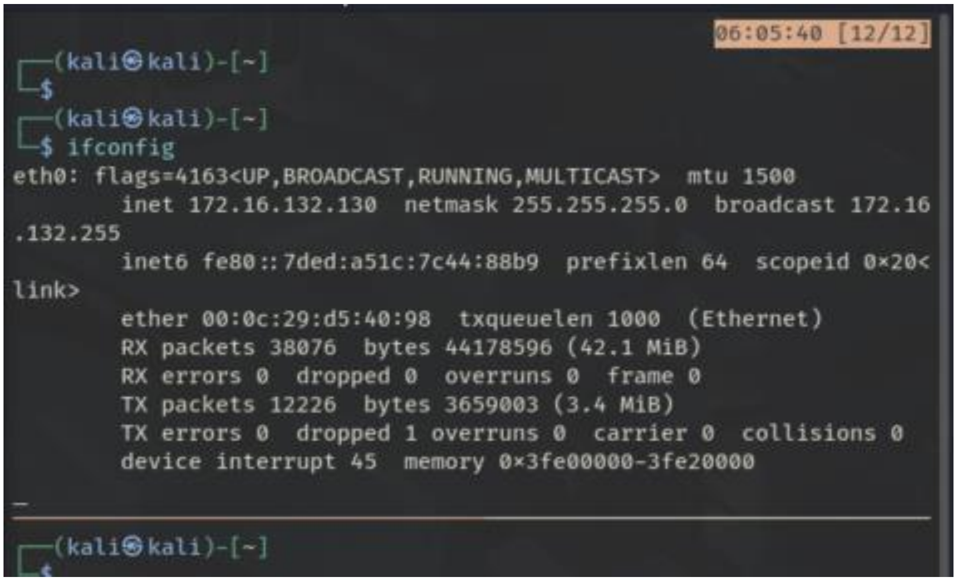
Task 1

1. Nmap installation (I personally use kali linux which has Nmap pre-installed but for the sake of this task i will provide with the method to install Nmap)
   - Go to the official Nmap website by searching the keyword “Nmap” in google or directly click this link: https://nmap.org/download
   - Then when you reach this link select the OS you use to install Nmap for it.
2. After Nmap is installed, to find your local IP range use the following command: for linux/macOS “ifconfig”

   Windows”ipconfig”

   My output:

   ```
                                                          06:05:40 [12/12]
   ┌──(kali㉿kali)-[~]
   └─$
   ┌──(kali㉿kali)-[~]
   └─$ ifconfig
   eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
           inet 172.16.132.130  netmask 255.255.255.0  broadcast 172.16
   .132.255
           inet6 fe80::7ded:a51c:7c44:88b9  prefixlen 64  scopeid 0x20<
   link>
           ether 00:0c:29:d5:40:98  txqueuelen 1000  (Ethernet)
           RX packets 38076  bytes 44178596 (42.1 MiB)
           RX errors 0  dropped 0  overruns 0  frame 0
           TX packets 12226  bytes 3659003 (3.4 MiB)
           TX errors 0  dropped 1 overruns 0  carrier 0  collisions 0
           device interrupt 45  memory 0x3fe00000-3fe20000

   ┌──(kali㉿kali)-[~]
   └─$
   ```

   From here we can see eth0 which is our local network card the 3 important points in this output is ip address, netmask, Broadcast

   - IP address: 172.16.132.130
   - Netmask: 255.255.255.0
   - Broadcast: 172.16.132.255

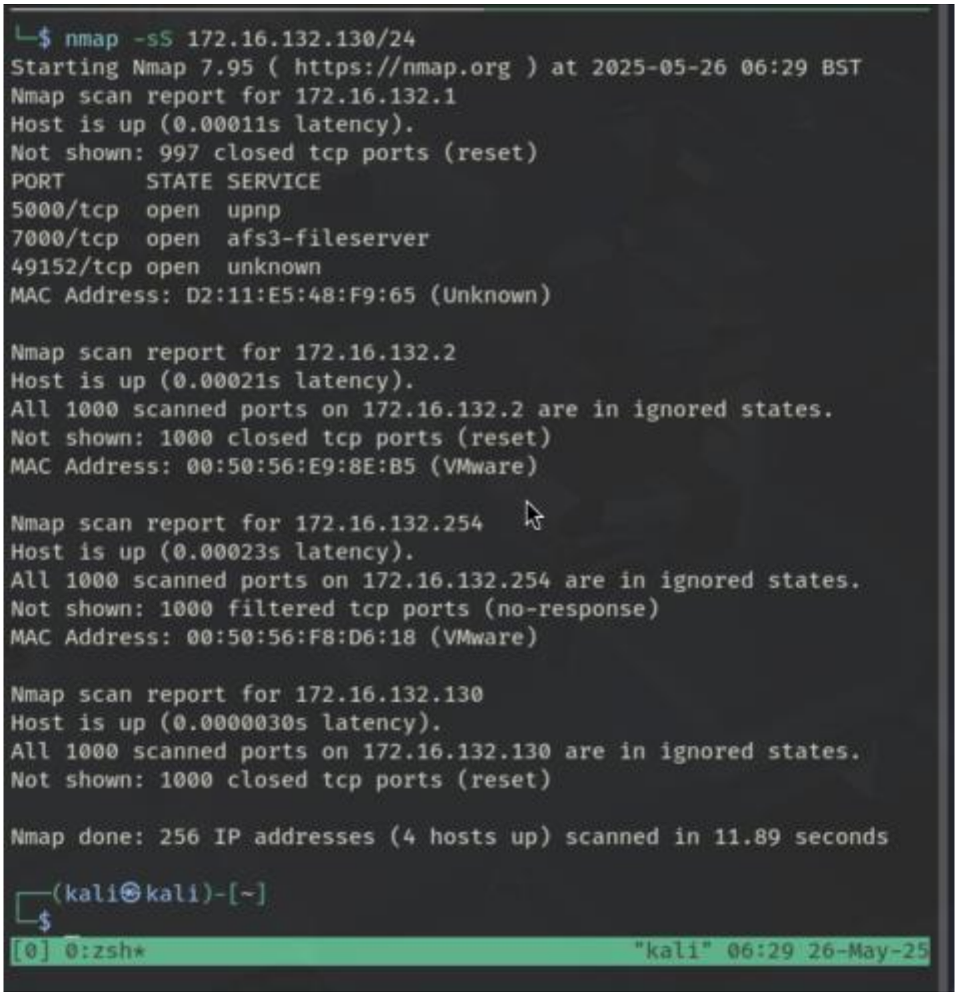
   From this we can infer

   Our ip range : 172.16.132.130/24

   Meaning our usable range will me from 172.16.132.1 to 172.16.132.254

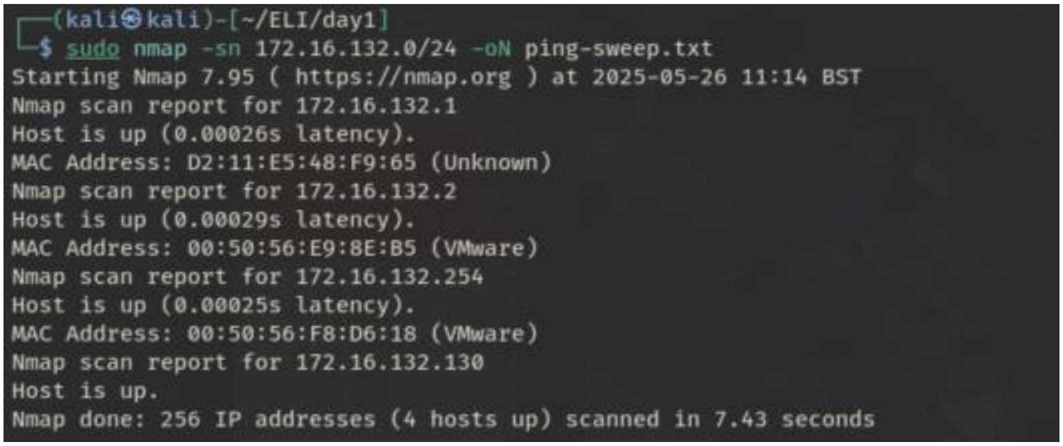
   172.16.132.255 is our broadcast IP
3. Nmap scan to see open and usable ports:

   Basic Nmap scan:



```
└─$ nmap -sS 172.16.132.130/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-26 06:29 BST
Nmap scan report for 172.16.132.1
Host is up (0.00011s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
5000/tcp  open  upnp
7000/tcp  open  afs3-fileserver
49152/tcp open  unknown
MAC Address: D2:11:E5:48:F9:65 (Unknown)

Nmap scan report for 172.16.132.2
Host is up (0.00021s latency).
All 1000 scanned ports on 172.16.132.2 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 00:50:56:E9:8E:B5 (VMware)

Nmap scan report for 172.16.132.254
Host is up (0.00023s latency).
All 1000 scanned ports on 172.16.132.254 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:50:56:F8:D6:18 (VMware)

Nmap scan report for 172.16.132.130
Host is up (0.0000030s latency).
All 1000 scanned ports on 172.16.132.130 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 256 IP addresses (4 hosts up) scanned in 11.89 seconds

┌──(kali㉿kali)-[~]
└─$
[0] 0:zsh*                                          "kali" 06:29 26-May-25
```

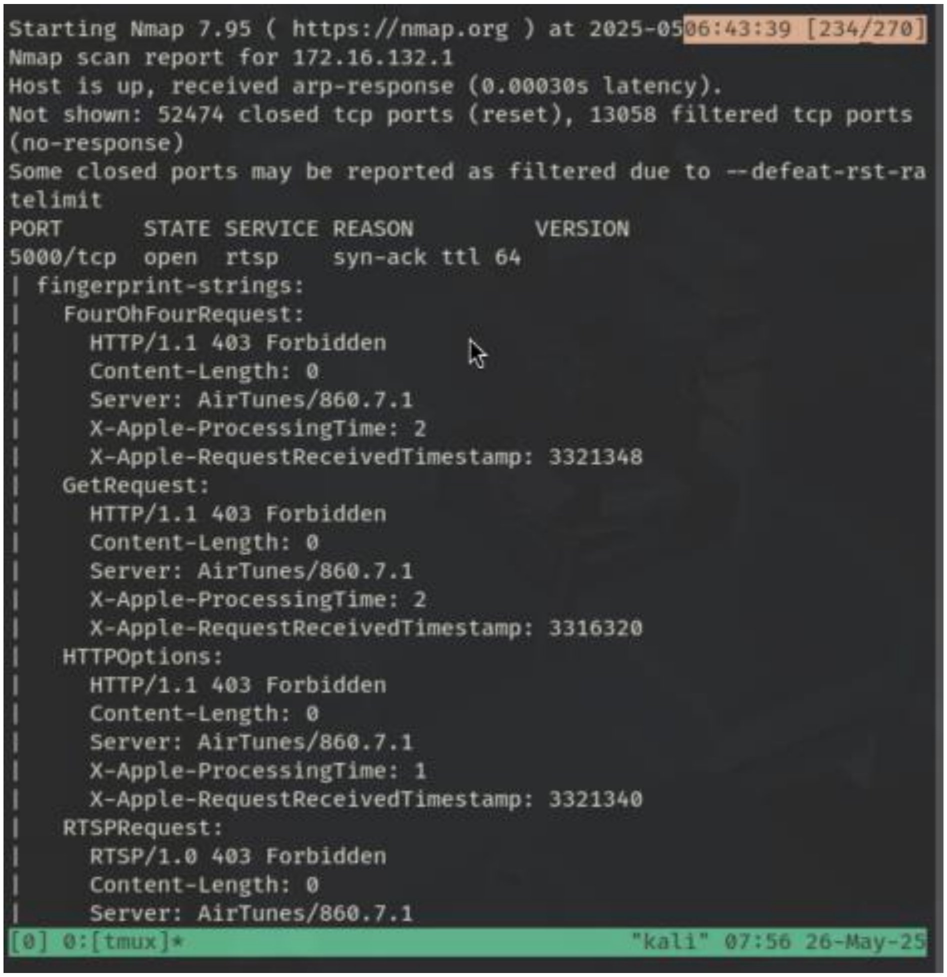
After that lets run ping sweep to verify how many host we have up on our network:



```
┌──(kali㉿kali)-[~/ELI/day1]
└─$ sudo nmap -sn 172.16.132.0/24 -oN ping-sweep.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-26 11:14 BST
Nmap scan report for 172.16.132.1
Host is up (0.00026s latency).
MAC Address: D2:11:E5:48:F9:65 (Unknown)
Nmap scan report for 172.16.132.2
Host is up (0.00029s latency).
MAC Address: 00:50:56:E9:8E:B5 (VMware)
Nmap scan report for 172.16.132.254
Host is up (0.00025s latency).
MAC Address: 00:50:56:F8:D6:18 (VMware)
Nmap scan report for 172.16.132.130
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 7.43 seconds
```

As we can see we have 4 hosts up which matches our basic and full nmap scan reports.

Advanced Nmap scan : “sudo nmap -A -T4 -p- 172.16.132.0/24 --max-retries 3 --open --reason -oN fullscan.txt”



```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-0506:43:39 [234/270]
Nmap scan report for 172.16.132.1
Host is up, received arp-response (0.00030s latency).
Not shown: 52474 closed tcp ports (reset), 13058 filtered tcp ports
(no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ra
telimit
PORT      STATE SERVICE REASON         VERSION
5000/tcp  open  rtsp    syn-ack ttl 64
| fingerprint-strings:
|   FourOhFourRequest:
|     HTTP/1.1 403 Forbidden
|     Content-Length: 0
|     Server: AirTunes/860.7.1
|     X-Apple-ProcessingTime: 2
|     X-Apple-RequestReceivedTimestamp: 3321348
|   GetRequest:
|     HTTP/1.1 403 Forbidden
|     Content-Length: 0
|     Server: AirTunes/860.7.1
|     X-Apple-ProcessingTime: 2
|     X-Apple-RequestReceivedTimestamp: 3316320
|   HTTPOptions:
|     HTTP/1.1 403 Forbidden
|     Content-Length: 0
|     Server: AirTunes/860.7.1
|     X-Apple-ProcessingTime: 1
|     X-Apple-RequestReceivedTimestamp: 3321340
|   RTSPRequest:
|     RTSP/1.0 403 Forbidden
|     Content-Length: 0
|     Server: AirTunes/860.7.1
[0] 0:[tmux]*                                      "kali" 07:56 26-May-25
```

Note: this is only starting part of the output the full can be viewed in the fullscan.txt file attached in the github repository

Why i used this command and what does it do:

Nmap –A means it will scan all of the simple scans we use individualy(eg. sS sV)

-T4 : this adjust the speed of the scan which is perfect for our case

-p- : it will scan all 65535 tcp ports

--max-retries3 : it will stop scanning if the host is unresponsive

--open : it will filter all cloed ports for us saving us time and only showing open ports

--reason: will show us why our port was showed to be open it is good for ctf purposes and real time pentesting

-oN fullscan.txt : simple command to save our output in a file for backup a purposes

So out of 65535 ports we found 52474 closed ports 13058 filtered ports meaning no response from them and then we found 3 usable ports on the IP address: 172.16.132.1 which has 3 open ports:

5000/tcp

7000/tcp

49152/tcp

Then the second ip address 172.16.132.2 which had no open ports

And third 172.16.132.130 which is my own IP and had no open ports thankfully

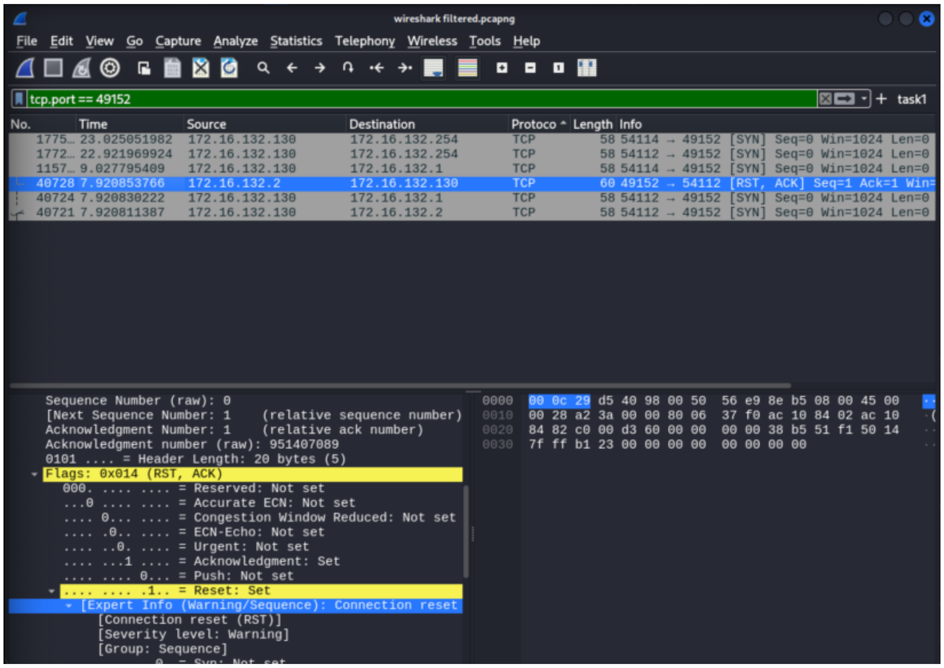
From this we can try and see potential treats from the open ports:

From our report we see that port 5000 and 7000 are using the rtsp protocol which is real time streaming protocol and the server it is running on is Airtunes which is a application that allows apple devices to stream any kind of media wirelessly. its version is 860.7.1 which does not have any registered vulnerablilities and airtunes was rebranded to airplay in 2010 which does not help us finding about it vulnerabilities.
NOTE: In our basic scan the service given for 7000/tcp was afs3-fileserver which was based on the port number which is by defualt used on 7000 and when we do the fullscan we can see it fully analyses the port and gives us the actual service on it.

Now for the open port 49152/tcp we will analyse it using a tool called wireshark

Wireshark is a packet analysing tool that helps you anlyse individual packets send and recieved on the network.

When we apply a display fiter in wireshark to sisplay only the packets related to the port 49152 mostly everything is normal except 1 packet where a series of tcp connection request attempts were made from 172.16.132.130 but were refused meaning the target host is refusing connection most likely because of a firewall
This is bad for security reasons because instead of silent dropping the packet the host is sending the RST response which will give away its network presence

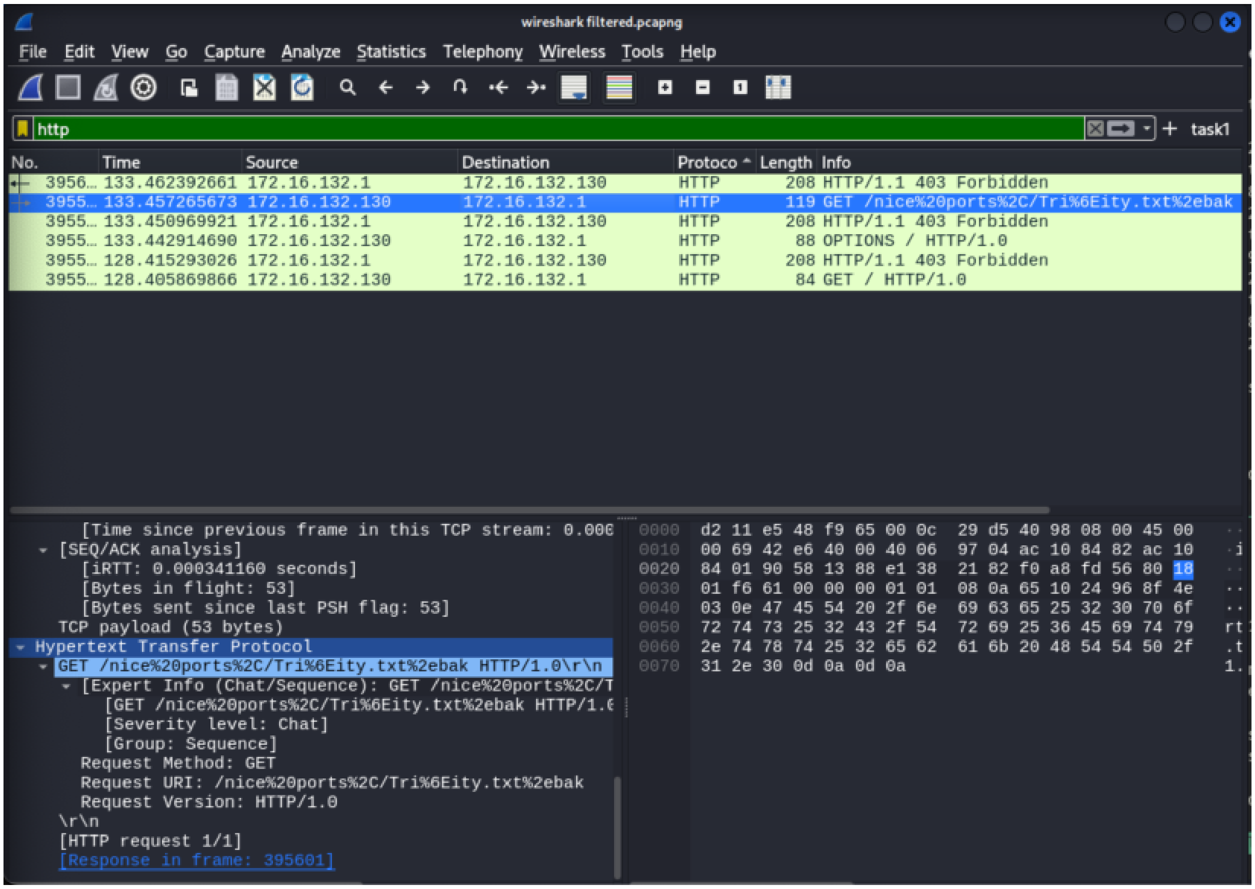

wireshark filtered.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
task1

```
tcp.port == 49152

No.        Time          Source          Destination      Protoco ^ Length Info
1775…  23.025051982  172.16.132.130  172.16.132.254   TCP       58 54114 → 49152 [SYN] Seq=0 Win=1024 Len=0
1772…  22.921969924  172.16.132.130  172.16.132.254   TCP       58 54112 → 49152 [SYN] Seq=0 Win=1024 Len=0
1157…  9.027795409   172.16.132.130  172.16.132.1     TCP       58 54114 → 49152 [SYN] Seq=0 Win=1024 Len=0
40728  7.920853766   172.16.132.2    172.16.132.130   TCP       60 49152 → 54112 [RST, ACK] Seq=1 Ack=1 Win=
40724  7.920830222   172.16.132.130  172.16.132.1     TCP       58 54112 → 49152 [SYN] Seq=0 Win=1024 Len=0
40721  7.920811387   172.16.132.130  172.16.132.2     TCP       58 54112 → 49152 [SYN] Seq=0 Win=1024 Len=0
```

```
    Sequence Number (raw): 0
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 951407089
    0101 .... = Header Length: 20 bytes (5)
  ▾ Flags: 0x014 (RST, ACK)
      000. .... .... = Reserved: Not set
      ...0 .... .... = Accurate ECN: Not set
      .... 0... .... = Congestion Window Reduced: Not set
      .... .0.. .... = ECN-Echo: Not set
      .... ..0. .... = Urgent: Not set
      .... ...1 .... = Acknowledgment: Set
      .... .... 0... = Push: Not set
    ▾ .... .... .1.. = Reset: Set
      ▾ [Expert Info (Warning/Sequence): Connection reset
            [Connection reset (RST)]
            [Severity level: Warning]
            [Group: Sequence]
```

```
0000  00 0c 29 d5 40 98 00 50  56 e9 8e b5 08 00 45 00   ..
0010  00 28 a2 3a 00 00 80 06  37 f0 ac 10 84 02 ac 10   .(
0020  84 82 c0 00 d3 60 00 00  00 00 38 b5 51 f1 50 14   ..
0030  7f ff b1 23 00 00 00 00  00 00 00 00               ..
```

Also i put up a http request filter but nothing was wrong in it


wireshark filtered.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
task1

```
http

No.    Time           Source          Destination     Protoco ^ Length Info
3956…  133.462392661  172.16.132.1    172.16.132.130  HTTP      208 HTTP/1.1 403 Forbidden
3955…  133.457265673  172.16.132.130  172.16.132.1    HTTP      119 GET /nice%20ports%2C/Tri%6Eity.txt%2ebak
3955…  133.450969921  172.16.132.1    172.16.132.130  HTTP      208 HTTP/1.1 403 Forbidden
3955…  133.442914690  172.16.132.130  172.16.132.1    HTTP       88 OPTIONS / HTTP/1.0
3955…  128.415293026  172.16.132.1    172.16.132.130  HTTP      208 HTTP/1.1 403 Forbidden
3955…  128.405869866  172.16.132.130  172.16.132.1    HTTP       84 GET / HTTP/1.0
```

```
      [Time since previous frame in this TCP stream: 0.000
    ▾ [SEQ/ACK analysis]
        [iRTT: 0.000341160 seconds]
        [Bytes in flight: 53]
        [Bytes sent since last PSH flag: 53]
    TCP payload (53 bytes)
▾ Hypertext Transfer Protocol
  ▾ GET /nice%20ports%2C/Tri%6Eity.txt%2ebak HTTP/1.0\r\n
    ▾ [Expert Info (Chat/Sequence): GET /nice%20ports%2C/T
          [GET /nice%20ports%2C/Tri%6Eity.txt%2ebak HTTP/1.0
          [Severity level: Chat]
          [Group: Sequence]
      Request Method: GET
      Request URI: /nice%20ports%2C/Tri%6Eity.txt%2ebak
      Request Version: HTTP/1.0
    \r\n
    [HTTP request 1/1]
    [Response in frame: 395601]
```

```
0000  d2 11 e5 48 f9 65 00 0c  29 d5 40 98 08 00 45 00   ..
0010  00 69 42 e6 40 00 40 06  97 04 ac 10 84 82 ac 10   .i
0020  84 01 90 58 13 88 e1 38  21 82 f0 a8 fd 56 80 18   ..
0030  01 f6 61 00 00 00 01 01  08 0a 65 10 24 96 8f 4e   ..
0040  03 0e 47 45 54 20 2f 6e  69 63 65 25 32 30 70 6f   ..
0050  72 74 73 25 32 43 2f 54  72 69 25 36 45 69 74 79   rt
0060  2e 74 78 74 25 32 65 62  61 6b 20 48 54 54 50 2f   .t
0070  31 2e 30 0d 0a 0d 0a                               1.
```

Overall summary of my network is that there are not many vulnerable devices in it