For students using VirtualBox

> These instructions are for if you are using the VirtualBox envorinment. If you are using the EVE environment, you can mark this activity as completed and move on. If you are using VMWare Fusion, keep scrolling below this to the section titled "For students using VMware Fusion".

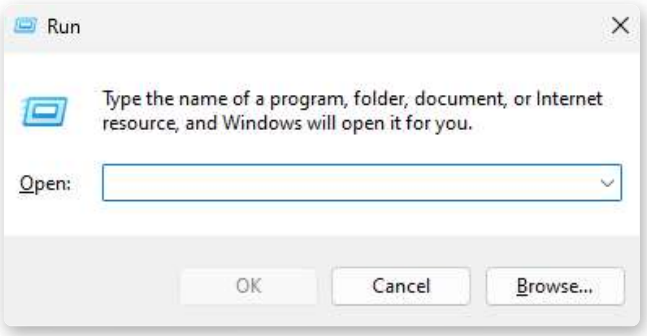
In this exercise, you will get comfortable changing network configuration and testing them within your virtual machines.

Part 1: Windows Network Settings

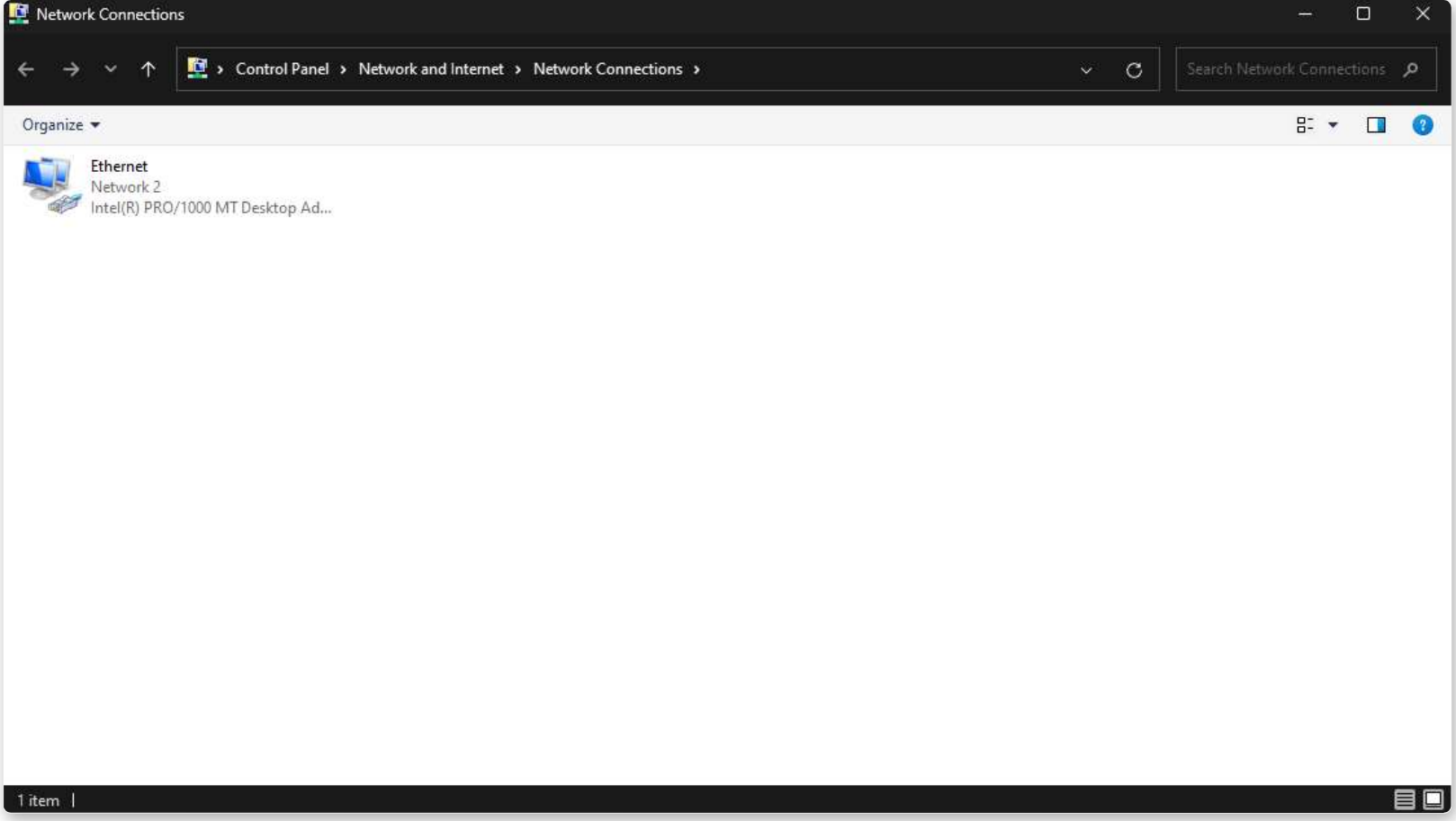
In cybersecurity, it is important to understand how IP addresses are assigned to devices and how to check what those IP addresses are. In this part, you will change the IP address of your Windows 11 virtual machine and check to ensure that they get updated properly.

Step 1: Open VirtualBox and turn your Windows11 virtual machine on.

Step 2: In the search bar at the bottom, search for 'run' and open the application. It should open a box like this.



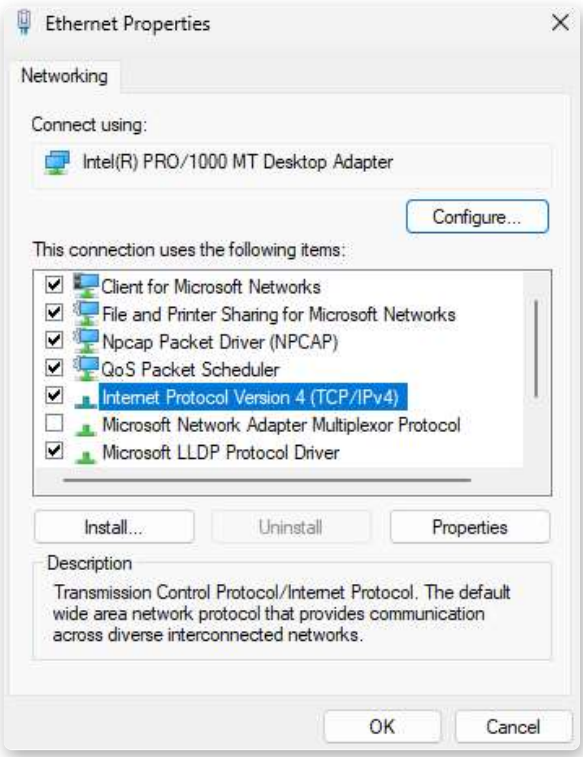
Step 3: In this run box, type in `ncpa.cpl` and hit enter. You should be taken to a screen like this.



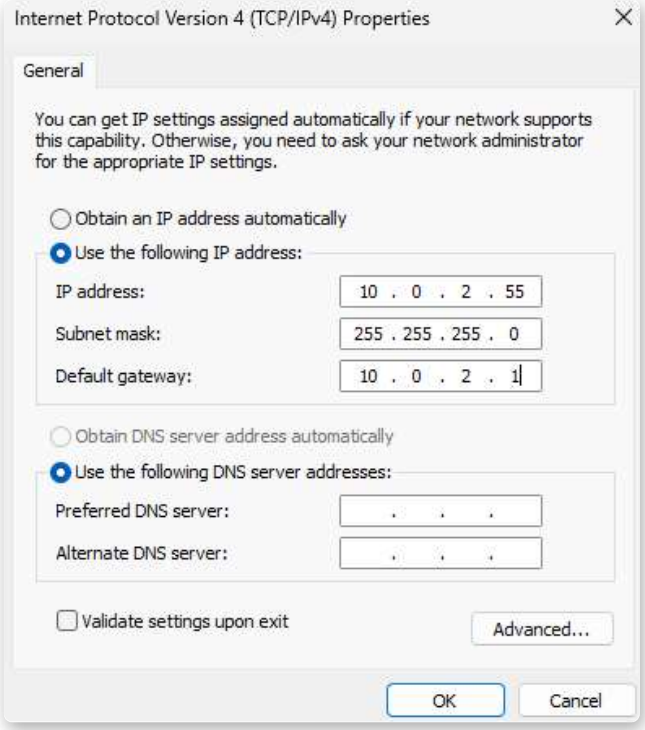
This new window is where we can change any networking settings on the device, such as IP address, subnet mask & default gateway.

Step 4: Double-click on the "Ethernet" option. Then in the new window that opened, click "Properties".

Step 5: There should have been another new window that opened, in it there should be a list of items with checkboxes next to them. Scroll through it until you find "Internet Protocol Version 4 (TCP/IPv4)" and double-click on it.



Step 6: Click on "Use the following IP address:" and then enter the information as shown below.



Step 7: Click 'OK' and close all the windows that are open.

Step 8: Now open a Command Prompt at the bottom and type the command `ipconfig`.

You'll notice that the IPv4 address has now changed to the one you set it to. This is how you change the IP address of a Windows based device. If you wish to change it back to the default one, you can follow steps 1-5, then select the option for 'Obtain an IP address automatically".

Part 2: VirtualBox Network Configuration

VirtualBox provides us with a few different types of network adapters. These adapters allow us to manipulate how the networks act and function within our virtual machines. In this task, you will go through a few of them and get an understanding about how they work, and why you would choose one adapter over the other.

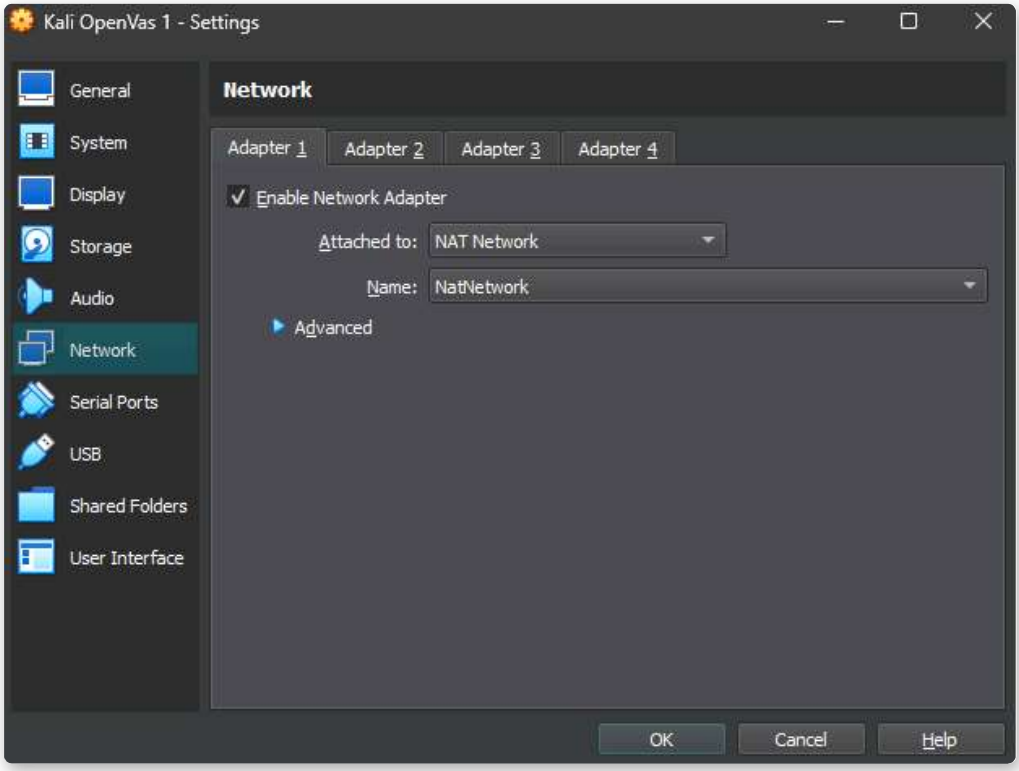
> Follow the steps below to set up your virtual network.

Step 1: Open VirtualBox and click on "Tools" at the top. In the "Tools" section, you will see three lines, click that icon and select "Network" like in the screenshot below.

Step 2: Click on the "Nat Networks" tab toward the top of this screen and then click "Create". It should automatically create a new network called "NatNetwork" but you can name it whatever you'd like at the bottom of the screen. Ensure you also have selected "Enable DHCP" at the bottom to be turned on.

Adding the NatNetwork to our VMs

Step 1: In VirtualBox, right-click on your Kali OpenVas machine and click on "settings". Then, go to the 'Network' tab on the left and make sure you are in the 'Adapter 1' section. It should be enabled and attached to "NAT Network". If it is not, select "Nat Network" in the "Attached to:" dropdown and make sure the "Name" is the newly created network you made.



NAT stands for Network Address Translation. VirtualBox has it's own way of applying NAT to apply IP addresses to the virtual machines. When you have the NAT Network selected, your virtual machine will have internet access, and it will be able to communicate with your other virtual machines, but it will not be able to communicate with your host device or any other devices on your network outside of VirtualBox such as smart phones and TVs.

Step 2: You can close the network settings menu now. Turn on your Kali OpenVas machine and your Windows 11 machine.

Step 3: Open a Terminal in your Kali OpenVas machine by clicking on the black box icon in the top left.

Step 4: In the terminal, type in the command `ip a`. It should give some results that look similar to this, but they may look slightly different.

This command gives up the IP Address information about our Kali machine. The important section for now is the `eth0` section as this is the network adapter that's currently giving us internet access. In the screenshot below you can see the IP address currently is `10.0.2.15` and highlighted in purple. Take note of this IP address as we will need it later.

```
┌──(student㉿kali)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group de
fault qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP
group default qlen 1000
    link/ether 08:00:27:1b:76:b0 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute eth0
       valid_lft 480sec preferred_lft 480sec
    inet6 fe80::a00:27ff:fe1b:76b0/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

Step 5: Naviagte to your Windows 11 machine and open a Command Prompt by clicking on the black box icon in the bottom task bar.

Step 6: Type in the command `ipconfig`. This is giving us the same information as when we ran the `ip a` command in Kali, but since this is a Windows device, the command looks a bit different.

You'll notice in the screenshot below that the IP address is `10.0.2.6`. Since this IP address starts with `10.0.2` and the Kali machine also starts with `10.0.2`, this tells us that these two devices are on the same network and they should be able to communicate with each other.

Step 7: In your Windows Command Prompt, type in the command `ping 10.0.2.15`.

You should see some feedback, which we call 'output' that shows replies from `10.0.2.15`. This is the responses from the Kali machine. If the pings were successful and you received these replies, that means these two devices are in fact on the same network and can communicate with each other. Let's now take a look at if we change this to a different network adapter and see what happens.

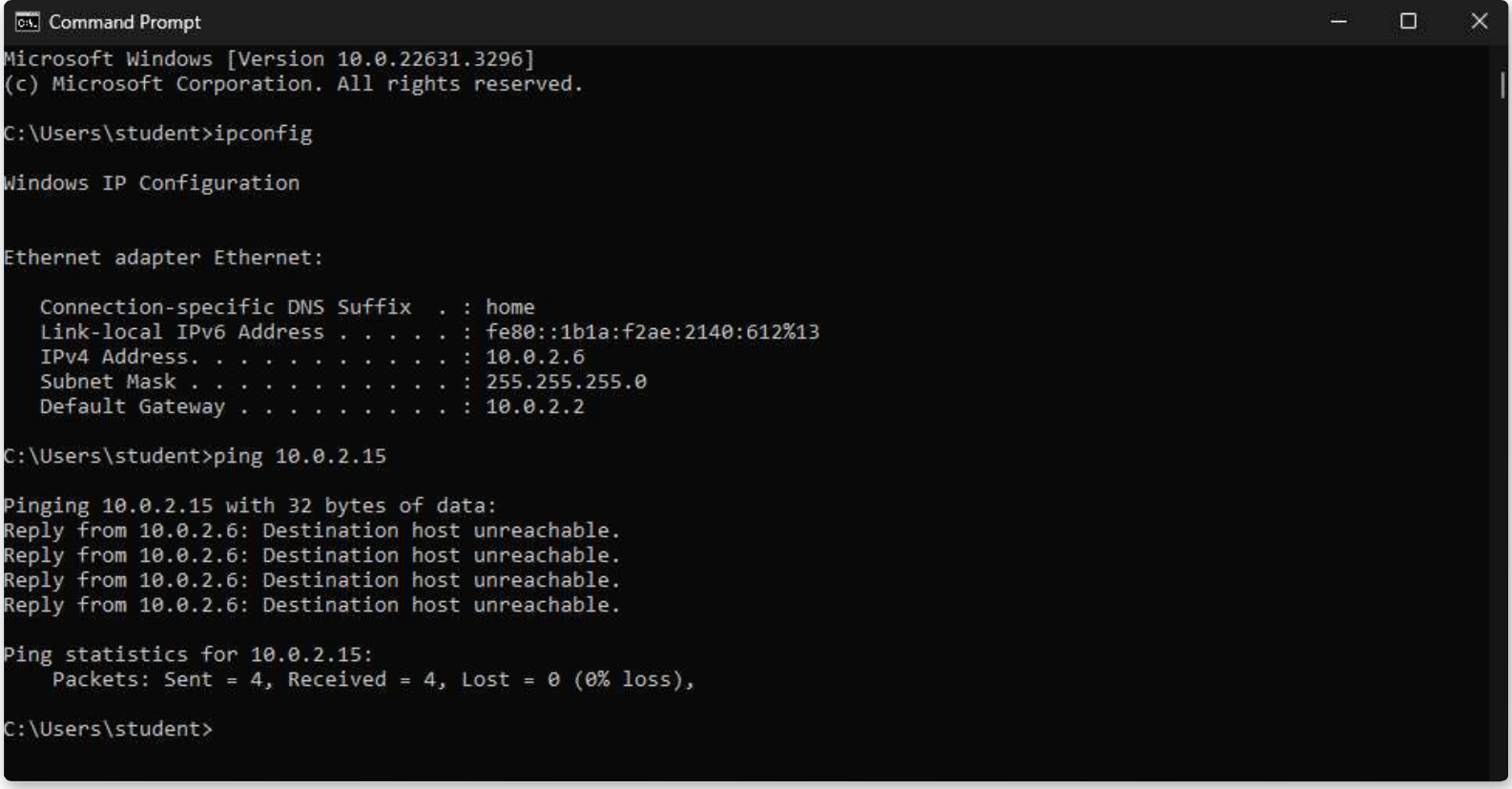
Step 8: With your virtual machines still on, go to the settings in either of them and change the network adapter to `NAT` instead of `NAT Network`.

Step 9: Wait about 15-30 seconds for the network settings to update, then run the command `ipconfig` again on your Windows Command Prompt.

> There's a chance that the IP address has changed, but it may also have stayed the same. Either way that is normal.

Step 10: Try to ping the Kali machine again using the `ping 10.0.2.15` command.

You may see that the replies now say "Destination host unreachable". That's because VirtualBox has now separated our Windows 11 network to be separate from the rest of the machines. The Windows 11 machine still has network connectivity, but you'll notice it can't ping any other device on your network.



There are other adapter types you can use as well, such as `Bridged` which would attach your virtual machine to your host network, meaning your virtual machine would be able to connect with any device that's connected to your host network, including smart phones and TVs.

Final Step: Don't forget to change your network adapter settings back to 'NAT Network' for now, so you don't get any issues in the following sections.

> Why would we want to manually assign an IP address to a specific machine? ????static-ip-addresses Sometimes we need to test a machine using tools over our network. Manually assigning an IP address to this machine ensures that we know we are sending the data to the proper machine. If you have the settings set to automatically assign an IP address, sometimes that IP address can change, which in a scenario like this would cause us issues. ????