Kevin Cendana
CSC 154
Spring 2024
Task 1

Lab 03-1 Network Fundamentals and ARP

Step 1) Checking network configurations, such as ip addresses, on both Kali & Windows

```
┌──(kevin㉿kali)-[~/Desktop]
└─$ 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:ba:c7:90 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute eth0
       valid_lft 85610sec preferred_lft 85610sec
    inet6 fe80::a00:27ff:feba:c790/64 scope link noprefixroute
       valid_lft forever preferred_lft forever

┌──(kevin㉿kali)-[~/Desktop]
└─$ $$$
```

```
Command Prompt
Microsoft Windows [Version 10.0.19045.2965]
(c) Microsoft Corporation. All rights reserved.

C:\Users\kevin>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : csus.edu
   Link-local IPv6 Address . . . . . : fe80::9d85:f149:4368:61f%3
   IPv4 Address. . . . . . . . . . . : 10.0.2.15
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.0.2.2

C:\Users\kevin>
```

Step 2) Modify Windows firewall to allow other VMs to interact with it.

File and Printer Sharing (Echo Request - I...	File and Printer Sharing	Private...	Yes	Allow
File and Printer Sharing (Echo Request - I...	File and Printer Sharing	Domain	Yes	Allow

Step 3) Pinging Windows & Kali OS together, checking if they can reach each other

```
┌──(kevin㉿kali)-[~/Desktop]
└─$ ping -c 4 10.0.2.15
PING 10.0.2.15 (10.0.2.15) 56(84) bytes of data.
64 bytes from 10.0.2.15: icmp_seq=1 ttl=64 time=0.027 ms
64 bytes from 10.0.2.15: icmp_seq=2 ttl=64 time=0.136 ms
64 bytes from 10.0.2.15: icmp_seq=3 ttl=64 time=0.111 ms
64 bytes from 10.0.2.15: icmp_seq=4 ttl=64 time=0.209 ms

--- 10.0.2.15 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3034ms
rtt min/avg/max/mdev = 0.027/0.120/0.209/0.065 ms

┌──(kevin㉿kali)-[~/Desktop]
```

```
:\Users\kevin>ping 10.0.2.15

inging 10.0.2.15 with 32 bytes of data:
eply from 10.0.2.15: bytes=32 time<1ms TTL=128
eply from 10.0.2.15: bytes=32 time<1ms TTL=128
eply from 10.0.2.15: bytes=32 time<1ms TTL=128
eply from 10.0.2.15: bytes=32 time<1ms TTL=128

ing statistics for 10.0.2.15:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
pproximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

:\Users\kevin>
```

Step 4) Using traceroute/tracert to see Google's path packets

```
┌──(kevin㉿kali)-[~/Desktop]
└─$ traceroute google.com
traceroute to google.com (142.250.191.46), 30 hops max, 60 byte packets
 1  10.0.2.2 (10.0.2.2)  0.363 ms  0.251 ms  0.135 ms
 2  10.113.255.254 (10.113.255.254)  3.861 ms  3.741 ms  3.637 ms
 3  130.86.1.252 (130.86.1.252)  8.019 ms  7.940 ms  7.842 ms
 4  130.86.249.166 (130.86.249.166)  8.112 ms  7.650 ms  7.904 ms
 5  dc-sac-dc2--sac-csu-cmf.cenic.net (137.164.41.201)  7.810 ms  7.727 ms  7
.285 ms
 6  sacr1-agg-01--sac-csu-2--100g--01.cenic.net (137.164.35.8)  9.183 ms  10.
871 ms  10.539 ms
 7  emvl1-agg-01--sacr1-agg-01--100g--01.cenic.net (137.164.11.98)  10.242 ms
  7.267 ms  9.026 ms
 8  svl-agg10--emvl1-agg-01--400g--01.cenic.net (137.164.11.94)  8.944 ms  8.
855 ms  8.748 ms
 9  74.125.50.18 (74.125.50.18)  11.280 ms 142.250.175.184 (142.250.175.184)
 9.235 ms  9.153 ms
10  * * *
11  142.251.65.136 (142.251.65.136)  9.373 ms 142.251.224.30 (142.251.224.30)
  10.707 ms 142.251.224.180 (142.251.224.180)  10.823 ms
12  142.251.65.129 (142.251.65.129)  9.253 ms 192.178.87.150 (192.178.87.150)
  9.695 ms  10.142 ms
13  nuq04s42-in-f14.1e100.net (142.250.191.46)  9.111 ms 192.178.105.99 (192.
178.105.99)  8.958 ms  8.780 ms

┌──(kevin㉿kali)-[~/Desktop]
└─$
```

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

Tracing route to google.com [142.250.191.46]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  10.0.2.2
  2    48 ms     9 ms    10 ms  10.113.255.254
  3     5 ms     4 ms     4 ms  130.86.1.252
  4     5 ms    27 ms     5 ms  130.86.249.166
  5     5 ms     5 ms     6 ms  dc-sac-dc2--sac-csu-cmf.cenic.net [137.164.41.201]
  6    10 ms    27 ms    14 ms  sacr1-agg-01--sac-csu-2--100g--01.cenic.net [137.164.35.8]
  7     9 ms    10 ms     8 ms  emvl1-agg-01--sacr1-agg-01--100g--01.cenic.net [137.164.11.98]
  8    18 ms     8 ms    10 ms  svl-agg10--emvl1-agg-01--400g--01.cenic.net [137.164.11.94]
  9    15 ms    12 ms   430 ms  74.125.50.18
 10   218 ms    15 ms    13 ms  142.251.231.99
 11    33 ms    11 ms    10 ms  142.251.65.129
 12     9 ms    19 ms    19 ms  nuq04s42-in-f14.1e100.net [142.250.191.46]

Trace complete.

C:\Users\kevin>_
```

Step 5) Located Google.com IPs w/ Windows & Kali.

```
┌──(kevin㉿kali)-[~/Desktop]
└─$ nslookup google.com
Server:         130.86.251.251
Address:        130.86.251.251#53

Non-authoritative answer:
Name:   google.com
Address: 142.250.191.46
Name:   google.com
Address: 2607:f8b0:4005:80f::200e


┌──(kevin㉿kali)-[~/Desktop]
└─$
```

```
C:\Users\kevin>nslookup google.com
Server:  ns4.csus.edu
Address:  130.86.251.251

Non-authoritative answer:
Name:    google.com
Addresses:  2607:f8b0:4005:80f::200e
          142.250.191.46


C:\Users\kevin>
```

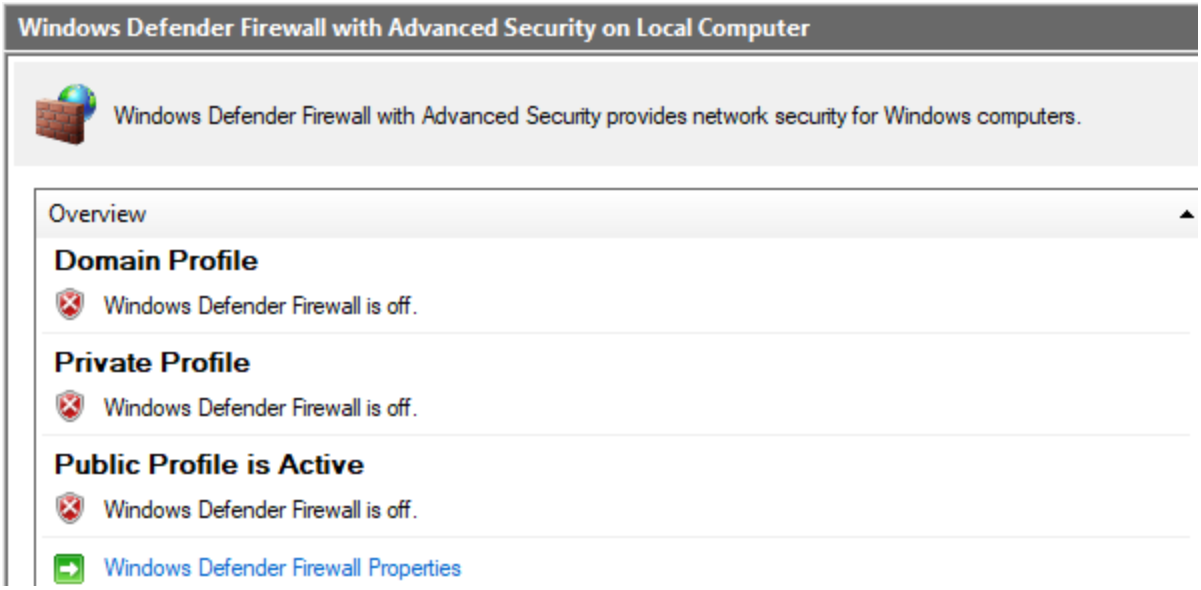
Step 6) Reviewing the open ports - they all say Listening. 1st screenshot has more than 2 but they're far apart in the terminal.

```
unix  2      [ ACC ]     STREAM     LISTENING     18816    @/tmp/.X11-unix/X0
unix  2      [ ACC ]     STREAM     LISTENING     20852    @/tmp/.ICE-unix/91
```

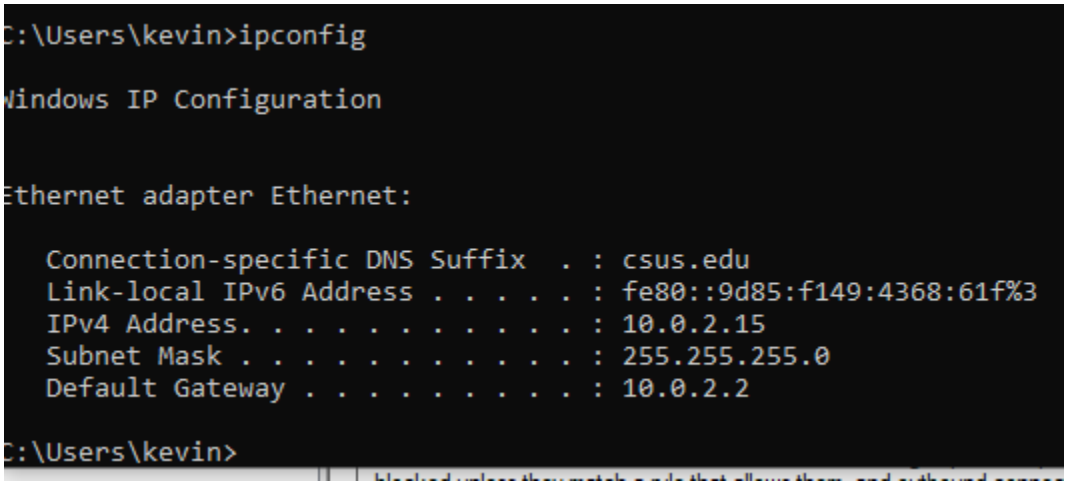
```
TCP    [::]:135              [::]:0                 LISTENING       908
TCP    [::]:445              [::]:0                 LISTENING       4
TCP    [::]:49664            [::]:0                 LISTENING       680
TCP    [::]:49665            [::]:0                 LISTENING       508
TCP    [::]:49666            [::]:0                 LISTENING       1292
TCP    [::]:49667            [::]:0                 LISTENING       1148
TCP    [::]:49668            [::]:0                 LISTENING       2520
TCP    [::]:49670            [::]:0                 LISTENING       644
```

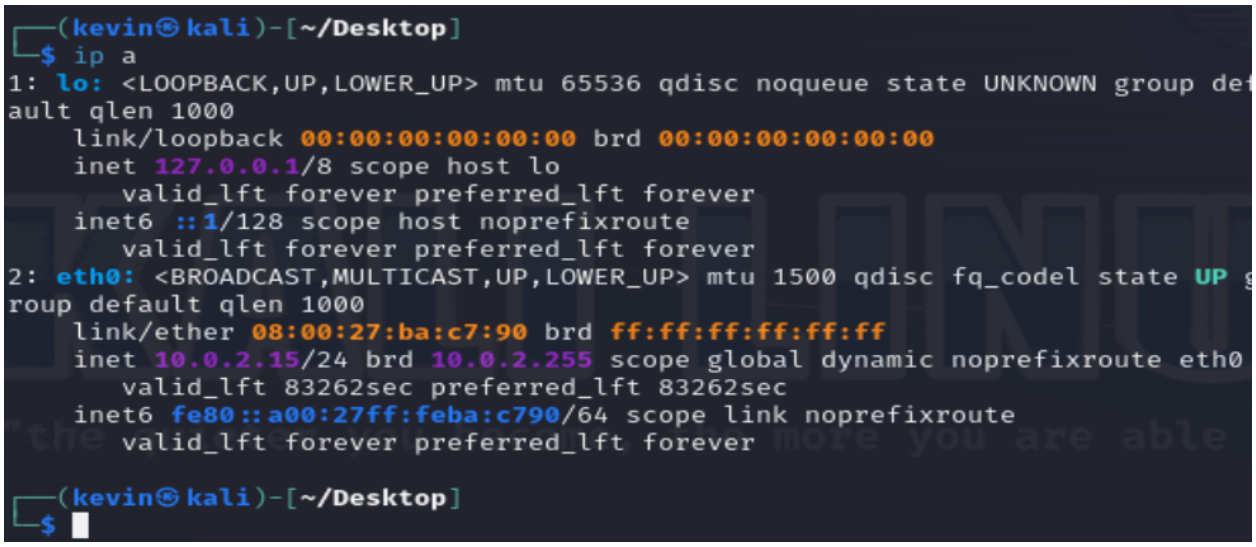
Task 2

Step 1) Turning off Windows firewall for all network traffic.



Step 2) Checking IPs of Windows, Kali to scan network





Step 3) Located live IPs in the network with NMAP

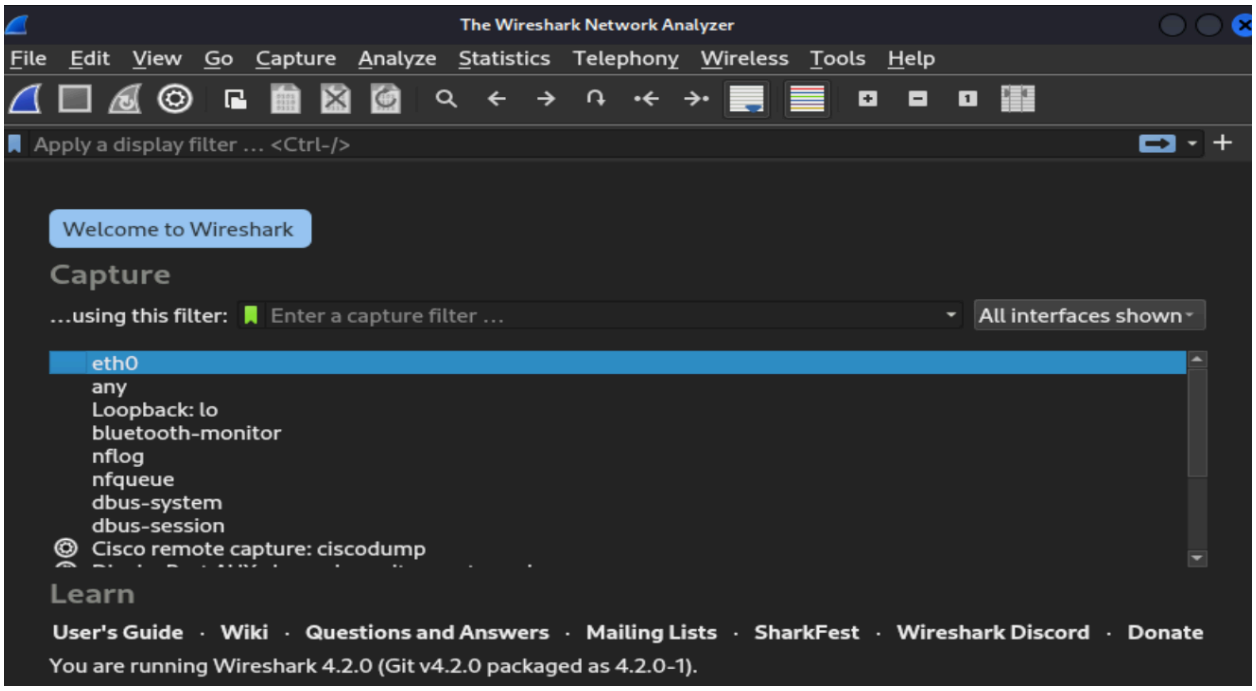
```
┌──(kevin㉿kali)-[~/Desktop]
└─$ nmap -sn 10.0.2.15
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-16 21:26 PST
Nmap scan report for 10.0.2.15
Host is up (0.00061s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.19 seconds
```

Step 4) Scanned Windows VM for open ports and any running services that are vulnerable

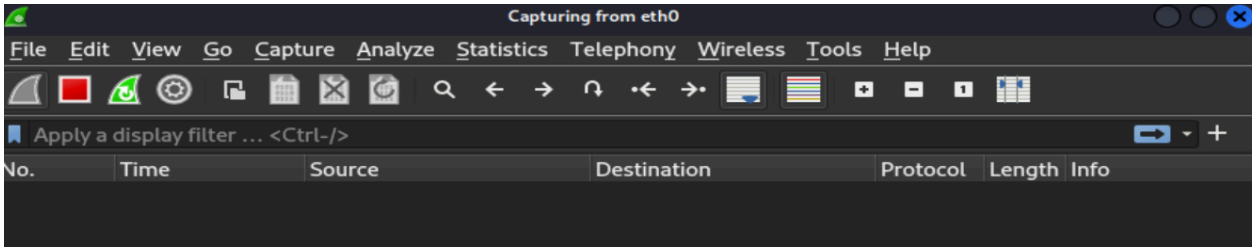
```
┌──(kevin㉿kali)-[~/Desktop]
└─$ nmap -sT -sV -p- 10.0.2.15
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-16 21:28 PST
Nmap scan report for 10.0.2.15
Host is up (0.00014s latency).
All 65535 scanned ports on 10.0.2.15 are in ignored states.
Not shown: 65535 closed tcp ports (conn-refused)

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 3.44 seconds
```

Task 3

Step 1) Launched Wireshark



Step 2) Started capturing packets



Step 3: Visited example.com and analyzed both HTTP/HTTPS traffic.

Wireshark · Follow HTTP Stream (tcp.stream eq 37) · eth0

```
GET / HTTP/1.1
Host: example.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/201001
01 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,imag
e/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Upgrade-Insecure-Requests: 1

HTTP/1.1 200 OK
Content-Encoding: gzip
Age: 562539
Cache-Control: max-age=604800
Content-Type: text/html; charset=UTF-8
Date: Sat, 17 Feb 2024 05:58:48 GMT
Etag: "3147526947+gzip"
Expires: Sat, 24 Feb 2024 05:58:48 GMT
Last-Modified: Thu, 17 Oct 2019 07:18:26 GMT
Server: ECS (laa/7B57)
Vary: Accept-Encoding
X-Cache: HIT
Content-Length: 648
```

1 client pkt(s), 1 server pkt(s), 1 turn(s).

Task 4

Step 1) Setting up the NAT network in VirtualBox to simulate a spoofing attack.

Name	IPv4 Prefix	IPv6 Prefix	DHCP Server
NatNetwork	10.0.2.0/24		Enabled

Step 2) Checked out the IP and gateway for Ubuntu

Attached to: NAT Network

Name: NatNetwork

Advanced

```
kevin@ubuntu: ~/Desktop
kevin@ubuntu:~/Desktop$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 100
0
    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
Rhythmbox :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 defaul
t qlen 1000
    link/ether 08:00:27:c3:66:fc 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 542sec preferred_lft 542sec
    inet6 fe80::d970:dce9:be36:adb1/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
kevin@ubuntu:~/Desktop$
```

```
Processing triggers for man-db (2.10.2-1) ...
root@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
```

Step 3) Prepared for ARP spoofing attack

1st terminal:

```
┌──(root㉿kali)-[~]
└─# arpspoof -i eth0 -t 10.0.2.1 10.0.2.4
8:0:27:ba:c7:90 52:54:0:12:35:0 0806 42: arp reply 10.0.2.4 is-at 8:0:27:ba
:c7:90
```

2nd terminal: Did not work :(

```
┌──(root㉿kali)-[~]
└─# arpspoof -i eth0 -t 10.0.2.4 10.0.2.1
arpspoof: couldn't arp for host 10.0.2.4
```

3rd terminal:

```
┌──(root㉿kali)-[~]
└─# tcpdump -i eth0 -s 0 'tcp port http' -vvv
tcpdump: listening on eth0, link-type EN10MB (Ethernet), snapshot length 2621
44 bytes
```

Step 4) I got stuck here :(The second terminal from the previous step does not work, so I didn't get this far.