

# Adversarial Resilience - Assessing Infrastructure Security

## Project Scenario

Adversarial Resilience - Assessing StaticSpeed's Infrastructure Security Posture Report  
Your employer, NuttyUtility, is a company in the technology sector with cutting edge software that is known to be targeted by foreign adversaries and has recently acquired a new company, StaticSpeed. Your job is to assess the security posture of the newly acquired company.

Specifically, your boss wants to know the current status of assets inside the perimeter (desktops, servers, remote access, firewalls, applications). Use the given information about the systems currently in place to understand better the possible vulnerabilities and exposures at this new company.

Upon an initial inspection as part of the acquisition, we suspect these systems have not been kept up to date. There is a likelihood that the servers and desktops at this location are running vulnerable applications and misconfigurations that may lead to compromises either by rogue insiders or external malicious actors. If this is the case, this would be an unacceptable scenario as we plan to combine StaticSpeeds systems with our extended network.

Your goal is to establish what assets are in place, perform a security assessment based on industry security controls and best practices, and execute a vulnerability assessment against servers and desktop assets. The result of this assessment will be a report that you must present to your stakeholders. They will relay your findings to the infrastructure team. Together they will decide if this new company is ready to be integrated or if appropriate controls and mitigations need to be in place before this happens.

## Windows Project VM Setup

### Getting Started

First, download and set up the virtual machines if you have not already done so.

NOTE: These VMs are used in both the course and the project. If you have already set them up, you do not need to do so again.

Step 1: Download the two (.ova) virtual machines to your computer.

- [Ubuntu1804student.ova](#)
- [win10ustudent.ova](#)

It will take some time to download. Start with the Ubuntu1804student.ova machine, then download the win10ustudent.ova.

Step 2: Download & Install Oracle VirtualBox software, which will be used as our virtualization tool for loading the OVA file downloaded above. You can download it at [Oracle VirtualBox Downloads](#). Please follow the instructions for installing Virtual Box from their website.

NOTE: Troubleshooting

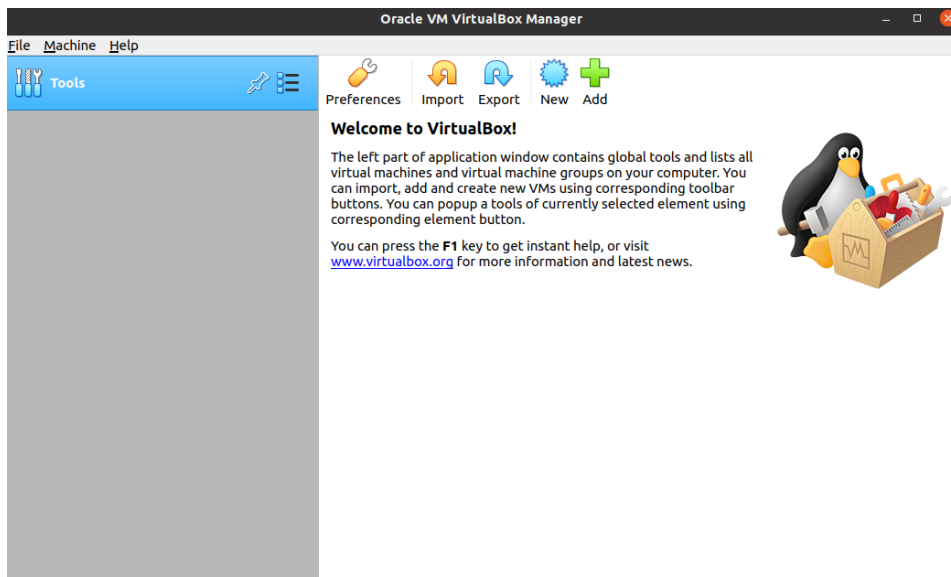
If the VM aborts shortly after startup, try starting VirtualBox using the terminal:

sudo Virtualbox

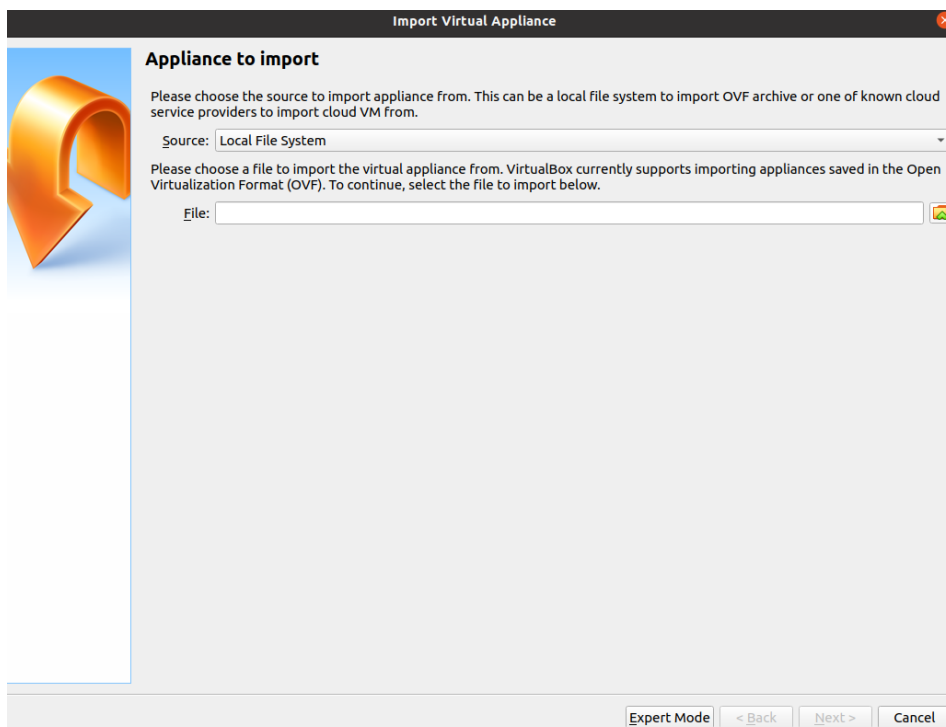
If that doesn't work, try these steps:

Go to File > Import Appliance > Expert Mode > . Uncheck the box for Import hard drives as VDI Import Security Onion OVA Right-click VM in the manager. Go to Settings > Display > Screen > Increase the Video Memory

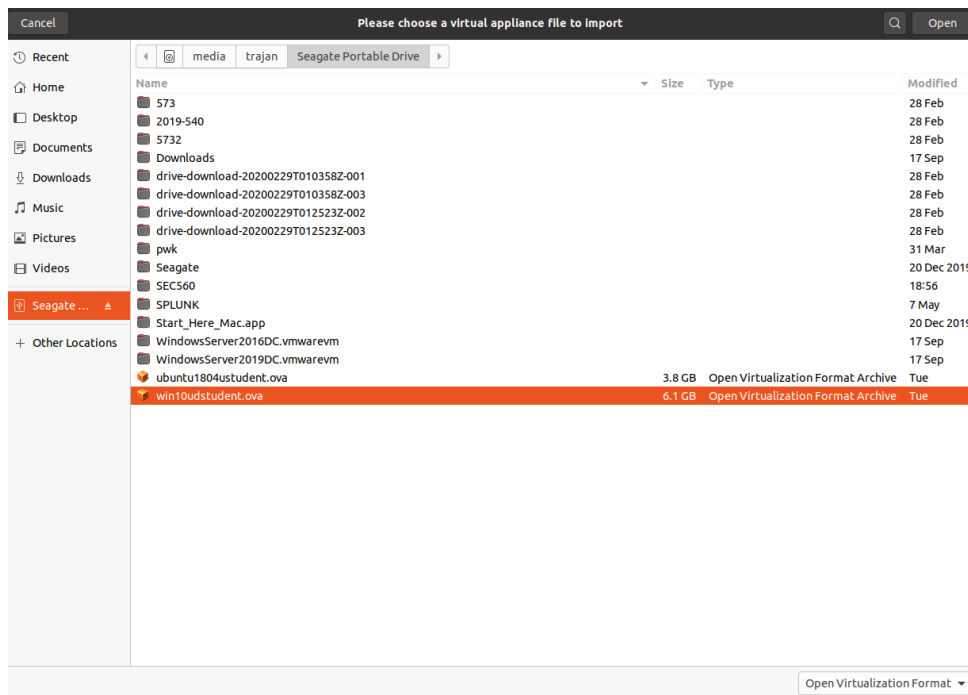
Step 3: Import virtual machines into your VirtualBox Manager. Please follow along with the screenshots below to complete this part. Then, repeat these steps for the second virtual machine. Once this is complete, you will set up a NAT network for the machines to communicate with each other and verify connectivity.



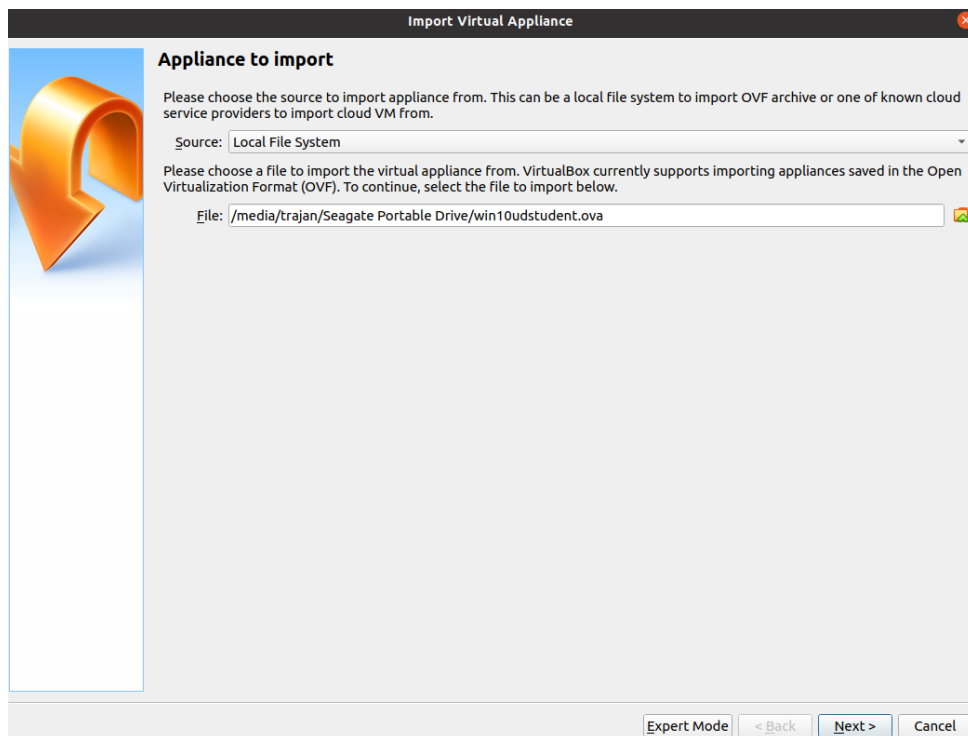
Virtualbox welcome screen, click import.



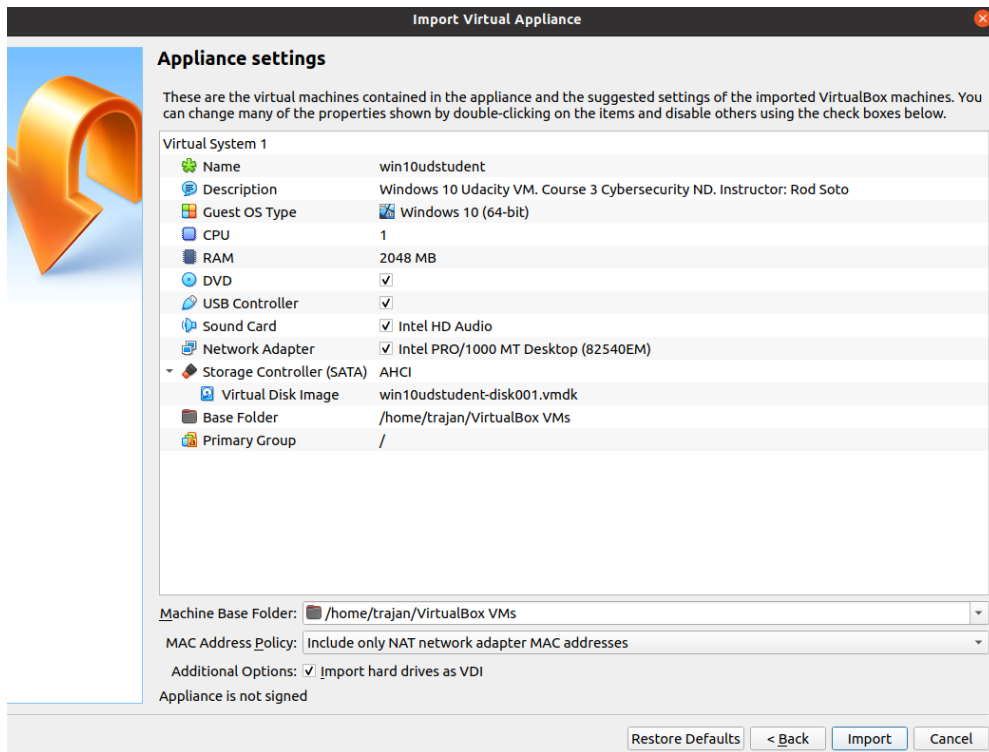
## Choose Your Source



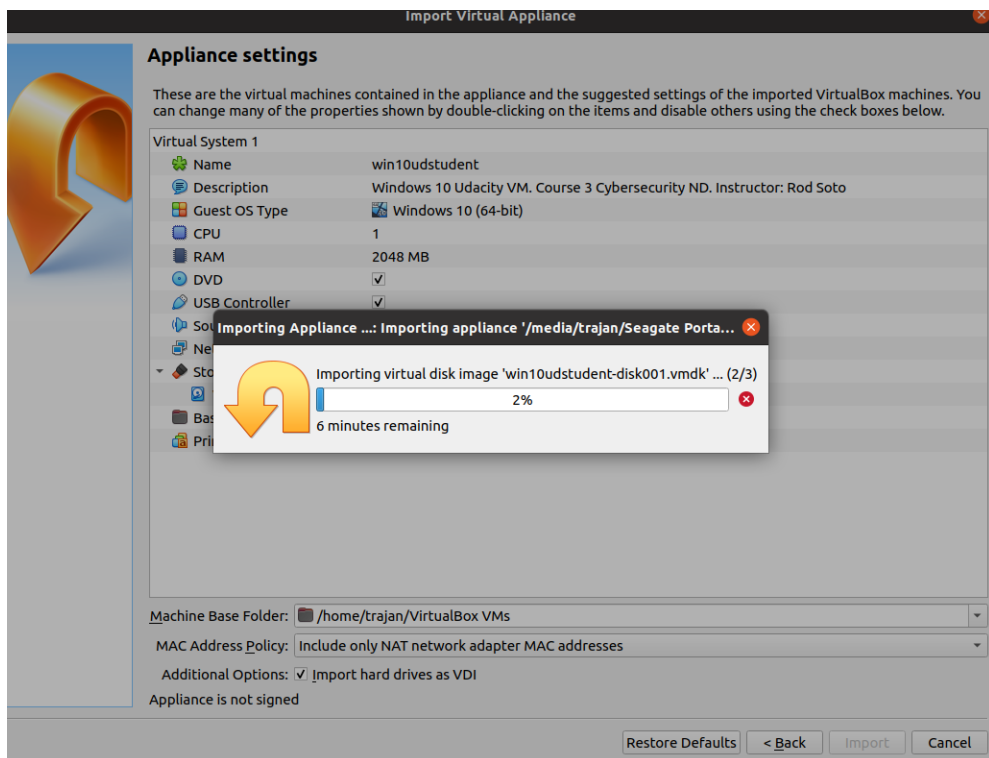
Choose the OVA file you want to import. Let's start with the Windows image.



After selecting the image you want to import, click next.

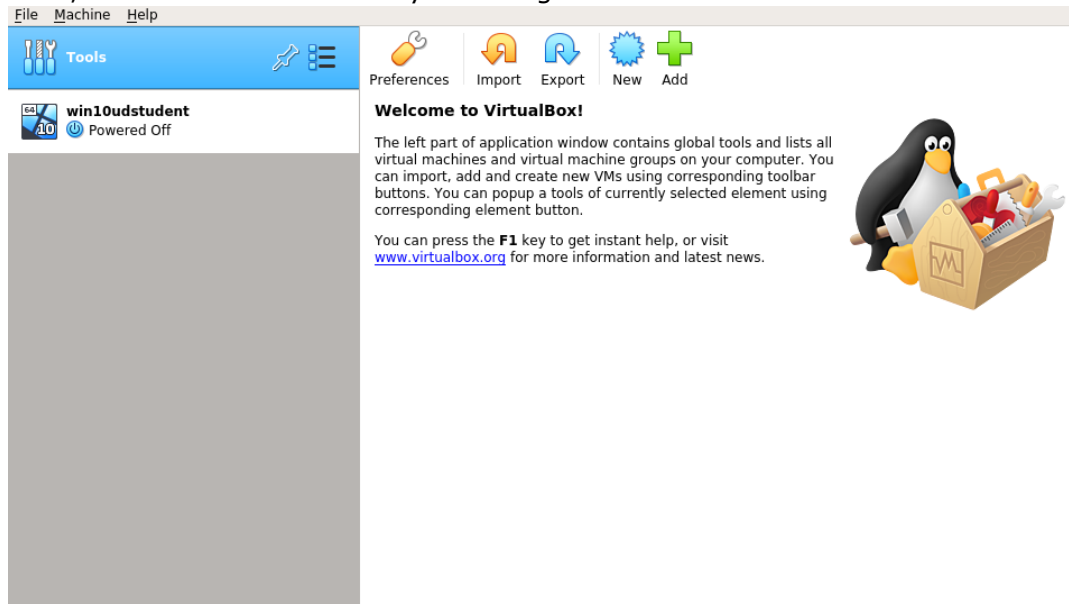


Use the default settings, and click next.

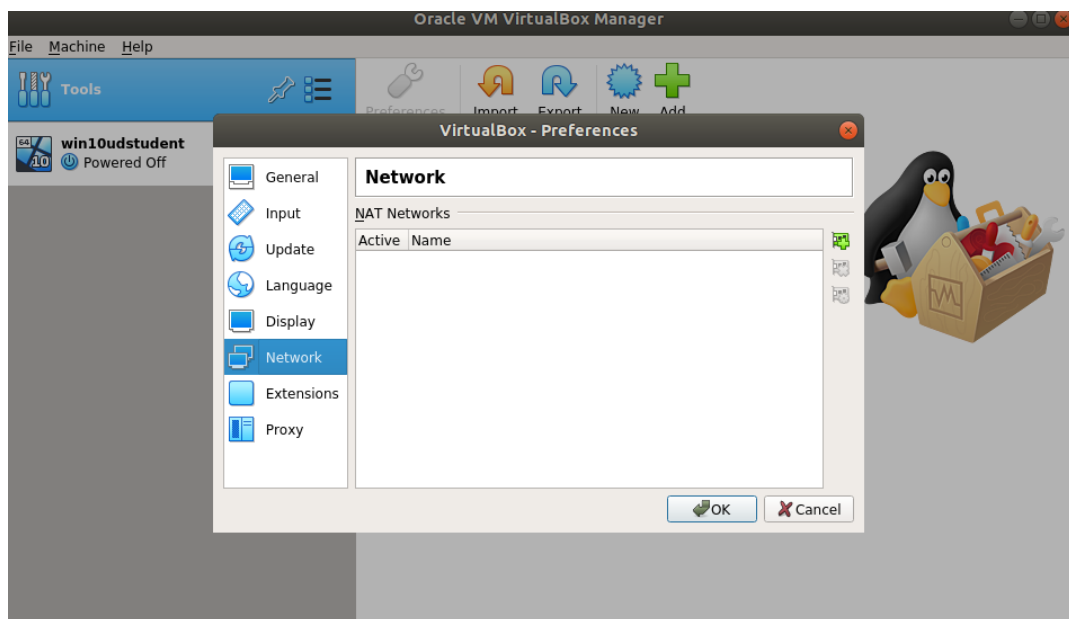


Let VirtualBox complete the import.

Next, create a NAT Network by following these screenshots and instructions:

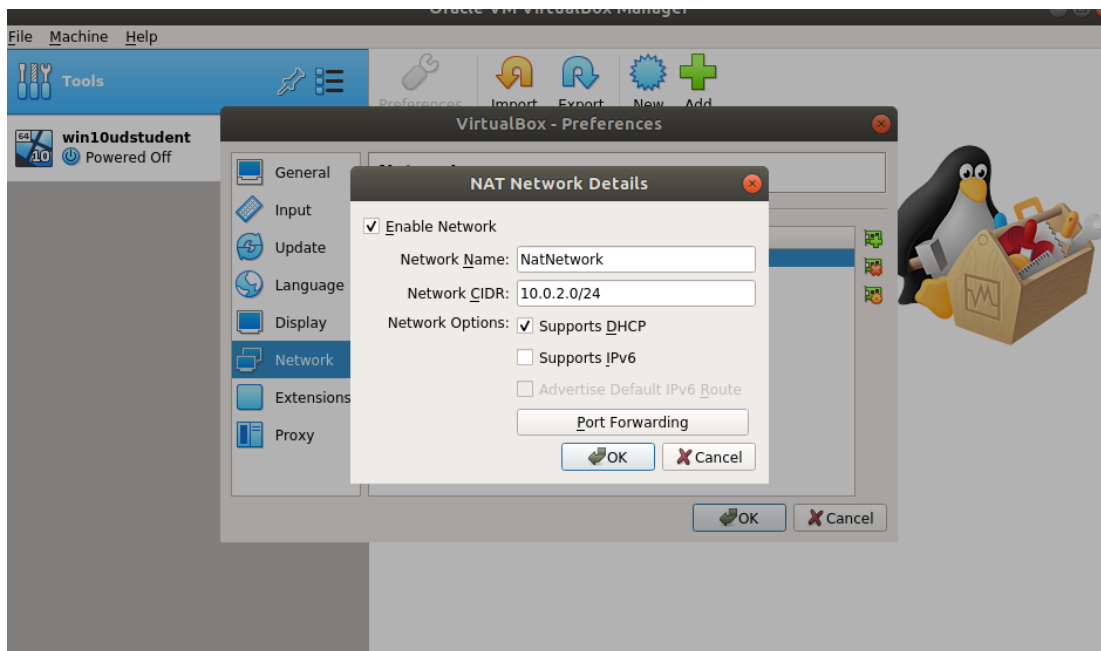


Click on tools, and then preferences in the upper left hand corner.



Then click on Network on the left side panel. Under Nat networks click on the + (plus) icon to the right of *Active Name*.

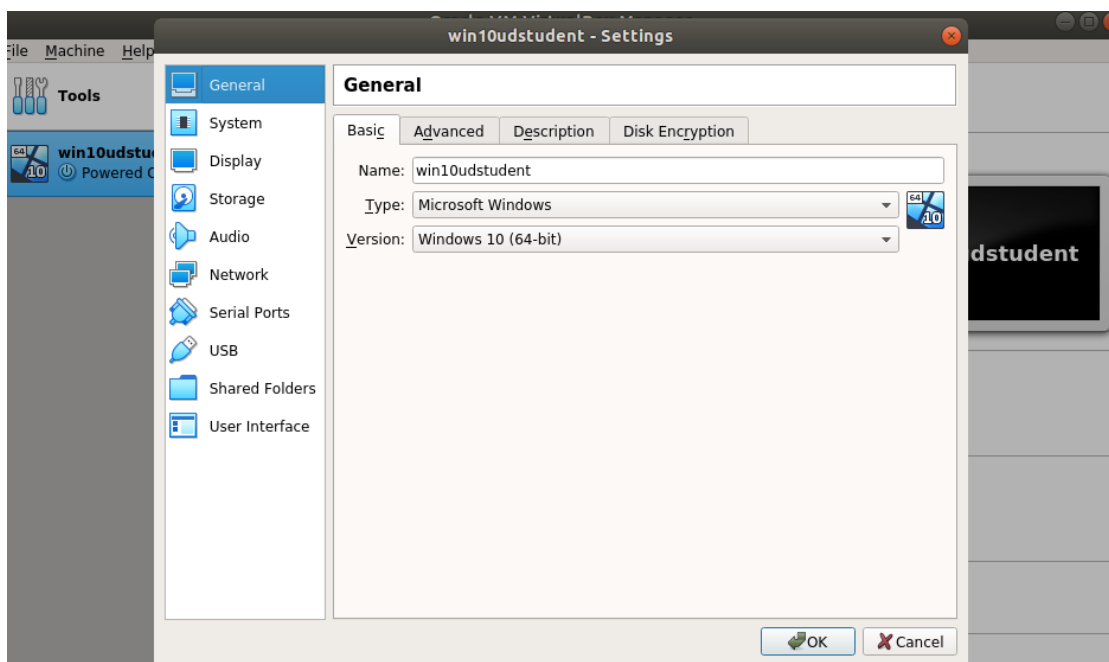
Next double click on the newly created network.



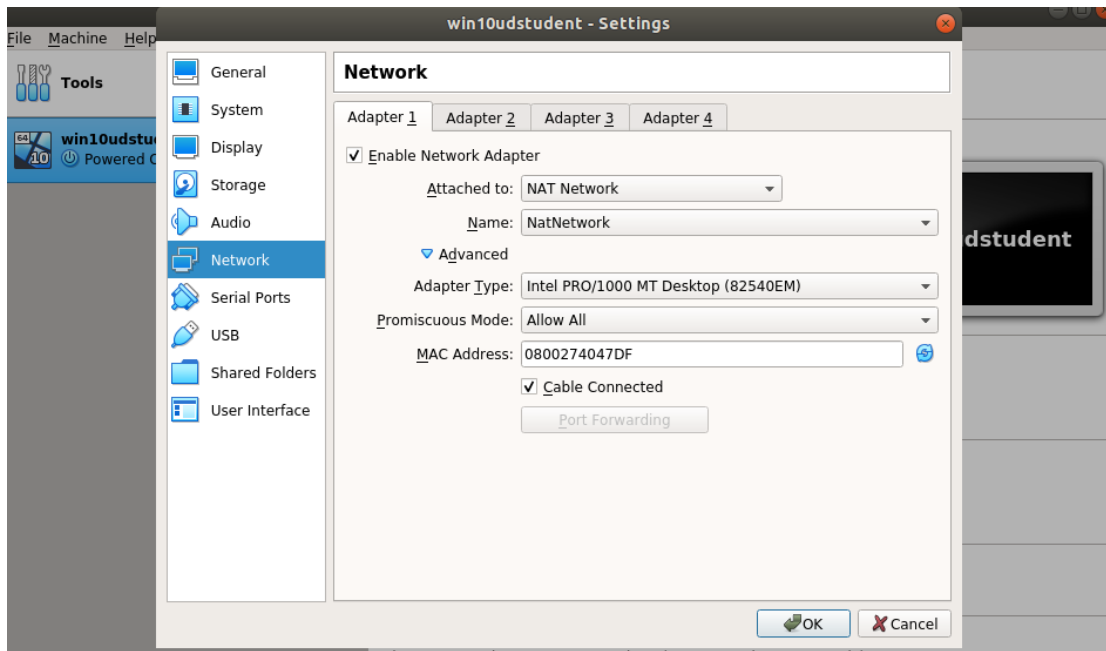
As seen above, this will be your Nat Network CIDR. This will be the network we will be using for our exercises and the final project.

Click *OK* when you are done. You might want to save these settings.

Next, configure the virtual machines to use this network. Click at the top of the name of your virtual machine and select settings.



Click on *Network* again to check the settings.



Settings for the VM to verify.

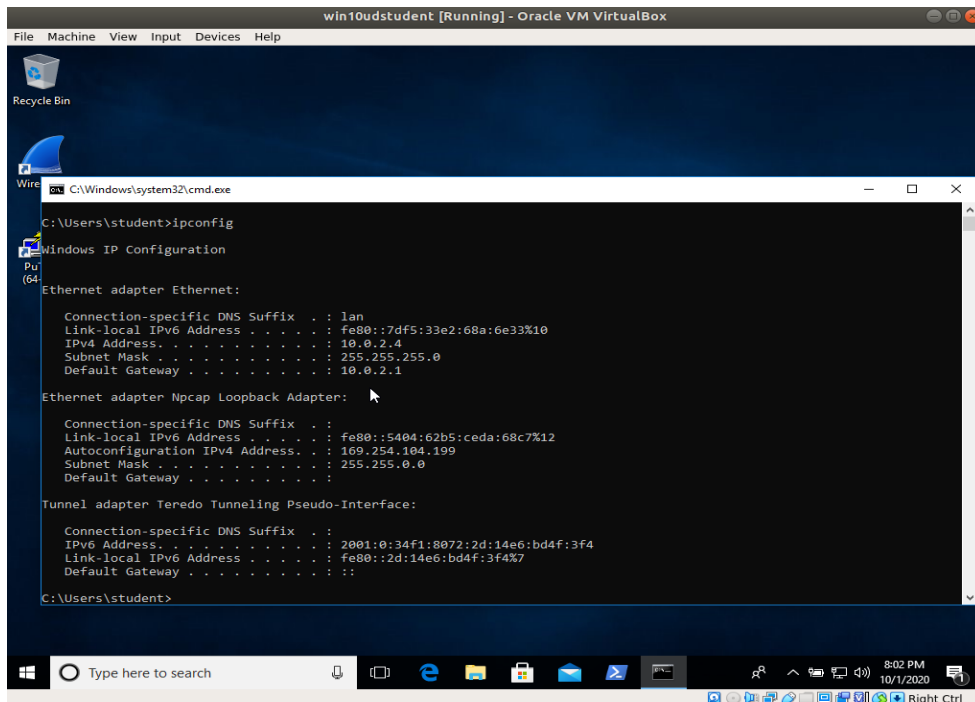
Be sure to check the following and ensure your settings match:

- Attached to: NatNetwork
- Name: NatNetwork
- Promiscuous Mode: Allow All

Then click *OK*.

Well done! Power on your virtual machine. It will automatically log in. Check its assigned IP by

- Right-clicking in the start menu
- Selecting run
- Typing cmd
- Then typing ipconfig.
- Finally, take note of the assigned IP

A screenshot of a Windows 10 virtual machine window titled "win10udstudent [Running] - Oracle VM VirtualBox". The desktop shows a Recycle Bin and a folder named "Wire". A command prompt window is open, showing the output of the "ipconfig" command. The output displays network configuration for three adapters: Ethernet, Npcap Loopback Adapter, and Teredo Tunneling Pseudo-Interface. The Ethernet adapter shows a link-local IPv6 address and an IPv4 address of 10.0.2.4. The Npcap Loopback Adapter shows an IPv4 address of 169.254.104.199. The Teredo Tunneling Pseudo-Interface shows an IPv6 address and a link-local IPv6 address. The taskbar at the bottom shows the search bar and several application icons. The system clock indicates 8:02 PM on 10/1/2020.

```
C:\Windows\system32\cmd.exe
C:\Users\student>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . : lan
    Link-local IPv6 Address . . . . . : fe80::7df5:33e2:68a:6e33%10
    IPv4 Address. . . . . : 10.0.2.4
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.0.2.1

Ethernet adapter Npcap Loopback Adapter:

    Connection-specific DNS Suffix  . :
    Link-local IPv6 Address . . . . . : fe80::5404:62b5:ceda:68c7%12
    Autoconfiguration IPv4 Address. . : 169.254.104.199
    Subnet Mask . . . . . : 255.255.0.0
    Default Gateway . . . . . :

Tunnel adapter Teredo Tunneling Pseudo-Interface:

    Connection-specific DNS Suffix  . :
    IPv6 Address. . . . . : 2001:0:34f1:8072:2d:14e6:bd4f:3f4
    Link-local IPv6 Address . . . . . : fe80::2d:14e6:bd4f:3f4%7
    Default Gateway . . . . . :

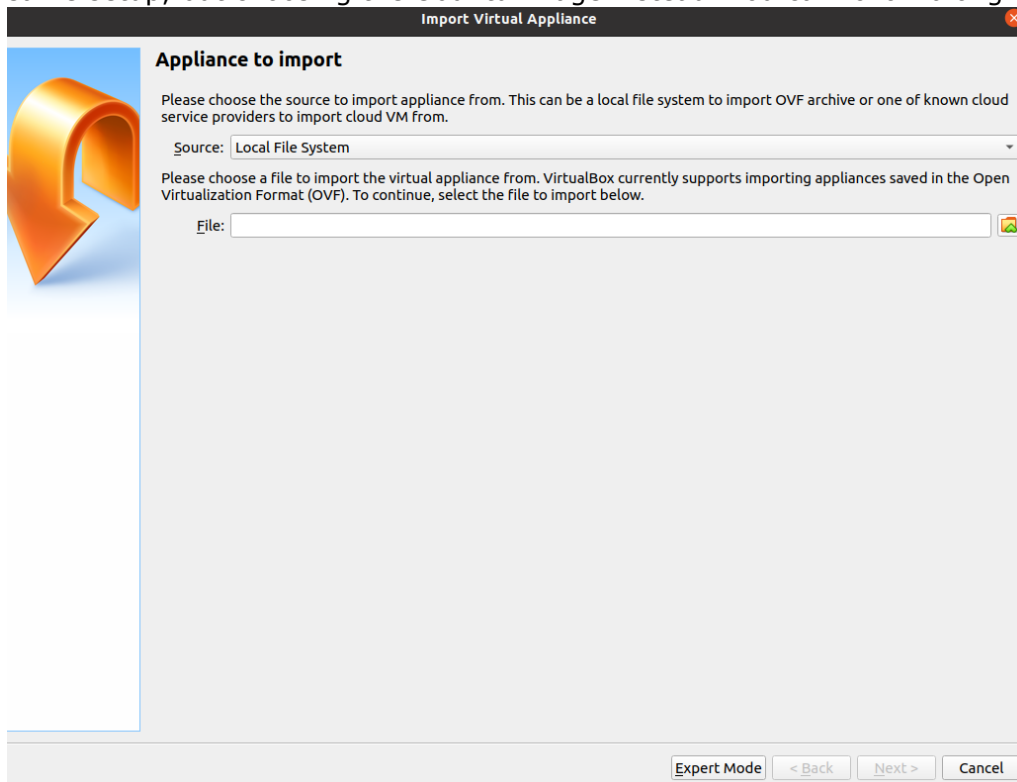
C:\Users\student>
```

Output from running ipconfig.

Great Job! Now let's move on to Ubuntu!

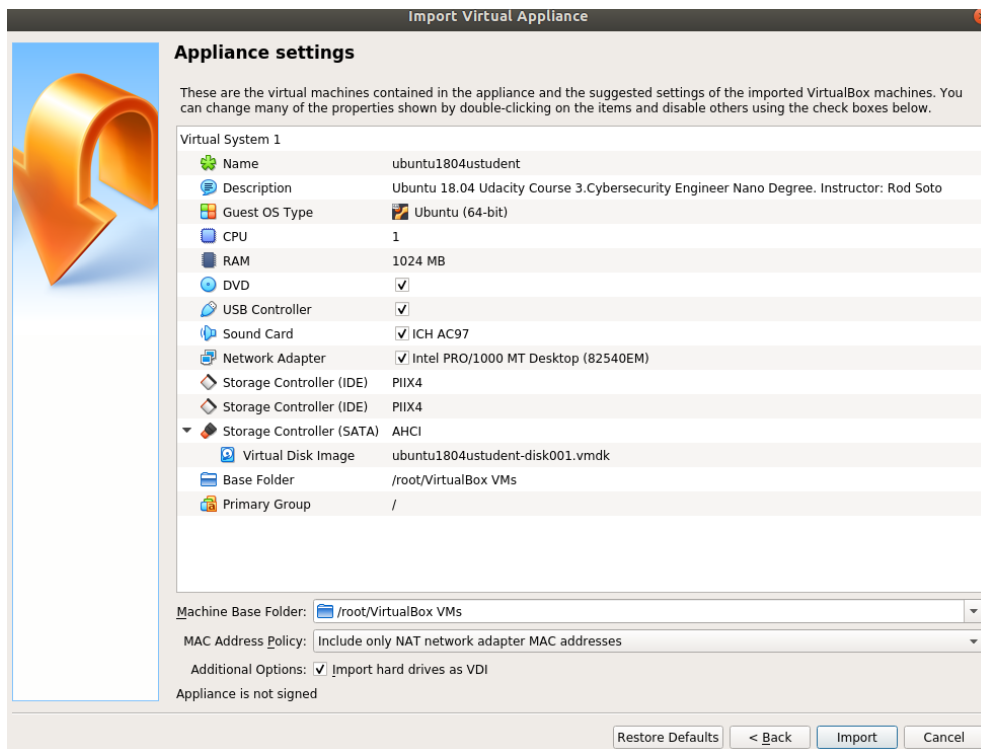
## Linux (Ubuntu) Project VM Setup

Next, you must replicate these settings on the Ubuntu virtual machine by *repeating* the same setup, but choosing the Ubuntu image instead. You can follow along below.



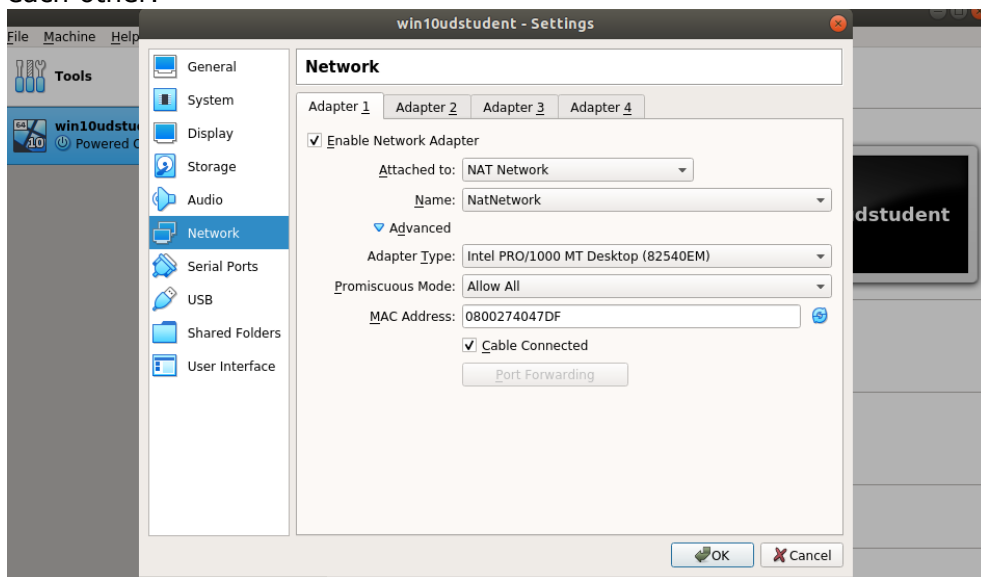
After clicking import, this time choose the Ubuntu image.





Use the default settings again and click import.

Next, login and apply the network settings so the two machines can communicate with each other.



Network Settings:

Your settings may differ slightly but should be similar to:

Network Settings for Adapter 1:

- Enable Network Adapter: Checked
- Attached to: NAT Network
- Name: NatNetwork

Under Advanced:

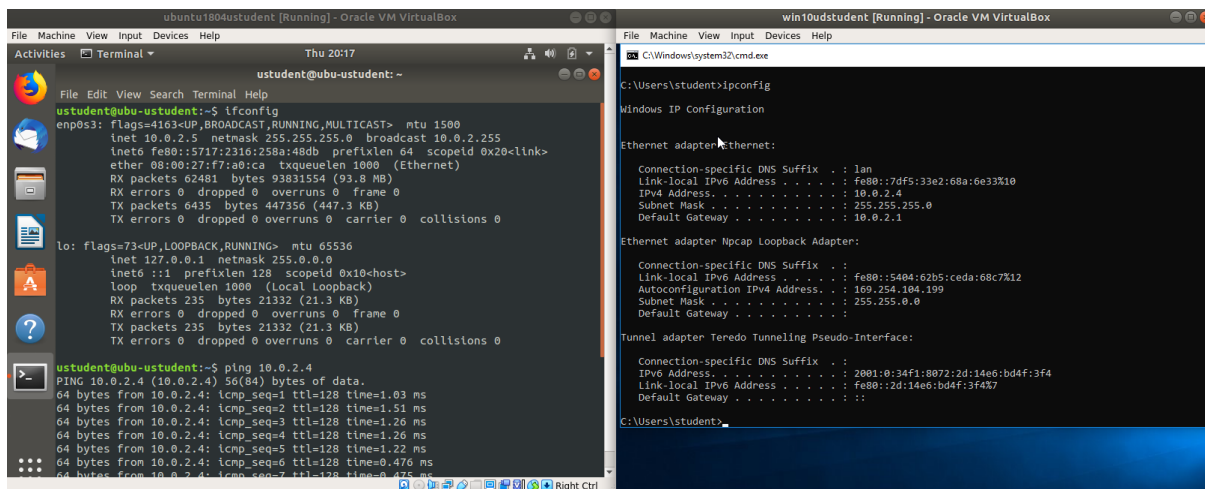
- Adaptor Type: Intel PRO/1000 MT Desktop
- Promiscuous Mode: Allow All
- MAC Address: 0800274947DF
- Cable Connected: Checked

Click *OK*.

And finally, after Ubuntu 18.04 auto logs in, bring up a terminal window.

Ping the Windows machine to see if we have connectivity.

See the screenshot below (Note: Your NAT network Ip addresses may differ in your machine).



```
ubuntu1804student [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal
Thu 20:17
ustudent@ubu-ustudent: ~
ustudent@ubu-ustudent:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
    inet 10.0.2.5  netmask 255.255.255.0  broadcast 10.0.2.255
    inet6 fe80::5717:2316:258a:48db  prefixlen 64  scopeid 0x20<link>
    ether 08:00:27:f7:a0:ca  txqueuelen 1000  (Ethernet)
    RX packets 62481  bytes 93831554 (93.8 MB)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 6435  bytes 447356 (447.3 KB)
    TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
    inet 127.0.0.1  netmask 255.0.0.0
    inet6 ::1  prefixlen 128  scopeid 0x10<host>
    loop txqueuelen 1000  (Local Loopback)
    RX packets 235  bytes 21332 (21.3 KB)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 235  bytes 21332 (21.3 KB)
    TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

ustudent@ubu-ustudent:~$ ping 10.0.2.4
PING 10.0.2.4 (10.0.2.4) 56(84) bytes of data:
64 bytes from 10.0.2.4: icmp_seq=1 ttl=128 time=1.03 ms
64 bytes from 10.0.2.4: icmp_seq=2 ttl=128 time=1.51 ms
64 bytes from 10.0.2.4: icmp_seq=3 ttl=128 time=1.26 ms
64 bytes from 10.0.2.4: icmp_seq=4 ttl=128 time=1.26 ms
64 bytes from 10.0.2.4: icmp_seq=5 ttl=128 time=1.22 ms
64 bytes from 10.0.2.4: icmp_seq=6 ttl=128 time=0.476 ms
64 bytes from 10.0.2.4: icmp_seq=7 ttl=128 time=0.455 ms
^C
ustudent@ubu-ustudent:~$

win10student [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
C:\Windows\system32\cmd.exe
C:\Users\student>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . : lan
    Link-local IPv6 Address . . . . . : fe80::7df5:33e2:68a:6e33%10
    IPv4 Address. . . . . : 10.0.2.4
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.0.2.1

Ethernet adapter Npcap Loopback Adapter:

    Connection-specific DNS Suffix  . :
    Link-local IPv6 Address . . . . . : fe80::5404:62b5:ceda:68c7%12
    Autoconfiguration IPv4 Address. . : 169.254.104.199
    Subnet Mask . . . . . : 255.255.0.0
    Default Gateway . . . . . :

Tunnel adapter Teredo Tunneling Pseudo-Interface:

    Connection-specific DNS Suffix  . :
    IPv6 Address. . . . . : 2001:0:34f1:8072:2d:14e6:bd4f:3f4
    Link-local IPv6 Address . . . . . : fe80::2d:14e6:bd4f:3f4%7
    Default Gateway . . . . . :

C:\Users\student>
```

## Windows Ping Results

We are now ready to go!

Step 4: Please take note of your machines credentials:

- Ubuntu18
  - User: ustudent
  - Password: 1234
- Windows 10
  - User: student
  - Password: 1234

## Project Steps

Use the staticspeed-vulnerability-report-template