**Task 1**

**Nmap, one** of the tools used in cyber security to do network analysis on hosts and servers, can be used to identify ports on a host to check for any potential vulnerability.

So I first started with checking my ip address and tried to ping it and as usual all the ports were closed so I worked around a little more trying different commands and the command given.

PORT STATE SERVICE

80/tcp closed http

This is what came while doing my Ip address.

Then I tried a different Ip address of my work laptop and ran the command again with that Ip on my mind and it did work.

135/tcp open msrpc

139/tcp open netbios-ssn

445/tcp open microsoft-ds

After doing some research on these ports as told to find the potential vulnerability here is what I got.

135/tcp MSRPC

-used by DCOM for network communication which enables remote admin powers.

-mainly vulnerable to malware, DoS attack.

139/tcp NetBIOS

-used for windows files and printers sharing in legacy system over TCP.

-mainly vulnerable to brute force attack and also null session attack where attackers connect

Without credentials and gather sensitive information.

445/tcp Microsoft-DS

-hosts SMB(Server Message Block) used for sharing file, authentication and domain service

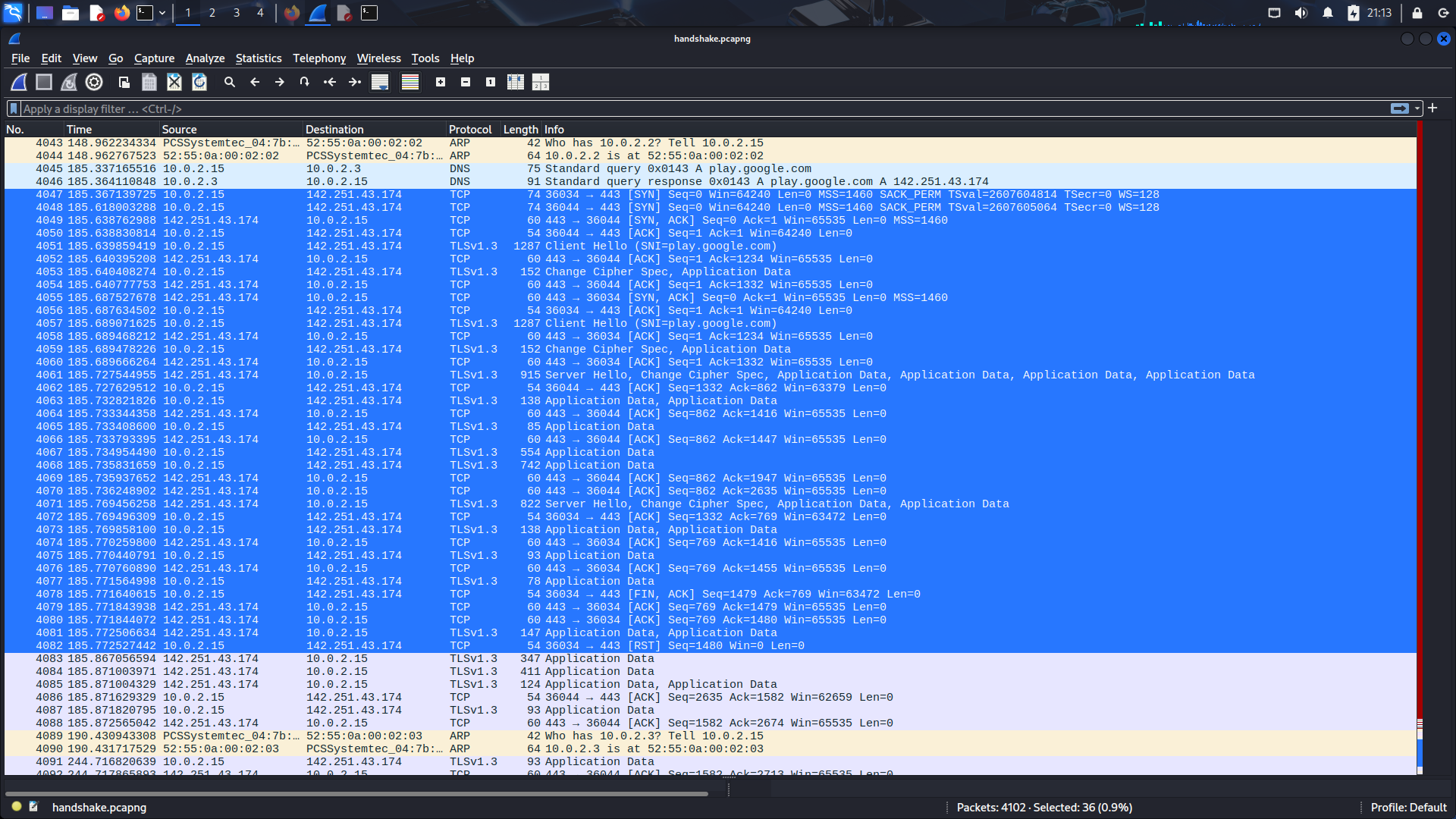
a better alternative to NetBios.

-mainly vulnerable to ransomware infection, data theft and man in the middle attacks

After doing some research on this I ran the command given

-nmap -sS ip and ran it

Here -sS is a protocol which make a 3 way handshake happens so if I want to go to a website my device will send SYN(Synchronization Packets) and the other side will give a response SYN ACK to tell it’s ready for the handshake and then to complete our device send ACK again.

Well these handshakes are usually unauthorised and the firewall interrupts and we can get caught that is why we are using the command -sS so as soon as we find the potential interruption of firewall so we reset or terminate the communication by using RTS Packets to killThis conversion of SYN here is an example of it.

As we can see after a little interruption by the firewall the connection is terminated.

I’ll attach the wire shark file of the entire conversion held between the devices.