

Redynox Internship

Task 1: INTRODUCTION TO NETWORK SECURITY BASICS:

Network Security Concepts:

For my first task I was to learn more about network security concepts and understand network threats so as to apply basic security measures in a small network (home/virtual lab). I'll also be using Wireshark and other network tools to monitor and analyze network traffic in my research.

Network Threats:

This can refer to any potential danger to an organization's network confidentiality, availability and integrity (CIA triad). You can see these threats in the form of unauthorized login attempts, interruption of services or compromising sensitive info. Though we have made advancements in modern technology, attackers keep finding a multitude of ways to get inside an organisation's infrastructure.

In my research I found a few that can be considered as threats when it comes to protecting networks being the following:

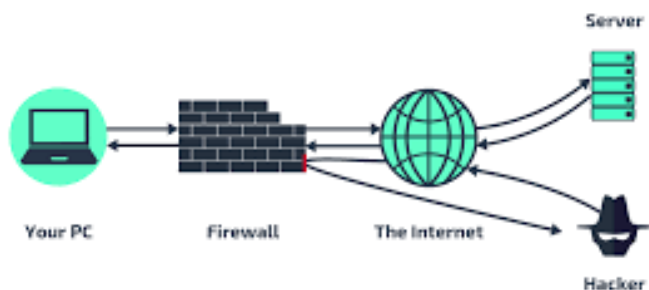
- **Phishing:** This is a type of attack where a threat actor makes use of digital communications to trick people into revealing sensitive data or deploying malicious software. The main motive of it is for a victim to click on the fake link of a legitimate website and provide sensitive credentials on that fake login page. Email is the most common tool that is used for phishing by attackers since they are easy to fake, cheap and almost everyone uses them on a daily basis.
- **Malware:** Malware basically stands for malicious software. A threat actor designs these softwares to harm devices or networks. There are several types of malware which organizations come across:
 1. **Virus:** Most common and a type of malware where the code is written to interfere with normal computer operations and cause damage to software and data. Although, this actually needs to be initiated by a user, as in open a file or visit a malicious link sent by the attacker. Famous examples being the Brain Virus(created to track illegal copies of medical software) and Morris Worm (created to find the size of the internet)
 2. **Trojans:** They basically just pretend to be safe software but are actually harmful for your devices. Common examples are games that are ripoffs of the original ones having unnecessary permissions and just might have a keylogger installed to observe your inputs.
 3. **Worm:** These can easily duplicate and spread itself across your network without having a user to initiate which makes it more scarier than a virus.
 4. **Ransomware:** Malicious attacks where the attacker encrypts an organization's sensitive data and the only way to decrypt is to pay the ransom amount provided by the attacker. Wannacry ransomware is a notable one that comes to mind where it encrypts your files and locks you out of the computer.

Redynox Internship

And there are many more like DDOS and MITM attacks, Zero-day exploits which come under network threats. With consistent threats like above, there arises a need to protect our networks and systems which is where protecting network/data, firewalls and encryption come into play.

Firewalls can either be in software, hardware, host-based or in a network form and you can choose based on your company or personal needs. They provide features like network protection, device and web security and threat prevention. Their main task being filtering the incoming and outgoing traffic based on rules set by an organization, allows trusted connections and also prevents port scanning.

HOW A FIREWALL WORKS

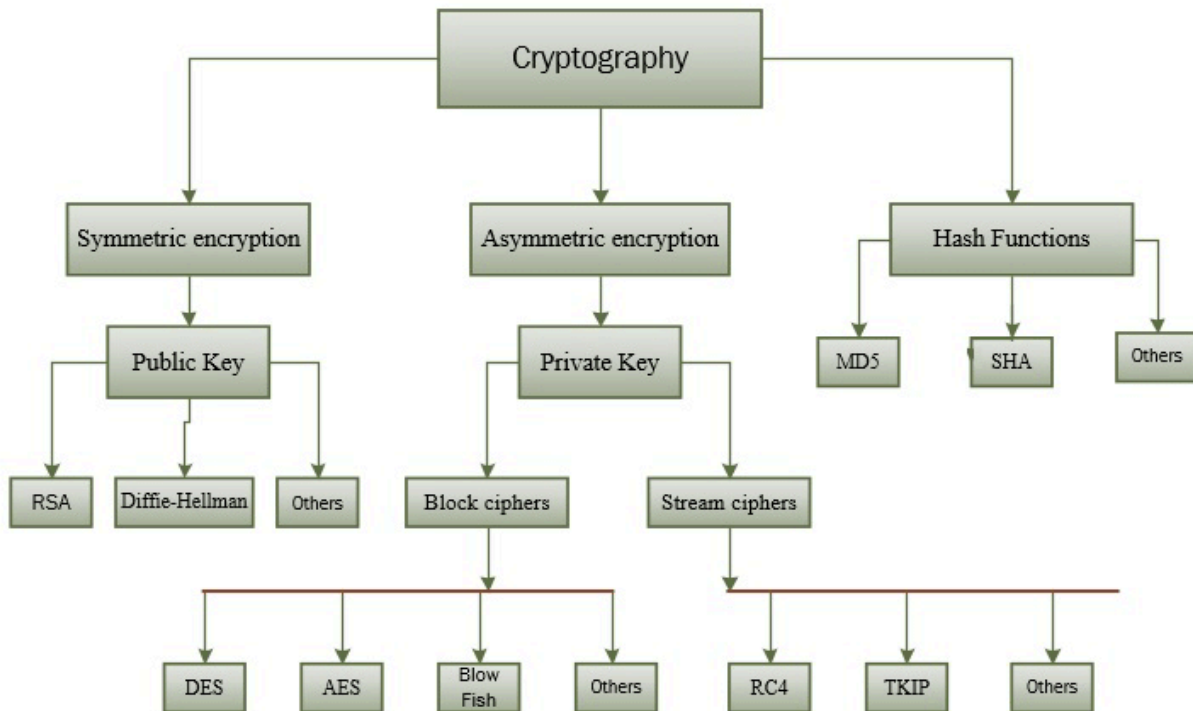


When it comes to data protection, encrypting data is the first thing that comes to mind. Encryption is basically converting your data in a code format which cannot be read without a decryption key. There are several types of encryption to encrypt your data ranging from symmetric(has one key)to asymmetric(has 2 keys), and data at rest(Applock) or if in transit(HTTPS). Data is encrypted to ensure security and integrity of the data.

Some notable ones:

- MD5 (Message Digest Algorithm 5)
- AES (Advanced Encryption Standard)
- Caesar Cipher
- Hashing
- SHA256 (Secure Hash Algorithm)

Redynox Internship



From that it also makes us question as to what we personally can do to keep our network clean so here are some network configurations which can make your network more secure:

- Making sure unused ports are disabled
- Using Nmap to see if you have any ports disclosed to the outside world.
- Dividing your network also known as network segmentation to achieve load balancing as well.
- Using strong firewall rules.
- Changing default settings of the router
- Enabling IDS/IPS
- Using MFA
- Having a system where we follow the principle of least privilege.
- Regularly updating switches, routers, OS and firmware.
- Enabling logging and monitoring
- Using VPN
- DNS filtering to avoid malicious sites.

2.

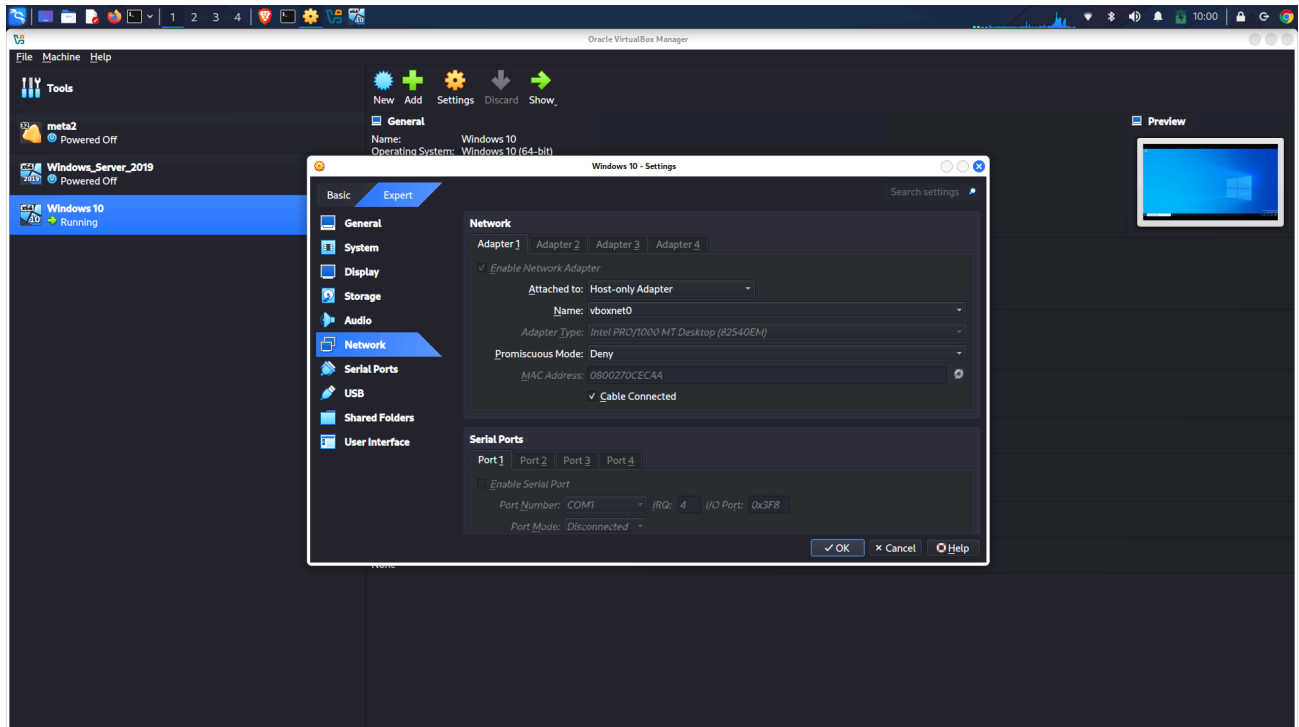
a. **Implementing Security Measures.**

For this I will be setting up a home virtual lab to set up a simple network environment to work on. Tools used here:

Redynox Internship

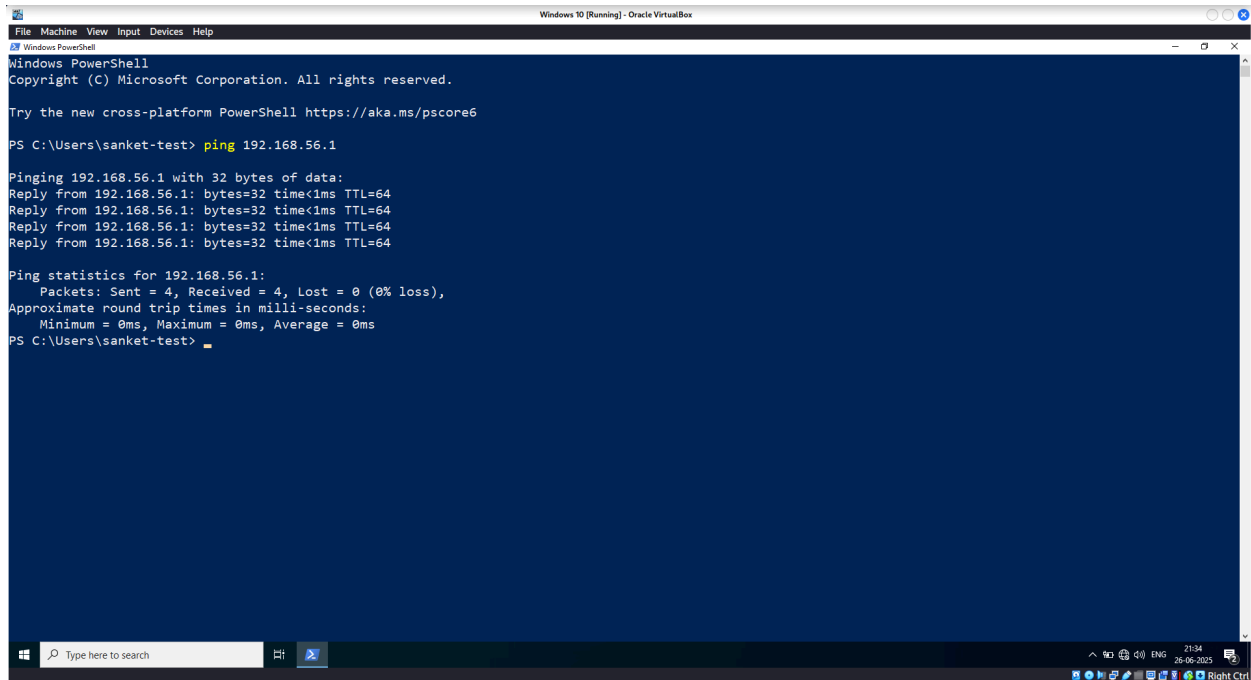
- Kali Linux (Host OS)
- Windows 10 LTSC (VM)
- VirtualBox (for setting up the lab)
- Windows Firewall Defender
- Ping (via powershell) and Nmap

First I downloaded VirtualBox and the [Windows 10 LTSC iso](#) from Microsoft's official page. Set up the Windows VM by giving it 4gb of RAM and keeping almost everything to default. Coming to the network settings, I made sure to configure the Network Adapter to "**Host-Only Adapter**" which allows my Host OS and Windows VM to be able to communicate without the internet which makes it safe for testing.



Once the VM was configured, I booted up the Windows VM and once it was loaded and had finished downloading the necessary updates, I headed over to powershell to ping my Host OS to check if the communication was established. And from the results we can confirm that I was able to communicate with the Host.

Redynox Internship



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

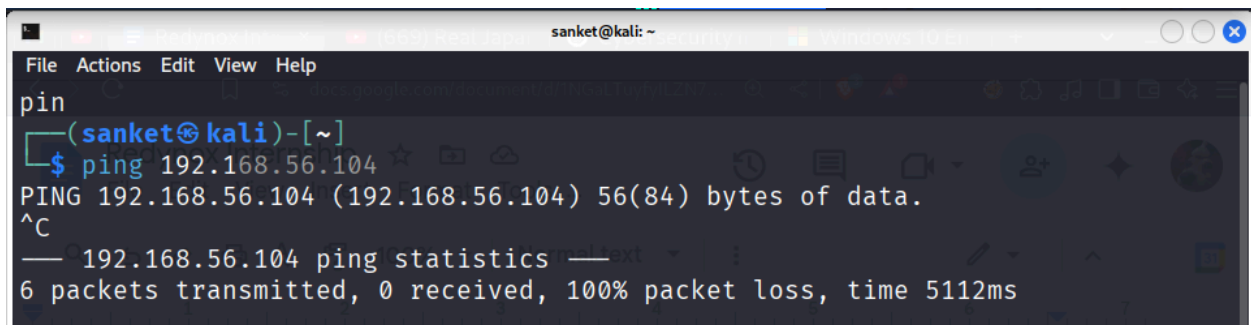
Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\sanket-test> ping 192.168.56.1

Pinging 192.168.56.1 with 32 bytes of data:
Reply from 192.168.56.1: bytes=32 time<1ms TTL=64
Reply from 192.168.56.1: bytes=32 time<1ms TTL=64
Reply from 192.168.56.1: bytes=32 time<1ms TTL=64
Reply from 192.168.56.1: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.56.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
PS C:\Users\sanket-test>
```

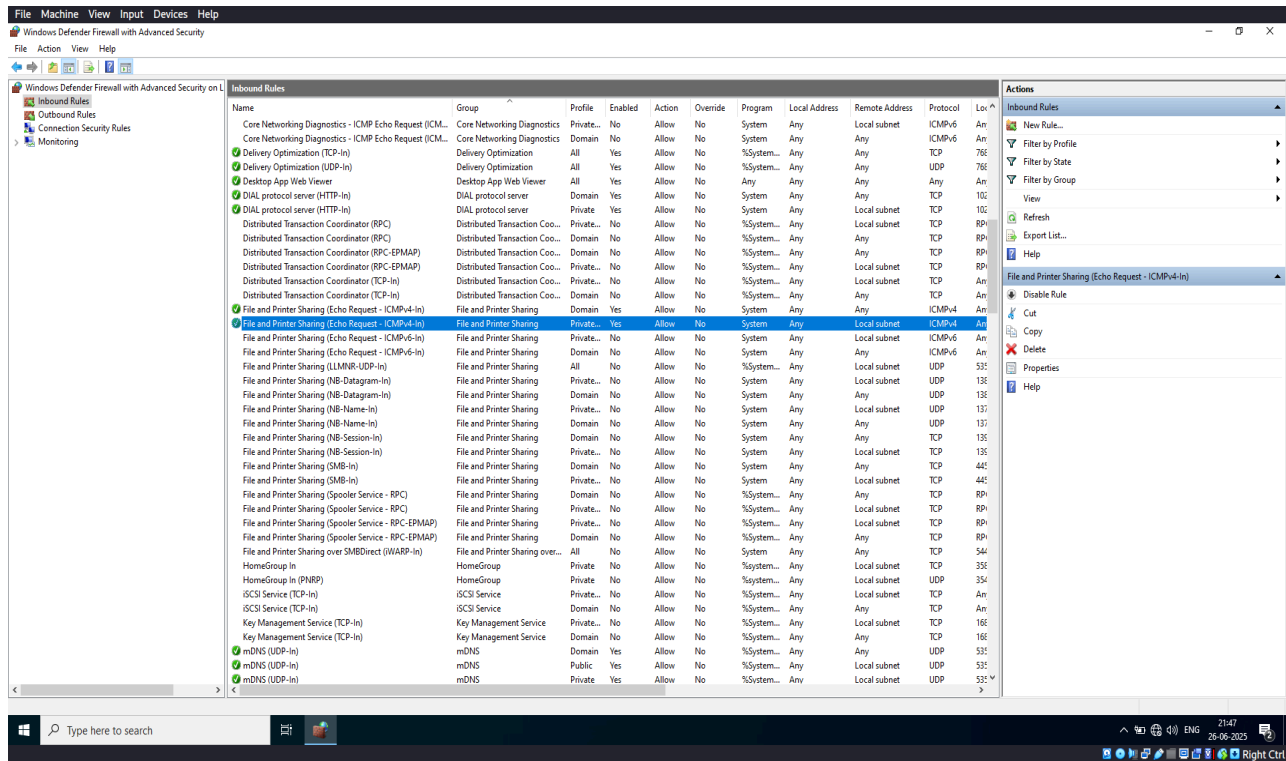
However, on performing the same thing but with my host to ping Windows, I noticed that I wasn't able to ping the Windows VM with my Host.



```
sanket@kali: ~
File Actions Edit View Help
pin
(sanket@kali)-[~]
$ ping 192.168.56.104
PING 192.168.56.104 (192.168.56.104) 56(84) bytes of data.
^C
— 192.168.56.104 ping statistics —
6 packets transmitted, 0 received, 100% packet loss, time 5112ms
```

On further checking, I was able to confirm that the most common reason as to why this happens is that Windows Firewall blocks ICMP (ping) requests by default. But it is an easy fix, and we just have to head to the **Windows Defender Firewall with Advanced Security > Inbound Rules** and then enable **File and Printer Sharing (ECHO request - ICMPv4 -In)** rule for both profiles of **Domain** and **Private**.

Redynox Internship



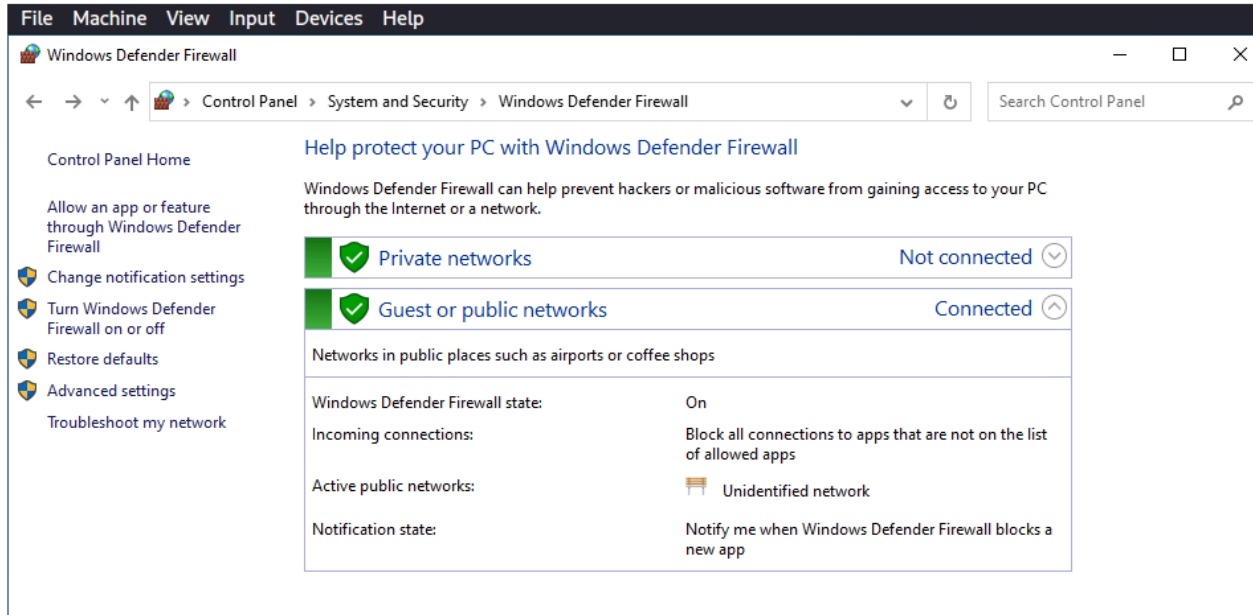
Once this was achieved, I was able to ping my Windows VM.

```
(sanket@kali)-[~]
$ ping 192.168.56.104
PING 192.168.56.104 (192.168.56.104) 56(84) bytes of data:
64 bytes from 192.168.56.104: icmp_seq=1 ttl=128 time=0.422 ms
64 bytes from 192.168.56.104: icmp_seq=2 ttl=128 time=0.379 ms
64 bytes from 192.168.56.104: icmp_seq=3 ttl=128 time=0.403 ms
^C
— 192.168.56.104 ping statistics —
3 packets transmitted, 3 received, 0% packet loss, time 2053ms
rtt min/avg/max/mdev = 0.379/0.401/0.422/0.017 ms
```

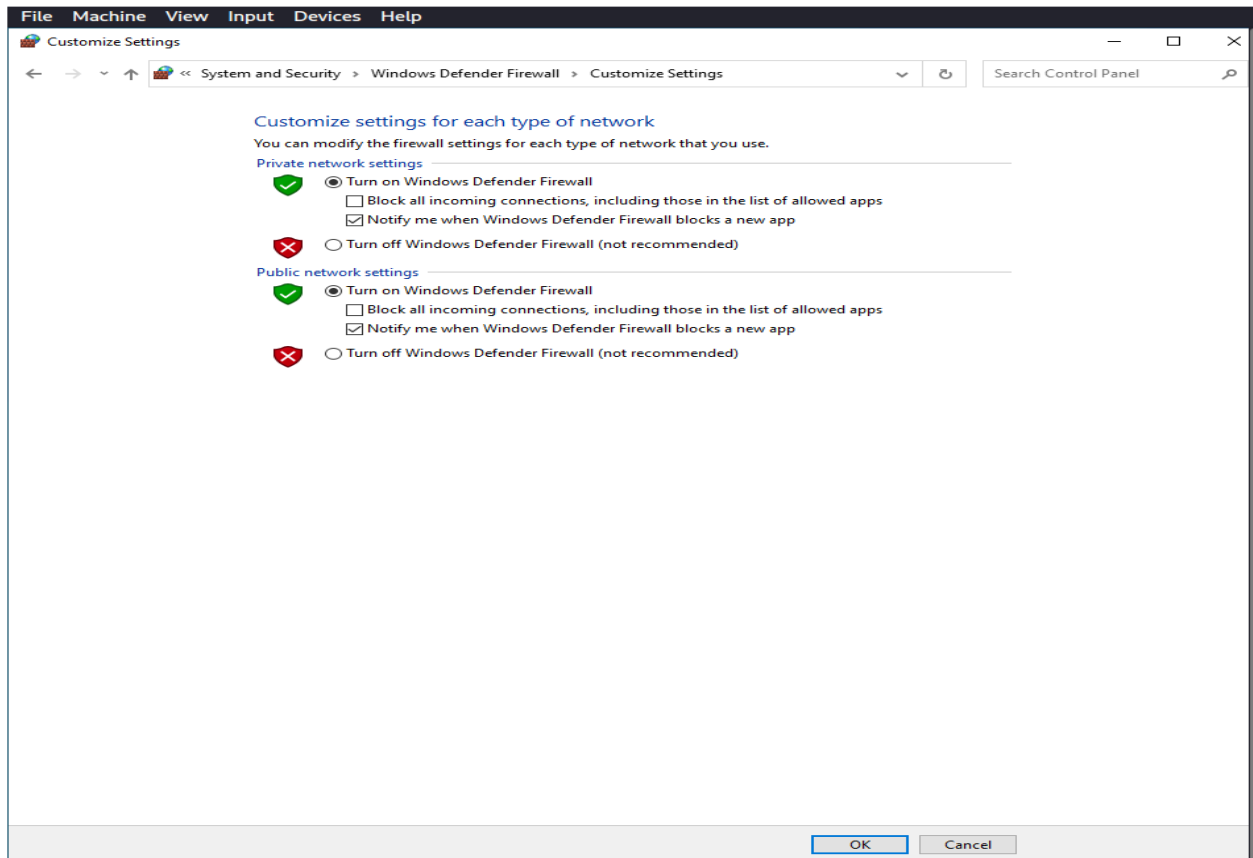
b. Firewall Config

When it comes to enabling and setting up a firewall, it is most likely enabled by default on most modern Windows systems unless it is manually disabled. Though, if you do wish to check , you can do so by opening **Control Panel > System and Security** and there you should see a green tick mark for both Private and Public Networks which indicates the Firewall is enabled.

Redynox Internship



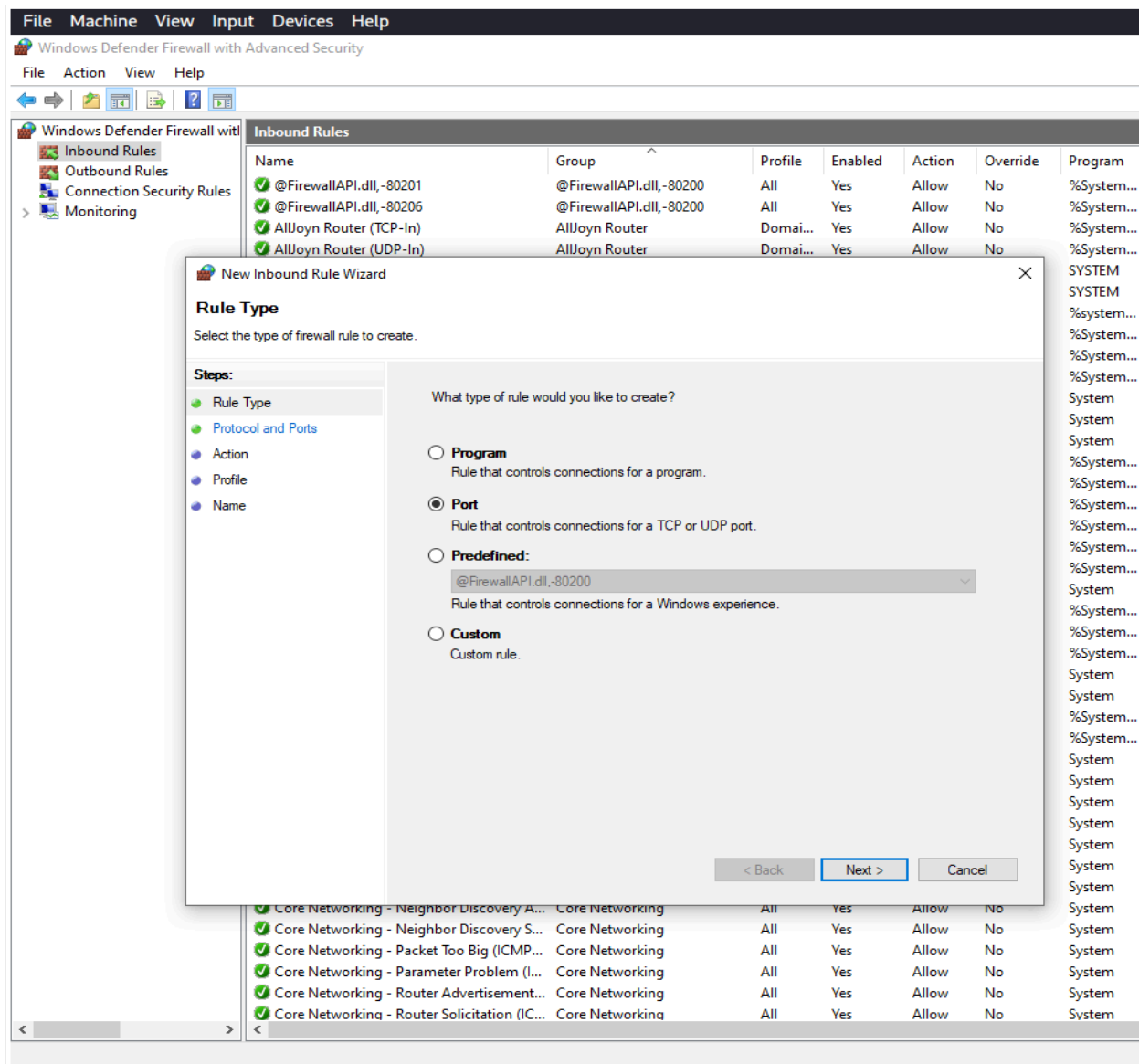
If you do wish to disable it to perform some tests, you can disable it by clicking on the **“Turn Windows Defender Firewall On or Off”** on the left hand side and from there you can disable it for both private or public networks.



Redynox Internship

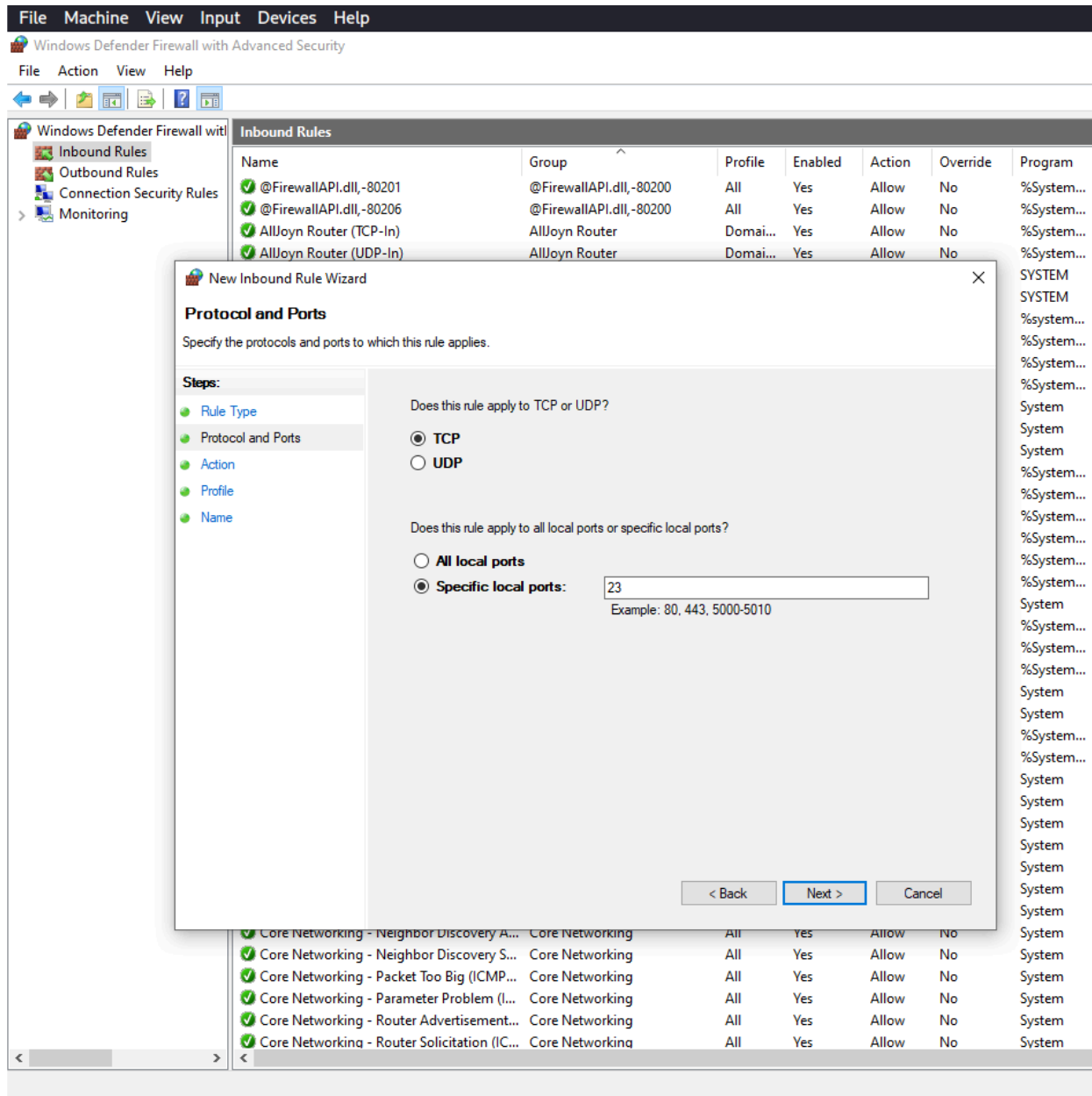
This was just about enabling and disabling Firewall, now we head over to configuring a firewall. For testing purposes, I tried implementing a rule to block a port specifically port 23 which is used for telnet and considering it is not secure, it is better to disable it.

First we head on over to **Windows Defender Firewall and Advanced Security > Inbound Rules**. Right clicking on it provides us with various options and since we are creating a new rule, we select “**New Rule**” from the menu. This opens up a wizard window to select what kind of rule we would like to add. And as I mentioned we will be adding the rule to disable a port, we will select the “**Port**” option in the wizard and click on “**Next**”.



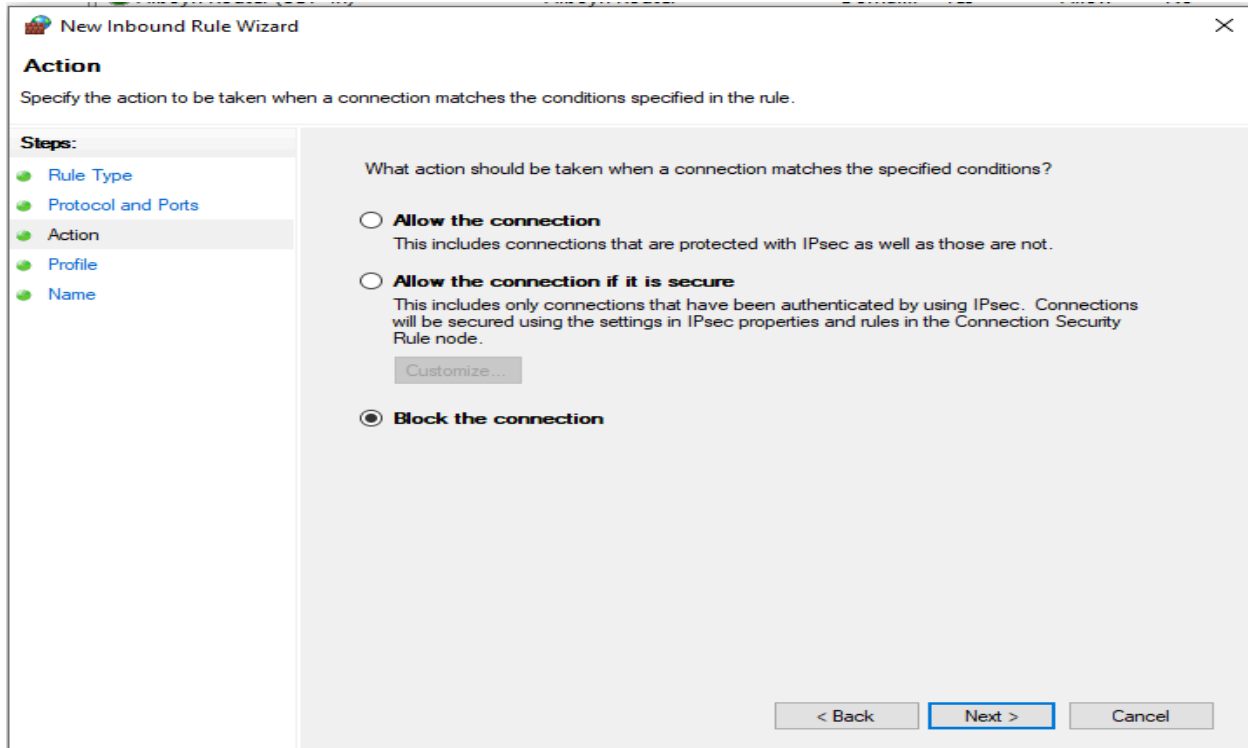
Redynox Internship

Then we enter the port number as “23” for telnet and click on “**Next**”.



Then we get to the Action tab where we have to select what action needs to be taken with that port number. As for this exercise, we will be blocking it so we select “**Block the connection**” and click “**Next**”.

Redynox Internship



New Inbound Rule Wizard

Action

Specify the action to be taken when a connection matches the conditions specified in the rule.

Steps:

- Rule Type
- Protocol and Ports
- Action**
- Profile
- Name

What action should be taken when a connection matches the specified conditions?

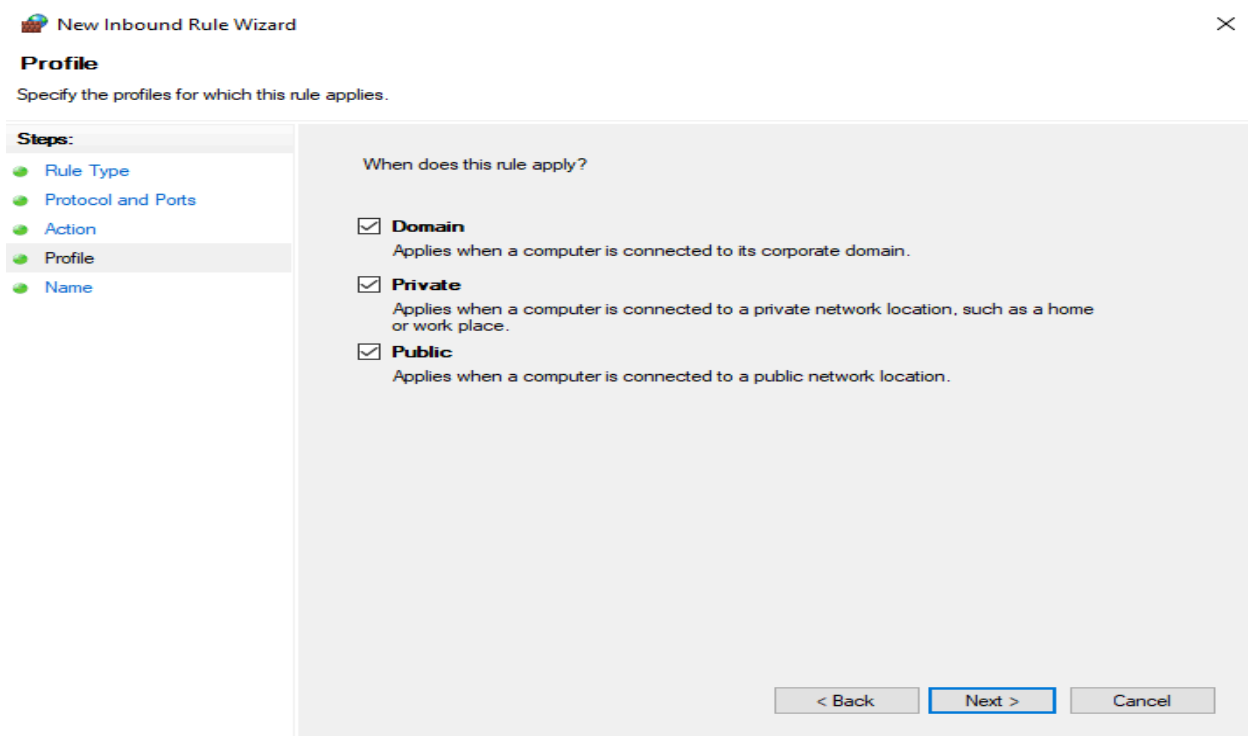
☐ **Allow the connection**
This includes connections that are protected with IPsec as well as those are not.

☐ **Allow the connection if it is secure**
This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.
[Customize...](#)

☒ **Block the connection**

< Back **Next >** Cancel

Then it asks which profile will this apply to, as for this exercise, we will be blocking it for all profiles. So we check the boxes for “**Domain, Private and Public**” and click “**Next**”.



New Inbound Rule Wizard

Profile

Specify the profiles for which this rule applies.

Steps:

- Rule Type
- Protocol and Ports
- Action
- Profile**
- Name

When does this rule apply?

☒ **Domain**
Applies when a computer is connected to its corporate domain.

☒ **Private**
Applies when a computer is connected to a private network location, such as a home or work place.

☒ **Public**
Applies when a computer is connected to a public network location.

< Back **Next >** Cancel

Redynox Internship

The final step is to give the rule a name to specify what exactly it does. Here, we name it as “**Block Telnet Port 23**”. You can add a short description as well as to what the rule does and then click on “Finish”.

New Inbound Rule Wizard

Name

Specify the name and description of this rule.

Steps:

- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

Name:
Block Telnet Port 23

Description (optional):
Blocks port 23 used for telnet.

< Back Finish Cancel

Now we can see that this new rule has been created and is enabled for all profiles!

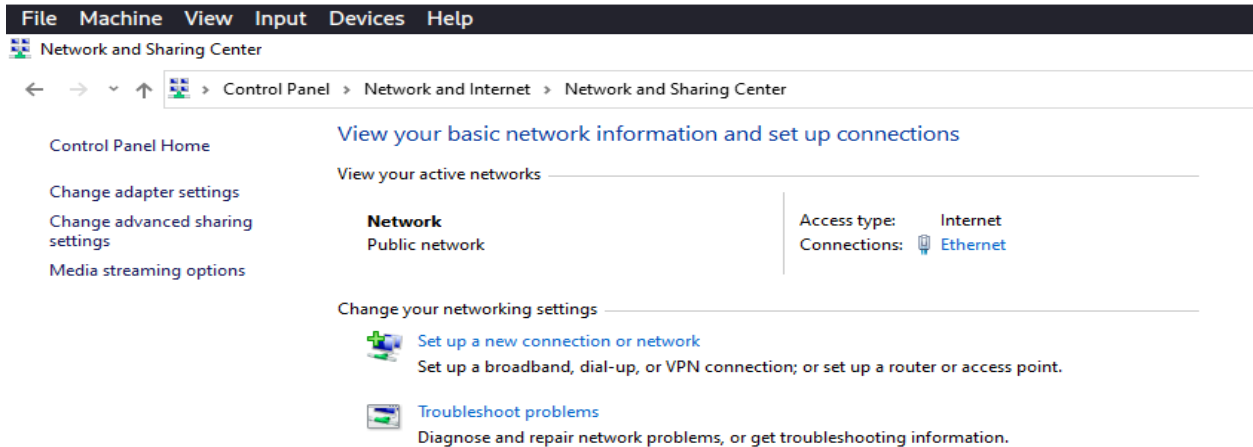
Inbound Rules						
Name	Group	Profile	Enabled	Action	Override	Program
Block Telnet Port 23		All	Yes	Block	No	Any
@FirewallAPI.dll, -80201	@FirewallAPI.dll, -80200	All	Yes	Allow	No	%System...
@FirewallAPI.dll, -80206	@FirewallAPI.dll, -80200	All	Yes	Allow	No	%System...
AllJoyn Router (TCP-In)	AllJoyn Router	Domai...	Yes	Allow	No	%System...
AllJoyn Router (UDP-In)	AllJoyn Router	Domai...	Yes	Allow	No	%System...
BranchCache Content Retrieval (HTTP-In)	BranchCache - Content Retr...	All	No	Allow	No	SYSTEM
BranchCache Hosted Cache Server (HTTP...	BranchCache - Hosted Cach...	All	No	Allow	No	SYSTEM
BranchCache Peer Discovery (WSD-In)	BranchCache - Peer Discove...	All	No	Allow	No	%system...
Cast to Device functionality (qWave-TCP...	Cast to Device functionality	Private...	Yes	Allow	No	%System...
Cast to Device functionality (qWave-UDP...	Cast to Device functionality	Private...	Yes	Allow	No	%System...
Cast to Device SSDP Discovery (UDP-In)	Cast to Device functionality	Public	Yes	Allow	No	%System...

Redynox Internship

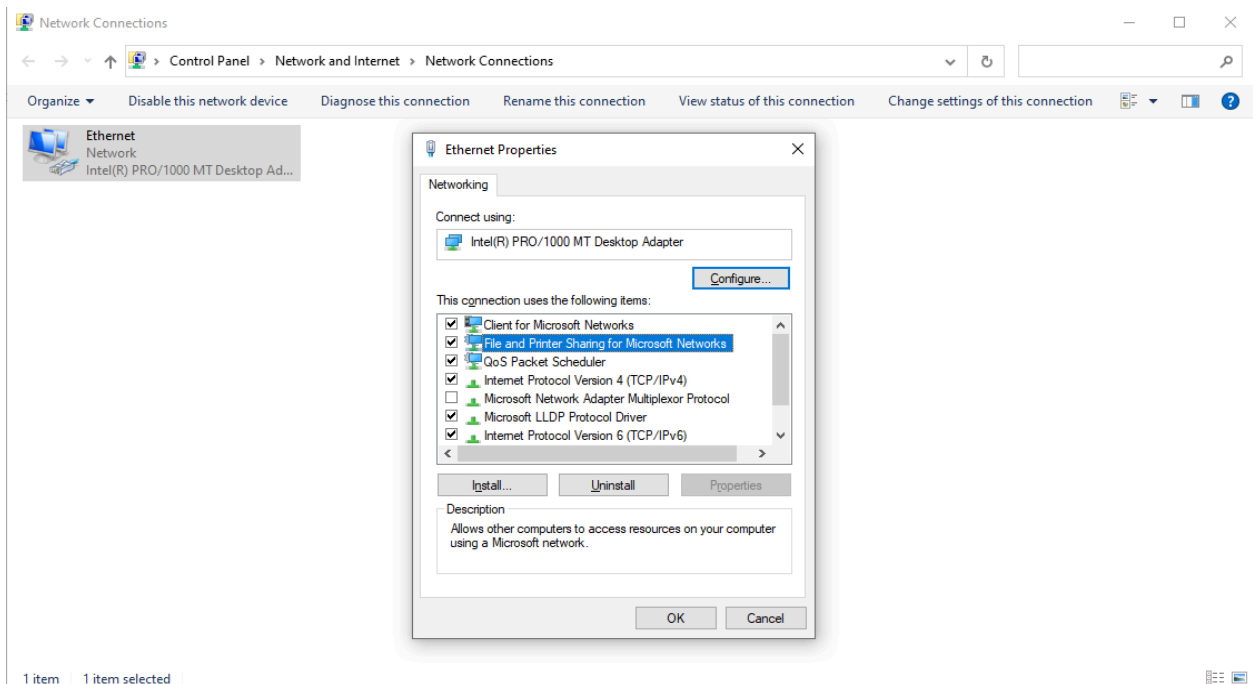
Securing your machine:

In this example, I will be securing my virtual machine from outside threats while also making sure that only necessary services are active on it.

To do so, we head over to “**Control Panel > Network and Internet > Network and Sharing Center**”. On the left hand side we select the “**Change Adapter Settings**” option which opens up another window displaying the adapters we currently have.

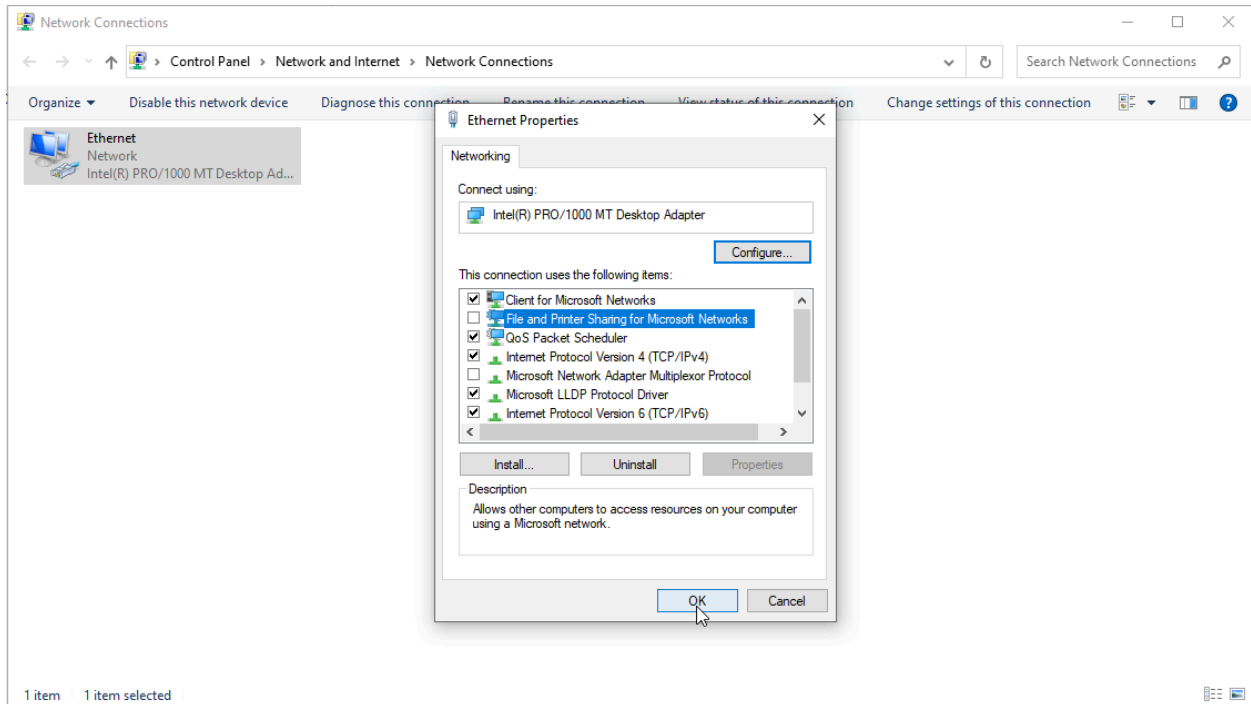


Here, we can see we have one active Adapter “**Ethernet**”. Right clicking on it, pulls out a drop down menu where we click on “**Properties**”. This displays the connections the selected adapter allows for your machine to send out and receive. Clicking on the items also provides a short description as to what the connection does.



Redynox Internship

For our exercise, I will be turning off the **“File and Printer Sharing for Microsoft Networks”** so other devices are not able to access the resources of our computer using a Microsoft Network. Once that’s done, we click on **“OK”** and your adapter is now a bit more secure than earlier!

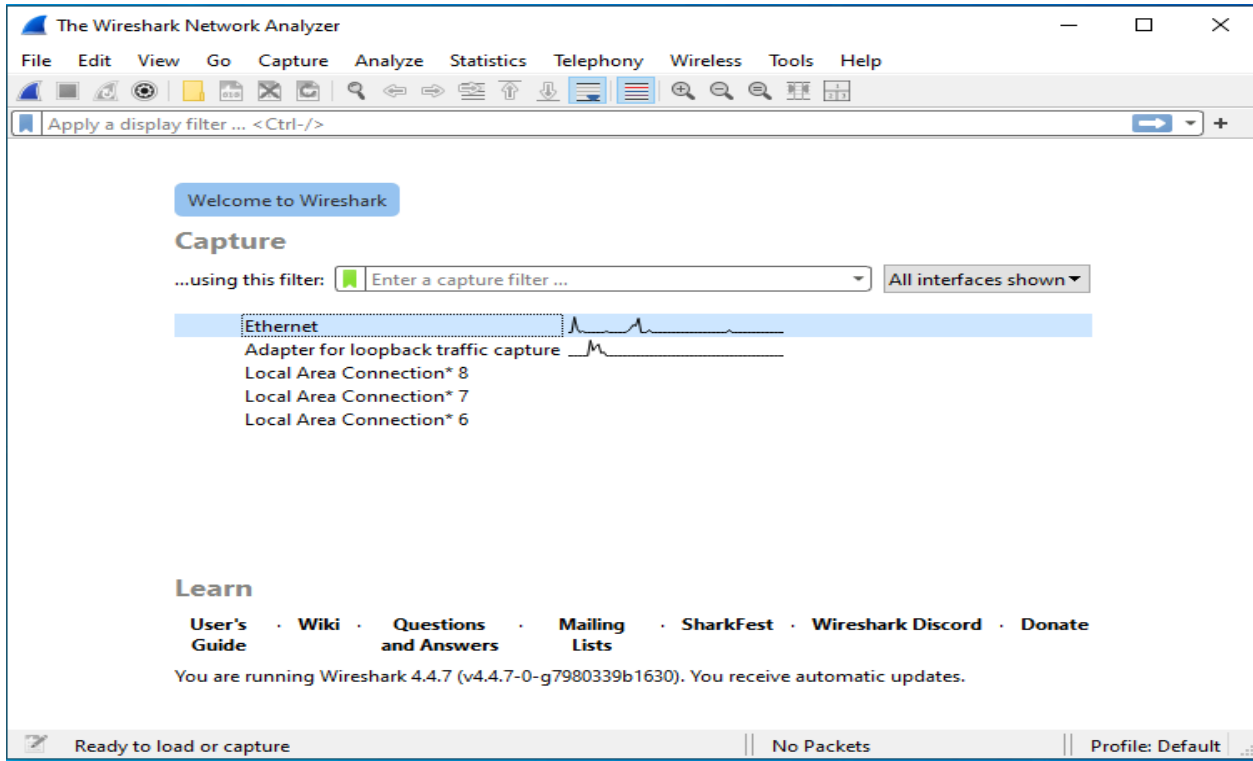


Other simple ways you could secure it is by also using a stronger password for your device. It is better to have one between 8 and 16 characters with symbols, capital and small letters with numbers to make it difficult for a threat actor to bruteforce it.

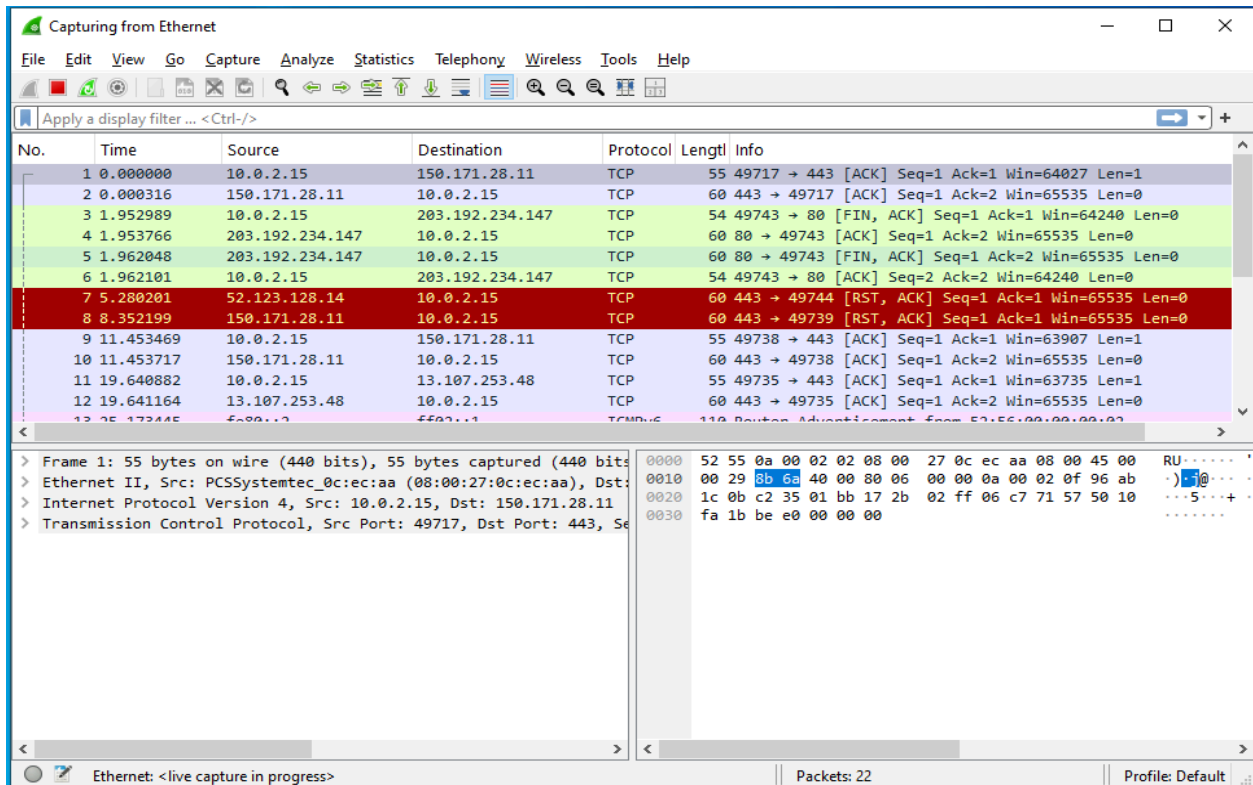
c. Monitoring Traffic

For the next task we will be needing an application called Wireshark which is a network protocol analyzer. It basically monitors incoming and outgoing network traffic and we will be working on the same. The following is the first thing you see when you open Wireshark.

Redynox Internship



Here we will select “**Ethernet**” since we want to monitor the internet traffic and once you select it, we can see that it starts to display network traffic.



Redynox Internship

For our practice, here I have searched for a website “testphp.vulnweb.com” for our test. To locate specific info about network traffic we make use of filters which allows us to enter a specific filter and it displays out only those for easier reading. Here I looked up for DNS requests made by the URL I entered which you can see in this image.

The screenshot shows a web browser window displaying the Acunetix website. The browser's address bar shows the URL testphp.vulnweb.com. The website content includes a search bar, navigation links, and a welcome message. Overlaid on the browser window is a Wireshark packet capture window. The Wireshark window shows a list of captured packets, with a filter set to 'dns'. The selected packet (No. 36) is expanded, showing the details of a DNS query from 10.0.2.15 to 10.0.2.3.

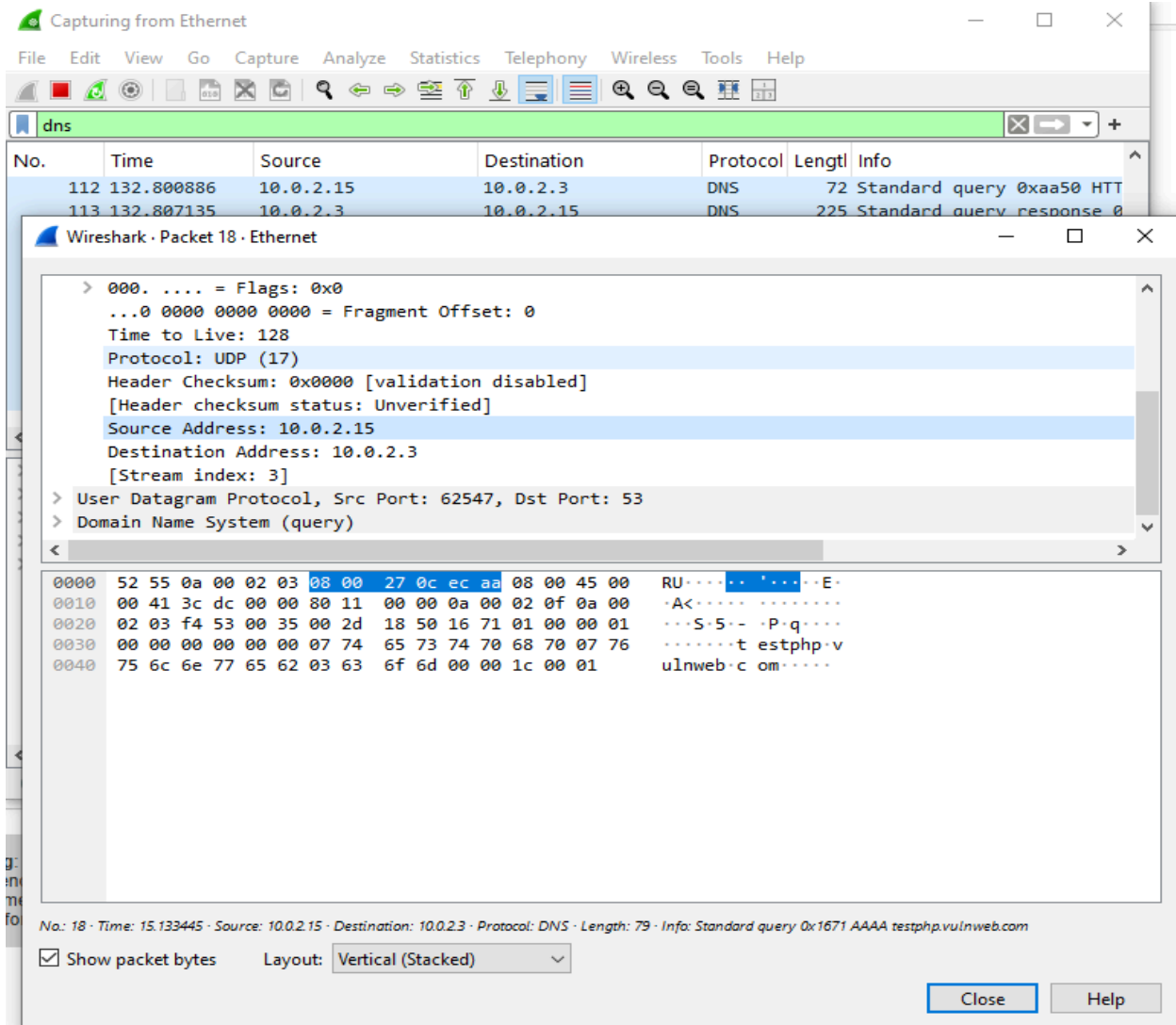
No.	Time	Source	Destination	Protocol	Length	Info
36	0.709297	10.0.2.15	10.0.2.3	DNS	79	Standard query 0x2434 AAAA testphp.vulnweb.com
37	0.709494	10.0.2.15	10.0.2.3	DNS	79	Standard query 0x6dc0 A testphp.vulnweb.com
46	0.715770	10.0.2.3	10.0.2.15	DNS	138	Standard query response 0x2434 AAAA testphp.vulnweb.com
48	0.715770	10.0.2.3	10.0.2.15	DNS	95	Standard query response 0x6dc0 A testphp.vulnweb.com
129	53.366423	10.0.2.15	10.0.2.3	DNS	72	Standard query 0xf81d AAAA www.bing.com
130	53.366890	10.0.2.15	10.0.2.3	DNS	72	Standard query 0xf6e6 A www.bing.com
131	53.367298	10.0.2.15	10.0.2.3	DNS	72	Standard query 0xbc70 HTTPS www.bing.com
132	53.370736	10.0.2.3	10.0.2.15	DNS	254	Standard query response 0xbc70 HTTPS www.bing.com
133	53.370736	10.0.2.3	10.0.2.15	DNS	225	Standard query response 0xf6e6 A www.bing.com
134	53.370736	10.0.2.3	10.0.2.15	DNS	249	Standard query response 0xf81d AAAA www.bing.com
254	113.428264	10.0.2.15	10.0.2.3	DNS	72	Standard query 0xc385 AAAA www.bing.com
255	113.428778	10.0.2.15	10.0.2.3	DNS	72	Standard query 0x4f40 A www.bing.com
256	113.430173	10.0.2.15	10.0.2.3	DNS	72	Standard query 0x3333 HTTPS www.bing.com

The expanded packet details show the following information:

- Frame 36: 79 bytes on wire (632 bits), 79 bytes captured (632) on interface 0
- Ethernet II, Src: PCSystemtec_0c:ec:aa (08:00:27:0c:ec:aa), Dst: 08:00:00:00:00:00
- Internet Protocol Version 4, Src: 10.0.2.15, Dst: 10.0.2.3
- User Datagram Protocol, Src Port: 56731, Dst Port: 53
- Domain Name System (query)

On expanding that specific request we can see a few options and since we want to see the source and destination IP we will click on “**Internet Protocol**” which gives a drop down menu and scrolling it a bit displays the **source IP (10.0.2.15)** and **destination IP(10.0.2.3)**

Redynox Internship



Similarly there are many other filters you can make use of like:

-

Purpose	Filter
All DNS traffic	<code>dns</code>
Only HTTP GET requests	<code>http.request.method == "GET"</code>
Packets to/from one IP	<code>ip.addr == 192.168.0.10</code>
FTP usernames	<code>ftp.request.command == "USER"</code>
Only SYN packets	<code>tcp.flags.syn == 1 && tcp.flags.ack == 0</code>

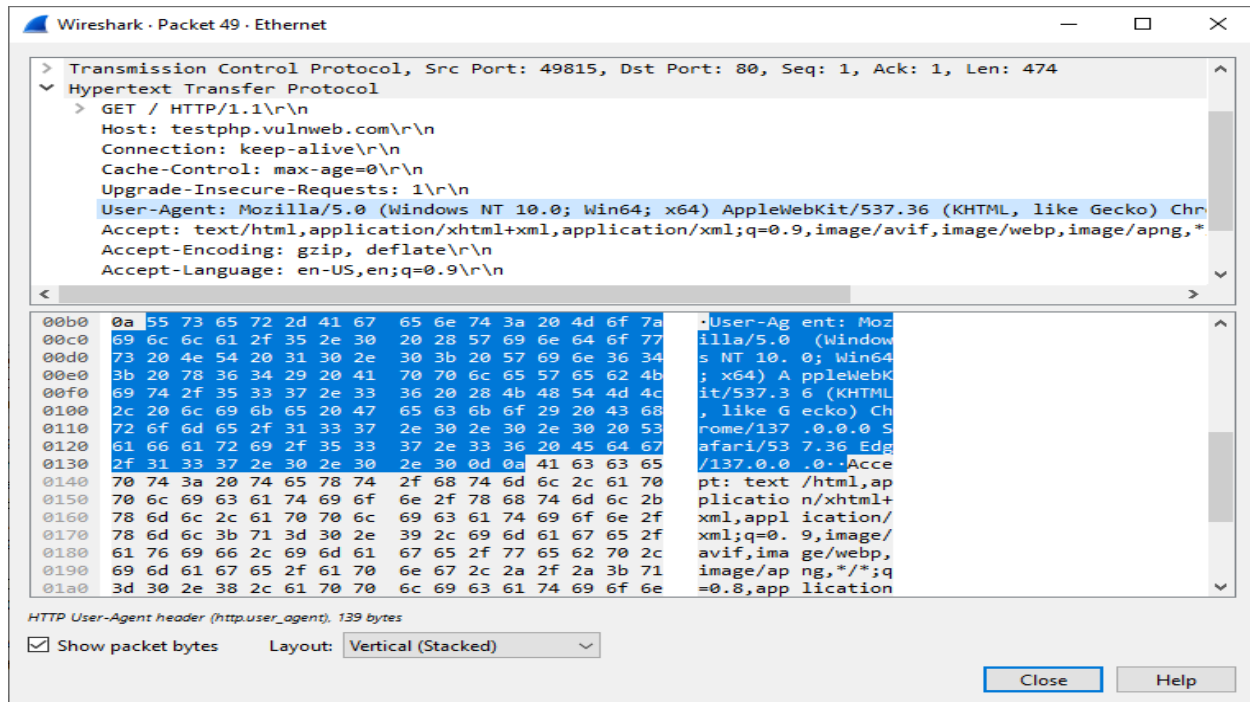
For specific ports:

Redynox Internship

Filter	Protocol	Use Case
http	HTTP	Inspect web traffic (GET, POST)
dns	DNS	View domain queries and responses
ftp	File Transfer Protocol	Look for login info (insecure)
smtp	Email sending traffic	View outbound mail traffic
ssh	Secure Shell	View SSH sessions
tls	TLS/SSL encrypted traffic	Filter encrypted HTTPS, etc.
icmp	Ping traffic (ICMP)	Troubleshoot network connectivity
dhcp	DHCP	View IP assignment requests
arp	Address Resolution Protocol	See MAC/IP lookups

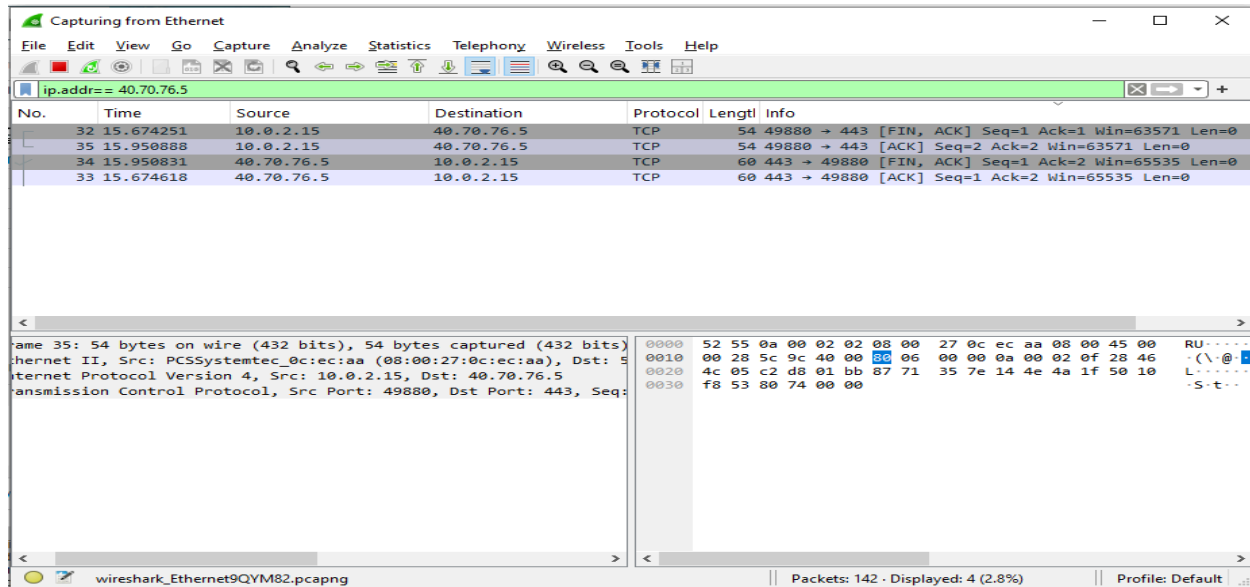
Let's experiment with other filters as well:

Here we used the “**http**” filter to check on the web traffic and inspecting one of the requests, we were able to find the GET request, User-Agent and the host that we are trying to open up(testphp.vulnweb.com)



Redynox Internship

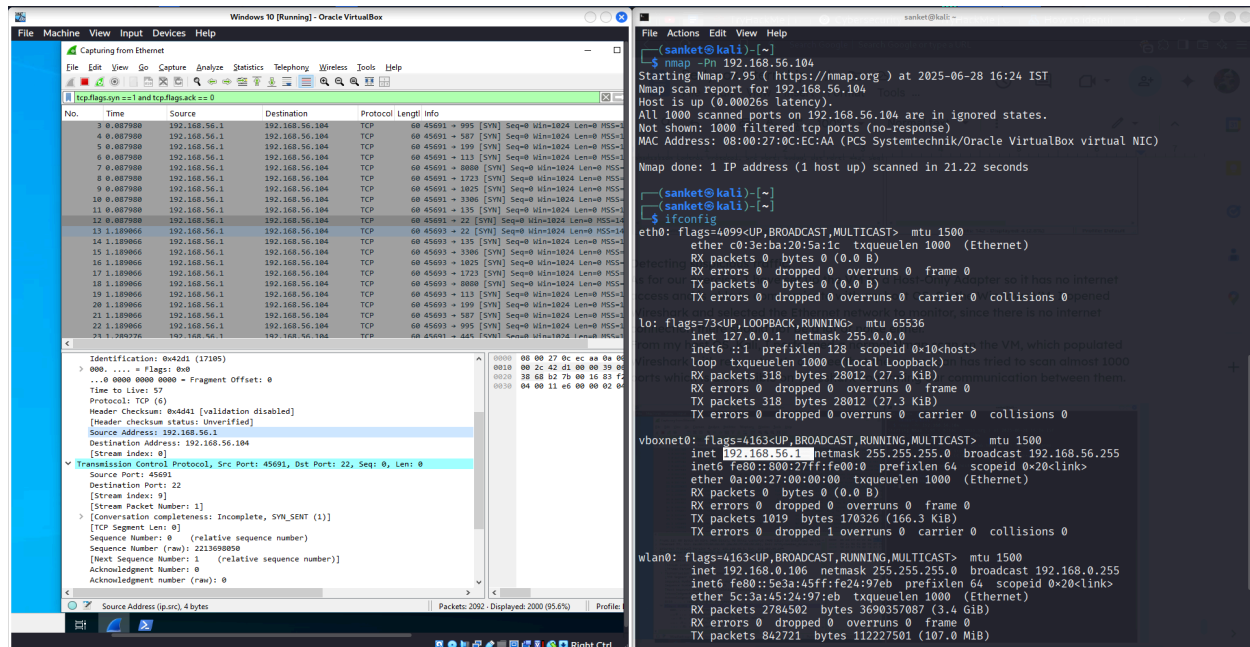
To check what source or destination IP we are receiving or sending data from/to:



Detecting suspicious traffic:

As for our exercise, I have set up the VM to a Host-Only Adapter so it has no internet access and is able to communicate with my host OS. On the Windows VM, I opened Wireshark and selected the Ethernet network to monitor, since there is no internet connection there should not be a lot of noise either.

From my host OS, Kali, I performed a normal Nmap scan on the VM, which populated Wireshark with requests. We can see that the nmap scan has tried to scan almost 1000 ports which is also visible on Wireshark confirming our communication between them.



Redynox Internship

When we are analyzing network traffic in a corporate environment as well, there are certain patterns and behaviours which help identify suspicious activities. For example:

- Unusual Port Usage: Traffic on uncommon ports or well-known malware ports
- Excessive DNS Queries: May indicate DNS tunneling or data exfiltration
- Unencrypted Credentials: Passwords sent in clear text
- Port Scanning: Multiple connection attempts to different ports
- Connection Attempts to Known Malicious IPs: Traffic to/from blacklisted addresses.

From the above activities, we can say that applying the above mentioned security measures can be very useful in keeping the network protected.

Method	Effect
Firewall Rules	Setting these up can help block out unused and risky ports from becoming an entry point for threat actors
Disabling sharing	ApplicationApplicationApplicationDoing so prevents exposing our data and services over the network.
Traffic monitoring	It helps us in detecting port scans and unnecessary traffic which can be blocked out.

Applying these measures altogether would make a network very secure be it personal or corporate. Understanding these basic steps helps in laying down it as the first line of defence paving way to lay down other advanced protection methods in the future. For example in a larger company, implementing tools like IDS(Intrusion Detection Systems) and IPS(Intrusion Prevention System), use of VPN's(Virtual Private Network), EDR's(Endpoint Detection and Response), Multi-Factor Authentication(MFA) are some ways to keep the clean and tightly secured.

Redynox Internship

One could think as to why would we need as many tools as I mentioned and they might think that having these many protection systems in place would be an overkill but I think I would explain it to them using simple analogies of how we lock doors, and though it may not be as practical to the ear but having as many locks on a door would only make it secure. I'd also recommend them to not click on any random links they receive that are from outside the company as this is one of the many easy ways an attacker could get access to their sensitive credentials potentially harming them and the company as well in the process. Just keeping your passwords strong, and not letting your curiosity to click on a link emerge could make a big difference in keeping yourself safe online.

SUMMARY:

In conclusion, I would say that this task gave me hands-on experience with basic network security topics. I learned how to block insecure services, disable risky settings, and monitor traffic using Wireshark. It also showed me how simple steps like firewall rules and traffic analysis can majorly help in protecting a network.