Simple Network Management and Traffic Capturing

**Purpose:**

In this lab, you will gain hands-on experience in configuring networks, capturing traffic, and analysing packets. Working with both Linux and Windows environments, you will set up network configurations, use tcpdump to capture traffic and analyse packets with Wireshark.

Completing this lab will provide you with practical experience in network configuration, traffic capture, and packet analysis. These skills are crucial for understanding network behaviour and identifying potential security issues.

**Lab Sections:**

1. **Network Configuration in Linux**  
   Explore essential commands and techniques to configure network settings in Linux environments.
2. **Network Configuration in Windows**Learn the necessary commands and techniques to configure network settings in Windows environments.
3. **Capturing Traffic with tcpdump**Master the installation, configuration, and deployment of tcpdump to effectively capture and analyse network traffic.
4. **Capturing Traffic with Wireshark**

Gain expertise in installing, configuring, and deploying Wireshark to capture and analyse network traffic accurately.

**Resources – Explore these before continuing with the lab:**

* **Configuring Linux Network Interface File:** <https://www.devtutorial.io/how-to-manage-network-interfaces-on-ubuntu-server-22-04-ubuntu-server-22-04-p3097.html>
* **What is the /etc/hosts file:** <https://linuxhandbook.com/etc-hosts-file/>
* **Windows PowerShell netsh Command Explained:** <https://adamtheautomator.com/netsh/>
* **Basic Understanding of tcpdump:** <https://www.hugeserver.com/kb/install-use-tcpdump-capture-packets/>
* **Advanced tcpdump and Output Explained:** <https://opensource.com/article/18/10/introduction-tcpdump>
* **Tcpdump cheat sheet:** <https://www.comparitech.com/net-admin/tcpdump-cheat-sheet/>
* **Wireshark Installation on Linux:** <https://linuxtechlab.com/install-wireshark-linux-centosubuntu/>

**Materials:**

Before beginning the lab, please ensure that you have the following set up:

* A **Kali Linux** virtual machine.
* A separate **Windows 10** virtual machine.
* Ensure that both virtual machines are **properly configured and operational**.
* **Verify** that **network connectivity is established** between the two virtual machines, allowing for communication.
* **Record the IP addresses** of the **Windows** and **Linux** machines respectively, as **you will need them** for configuration and testing purposes.

Windows IP address: 10.0.2.5

Kali IP address: 10.0.2.15

Completing these prerequisites will ensure a smooth experience while completing the lab exercises.

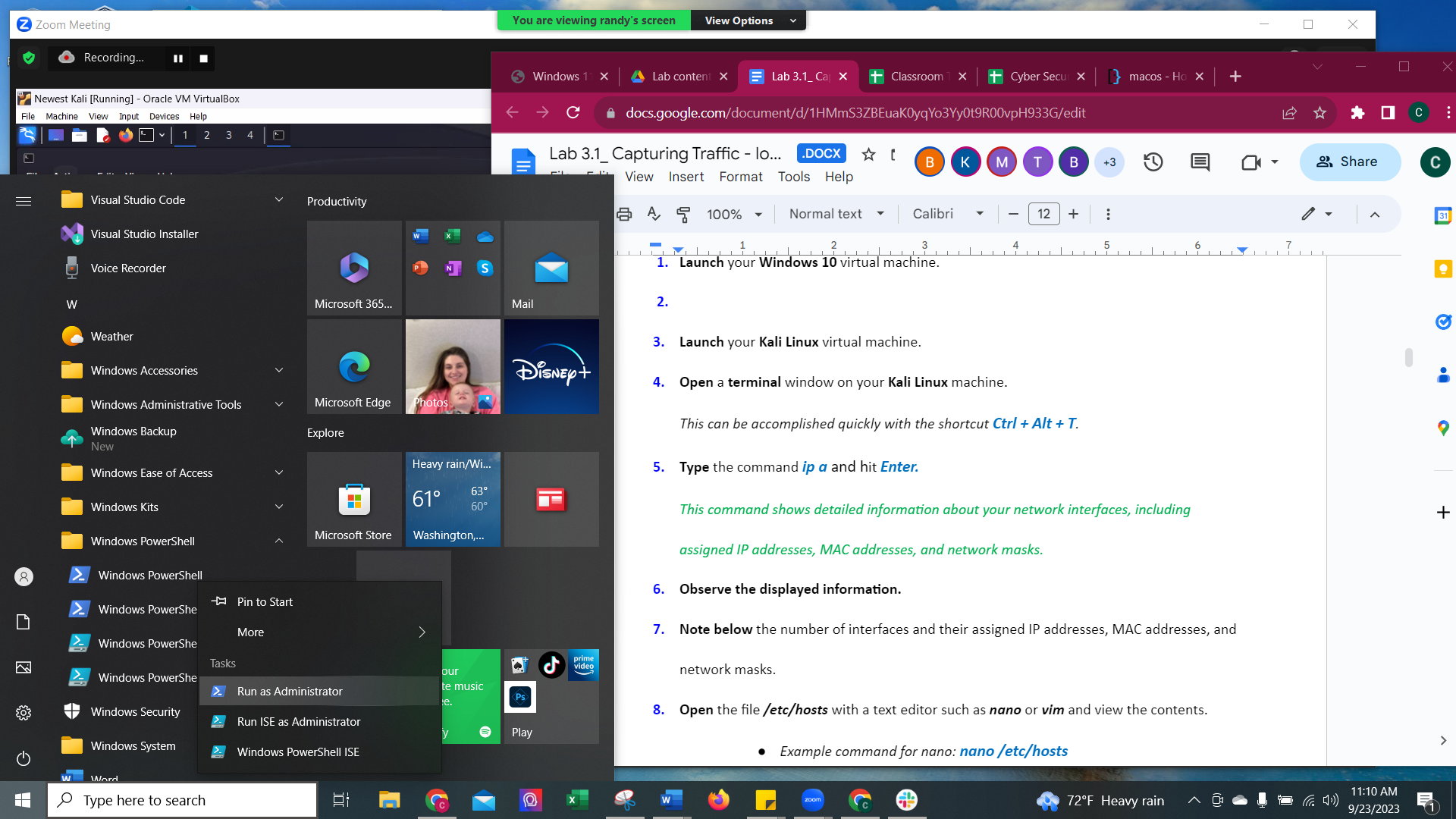
**Part 1 - Network Configuration in Linux**

This exercise aims to showcase the Linux command line terminal's practical application and associated tools, including text editors like Nano or Vim. Through this exercise, you will gain hands-on experience in exploring your machine's network configuration, efficiently viewing and editing configuration files, and mastering the technique of mapping an IP address in the /etc/hosts file.

**Instructions:**

**Retrieve your Windows VM IP Address**

1. **Launch** your **Windows 10** virtual machine.
2. Run Powershell as administrator. This can be accomplished by:
   * Open your Windows Start Menu
   * Find Powershell in Applications
   * Right click on Powershell
   * Select run as administrator



1. In powershell, type command *IPConfig*
2. Write down the IPv4 address it shows. It should be something like “10.0.2.15”

IPv4 Address: 10.0.2.5

1. **Launch** your **Kali Linux** virtual machine.
2. **Open** a **terminal** window on your **Kali Linux** machine.

*This can be accomplished quickly with the shortcut* ***Ctrl + Alt + T****.*

1. **Type** the command ***ip a*** and hit ***Enter.****This command shows detailed information about your network interfaces, including assigned IP addresses, MAC addresses, and network masks.*

****

1. **Observe the displayed information.**
2. **Note below** the number of interfaces and their assigned IP addresses, MAC addresses, and network masks.

**IP address: 10.0.2.15**

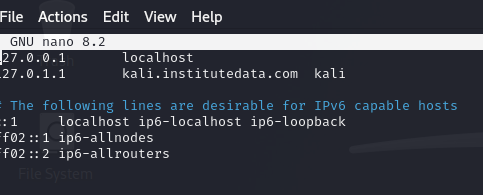
**MAC address: 08:00:27:6b:4a:62**

**Network masks: 10.0.2.255**

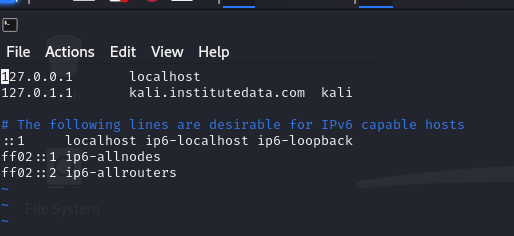
1. **Open** the file ***/etc/hosts*** in the terminal with a text editor such as ***nano*** or ***vim*** and view the contents.
   * *Example command for nano:* ***sudo*** ***nano /etc/hosts***
   * *Example command for vim:* ***sudo*** ***vim /etc/hosts***

*This file works as your local Domain Name System (DNS) by mapping IP addresses to names.*

***sudo*** ***nano /etc/hosts***

**

***sudo*** ***vim /etc/hosts***

**

1. **Exit** the text file **without making any changes**.
   * *To exit out of nano:* ***Ctrl +X****, then* ***Y*** *for yes to save changes, and hit* ***Enter*** *to quit.*
   * *To exit out of Vim: Press the* ***Esc*** *key, type* ***:wq*** *and hit* ***Enter*** *to save changes and quit.*
2. **Edit** the file ***/etc/hosts*** and enter the following line:

***<IP\_Address> winmachine***   
*(<IP\_Address> should be replaced by your Windows virtual machine’s IP address).   
Example: 192.168.56.1 winmachine*

*Remember that editing a system file requires root/admin privileges. Preface your command with* ***sudo*** *to run as root/admin.*

*Example: sudo nano /etc/hosts*

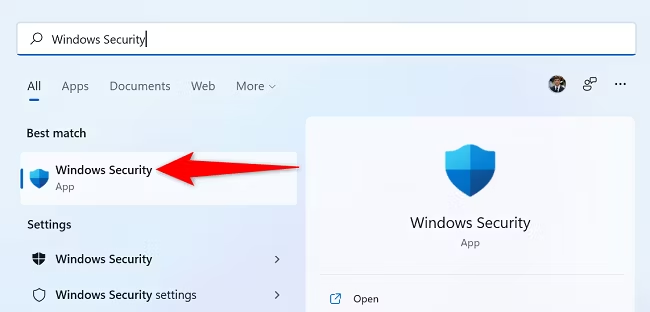
1. **Save** the changes made to the file ***/etc/hosts***.  
   *This configuration will allow you to use the name winmachine instead of the IP address to access your Windows virtual machine.*
2. **Launch** your **Windows** virtual machine to test your configuration.
3. **Test** the configuration by typing ***ping winmachine*** in the **Kali Linux** terminal.

Hit ***Enter***.

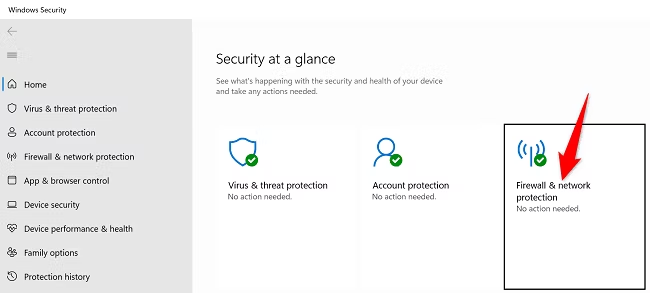
*You should see a response from the Windows virtual machine in the same way you would if you had pinged the full IP address. This verifies that the configuration you put in place is successful. To make the ping command stop type ctrl C.*

Note: if your Ping is not going through to your Windows machine, check to make sure that the firewalls are turned off on your Windows machine by going to the following:

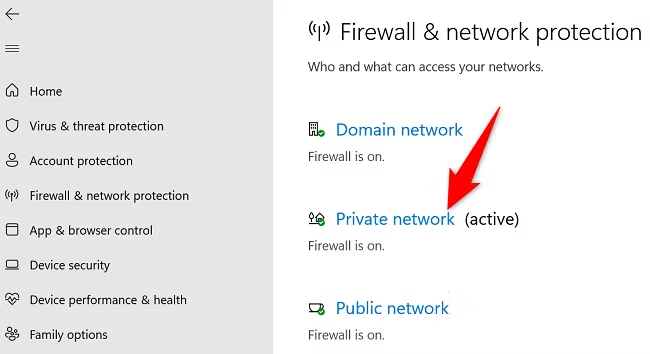
Type in Windows Security by the magnifying glass



Go to Firewall & Network Protection



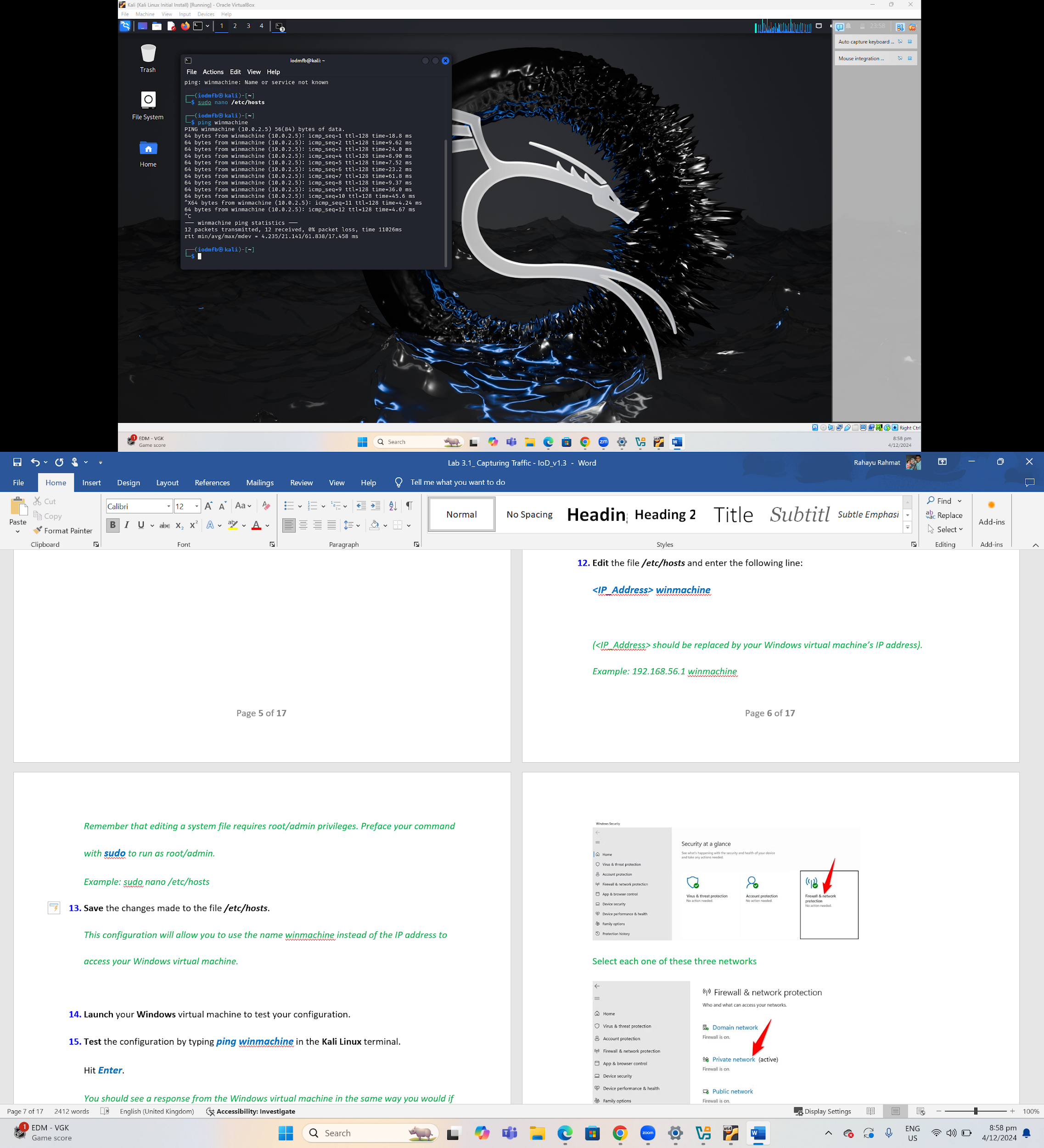
Select each one of these three networks



And switch the toggle button from on to off



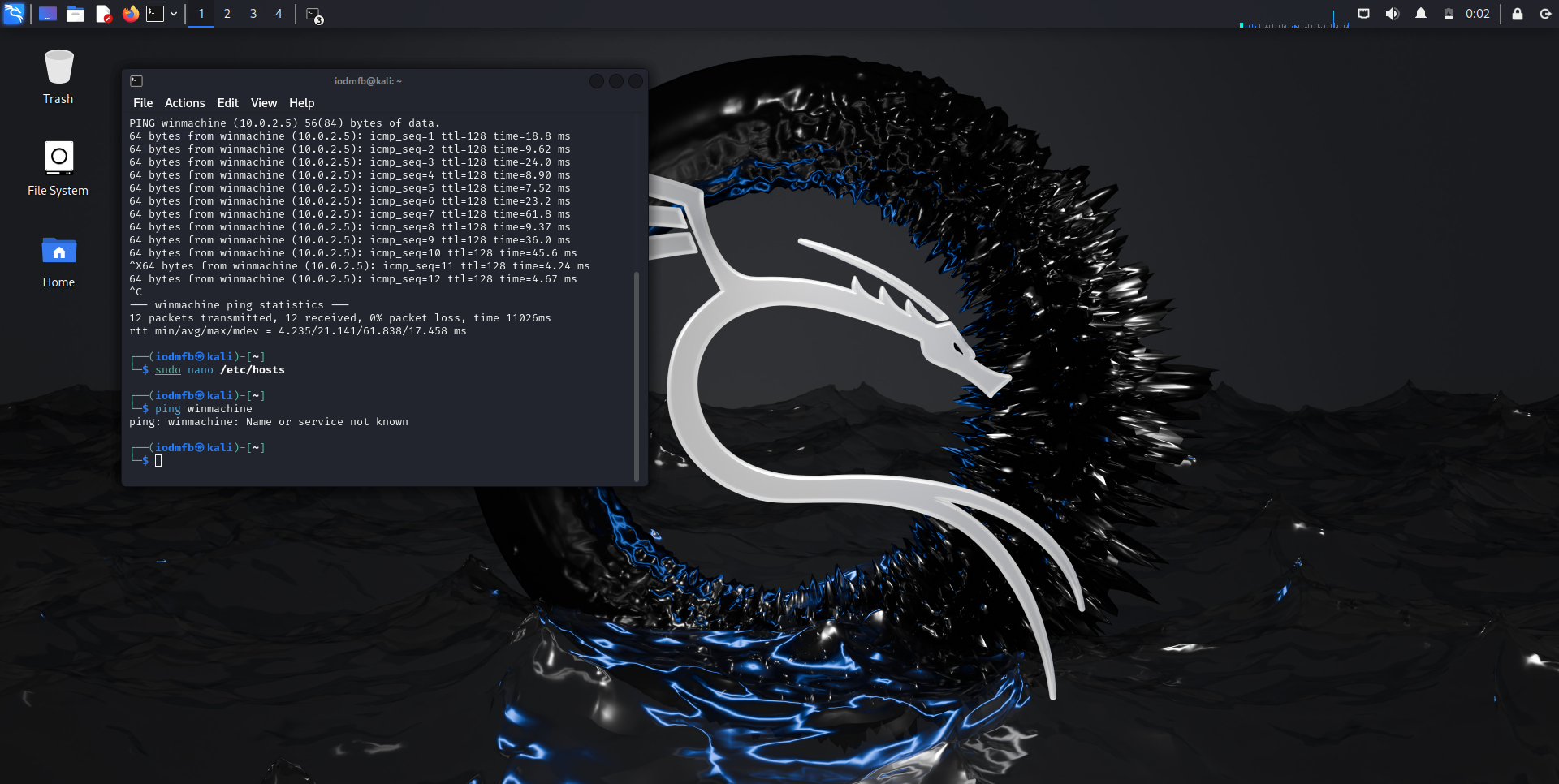
***ping winmachine***



1. **Edit** the **/etc/hosts** file again and **add a *#* to the beginning of the line** you put in place in **Step 12**.

Note: **Disable** any configuration by placing a ***#*** symbol at the beginning of the respective line.

1. **Save** the file.
2. **Test** the effect of your change by running ***ping winmachine*** again.



**Part 2 - Network Configuration on Windows**

This exercise aims to showcase the practical application of Windows PowerShell and its associated tools, including ncpa.cpl and netsh. Through this exercise, you will gain hands-on experience in exploring your machine's network configuration and master the art of DNS server configuration.

**Instructions:**

1. **Switch** **over** **to** your **Windows** virtual machine.
2. **Access Windows PowerShell** as an administrator by pressing the ***Windows key + X*** simultaneously.  
   *This keyboard shortcut will open a menu from the start menu.*
3. **Select** the option titled ***Windows PowerShell (Admin)***.

*This will cause a PowerShell window to pop up on the screen.*

1. **Type** the command ***ncpa.cpl*** and hit ***Enter***.

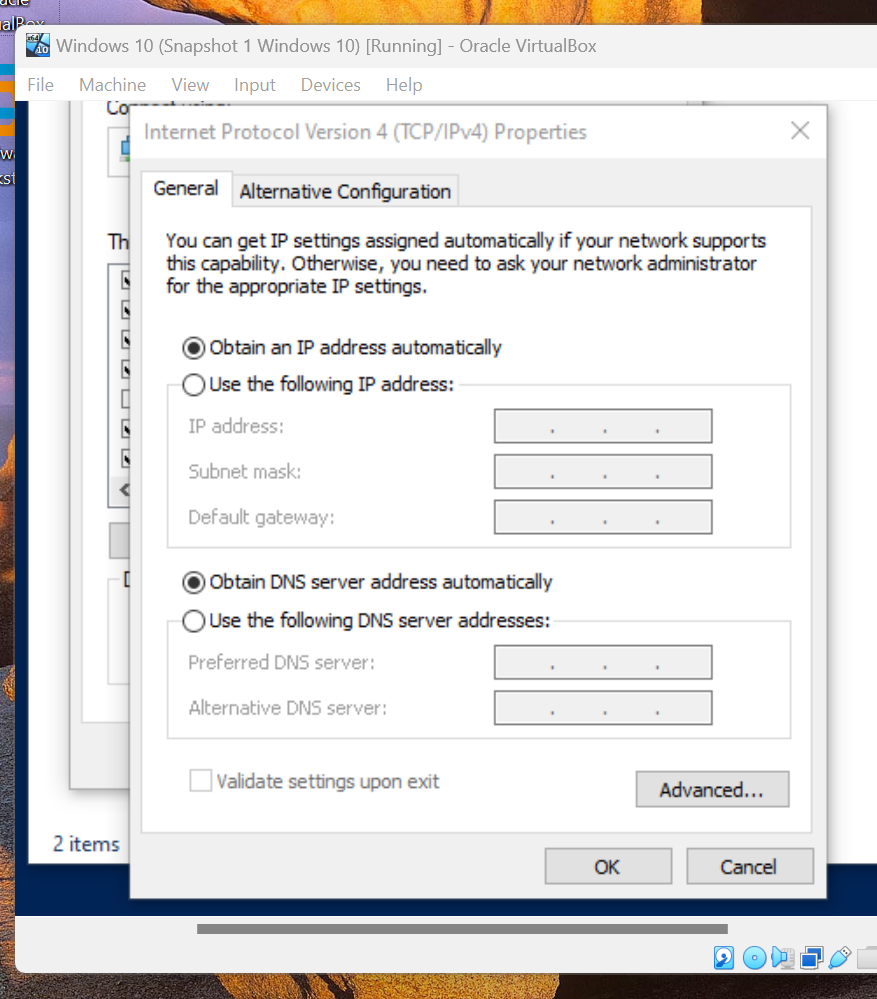
*This will open a new window for the network configuration manager.*

1. **Right-click** the network adapter and select ***Properties***.

*This will open a new window for the settings of the selected network adapter.*

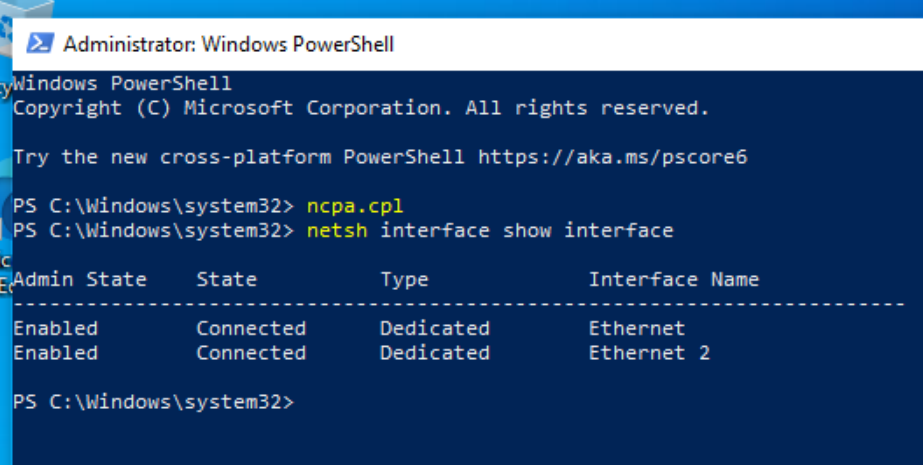
1. **Double-click** the option titled ***Internet Protocol Version 4 (TCP/IPv4)*** to view the IPv4 network settings of the adapter.
2. **Note the current settings** for the selected adapter.

*You will review these settings later in the exercise to view changes made in PowerShell.*

**

1. **Close** all the windows.
2. **Return to PowerShell (Admin)** and execute the command ***netsh interface show interface***

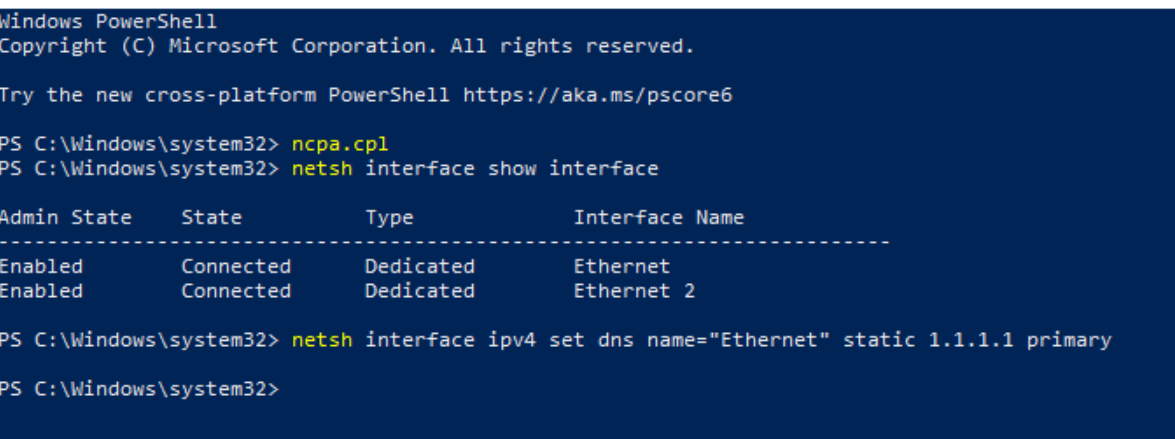
*This will display details of all network adapters on the machine.*

*i*

1. **Note** the ***Interface Name*** of your network adapter.
2. **Execute** the command ***netsh interface ipv4 set dns name=”<Interface\_Name>” static 1.1.1.1 primary***

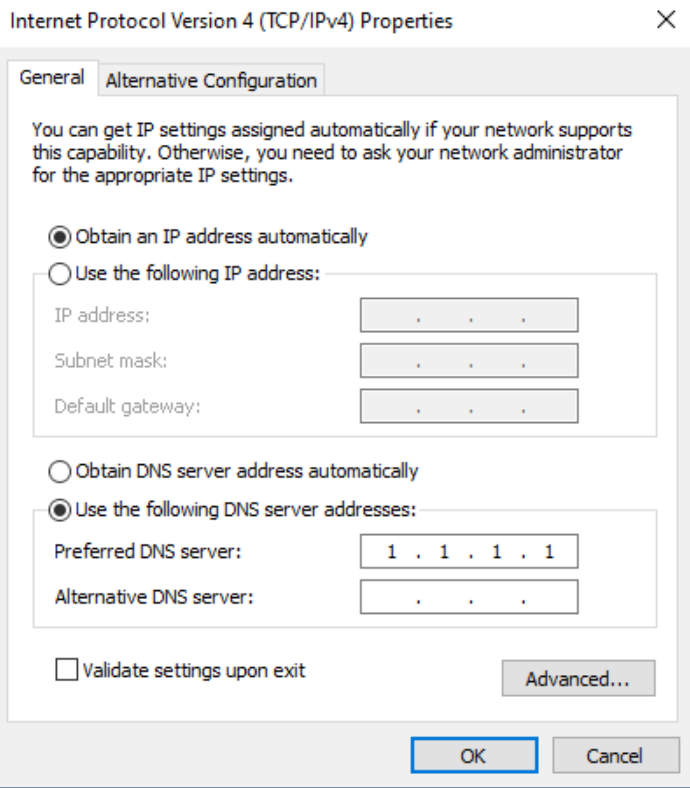
*(<Interface\_Name> should be replaced with the name you noted in Step 10. Make sure to include the “ ” around your interface name.)*

*Example:* ***netsh interface ipv4 set dns name=”Ethernet” static 1.1.1.1 primary***

**

1. **Return** to the network configuration manager and **repeat steps 4 to 6**.

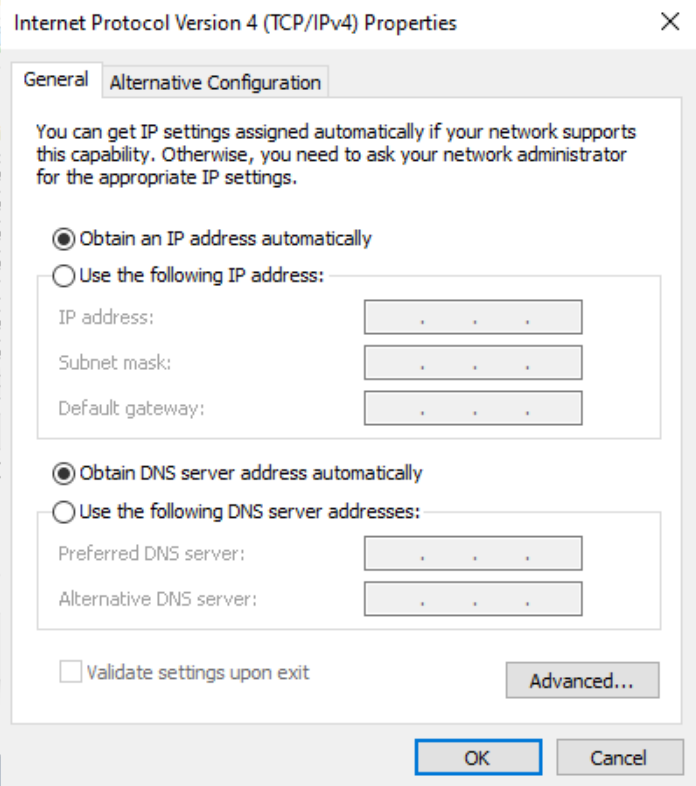
**Can you see the change that has occurred?**

****

1. **Detail** any further findings from your exploration of ***netsh*** and ***ncpa.cpl*** below.
2. **Execute** the command ***netsh interface ipv4 set dns name=”<Interface\_Name>” dhcp.*** This returns it back to the original configuration.

*(<Interface\_Name> should be replaced with the name you noted in Step 10. Make sure to include the “ ” around your interface name.)*

*Example:* ***netsh interface ipv4 set dns name=”Ethernet” dhcp***



**Part 3 - Capturing Traffic with tcpdump**

Tcpdump is a Linux command line utility that enables you to capture and analyse network traffic travelling through your system. It is often used for network troubleshooting and analysis.  
  
This exercise aims to showcase the practical application of the Linux command line terminal and the tool tcpdump. This exercise will give you hands-on experience in capturing network traffic and generating output files for further analysis.

**Instructions:**

1. **Switch** **over** to your **Linux** machine.
2. **Open** a terminal window.
3. **Before installing** the tcpdump service, you will **need to update** the repository/package list **and upgrade** to the latest package versions for your Linux machine.

i. **Type** the command ***sudo apt-get update*** and hit ***Enter***.

*This command requests an update of all repositories, dependencies and packages installed in Linux.*

ii. **Type** the command ***sudo apt-get upgrade*** and hit ***Enter***.

*This command begins the upgrade process of all repositories, dependencies and packages installed in Linux.*

*Remember that sudo at the beginning of the command is necessary if you are not running the command as the root user.*

1. **If installed**, you will see output such as ***/usr/sbin/tpdump***.

*Skip to Step 8*

1. **If not installed**, you will see **no response or output**.
2. **Type** the command ***sudo apt install tcpdump*** and hit ***Enter*** to **install**.
3. **Type** the command ***tcpdump -D*** and hit ***Enter***.

*This command runs tcpdump and the -D switch applies the option to list all available network interfaces.*

1. **How many do you have?**

****

1. **Type** the command ***sudo*** ***tcpdump -i <Adapter\_Name>*** and hit ***Enter***

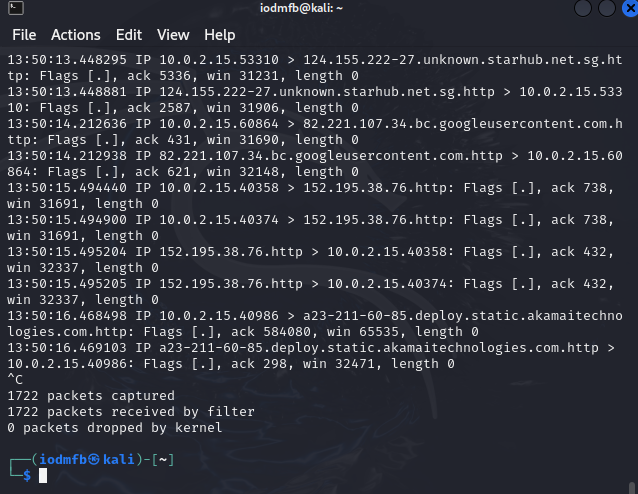
*(Where <Adapter\_Name> is the name provided in the result of Step 8.*

*Example:* ***sudo******tcpdump -i eth0***

*The -i switch applies the condition to capture traffic only on one specific network interface.*

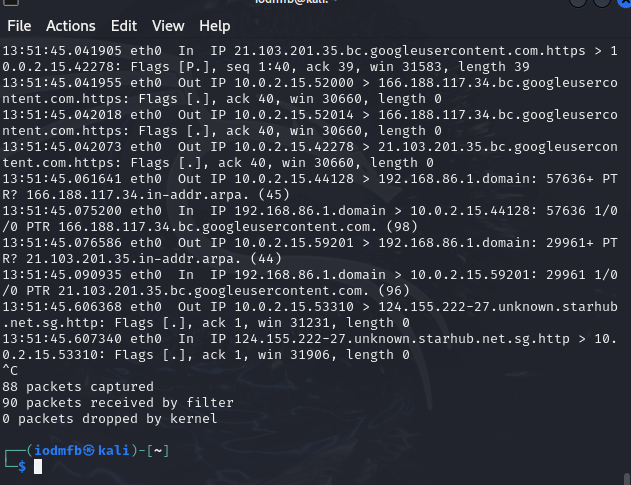
**

1. **Open** your firefox web browser, then minimise the web browser window and return to the terminal to see results. *To stop the flow of packets you can simply use the combination* ***Ctrl+C***.

****

1. **Type** the command **sudo** ***tcpdump -i any*** and hit ***Enter***. Repeat Step 11 to see results.  
   *This command will capture packets from all available interfaces simultaneously.*

*To stop the flow of packets you can simply use the combination* ***Ctrl+C***.



1. **Type** the command **sudo** ***tcpdump -i any -c5*** and hit ***Enter***. Repeat Step 11 to see results.

*The addition of the switch -c followed by the desired number of packets, in this case, 5, tells tcpdump to limit the capture to 5 packets.*

**

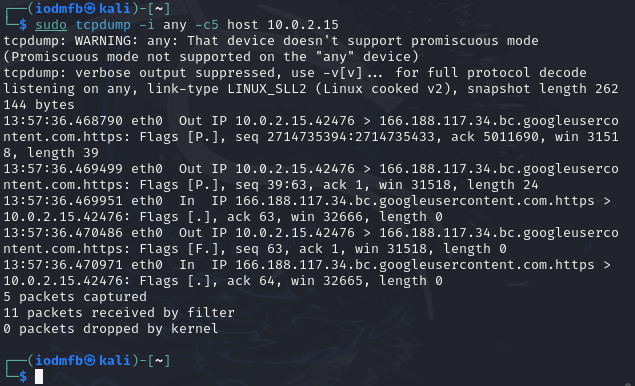
1. **Further options** can be used to filter packet capture based on various criteria. See Step 15.

* Options can be applied to specify capture such as below:
  + ***host*** – *Specify a host machine IP address to capture data from*
  + ***port*** – *Specify the port to capture data on. E.g. Port 80 for HTTP*
  + ***src*** – *Specify a source IP address to capture data from*
  + ***dst*** – *Specify a destination IP address to capture data from*
* *Make sure to use lowercase format!*

1. **Type** the command **sudo** ***tcpdump -i any -c5 host <IP\_Address>*** and hit ***Enter***.

*(Where <IP\_Address> should be replaced by the host address of your Kali virtual machine. Example:* ***tcpdump -i any -c5 host 54.204.39.132****)*

*This command will capture packets from a specific host.*

**

1. **Additional filtering** can be accomplished with the use of logical operators such as:
   * ***and*** – *Allows a combination of filtering options. E.g. source and destination*
   * ***or*** – *Either of the conditions specified in the command can be applied to filter capture data*
   * ***Example****:* ***tcpdump -i any -c5 src 192.168.0.100 and dst port 80***
2. **Experiment** with various combinations of options with the logical operators ***and***/***or***.   
   *Provide screenshots of your results below.*

****

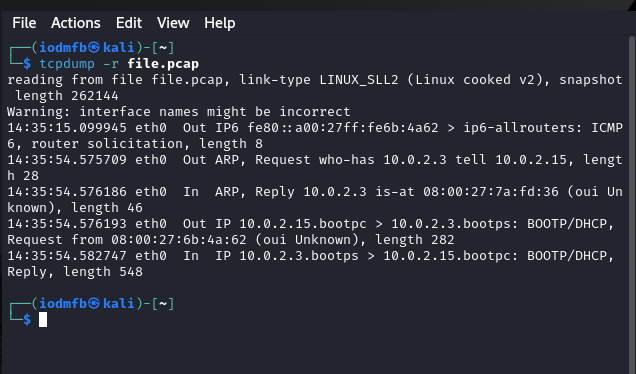
1. **Type** the command **sudo *tcpdump -i any -c5 -w file.pcap*** and hit ***Enter***.

*This command uses the -w switch to write the data captured within the limit of 5 packets to a .pcap file named file.pcap.*

**

1. **Type** the command ***tcpdump -r file.pcap*** and hit ***Enter***.

*This command is run with the -r switch to read the .pcap file output in Step 17. .pcap files are used to analyse network data by security analysts every day in the industry.*

**

1. **Critical Thinking: Configure** tcpdump to **exclusively capture ICMP packets**. **Ping** your Linux machine from another virtual machine **to verify** if **ICMP** packets are exclusively captured.

*Use the provided resources and conduct online research to configure tcpdump.  
 Provide screenshots below.*

**Part 4 - Capturing Traffic with Wireshark**

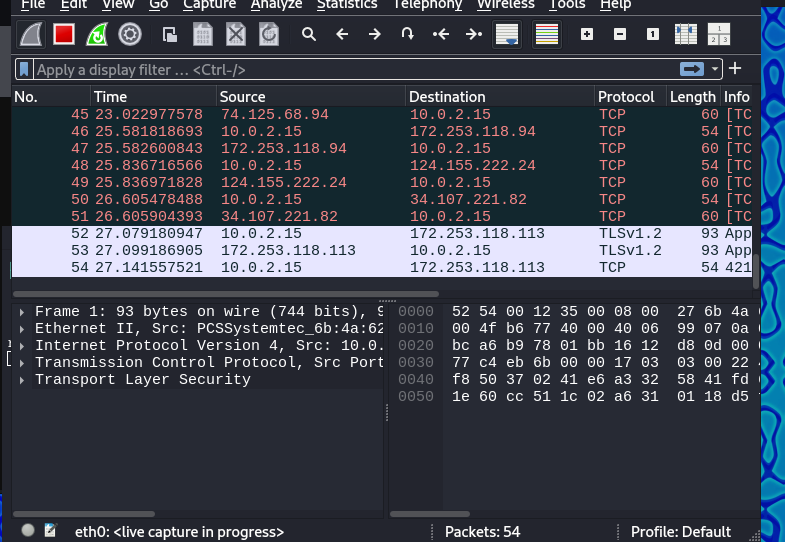
Wireshark is an open-source application that captures and displays data travelling back and forth on a network. Wireshark is the world’s leading network traffic analyser and is used by security professionals and system administrators every day as it can examine and display packet data in high detail.  
  
This exercise aims to showcase the practical application of the Linux command line terminal and the tool Wireshark. Through this exercise, you will gain hands-on experience in capturing network traffic and inspecting relayed data on the network.

**Instructions:**

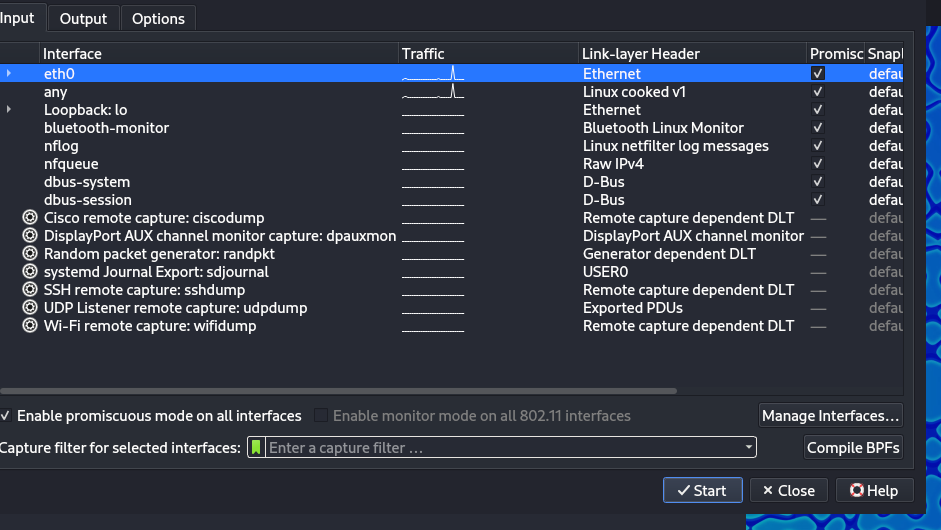
1. **Open** a Kali Linux terminal window.
2. **Type** the command ***sudo apt install wireshark*** and hit ***Enter*** to install Wireshark.
3. **Type** the command ***wireshark*** and hit ***Enter*** to launch Wireshark.
4. **Double-click** on the interface named ***“eth0”*** in the ***Capture*** window presented on the main page when Wireshark launches.

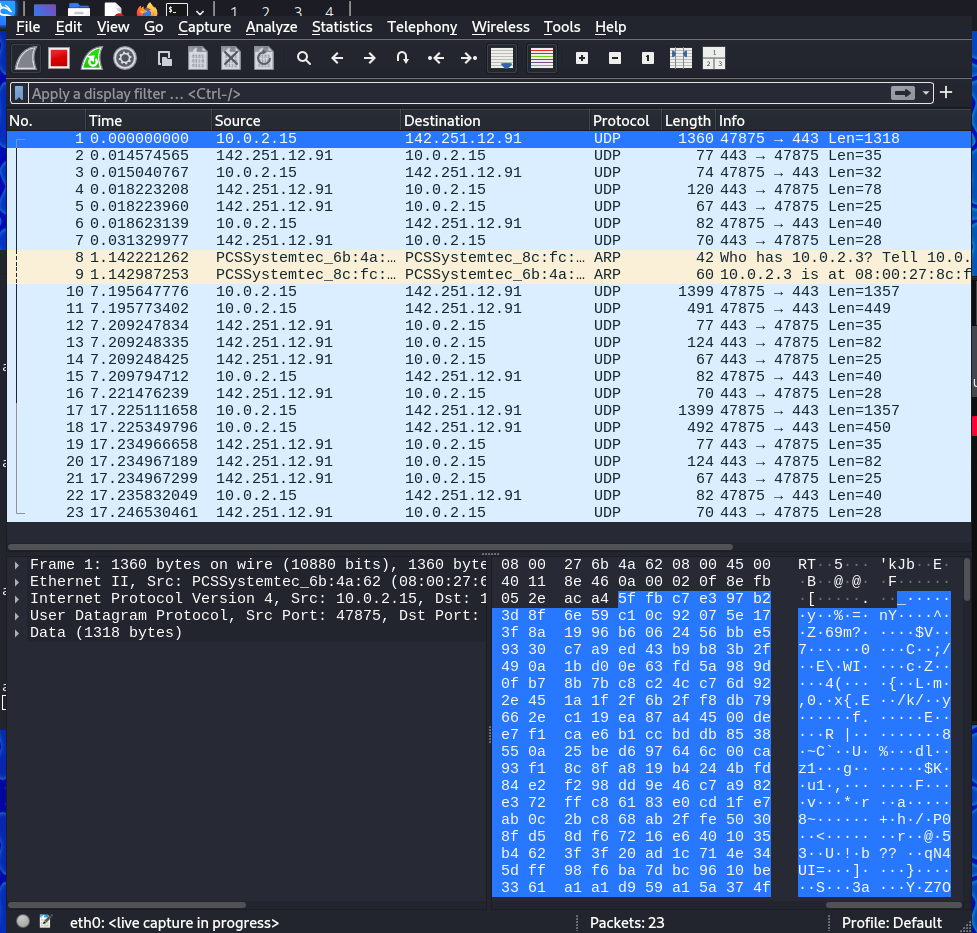
*This will begin the capture of network data on the Ethernet network adapter. Try opening a website on the firefox web browser to see the data captured in Wireshark. Minimise the window once you open a webpage.*

1. **Explore** the results from **Step 4**.

****

1. **Click** the ***red square*** on the **top left** to **stop capturing** network traffic.
2. **Click *File*** and select ***Close*** to exit capture. Continue without saving.
3. **Click** on the ***“Capture”*** button on **the toolbar at the top** of the window and then **click** ***“Options”***.
4. **Explore** the network **interfaces available** and the **options provided**.

****

****

1. **Critical Thinking: Explain** what ***“Promiscuous Mode”*** refers to on the capture options page.

*Detail your explanation below.*

* The network interface passes all packets to the system's network stack, even those not addressed to the host machine.
* This allows Wireshark to capture and analyze packets intended for other devices on the same network segment.

1. **After starting a capture, try typing** the string ***http.request.method == “GET”*** in the ***“Apply a display filter …”*** section at the top of the capture result window. Go to the firefox web browser and go to a webpage you have not visited yet on this machine.

*This will filter and display only packet data relevant to the specified string.*

*Note that the display filter provides an entry completion feature that helps you choose the right filter when you do it manually.*

1. **View** the **lowest level** of detail in the packet “Packet Bytes” which is the **binary numbers** on the bottom right of the Wireshark Window.
2. **Change** the view of the “Packet Bytes” by **right-clicking** on the ***"Packet Bytes"*** area (the window outputting data on the bottom right of Wireshark) and choosing ***“Show bytes as hexadecimal”*** from the context menu. Swap through the different views under this heading to see the information change in presentation. Example: …as octal, ….as bits

*By changing the view, you can analyse the packet contents in a different format.*

