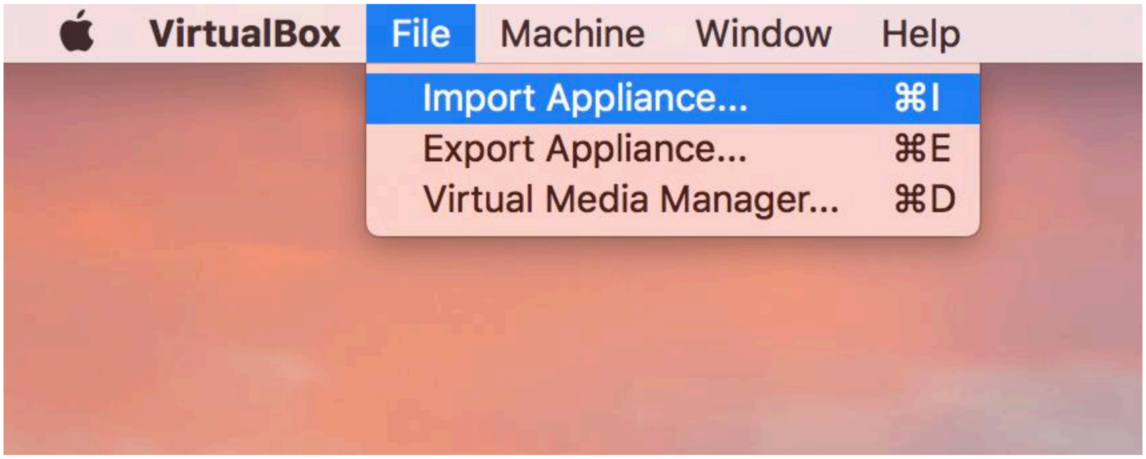
7. Click “OK”

STEP 5 - IMPORT PFSENSE AND KALI VIRTUAL MACHINES

First, download the preconfigured PFSense and Kali virtual machines from the following Google Drive URL:

- https://drive.google.com/drive/folders/0BwFgM9oAhmd_c2JJaG1iUmhkZTg

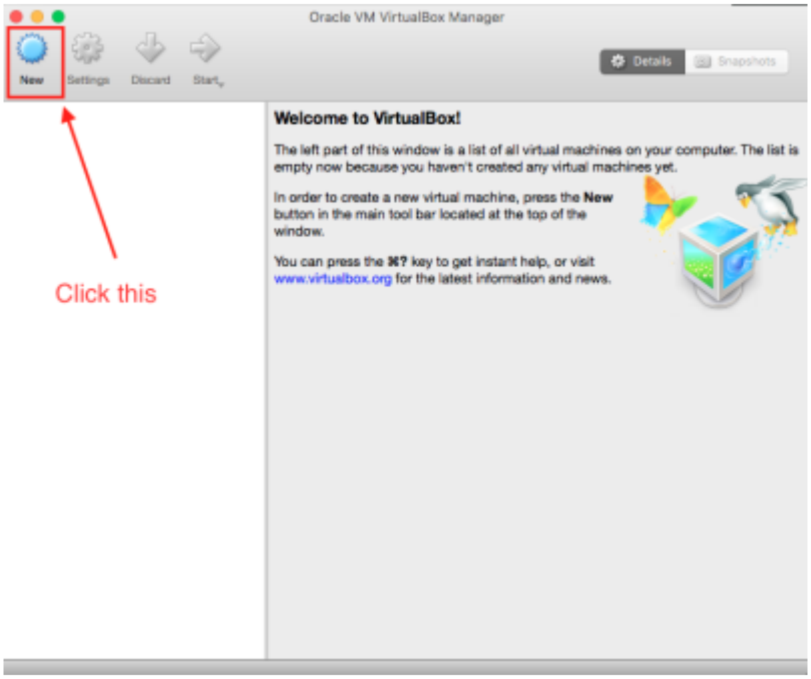
Next, import each of the virtual machines you just downloaded into VirtualBox by selecting Preferences > Import Appliance as shown in the screenshot below, then selecting the virtual machine you wish to import.



STEP 6 - INSTALL DOMAIN CONTROLLER

Before proceeding any further, make sure that your PFSense virtual machine has been started. Then, use the following steps to install the lab's Domain Controller:

1. Start the VirtualBox application
2. Click the blue circular icon at the top left of the screen to add a new Virtual Machine



Welcome to VirtualBox!

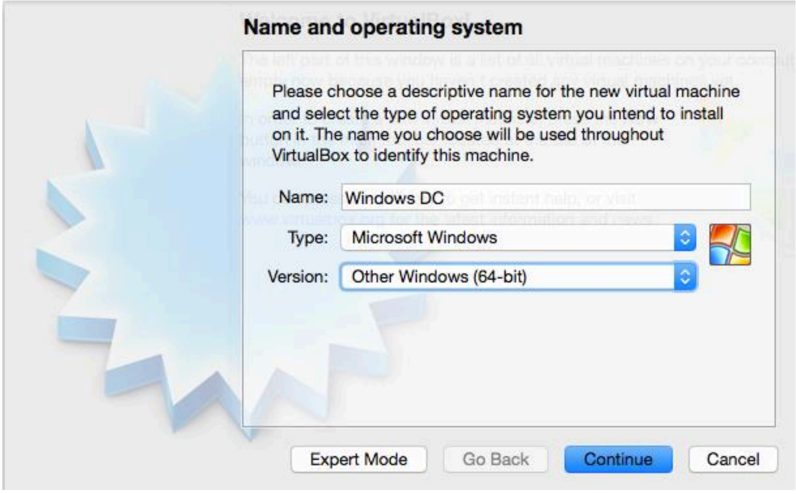
The left part of this window is a list of all virtual machines on your computer. The list is empty now because you haven't created any virtual machines yet.

In order to create a new virtual machine, press the **New** button in the main tool bar located at the top of the window.

You can press the **⌘?** key to get instant help, or visit www.virtualbox.org for the latest information and news.

Click this

3. Click the "Expert Mode" button
4. Set the following attributes for the new VM:
   a. Name: Windows DC
   b. Type: Microsoft Windows
   c. Version: Other Windows (64-bit)
   d. Memory size: 1024 MB
   e. Hard Disk: Create a virtual hard disk now



Name and operating system

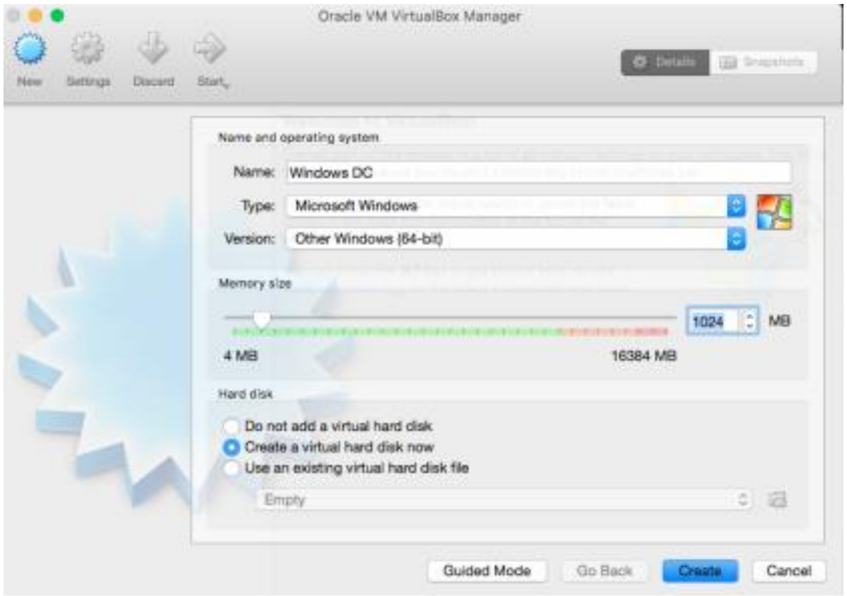
Please choose a descriptive name for the new virtual machine and select the type of operating system you intend to install on it. The name you choose will be used throughout VirtualBox to identify this machine.

Name: Windows DC

Type: Microsoft Windows

Version: Other Windows (64-bit)

5. Click the “Create” button
6. Set the following attributes for the new VM:
   a. File location: Windows DC
   b. File size: 20.00 GB
   c. Hard disk file type: VDI (VirtualBox Disk Image)
   d. Storage on physical hard disk: Dynamically Allocated



Name and operating system

Name: Windows DC

Type: Microsoft Windows

Version: Other Windows (64-bit)

Memory size

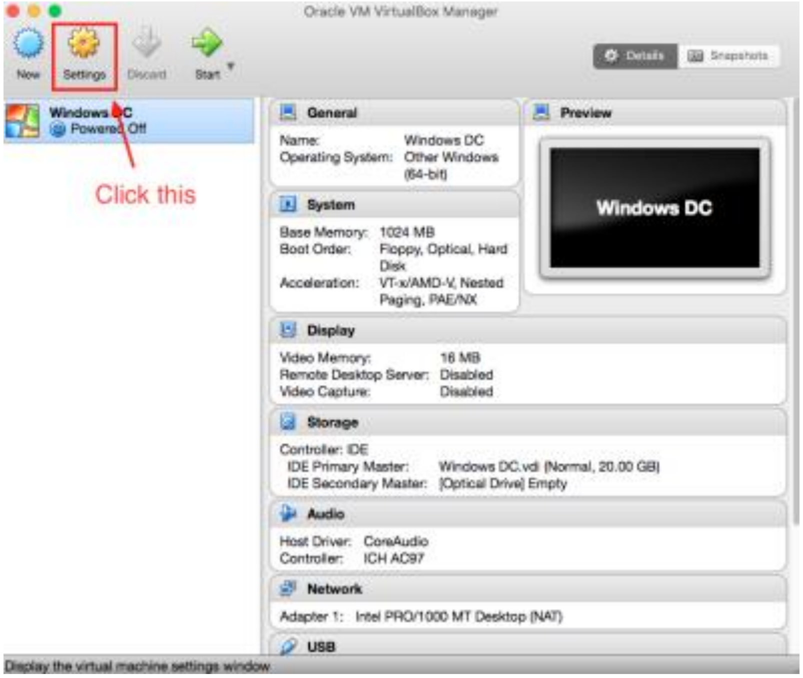
1024 MB

Hard disk

○ Do not add a virtual hard disk
● Create a virtual hard disk now
○ Use an existing virtual hard disk file

Empty

7. Click the “Create” button
8. From the main VirtualBox menu, select your “Windows DC” VM from the list on the left
9. Click the yellow gear icon at the top left of the screen to edit the settings for your “Windows DC” VM



General

Name: Windows DC
Operating System: Other Windows (64-bit)

System

Base Memory: 1024 MB
Boot Order: Floppy, Optical, Hard Disk
Acceleration: VT-x/AMD-V, Nested Paging, PAE/NX

Display

Video Memory: 16 MB
Remote Desktop Server: Disabled
Video Capture: Disabled

Storage

Controller: IDE
IDE Primary Master: Windows DC.vdi (Normal, 20.00 GB)
IDE Secondary Master: [Optical Drive] Empty

Audio

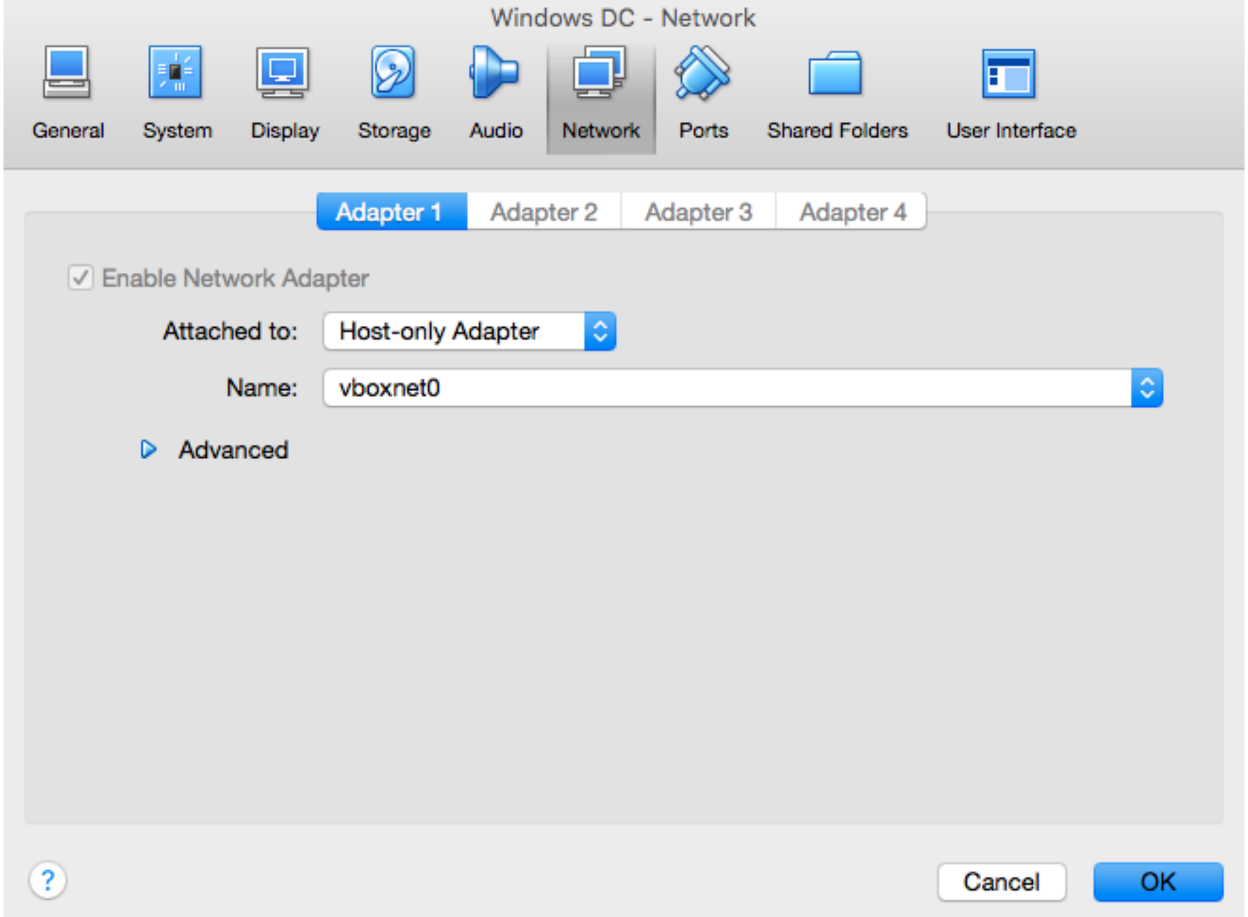
Host Driver: CoreAudio
Controller: ICH AC97

Network

Adapter 1: Intel PRO/1000 MT Desktop (NAT)

USB

10. In Settings > Network, enable “Adapter 1” network adapter and attach it to the Host-only network we created in Step 5 – Configure VirtualBox as shown in the screenshot below.

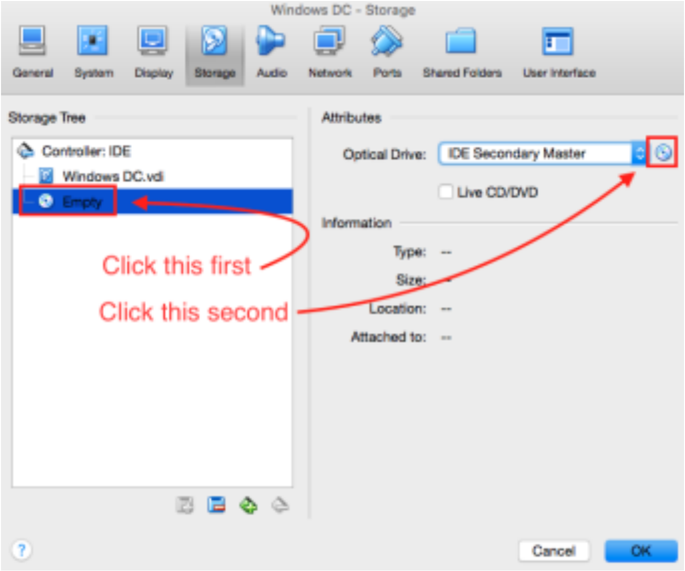


☑ Enable Network Adapter

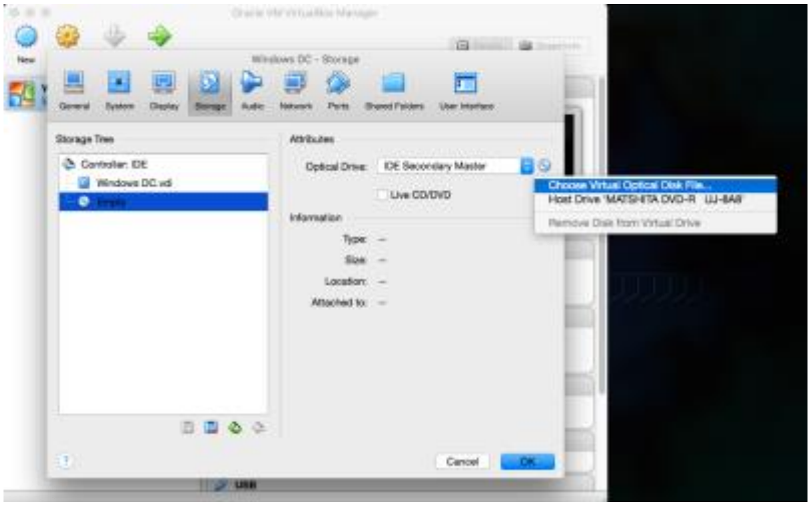
Attached to: Host-only Adapter

Name: vboxnet0

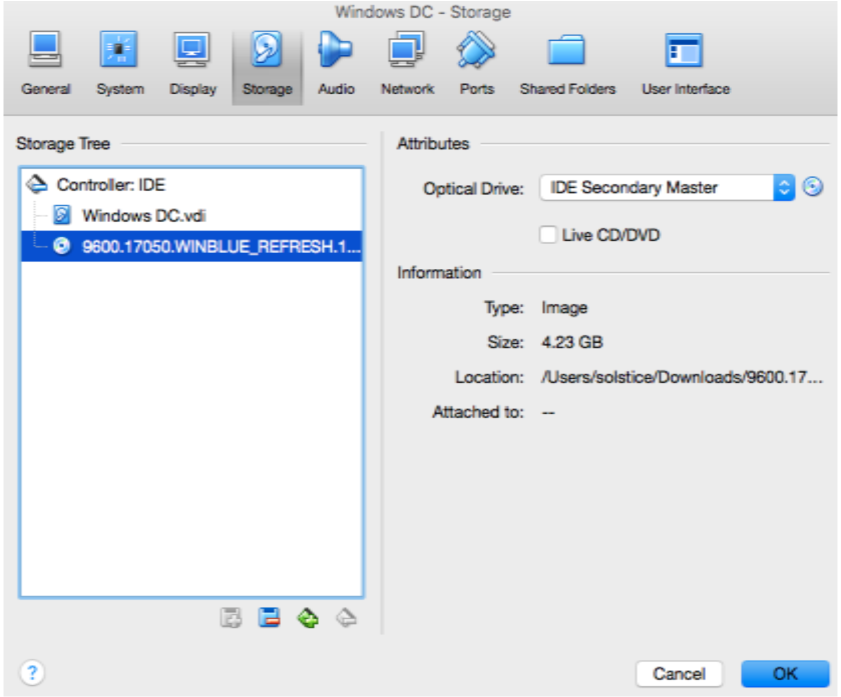
11. Switch to the “Storage” tab as shown in the screenshot below. In the “Storage Tree” menu located to the left, click the word “Empty” to select your VM’s disk drive. Then click the blue disk icon near the top right of the window to reveal a dropdown menu.



12. Select "Choose Virtual Optical Disk File…" from the dropdown menu.



13. Select the Windows Server 2012 R2 ISO file that you downloaded earlier
14. Click the "OK" button to return to the main Virtual Box menu



Storage Tree

- Controller: IDE
  - Windows DC.vdi
  - 9600.17050.WINBLUE_REFRESH.1...

Attributes

Optical Drive: IDE Secondary Master

□ Live CD/DVD

Information

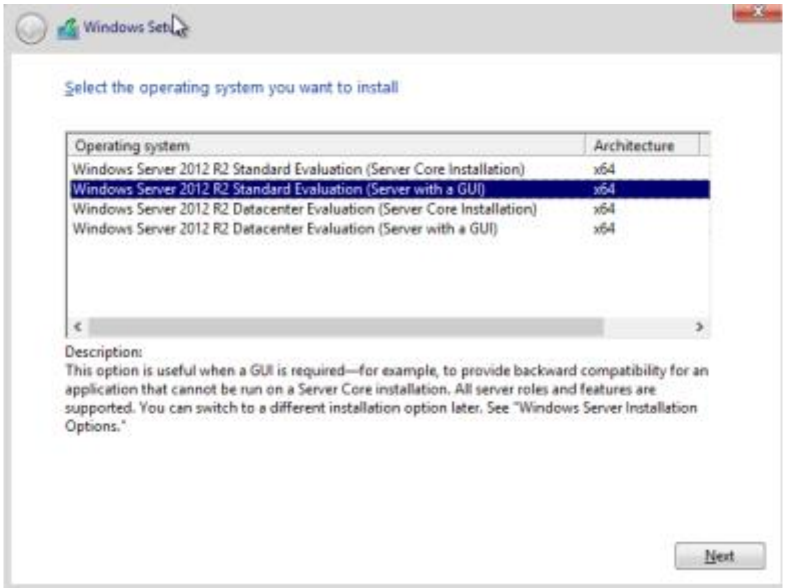
Type: Image

Size: 4.23 GB

Location: /Users/solstice/Downloads/9600.17...

Attached to: --

15. Start the Windows DC virtual machine
16. Click "next" through all the prompts until you reach the window shown in the screenshot below. Then select "Windows Server 2012 R2 Standard Evaluation (Server with a GUI)" and click "Next"



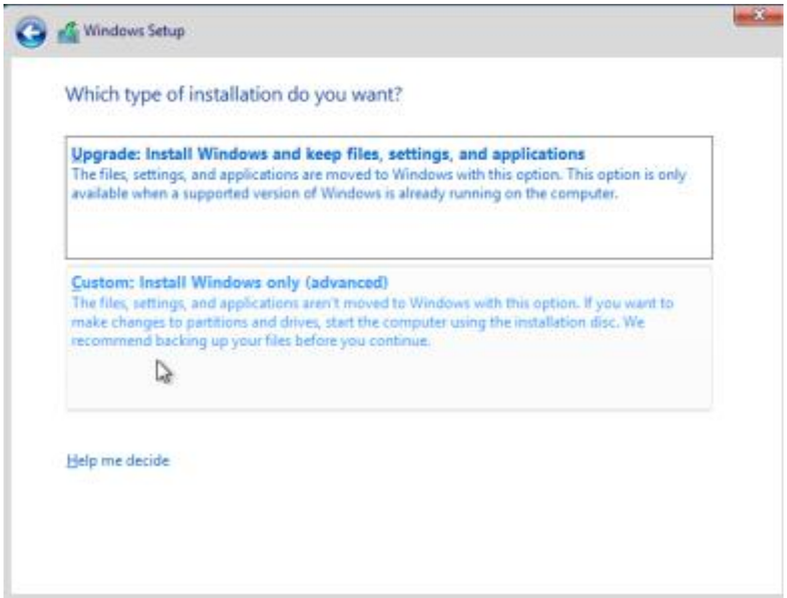
Select the operating system you want to install

Operating system	Architecture
Windows Server 2012 R2 Standard Evaluation (Server Core Installation)	x64
Windows Server 2012 R2 Standard Evaluation (Server with a GUI)	x64
Windows Server 2012 R2 Datacenter Evaluation (Server Core Installation)	x64
Windows Server 2012 R2 Datacenter Evaluation (Server with a GUI)	x64

Description:
This option is useful when a GUI is required—for example, to provide backward compatibility for an application that cannot be run on a Server Core installation. All server roles and features are supported. You can switch to a different installation option later. See "Windows Server Installation Options."

17. Accept the Microsoft Licensing agreement then click "Next"

18. When you see the prompt shown in the screenshot below, click “Custom: Install Windows Only (Advanced)”



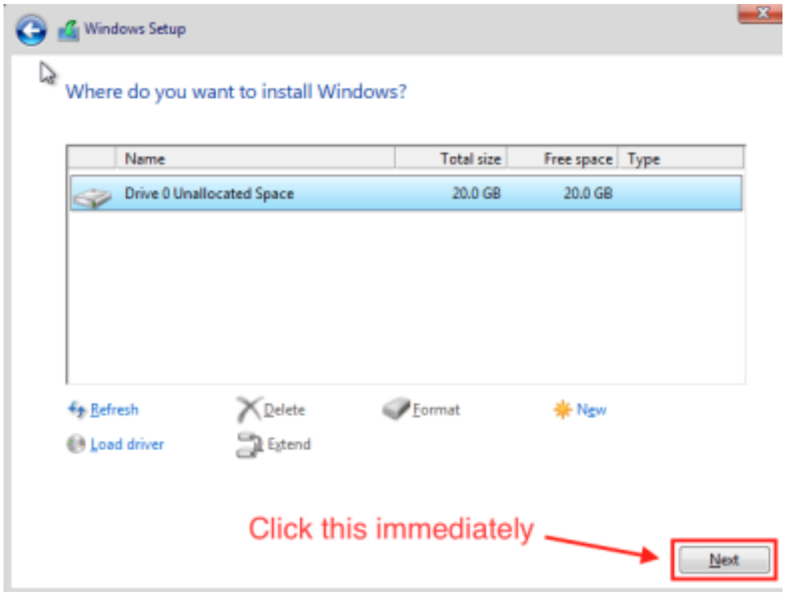
Which type of installation do you want?

Upgrade: Install Windows and keep files, settings, and applications
The files, settings, and applications are moved to Windows with this option. This option is only available when a supported version of Windows is already running on the computer.

Custom: Install Windows only (advanced)
The files, settings, and applications aren't moved to Windows with this option. If you want to make changes to partitions and drives, start the computer using the installation disc. We recommend backing up your files before you continue.

Help me decide

19. Click the Next button immediately without modifying any options

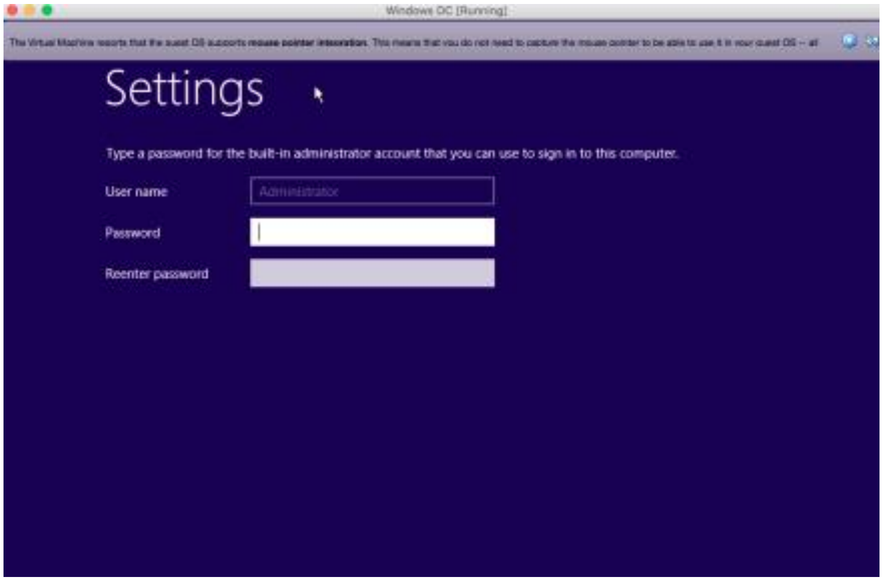


Where do you want to install Windows?

Name	Total size	Free space	Type
Drive 0 Unallocated Space	20.0 GB	20.0 GB	

Click this immediately

20. Set the Administrator password when prompted



The Virtual Machine reports that the guest OS supports **mouse pointer integration**. This means that you do not need to capture the mouse pointer to be able to use it in your guest OS -- all

Settings

Type a password for the built-in administrator account that you can use to sign in to this computer.

User name: Administrator

Password:

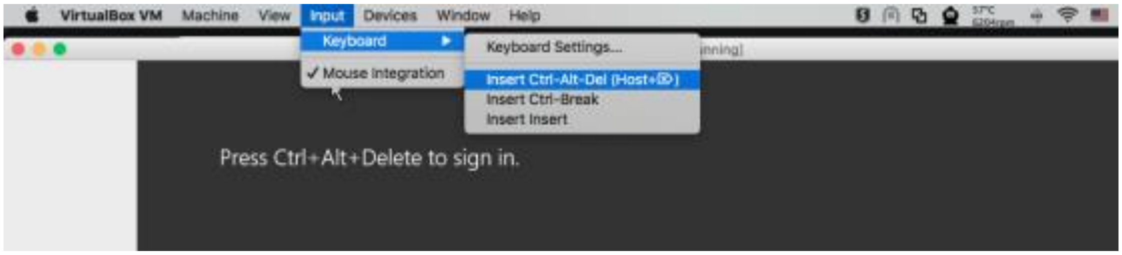
Reenter password:

We’re now finished with installing the Domain Controller.

STEP 7 - INSTALL GUEST ADDITIONS ON DOMAIN CONTROLLER

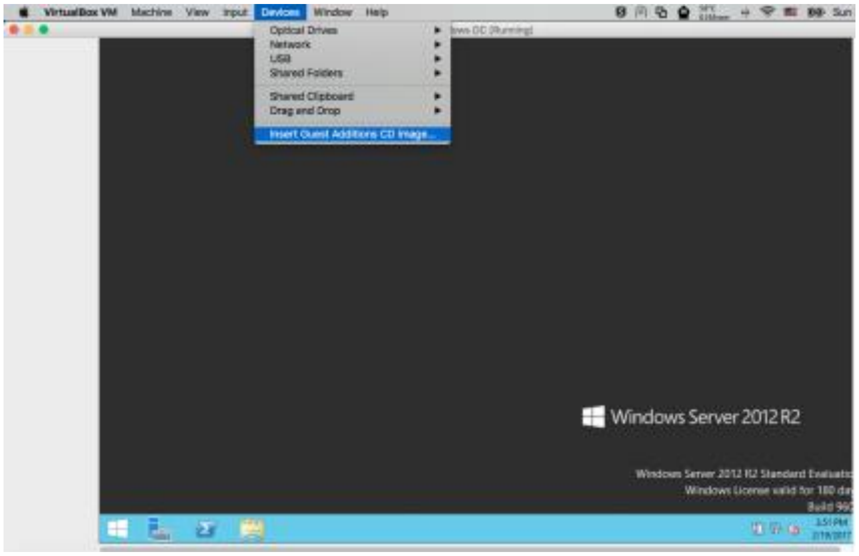
Next, we need to install VirtualBox guest additions the domain controller. The following steps illustrate how to do this on the Windows DC virtual machine, although they should work on each of your other Windows machines as well.

1. Start the Windows DC VM
2. Press [ctrl]+[alt]+[delete] to logon.
    a. Note to Mac users: since your delete key is actually a backspace, you must press [right command]+[fn]+[delete]. If that doesn't work select Input > Keyboard > Insert Ctrl-Alt-Del from the menu bar at the top of the screen.



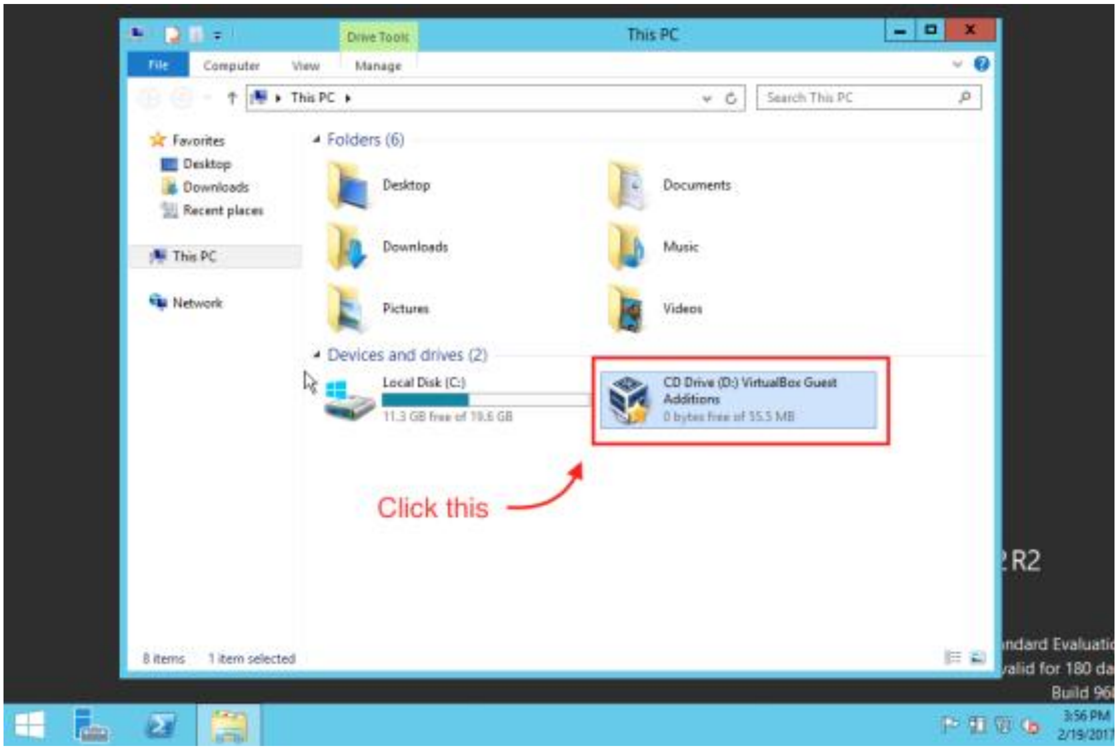
Press Ctrl+Alt+Delete to sign in.

3. If prompted to automatically connect to devices such as printers and TVs, select "No"
4. In the toolbar at the top of your VirtualBox window, select Devices > Insert Guest Additions CD Image



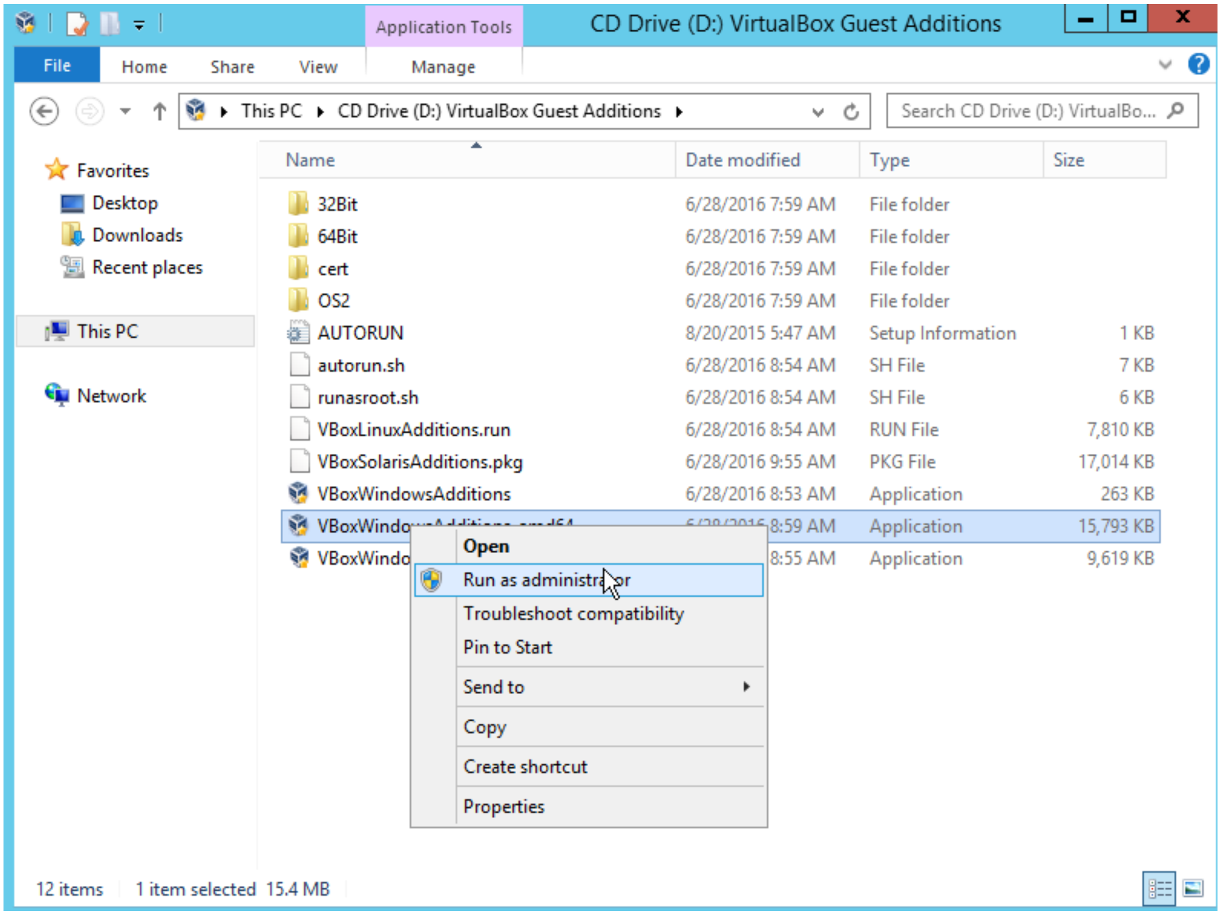
Windows Server 2012 R2 Standard Evaluatio
Windows License valid for 180 da
Build 96

5. As shown in the screenshot below, go to File Explorer > This PC > CD Drive (D:) VirtualBox Guest Additions



Click this

6. As shown in the screenshot below, right click VBoxWindowsAdditions-amd64 and select “Run As Administrator”



Name	Date modified	Type	Size
32Bit	6/28/2016 7:59 AM	File folder	
64Bit	6/28/2016 7:59 AM	File folder	
cert	6/28/2016 7:59 AM	File folder	
OS2	6/28/2016 7:59 AM	File folder	
AUTORUN	8/20/2015 5:47 AM	Setup Information	1 KB
autorun.sh	6/28/2016 8:54 AM	SH File	7 KB
runasroot.sh	6/28/2016 8:54 AM	SH File	6 KB
VBoxLinuxAdditions.run	6/28/2016 8:54 AM	RUN File	7,810 KB
VBoxSolarisAdditions.pkg	6/28/2016 9:55 AM	PKG File	17,014 KB
VBoxWindowsAdditions	6/28/2016 8:53 AM	Application	263 KB
VBoxWindowsAdditions-amd64	6/28/2016 8:59 AM	Application	15,793 KB
VBoxWindo	8:55 AM	Application	9,619 KB

7. Follow the prompts to install VirtualBox guest additions, then select “Reboot Now” when finished

STEP 8 - CONFIGURE ACTIVE DIRECTORY

Before you begin, make sure to download the AWAE Active Directory setup scripts from the following link and place them on your Windows Server virtual machine.

- https://github.com/s0lst1c3/awae-ad-setup-scripts/archive/master.zip

As with the previous section, your PFSense virtual machine must remain running throughout the duration of this section.

STEP 1 - SET POWERSHELL EXECUTION POLICY ON DOMAIN CONTROLLER.

First, we need to configure Powershell to allow us to run scripts from the command line. To do this, open a new Powershell prompt as administrator and run the following command:

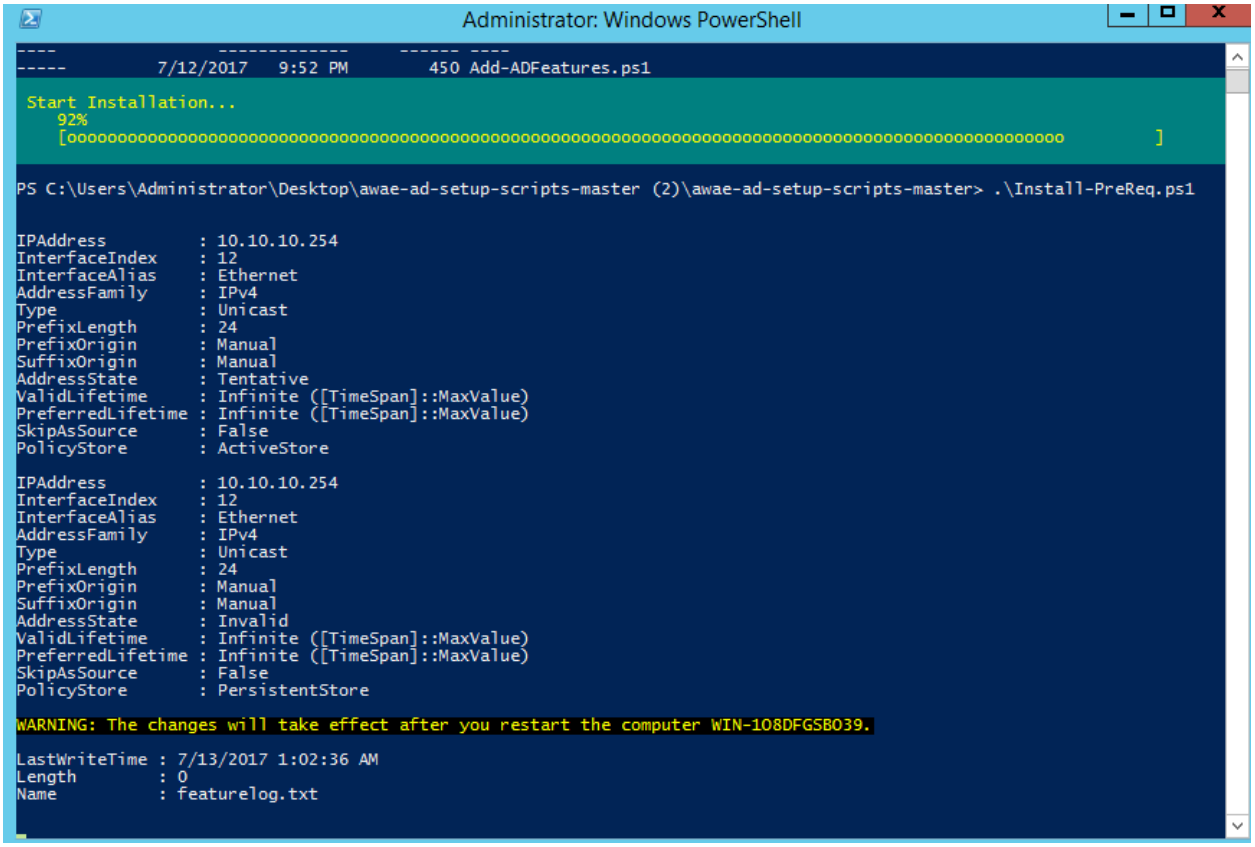
```
PS>  set executionpolicy unrestricted
```

Please note that due to security concerns, this is not something you'd want to do in a production environment.

STEP 2 - INSTALL PREREQUISITES

Next, run the following script using your Powershell command prompt:

- Install-PreReq.ps1

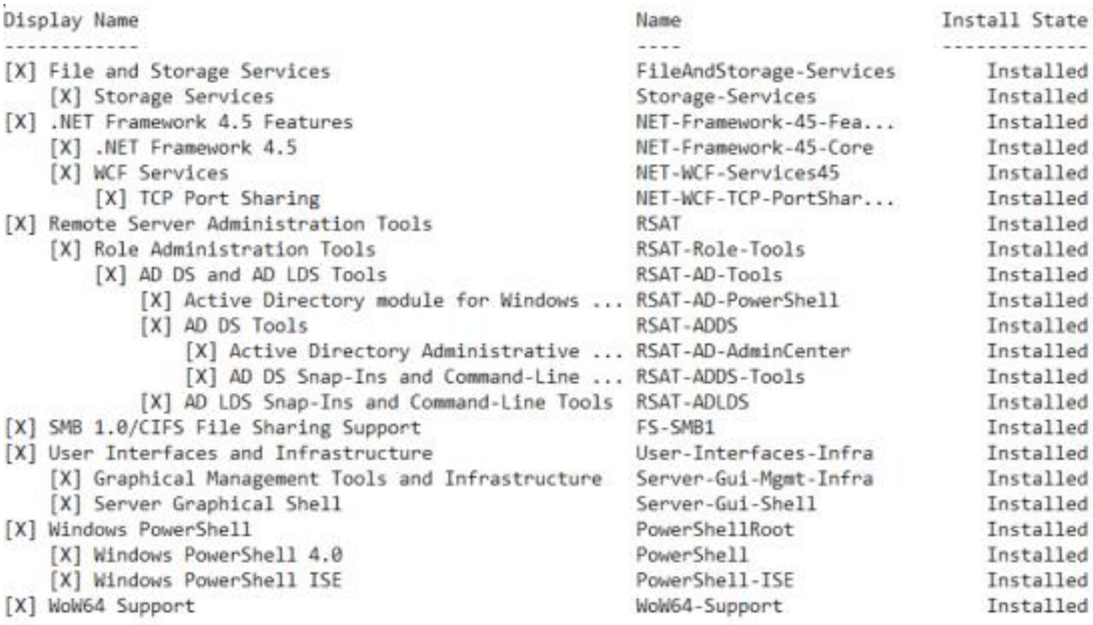


```
----          -------------     ------ ----
-----         7/12/2017   9:52 PM        450 Add-ADFeatures.ps1

 Start Installation...
    92%
    [ooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooo         ]

PS C:\Users\Administrator\Desktop\awae-ad-setup-scripts-master (2)\awae-ad-setup-scripts-master> .\Install-PreReq.ps1


IPAddress         : 10.10.10.254
InterfaceIndex    : 12
InterfaceAlias    : Ethernet
AddressFamily     : IPv4
Type              : Unicast
PrefixLength      : 24
PrefixOrigin      : Manual
SuffixOrigin      : Manual
AddressState      : Tentative
ValidLifetime     : Infinite ([TimeSpan]::MaxValue)
PreferredLifetime : Infinite ([TimeSpan]::MaxValue)
SkipAsSource      : False
PolicyStore       : ActiveStore

IPAddress         : 10.10.10.254
InterfaceIndex    : 12
InterfaceAlias    : Ethernet
AddressFamily     : IPv4
Type              : Unicast
PrefixLength      : 24
PrefixOrigin      : Manual
SuffixOrigin      : Manual
AddressState      : Invalid
ValidLifetime     : Infinite ([TimeSpan]::MaxValue)
PreferredLifetime : Infinite ([TimeSpan]::MaxValue)
SkipAsSource      : False
PolicyStore       : PersistentStore

WARNING: The changes will take effect after you restart the computer WIN-108DFGSB039.

LastWriteTime : 7/13/2017 1:02:36 AM
Length        : 0
Name          : featurelog.txt
```

Once your computer has rebooted, open the following file in Notepad.

- C:\poshlog\featurelog

The contents of the file should be similar to what is shown in the screenshot below. If it isn't, stop and contact the instructor for assistance.



```
Display Name                                            Name                       Install State
------------                                            ----                       -------------
[X] File and Storage Services                           FileAndStorage-Services        Installed
    [X] Storage Services                                Storage-Services               Installed
[X] .NET Framework 4.5 Features                         NET-Framework-45-Fea...        Installed
    [X] .NET Framework 4.5                              NET-Framework-45-Core          Installed
    [X] WCF Services                                    NET-WCF-Services45             Installed
        [X] TCP Port Sharing                            NET-WCF-TCP-PortShar...        Installed
[X] Remote Server Administration Tools                  RSAT                           Installed
    [X] Role Administration Tools                       RSAT-Role-Tools                Installed
        [X] AD DS and AD LDS Tools                      RSAT-AD-Tools                  Installed
            [X] Active Directory module for Windows ... RSAT-AD-PowerShell             Installed
            [X] AD DS Tools                             RSAT-ADDS                      Installed
                [X] Active Directory Administrative ... RSAT-AD-AdminCenter            Installed
                [X] AD DS Snap-Ins and Command-Line ... RSAT-ADDS-Tools                Installed
            [X] AD LDS Snap-Ins and Command-Line Tools  RSAT-ADLDS                     Installed
[X] SMB 1.0/CIFS File Sharing Support                   FS-SMB1                        Installed
[X] User Interfaces and Infrastructure                  User-Interfaces-Infra          Installed
    [X] Graphical Management Tools and Infrastructure   Server-Gui-Mgmt-Infra          Installed
    [X] Server Graphical Shell                          Server-Gui-Shell               Installed
[X] Windows PowerShell                                  PowerShellRoot                 Installed
    [X] Windows PowerShell 4.0                          PowerShell                     Installed
    [X] Windows PowerShell ISE                          PowerShell-ISE                 Installed
[X] WoW64 Support                                       WoW64-Support                  Installed
```

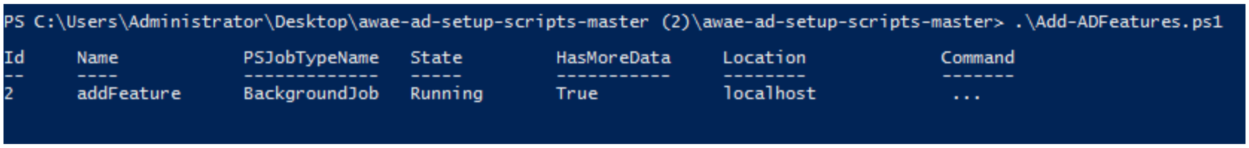
STEP 3 - INSTALL ACTIVE DIRECTORY FEATURES

Next, we need to install the following items to the domain controller:

- Active Directory Domain Services role
- DNS Server role
- Group Policy management feature

To do this, run the following script:

- Add-ADFeatures.ps1

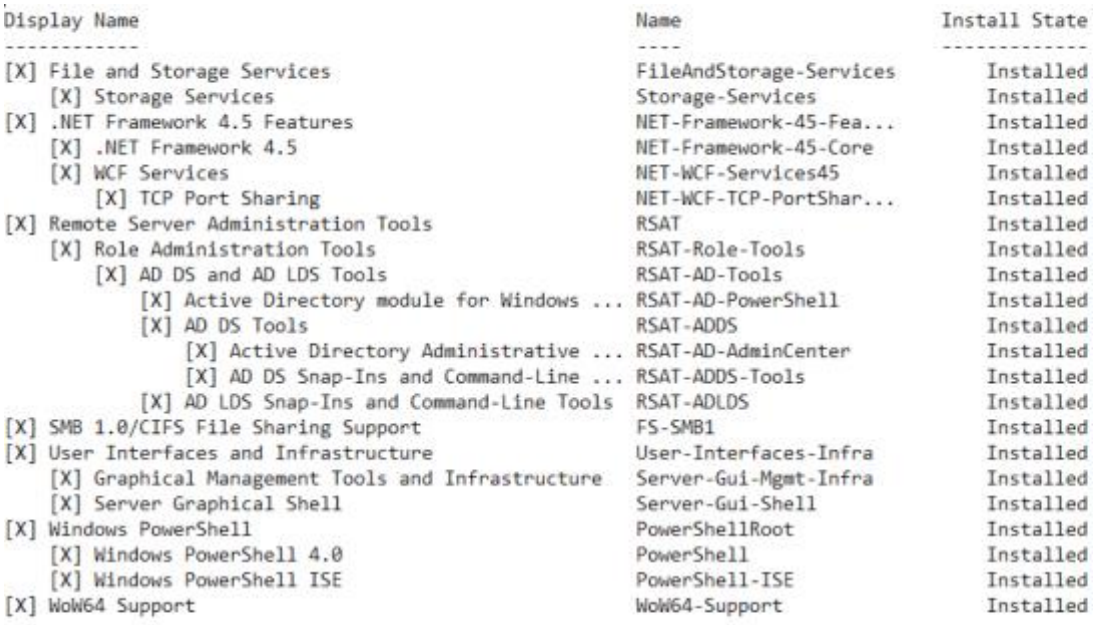


```
PS C:\Users\Administrator\Desktop\awae-ad-setup-scripts-master (2)\awae-ad-setup-scripts-master> .\Add-ADFeatures.ps1

Id     Name            PSJobTypeName   State         HasMoreData     Location             Command
--     ----            -------------   -----         -----------     --------             -------
2      addFeature      BackgroundJob   Running       True            localhost             ...
```

Once the script has finished executing, open the following file in Notepad as before:

- C:\poshlog\featurelog

The contents of the file should be similar to what is shown in the screenshot below. If it isn't, stop and contact the instructor for assistance.

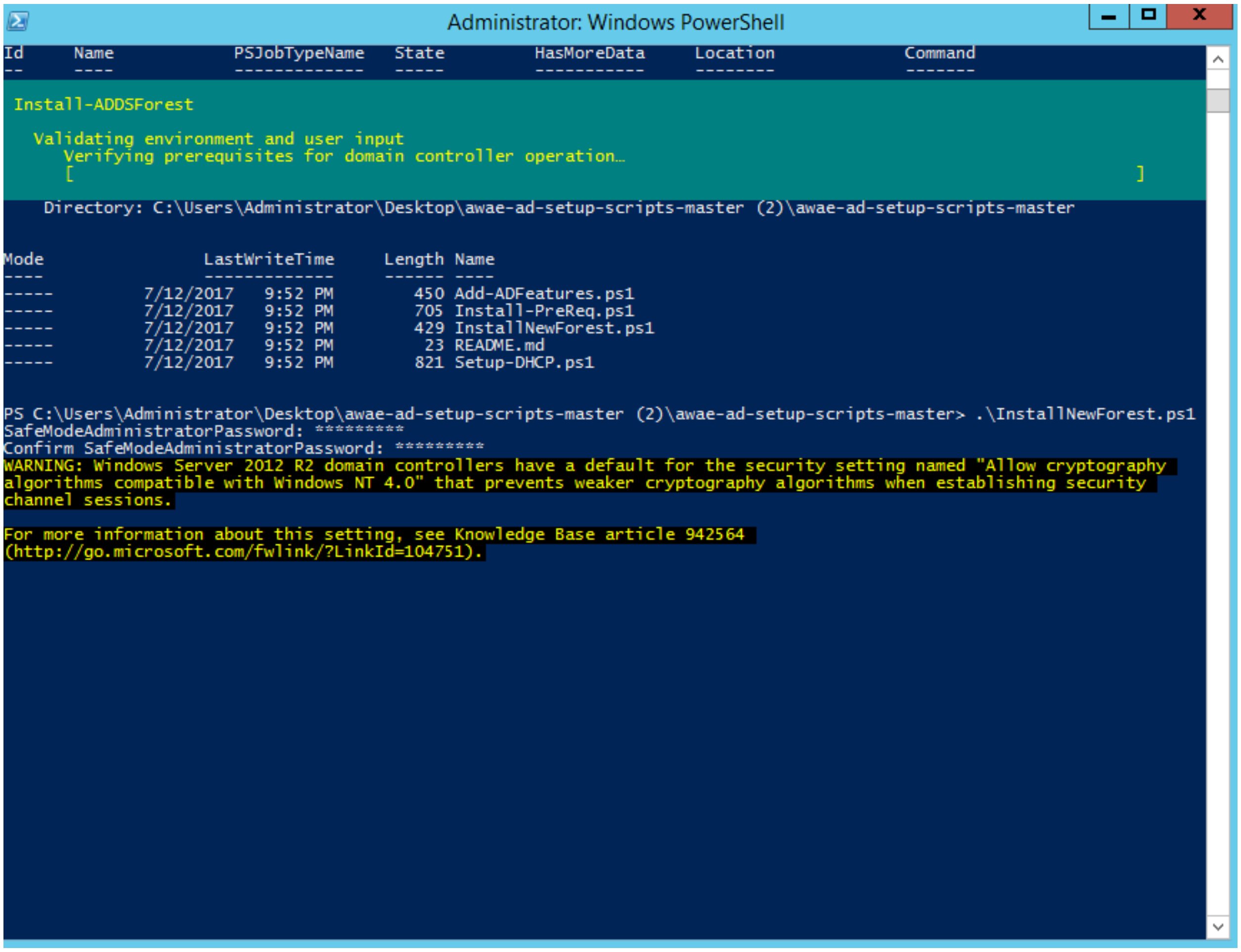


```
Display Name                                            Name                       Install State
------------                                            ----                       -------------
[X] File and Storage Services                           FileAndStorage-Services        Installed
    [X] Storage Services                                Storage-Services               Installed
[X] .NET Framework 4.5 Features                         NET-Framework-45-Fea...        Installed
    [X] .NET Framework 4.5                              NET-Framework-45-Core          Installed
    [X] WCF Services                                    NET-WCF-Services45             Installed
        [X] TCP Port Sharing                            NET-WCF-TCP-PortShar...        Installed
[X] Remote Server Administration Tools                  RSAT                           Installed
    [X] Role Administration Tools                       RSAT-Role-Tools                Installed
        [X] AD DS and AD LDS Tools                      RSAT-AD-Tools                  Installed
            [X] Active Directory module for Windows ... RSAT-AD-PowerShell             Installed
            [X] AD DS Tools                             RSAT-ADDS                      Installed
                [X] Active Directory Administrative ... RSAT-AD-AdminCenter            Installed
                [X] AD DS Snap-Ins and Command-Line ... RSAT-ADDS-Tools                Installed
            [X] AD LDS Snap-Ins and Command-Line Tools  RSAT-ADLDS                     Installed
[X] SMB 1.0/CIFS File Sharing Support                   FS-SMB1                        Installed
[X] User Interfaces and Infrastructure                  User-Interfaces-Infra          Installed
    [X] Graphical Management Tools and Infrastructure   Server-Gui-Mgmt-Infra          Installed
    [X] Server Graphical Shell                          Server-Gui-Shell               Installed
[X] Windows PowerShell                                  PowerShellRoot                 Installed
    [X] Windows PowerShell 4.0                          PowerShell                     Installed
    [X] Windows PowerShell ISE                          PowerShell-ISE                 Installed
[X] WoW64 Support                                       WoW64-Support                  Installed
```

STEP 4 - SETUP ACTIVE DIRECTORY

Next, we need to create a new forest and promote our server to the role of Domain Controller. To do this, run the following Powershell script:

- InstallNewForest.ps1



```
Id     Name            PSJobTypeName   State         HasMoreData     Location             Command
--     ----            -------------   -----         -----------     --------             -------

 Install-ADDSForest

   Validating environment and user input
      Verifying prerequisites for domain controller operation…
      [                                                                                                  ]

    Directory: C:\Users\Administrator\Desktop\awae-ad-setup-scripts-master (2)\awae-ad-setup-scripts-master


Mode                LastWriteTime     Length Name
----                -------------     ------ ----
-----         7/12/2017   9:52 PM        450 Add-ADFeatures.ps1
-----         7/12/2017   9:52 PM        705 Install-PreReq.ps1
-----         7/12/2017   9:52 PM        429 InstallNewForest.ps1
-----         7/12/2017   9:52 PM         23 README.md
-----         7/12/2017   9:52 PM        821 Setup-DHCP.ps1


PS C:\Users\Administrator\Desktop\awae-ad-setup-scripts-master (2)\awae-ad-setup-scripts-master> .\InstallNewForest.ps1
SafeModeAdministratorPassword: *********
Confirm SafeModeAdministratorPassword: *********
WARNING: Windows Server 2012 R2 domain controllers have a default for the security setting named "Allow cryptography
algorithms compatible with Windows NT 4.0" that prevents weaker cryptography algorithms when establishing security
channel sessions.

For more information about this setting, see Knowledge Base article 942564
(http://go.microsoft.com/fwlink/?LinkId=104751).
```

The script will prompt you to set your Active Directory recovery password. Set this to something memorable. When prompted to reboot, click accept.

At this point it's important to make sure DNS is still working, so try pinging google.com from the command line as follows:

```
PS>  ping google.com
```

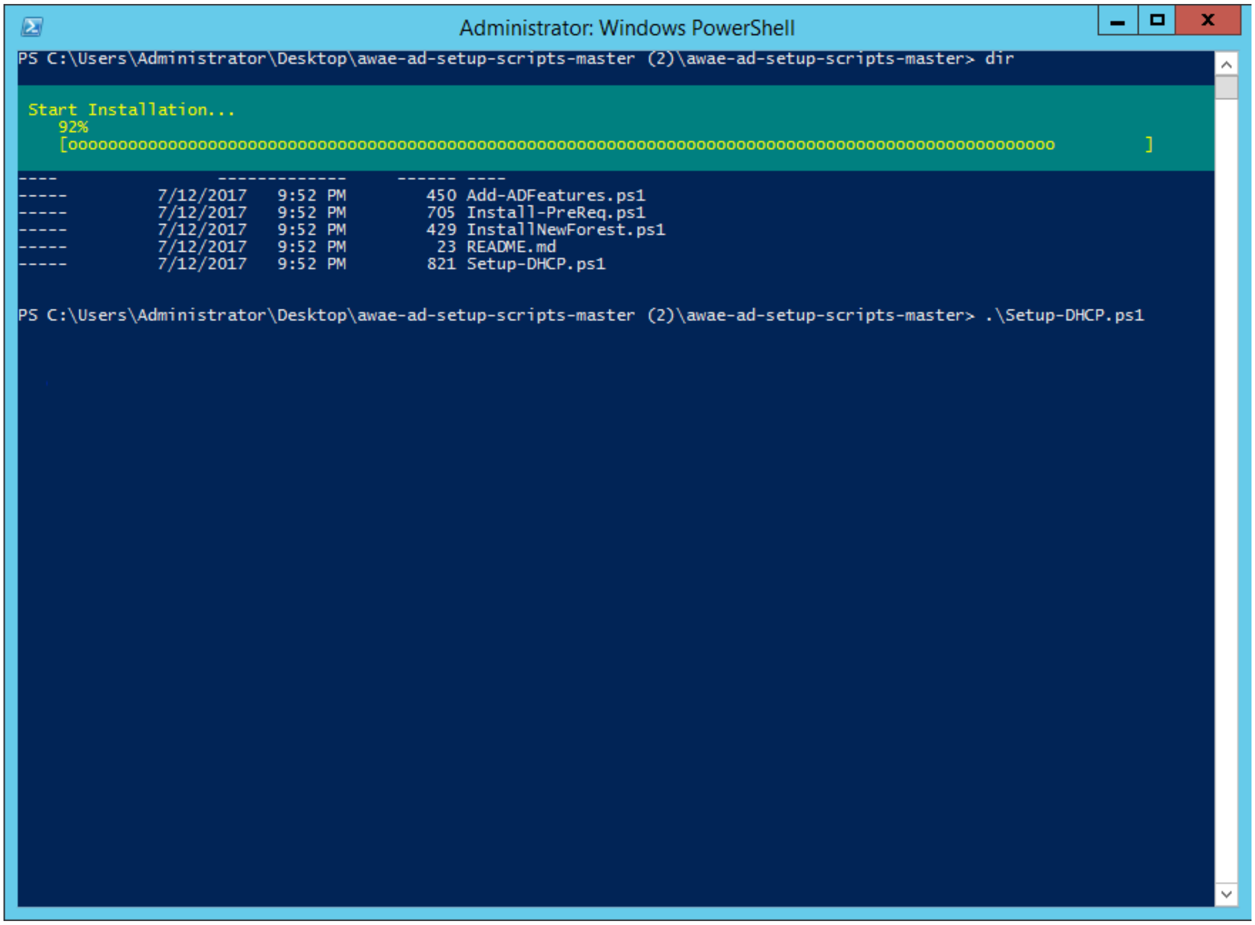
If you can't ping google.com, contact the instructor for assistance.

STEP 5 - CONFIGURE DHCP

Next we need to add the DCHP role to our Domain controller. To do this, run the following Powershell script as Administrator:

- Setup-DHCP.ps1

Once again, this probably isn’t something you’d want to do in a production environment because it creates a single point of failure. For our lab, however, it works just fine.



```
PS C:\Users\Administrator\Desktop\awae-ad-setup-scripts-master (2)\awae-ad-setup-scripts-master> dir

 Start Installation...
    92%
    [ooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooo         ]
----                -------------      ------ ----
-----         7/12/2017   9:52 PM         450 Add-ADFeatures.ps1
-----         7/12/2017   9:52 PM         705 Install-PreReq.ps1
-----         7/12/2017   9:52 PM         429 InstallNewForest.ps1
-----         7/12/2017   9:52 PM          23 README.md
-----         7/12/2017   9:52 PM         821 Setup-DHCP.ps1


PS C:\Users\Administrator\Desktop\awae-ad-setup-scripts-master (2)\awae-ad-setup-scripts-master> .\Setup-DHCP.ps1
```

STEP 6 - DISABLE WINDOWS FIREWALL

Using a firewall is generally a good thing. However, in the interest of spending more time hacking and less time troubleshooting, let’s disable Windows Firewall for all computers within the domain using a Group Policy Object.

To do this, first open up your Powershell prompt as Administrator and run the following command:

```
PS>  New-GPO DisableFirewall | New-GPLink -Target “DC=example.com,DC=com” -
LinkEnabled yes
```

This will create a new Group Policy Object named “DisableFirewall” and link it to our example.com domain.

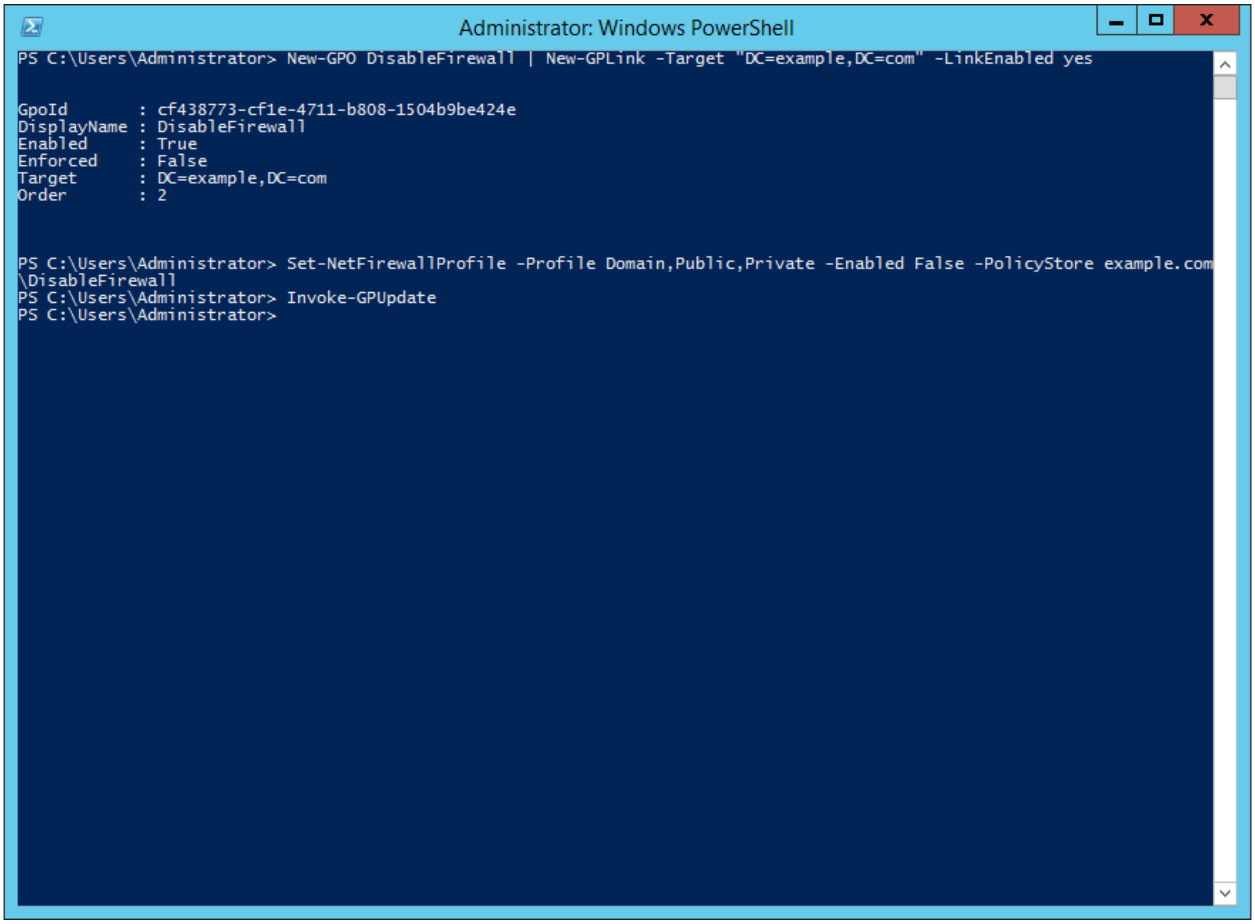
Next, we apply the appropriate firewall configuration to the Group Policy Object that we just created:

```
PS> Set-NetFirewallProfile -Profile Domain,Public,Private -Enabled False -PolicyStore
example.com\DisableFirewall
```

Finally, we use the Invoke-GPUpdate cmdlet to pull our newly created Group Policy Object:

```
PS> Invoke-GPUpdate
```

Note that it may take some time for these changes to take effect, so don’t be alarmed if Windows Firewall does not become disabled immediately.



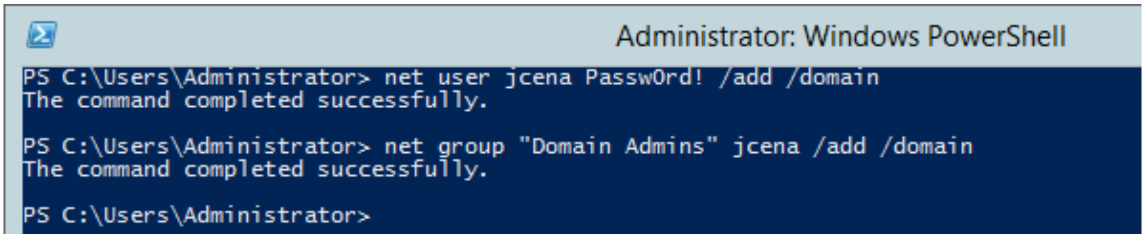
```
PS C:\Users\Administrator> New-GPO DisableFirewall | New-GPLink -Target "DC=example,DC=com" -LinkEnabled yes


GpoId       : cf438773-cf1e-4711-b808-1504b9be424e
DisplayName : DisableFirewall
Enabled     : True
Enforced    : False
Target      : DC=example,DC=com
Order       : 2


PS C:\Users\Administrator> Set-NetFirewallProfile -Profile Domain,Public,Private -Enabled False -PolicyStore example.com
\DisableFirewall
PS C:\Users\Administrator> Invoke-GPUpdate
PS C:\Users\Administrator>
```

STEP 7 – ADD DOMAIN ADMIN USER

This part is pretty simple. Just create a new user and promote it to Domain Admin using the following two commands:

```
net user jcena Passw0rd! /add /domain

net group “Domain Admins” jcena /add /domain
```

Feel free to use a different username and password.



```
PS C:\Users\Administrator> net user jcena Passw0rd! /add /domain
The command completed successfully.

PS C:\Users\Administrator> net group "Domain Admins" jcena /add /domain
The command completed successfully.

PS C:\Users\Administrator>
```

STEP 9 - ADD WINDOWS WORKSTATIONS TO DOMAIN

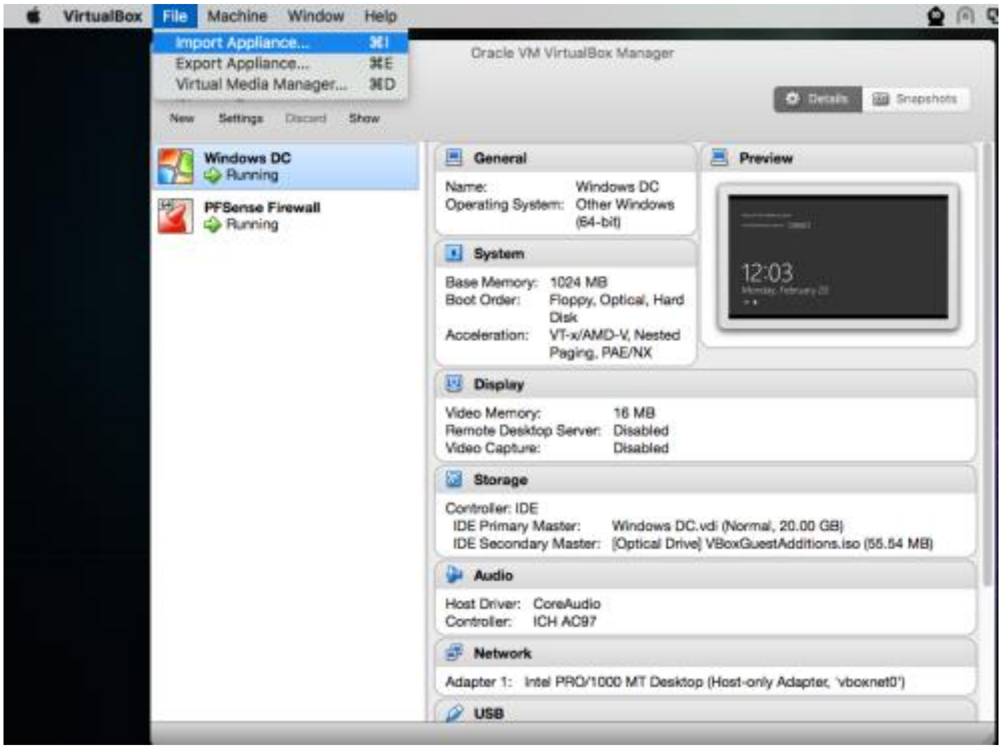
Congrats. You've made it through what is by far the most time consuming section of this setup guide. Give yourself a pat on the back before you move on.

Before proceeding any further, make sure that both your PFSense virtual machine and your Domain Controller are running.

ADD WINDOWS 10 WORKSTATION

It's time to add workstations to our Active Directory environment. We'll start by adding our Windows 10 workstation using the following steps:

1. Extract the zip archive that we downloaded in Step 1 – Download a Windows 10 Developer VM.
2. Open VirtualBox
3. From the VirtualBox main menu, select File > Import Appliance as shown in the screenshot below.



General
Name: Windows DC
Operating System: Other Windows (64-bit)

System
Base Memory: 1024 MB
Boot Order: Floppy, Optical, Hard Disk
Acceleration: VT-x/AMD-V, Nested Paging, PAE/NX

Display
Video Memory: 16 MB
Remote Desktop Server: Disabled
Video Capture: Disabled

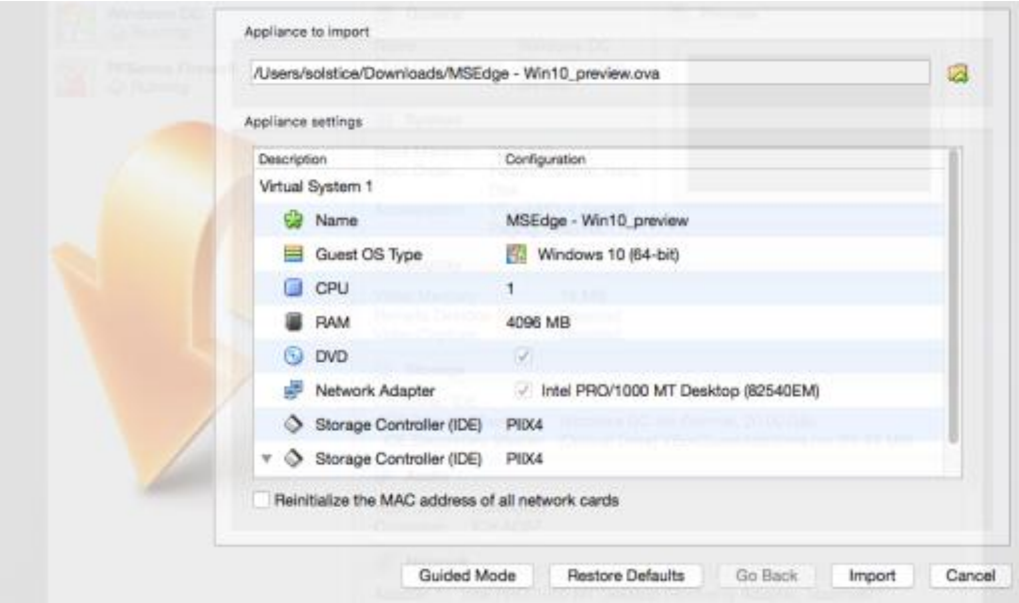
Storage
Controller: IDE
IDE Primary Master: Windows DC.vdi (Normal, 20.00 GB)
IDE Secondary Master: [Optical Drive] VBoxGuestAdditions.iso (55.54 MB)

Audio
Host Driver: CoreAudio
Controller: ICH AC97

Network
Adapter 1: Intel PRO/1000 MT Desktop (Host-only Adapter, 'vboxnet0')

USB

4. Select the path of your Windows 10 virtual machine (the .ovf you just extracted). If you can, give the virtual machine at least 2 GB of RAM. Then click "Import".



Appliance to import

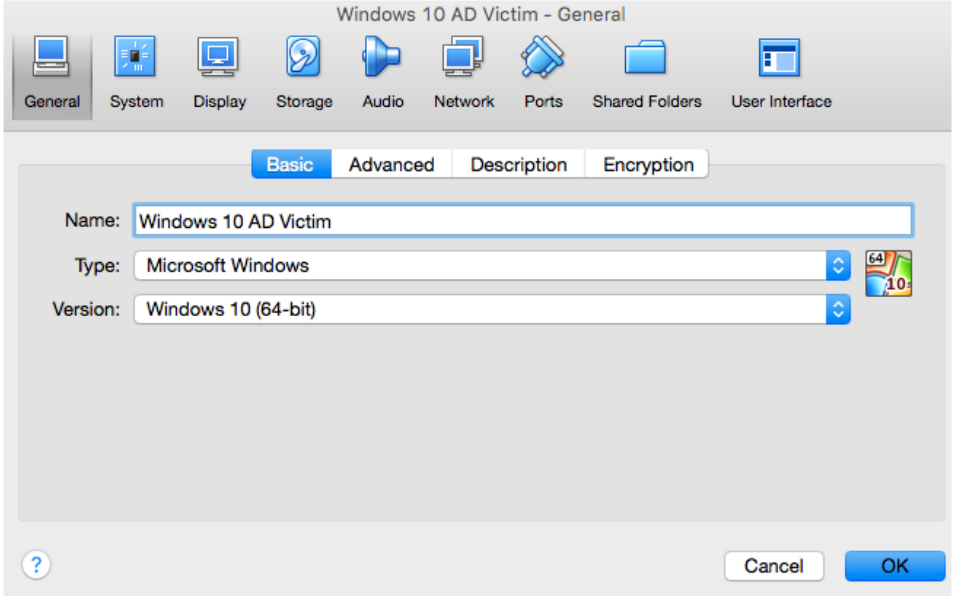
/Users/solstice/Downloads/MSEdge - Win10_preview.ova

Appliance settings

Description	Configuration
Virtual System 1	
Name	MSEdge - Win10_preview
Guest OS Type	Windows 10 (64-bit)
CPU	1
RAM	4096 MB
DVD	✓
Network Adapter	✓ Intel PRO/1000 MT Desktop (82540EM)
Storage Controller (IDE)	PIIX4
Storage Controller (IDE)	PIIX4

☐ Reinitialize the MAC address of all network cards

5. When the VM import process is complete, select the new Windows 10 virtual machine in the list to the left. Then go to Settings > General and change the virtual machine's name to "Windows 10 AD Victim".



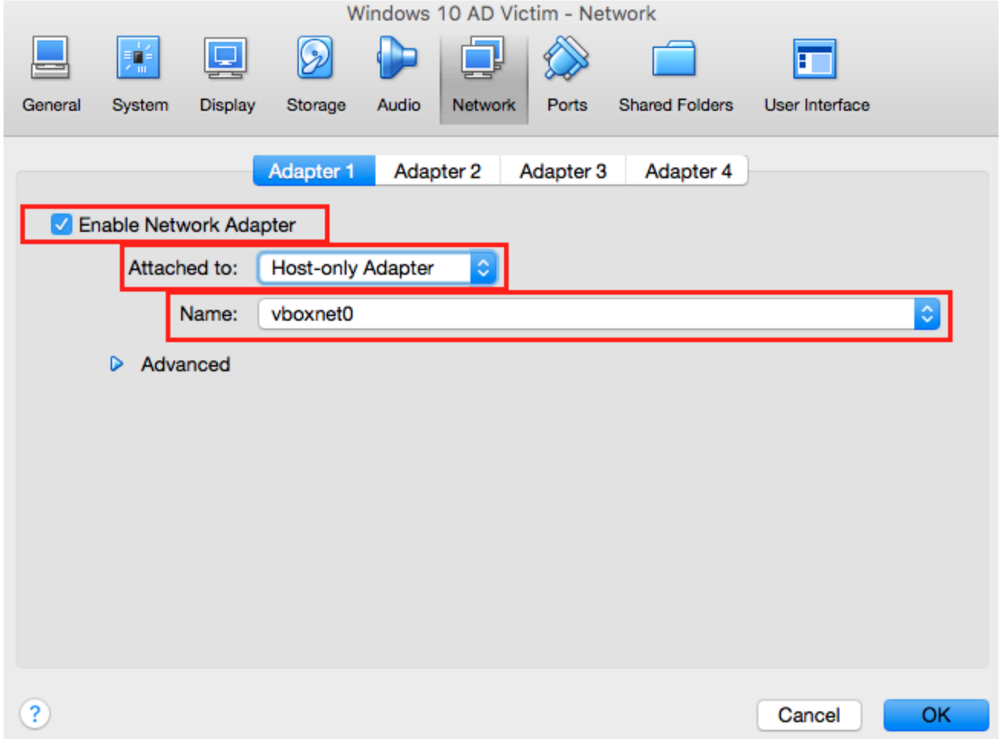
Windows 10 AD Victim - General

Name: Windows 10 AD Victim

Type: Microsoft Windows

Version: Windows 10 (64-bit)

6. Next, navigate to the Settings > Network > Adapter 1 as shown in the screenshot below. Then perform the following configurations as shown in the screenshot below:
   a. Ensure that the "Enable Network Adapter" box is checked.
   b. Set "Attached to" to "Host-only Adapter".
   c. Set "name" to vboxnet0.

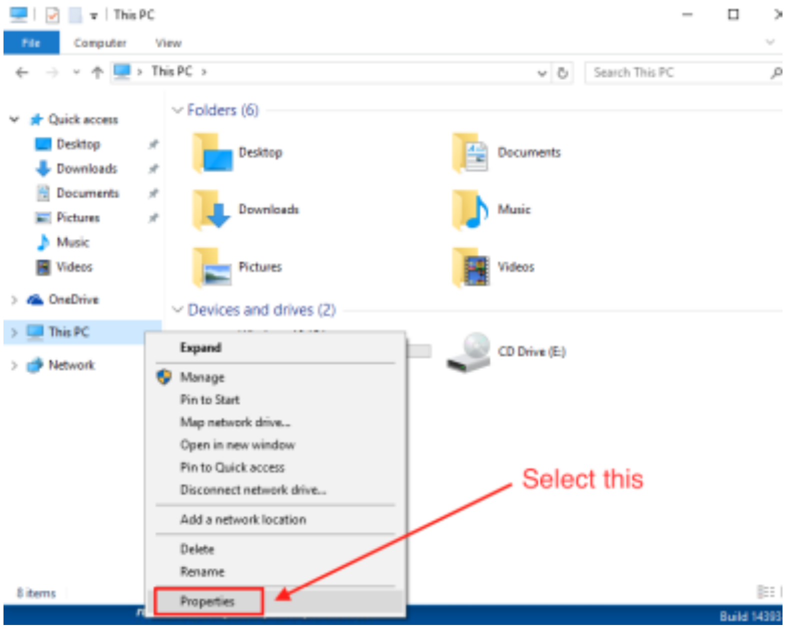


☑ Enable Network Adapter

Attached to: Host-only Adapter

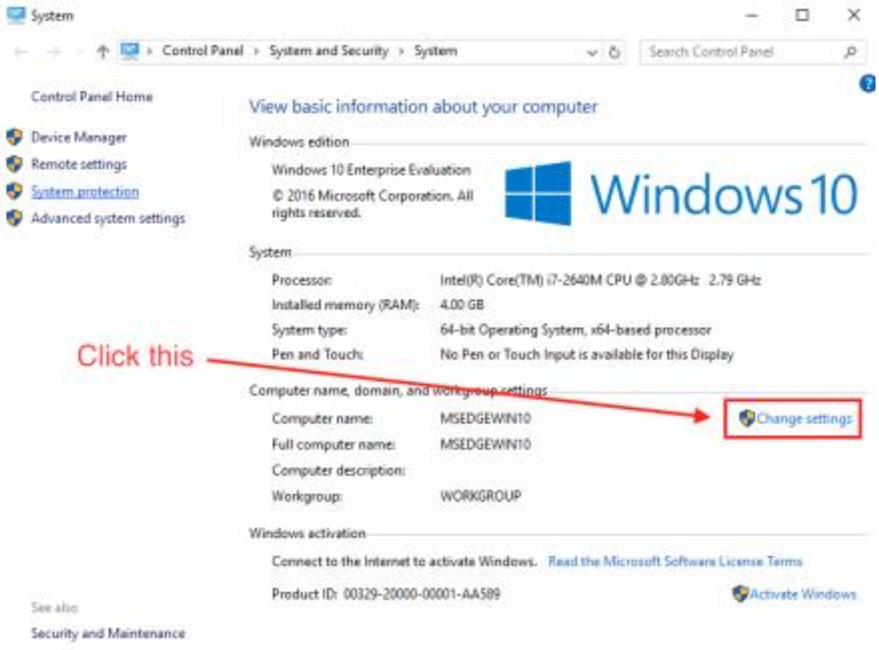
Name: vboxnet0

7. Click "OK" to return to the main VirtualBox menu.
8. Power-on the Windows 10 Ad Victim virtual machine.
9. Go to Explorer > This PC > Properties as shown in the screenshot below.



Select this

10. In the Properties window, click on “Change Settings” as shown in the screenshot below.



View basic information about your computer

Windows edition

Windows 10 Enterprise Evaluation

© 2016 Microsoft Corporation. All rights reserved.

System

Processor: Intel(R) Core(TM) i7-2640M CPU @ 2.80GHz 2.79 GHz

Installed memory (RAM): 4.00 GB

System type: 64-bit Operating System, x64-based processor

Pen and Touch: No Pen or Touch Input is available for this Display

Computer name, domain, and workgroup settings

Computer name: MSEDGEWIN10

Full computer name: MSEDGEWIN10

Computer description:

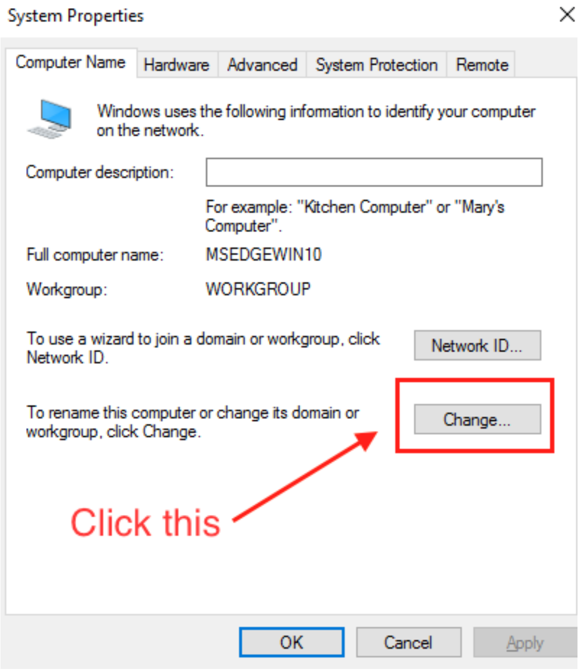
Workgroup: WORKGROUP

Windows activation

Connect to the Internet to activate Windows. Read the Microsoft Software License Terms

Product ID: 00329-20000-00001-AA589

11. In the popup window, go to the “Computer Name” tab then click the “Change” button.



Windows uses the following information to identify your computer on the network.

Computer description:

For example: "Kitchen Computer" or "Mary's Computer".

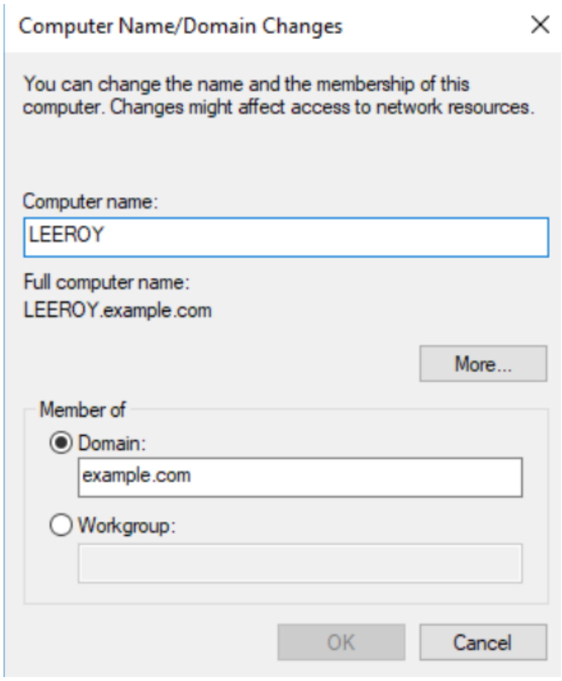
Full computer name: MSEDGEWIN10

Workgroup: WORKGROUP

To use a wizard to join a domain or workgroup, click Network ID.

To rename this computer or change its domain or workgroup, click Change.

12. In the popup window that appears, do the following as shown in the screenshot below:
    d. Set the “Computer Name” to whatever you want
    e. Select the “Domain” radio button
    f. Set the “Domain” field to “example.com”
    g. Click “OK”



Computer Name/Domain Changes

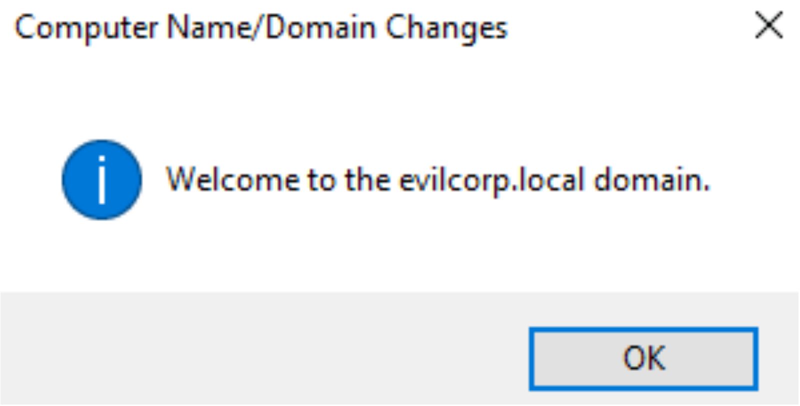
You can change the name and the membership of this computer. Changes might affect access to network resources.

Computer name:
LEEROY

Full computer name:
LEEROY.example.com

Member of
● Domain:
example.com
○ Workgroup:

13. You will be prompted to enter credentials. Enter the username and password for the Domain Admin account you created earlier.
14. If the authentication is successful, you will see a prompt similar the one shown in the screenshot below. Click “OK”.



Computer Name/Domain Changes

Welcome to the evilcorp.local domain.

15. You will be issued a prompt stating that a reboot is necessary. When this occurs, click “Restart Now”.
16. Finally, install VirtualBox guest additions using the same steps you followed in Step 7 - Install Guest Additions on Domain Controller.

ADD WINDOWS 8 WORKSTATION

Repeat each of the steps you followed to add the Windows 10 workstation to your domain, but this time use your Windows 8 virtual machine instead. Make sure that you give your Windows 8 machine a unique hostname and name it something other than “Windows 10 AD Victim”.

Congratulations. You have completed the lab setup guide.