# Basic Networking

## Exercise 1 – Basic network stuff

1. Use the **arp** command and paste the output from the arp table on your system:

-We can do this with the command **arp -a**

Interface: 192.168.56.1 --- 0x4

Internet Address Physical Address Type

192.168.56.255 ff-ff-ff-ff-ff-ff static

224.0.0.7 01-00-5e-00-00-07 static

224.0.0.22 01-00-5e-00-00-16 static

224.0.0.250 01-00-5e-00-00-fa static

224.0.0.251 01-00-5e-00-00-fb static

224.0.0.252 01-00-5e-00-00-fc static

239.255.255.250 01-00-5e-7f-ff-fa static

239.255.255.251 01-00-5e-7f-ff-fb static

Interface: 192.168.100.29 --- 0x10

Internet Address Physical Address Type

192.168.100.1 f8-bf-09-85-6a-1e dynamic

192.168.100.30 ac-67-84-60-d1-5b dynamic

192.168.100.31 dc-e5-5b-44-b0-95 dynamic

192.168.100.255 ff-ff-ff-ff-ff-ff static

224.0.0.7 01-00-5e-00-00-07 static

224.0.0.22 01-00-5e-00-00-16 static

224.0.0.250 01-00-5e-00-00-fa static

224.0.0.251 01-00-5e-00-00-fb static

224.0.0.252 01-00-5e-00-00-fc static

239.255.255.250 01-00-5e-7f-ff-fa static

239.255.255.251 01-00-5e-7f-ff-fb static

255.255.255.255 ff-ff-ff-ff-ff-ff static

Interface: 172.21.208.1 --- 0x36

Internet Address Physical Address Type

172.21.223.255 ff-ff-ff-ff-ff-ff static

224.0.0.7 01-00-5e-00-00-07 static

224.0.0.22 01-00-5e-00-00-16 static

224.0.0.250 01-00-5e-00-00-fa static

224.0.0.251 01-00-5e-00-00-fb static

224.0.0.252 01-00-5e-00-00-fc static

224.0.1.187 01-00-5e-00-01-bb static

239.192.152.143 01-00-5e-40-98-8f static

239.255.255.250 01-00-5e-7f-ff-fa static

239.255.255.251 01-00-5e-7f-ff-fb static

255.255.255.255 ff-ff-ff-ff-ff-ff static

Interface: 172.30.16.1 --- 0x42

Internet Address Physical Address Type

172.30.31.255 ff-ff-ff-ff-ff-ff static

224.0.0.7 01-00-5e-00-00-07 static

224.0.0.22 01-00-5e-00-00-16 static

224.0.0.250 01-00-5e-00-00-fa static

224.0.0.251 01-00-5e-00-00-fb static

224.0.0.252 01-00-5e-00-00-fc static

224.0.1.187 01-00-5e-00-01-bb static

239.192.152.143 01-00-5e-40-98-8f static

239.255.255.250 01-00-5e-7f-ff-fa static

239.255.255.251 01-00-5e-7f-ff-fb static

1. Use the **route** command and paste the output from the routing table on your system:

-We can do this with the command **route print**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| IPv4 Route Table |  |  |  |  |
|  |  |  |  |  |
| Active Routes: |  |  |  |  |
| Network Destination | Netmask | Gateway | Interface | Metric |
| 0.0.0.0 | 0.0.0.0 | 192.168.100.1 | 192.168.100.29 | 45 |
| 127.0.0.0 | 255.0.0.0 | On-link | 127.0.0.1 | 331 |
| 127.0.0.1 | 255.255.255.255 | On-link | 127.0.0.1 | 331 |
| 127.255.255.255 | 255.255.255.255 | On-link | 127.0.0.1 | 331 |
| 172.21.208.0 | 255.255.240.0 | On-link | 172.21.208.1 | 5256 |
| 172.21.208.1 | 255.255.255.255 | On-link | 172.21.208.1 | 5256 |
| 172.21.223.255 | 255.255.255.255 | On-link | 172.21.208.1 | 5256 |
| 172.30.16.0 | 255.255.240.0 | On-link | 172.30.16.1 | 5256 |
| 172.30.16.1 | 255.255.255.255 | On-link | 172.30.16.1 | 5256 |
| 172.30.31.255 | 255.255.255.255 | On-link | 172.30.16.1 | 5256 |
| 192.168.56.0 | 255.255.255.0 | On-link | 192.168.56.1 | 281 |
| 192.168.56.1 | 255.255.255.255 | On-link | 192.168.56.1 | 281 |
| 192.168.56.255 | 255.255.255.255 | On-link | 192.168.56.1 | 281 |
| 192.168.100.0 | 255.255.255.0 | On-link | 192.168.100.29 | 301 |
| 192.168.100.29 | 255.255.255.25 | On-link | 192.168.100.29 | 301 |
| 192.168.100.255 | 255.255.255.255 | On-link | 192.168.100.29 | 301 |
| 224.0.0.0 | 240.0.0.0 | On-link | 127.0.0.1 | 331 |
| 224.0.0.0 | 240.0.0.0 | On-link | 192.168.56.1 | 281 |
| 224.0.0.0 | 240.0.0.0 | On-link | 192.168.100.29 | 301 |
| 224.0.0.0 | 240.0.0.0 | On-link | 172.21.208.1 | 5256 |
| 224.0.0.0 | 240.0.0.0 | On-link | 172.30.16.1 | 5256 |
| 255.255.255.255 | 255.255.255.255 | On-link | 127.0.0.1 | 331 |
| 255.255.255.255 | 255.255.255.255 | On-link | 192.168.56.1 | 281 |
| 255.255.255.255 | 255.255.255.255 | On-link | 192.168.100.29 | 301 |
| 255.255.255.255 | 255.255.255.255 | On-link | 172.21.208.1 | 5256 |
| 255.255.255.255 | 255.255.255.255 | On-link | 172.30.16.1 | 5256 |

1. Use the **traceroute** command on your system and observe the hops to Google’s DNS,8.8.8.8. Paste the full output from the command bellow showing all the hops from yoursystem to 8.8.8.8

-We can use the command **tracert 8.8.8.8**

Tracing route to dns.google [8.8.8.8]

over a maximum of 30 hops:

1 3 ms 4 ms 2 ms 192.168.100.1

2 7 ms 10 ms 7 ms 62.162.200.210

3 8 ms 9 ms 7 ms 62.162.201.9

4 14 ms 18 ms 12 ms 95.158.152.45

5 \* \* 21 ms 95.158.131.238

6 16 ms 14 ms 13 ms 95.158.188.213

7 48 ms 47 ms 44 ms 108.170.250.177

8 43 ms 43 ms 40 ms 216.239.49.217

9 41 ms 41 ms 41 ms dns.google [8.8.8.8]

1. Why would you need to use the **ping** command?

Answer: Ping is utility that sends signal to another computer over a network and then receives a reply from the computer that was pinged and sends it back to the computer. We use ping to troubleshoot connectivity, reachability and name resolution over the Internet Protocol TCP/IP. With the ping command we can quickly determine if a machine has internet access and can communicate with other computers or network devices.

1. Write down the TCP/UDP ports of the most commonly used services bellow in theform of TCP[PORT] or UDP[PORT]

• HTTP – TCP80

• SNMP – UDP161

• HTTPS - TCP443

• DNS client – UDP53/TCP53

• DNS zone transfer – TCP53

• SMTP - TCP25

• SSH - TCP22

• FTP - TCP21

• Telnet - TCP23

• MSSQL - TCP1433

• MySQL - TCP3306

• PostgreSQL – TCP5432

• RDP (Remote Desktop Protocol) - TCP3389

• NTP – UDP123

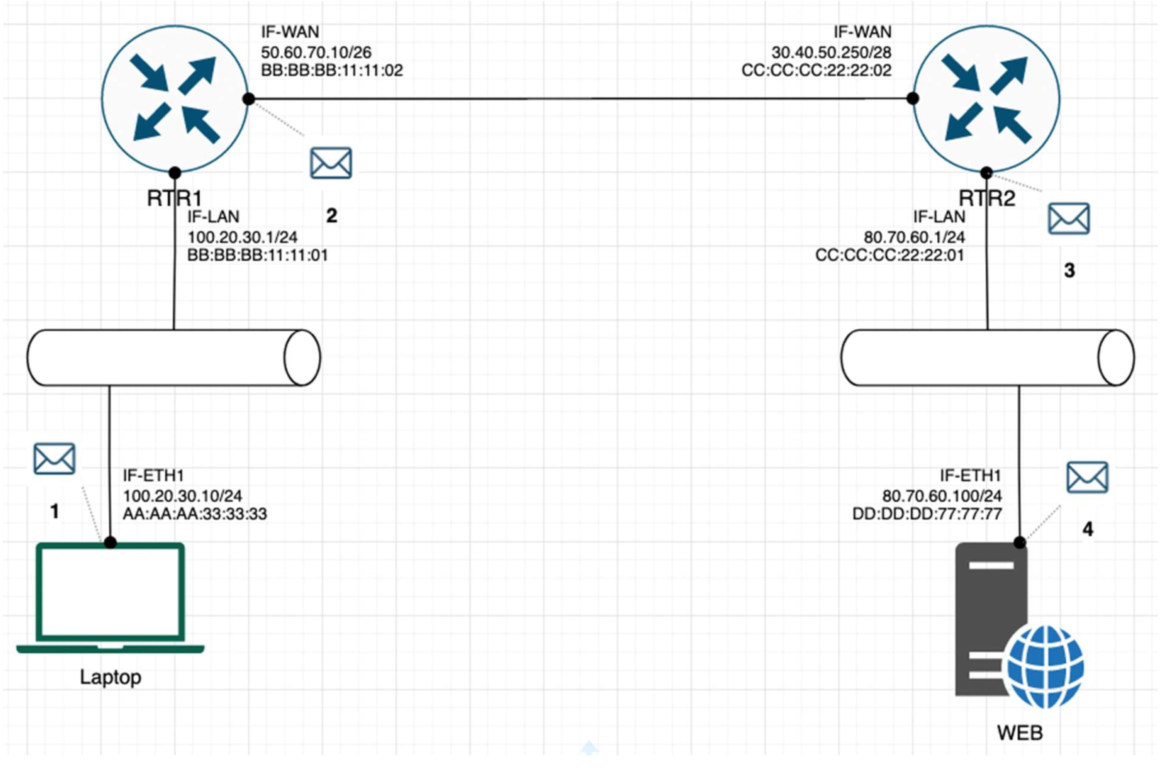
• NFS –TCP/UDP2049 and TCP/UDP111 for portmapper

## Exercise 2 – TCP/IP Basics

**Refer to the exhibit and answer the questions below.**

The letter symbol ✉, represents the IP packet as it travels across the network.

In the example shown, the laptop attempts to communicate with the web server in question. During its travel the packet will be forwarded across the network nodes and will eventually end up across six network interfaces before it reaches the web server. Each packet as part of the TCP/IP Stack contains fields for the source and destination MAC Address, IP Address and the TCP/UDP Port.



**For each of the packet locations shown, 1 to 4 write down the source and destination MAC addresses of the packet as it travels across the network interfaces.**

1. The laptop initiates communication with the web server and prepares a packet. What would the packet look like at this stage?

* SRC IP: 100.20.30.10/24
* DST IP: 80:70:60.100/24
* SRC MAC: AA:AA:AA:33:33:33
* DST MAC: BB:BB:BB:11:11:01

2. RTR1 receives the packet on its IF-LAN interface, prepares it accordingly and forwards it out its IFWAN. What would the packet look like at this stage?

* SRC IP: 100.20.30.10/24
* DST IP: 80:70:60.100/24
* SRC MAC: BB:BB:BB:11:11:02
* DST MAC: CC:CC:CC:22:22:01

3. RTR2 receives the packet on its IF-WAN interface, prepares it accordingly and forwards it out via IFLAN. What would the packet look like at this stage?

* SRC IP: 100.20.30.10/24
* DST IP: 80:70:60.100/24
* SRC MAC: CC:CC:CC:22:22:01
* DST MAC: DD:DD:DD:77:77:77

4. The web server receives the packet and prepares a response packet back. What would the packet look like at this stage?

* SRC IP: 80:70:60.100/24
* DST IP: 100.20.30.10/24
* SRC MAC: DD:DD:DD:77:77:77
* DST MAC: CC:CC:CC:22:22:01

**Since we are talking about web traffic (www) in the example, which transport layer protocol will most probably be used?**

* TCP
* UDP

**If we do a traffic analysis with a network packet monitoring tool like Wireshark, what can we expect to see for the source and destination ports when the laptop sends the packet?**

* SRC PORT: Ephemeral ports range 1024 – 65535
* DST PORT: port 80 (or 443 if it is https)

**Similarly, and vice versa, what can we expect to see as destination ports when the Web server sends a response packet back?**

* SRC PORT: port 80 (or 443 if it is https)
* DST PORT: The ephemeral port that was used to start the communication.

**How many broadcast domains are there in the exhibit shown?**

There are 3 broadcast domains

## Exercise 3 – Traffic analysis and identifying the OSI layers of the network packets

**Prerequisite:**

Search online and get familiar with the TCP’s three-way handshake. Learn how to capture the three-way handshake using Wireshark.

Install Wireshark on your computer and use it to capture traffic against a website or a server or your choice. It is recommended that you capture traffic against a simple website.

Name and the IP address of the website you plan to capture traffic: spacefre.com / 168.119.151.119

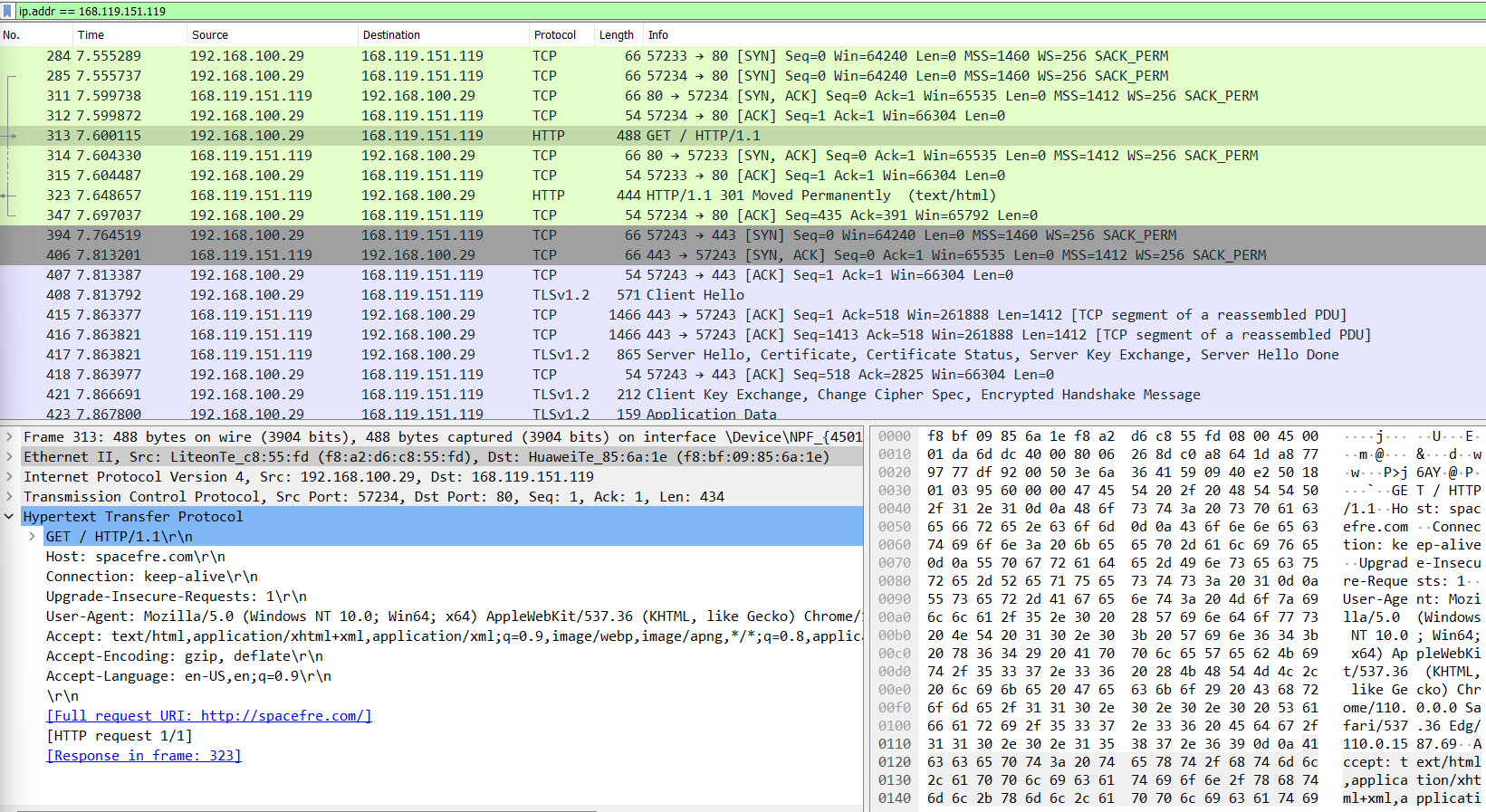
**Analyze the TCP’s three-way handshake and using screenshots from the Wireshark window answer the questions bellow:**

1. What is the source IP (of the initiating host):

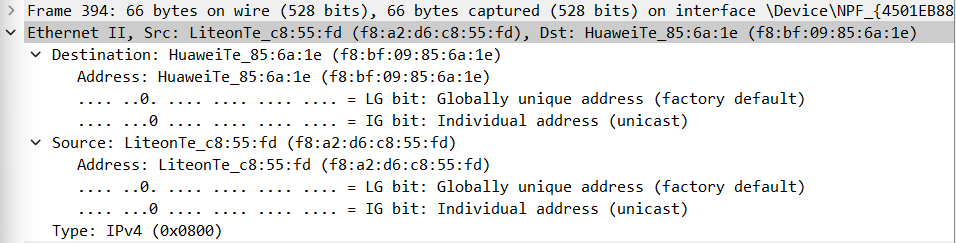
The source IP is 192.168.100.29

2. What is the destination IP? (target website):

The destination IP is 168.119.151.119



**Identify the Network Interface (Layer 1 & 2) section of the SYN packet and paste a screenshot from it:**

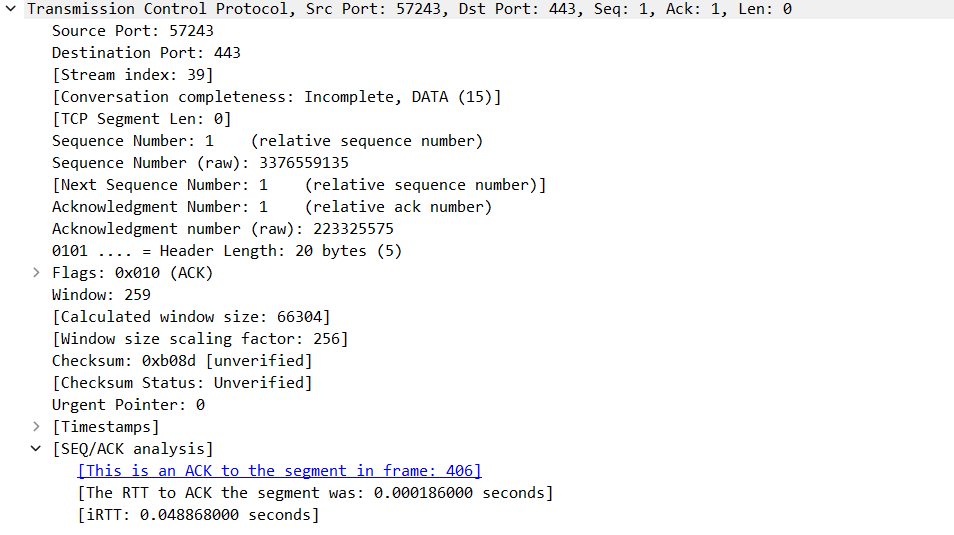
****

**Identify the Network Layer 3 section of the SYN/ACK packet and paste a screenshot from it**:

**Graphical user interface, text

Description automatically generated**

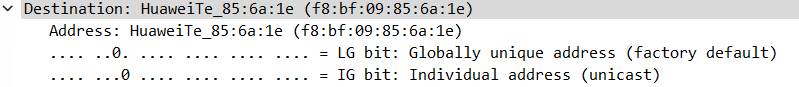
**Identify the Transport Layer 4 section of the ACK packet and paste a screenshot from it bellow:**



Look closely at the L2 section of the three-way handshake packet details. Each of them shows the source and destination MAC address of the packets.

**Who is the owner of the destination MAC address of the SYN packet?**

The owner of the destination MAC address of the SYN packet is my Huawei router



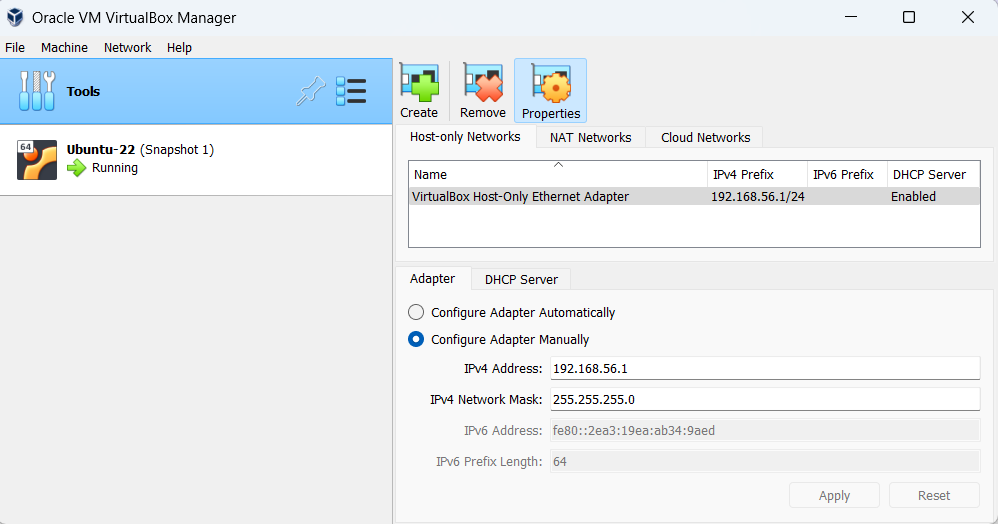
## Exercise 4 – Hacking mockup (for Bonus points)

Use Wireshark to capture the packet’s application layer data and discover the implications of using unencrypted communication over a network.

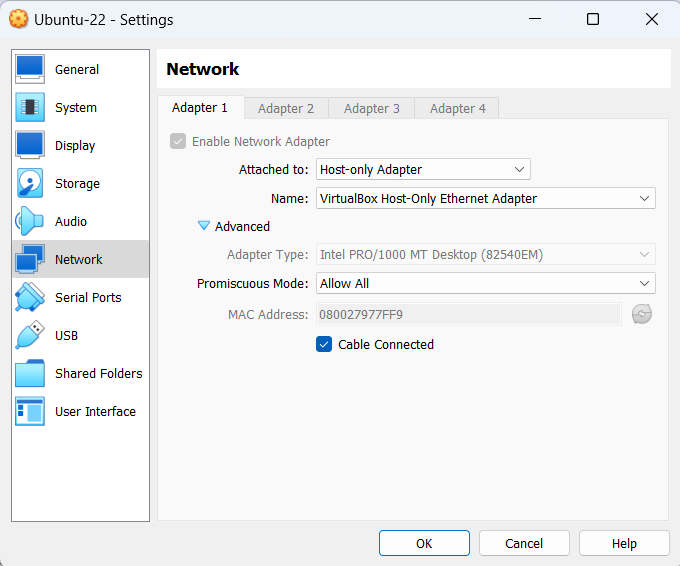
It is recommended that you use your own Linux Virtual Machine on your system on which you need to confiture a telnet server.

From your own system try to login with a Telnet on the target VM all while capturing the traffic with a Wireshark. As a proof of competition for this exercise paste in bellow a screenshot of the application layer data containing visible username and password.

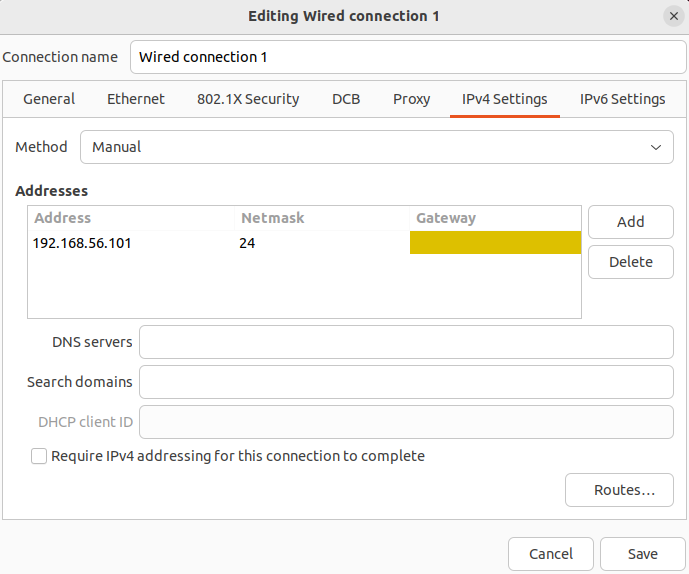
* First, we set host-only adapter in VirtualBox with static IP



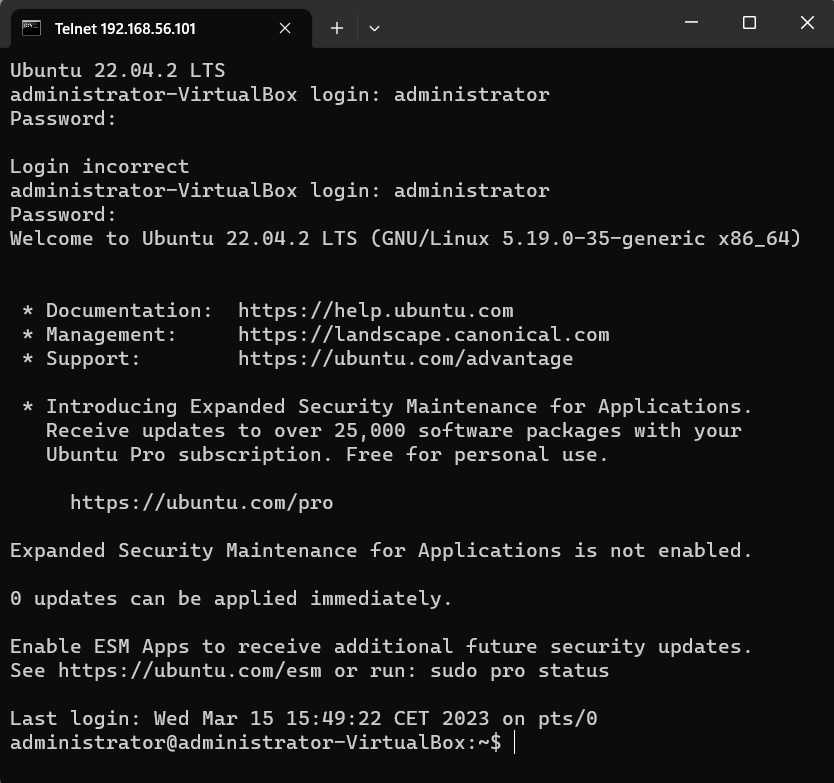
* Then we select the adapter for our VM



* After that we login to our VM and set static IP



* Now we start capturing with Wireshark and can Telnet from CMD



* Now we can review the results in Wireshark

Graphical user interface, application, table

Description automatically generated

* And we can follow the stream to find the user input that was captured

