

21CY681: IP LAB – Assignment 2

Name: Ramya Ajay

Roll No: CB.EN.P2CYS22004

Date:26-10-2022

AIM: Understand and analyse network traffic using Wireshark.

Tools:

- Windows OS
- Command Prompt(Administrator Privileges to run the tools)
- Wireshark

Questions:

1. Understand PING and document it, then answer the following question:

PING (Packet Internet Groper) command The ping command is used to test the ability of the source computer to reach a specified destination computer. This command takes the IP address or the URL as input and operates by sending Internet Control Message Protocol (ICMP) Echo Request messages to the destination computer and awaits for the response.

a. Use ping on google.com and document your results on the output you received. [Find the IP address, Time to live value, and round-trip time value from the results you got].

```
C:\Windows\System32>ping google.com

Pinging google.com [142.250.195.46] with 32 bytes of data:
Reply from 142.250.195.46: bytes=32 time=487ms TTL=109
Reply from 142.250.195.46: bytes=32 time=90ms TTL=109
Reply from 142.250.195.46: bytes=32 time=89ms TTL=109
Reply from 142.250.195.46: bytes=32 time=91ms TTL=109

Ping statistics for 142.250.195.46:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 89ms, Maximum = 487ms, Average = 189ms

C:\Windows\System32>_
```

IP Address - 142.250.195.46

TTL - 109 ms

Round trip time – 189 ms

- b. By default, ping will send 4 packets to check the details, here you have to send 8 packets to check the output over google.com. Explain what the purpose of this doing is.

```
Administrator: Command Prompt
C:\Windows\System32>ping -n 8 google.com

Pinging google.com [142.250.195.46] with 32 bytes of data:
Reply from 142.250.195.46: bytes=32 time=88ms TTL=109
Reply from 142.250.195.46: bytes=32 time=90ms TTL=109
Reply from 142.250.195.46: bytes=32 time=90ms TTL=109
Reply from 142.250.195.46: bytes=32 time=118ms TTL=109
Reply from 142.250.195.46: bytes=32 time=89ms TTL=109
Reply from 142.250.195.46: bytes=32 time=151ms TTL=109
Reply from 142.250.195.46: bytes=32 time=89ms TTL=109
Reply from 142.250.195.46: bytes=32 time=88ms TTL=109

Ping statistics for 142.250.195.46:
    Packets: Sent = 8, Received = 8, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 88ms, Maximum = 151ms, Average = 100ms

C:\Windows\System32>
```

Setting a higher number allows the ping to continue to run either as a way of gathering more data or as a way of ensuring that a system continues to be responsive.

- c. Ping your local host. Explain what the purpose.

```
C:\Windows\System32>ping localhost

Pinging Ramya [::1] with 32 bytes of data:
Reply from ::1: time<1ms
Reply from ::1: time<1ms
Reply from ::1: time<1ms
Reply from ::1: time<1ms

Ping statistics for ::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Windows\System32>
```

We use ping command to see if the localhost is up and running. It is a way to test the Windows' network features are working properly but it says nothing about your own network hardware or your connection to any other computer or device.

2. Read the Unix manual page for traceroute OR help for tracert. Experiment with the various options. Describe the three things that you found most useful in the result.

Answer the following question:

- a. Try tracert over google.com

```

CA Administrator: Command Prompt
Microsoft Windows [Version 10.0.22621.521]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\System32>tracert google.com

Tracing route to google.com [2404:6800:4007:829::200e]
over a maximum of 30 hops:

  1  103 ms    4 ms      2 ms    2409:4072:2e88:8a85::47
  2  *          *          *        Request timed out.
  3   77 ms    52 ms    36 ms    2405:200:368:eeee:20::412
  4   62 ms    54 ms    69 ms    2405:200:801:900::16f2
  5   80 ms    41 ms    57 ms    2405:200:801:900::16f3
  6   45 ms    32 ms    60 ms    2405:200:801:900::877
  7   65 ms    49 ms    63 ms    2001:4860:1:1::15aa
  8   47 ms    60 ms    82 ms    2001:4860:1:1::15aa
  9   63 ms    42 ms    57 ms    2404:6800:80d9::1
 10   83 ms    85 ms    86 ms    2001:4860:0:1::448c
 11   51 ms    35 ms    84 ms    2001:4860:0:135f::3
 12   49 ms    37 ms    56 ms    2001:4860:0:1340::1
 13   204 ms   58 ms    97 ms    2001:4860:0:1::55b5
 14   57 ms    39 ms    56 ms    maa03s44-in-x0e.1e100.net [2404:6800:4007:829::200e]

Trace complete.

C:\Windows\System32>

```

b. Type `tracert -d google.com`

```

C:\Windows\System32>tracert -d google.com

Tracing route to google.com [2404:6800:4007:829::200e]
over a maximum of 30 hops:

  1   5 ms     2 ms     2 ms    2409:4072:2e88:8a85::47
  2  *          *          *        Request timed out.
  3   78 ms    45 ms    54 ms    2405:200:368:eeee:20::412
  4   78 ms    75 ms    43 ms    2405:200:801:900::16f2
  5   97 ms    43 ms    33 ms    2405:200:801:900::16f3
  6   58 ms    36 ms    72 ms    2405:200:801:900::877
  7   50 ms    73 ms    *        2001:4860:1:1::15aa
  8   48 ms   113 ms   61 ms    2001:4860:1:1::15aa
  9   60 ms    72 ms    76 ms    2404:6800:80d9::1
 10   59 ms    59 ms    34 ms    2001:4860:0:1::448c
 11   62 ms    41 ms    58 ms    2001:4860:0:135f::3
 12   51 ms    82 ms    65 ms    2001:4860:0:1340::1
 13   44 ms    34 ms    57 ms    2001:4860:0:1::55b5
 14   61 ms    33 ms    56 ms    2404:6800:4007:829::200e

Trace complete.

C:\Windows\System32>

```

1. How many hops is your machine away from google.com? - 14 Hops
2. Wait for a while and execute the same command again. Is the output the same as the first time? Observe and compare the difference and explain the reason.

```
Administrator: Command Prompt
over a maximum of 30 hops:
  1  5 ms  2 ms  2 ms  2409:4072:2e88:8a85::47
  2  *      *      *      Request timed out.
  3  78 ms  45 ms  54 ms  2405:200:368:eeee:20::412
  4  78 ms  75 ms  43 ms  2405:200:801:900::16f2
  5  97 ms  43 ms  33 ms  2405:200:801:900::16f3
  6  58 ms  36 ms  72 ms  2405:200:801:900::877
  7  50 ms  73 ms  *      2001:4860:1:1::15aa
  8  48 ms  113 ms  61 ms  2001:4860:1:1::15aa
  9  60 ms  72 ms  76 ms  2404:6800:80d9::1
 10  59 ms  59 ms  34 ms  2001:4860:0:1::448c
 11  62 ms  41 ms  58 ms  2001:4860:0:135f::3
 12  51 ms  82 ms  65 ms  2001:4860:0:1340::1
 13  44 ms  34 ms  57 ms  2001:4860:0:1::55b5
 14  61 ms  33 ms  56 ms  2404:6800:4007:829::200e

Trace complete.

C:\Windows\System32>tracert -d google.com

Tracing route to google.com [2404:6800:4007:82b::200e]
over a maximum of 30 hops:
  1  150 ms  7 ms  5 ms  2409:4072:2e88:8a85::47
  2  *      *      *      Request timed out.
  3  3247 ms  101 ms  53 ms  2405:200:368:eeee:20::412
  4  66 ms  62 ms  60 ms  2405:200:801:900::16f6
  5  *      50 ms  78 ms  2405:200:801:900::16f7
  6  *      *      *      Request timed out.
  7  401 ms  *      2351 ms  2001:4860:1:1::15aa
  8  151 ms  *      104 ms  2001:4860:1:1::15aa
  9  76 ms  186 ms  98 ms  2404:6800:8131::1
 10  69 ms  115 ms  221 ms  2001:4860:0:1::55cc
 11  70 ms  149 ms  81 ms  2001:4860:0:1::55fd
 12  66 ms  69 ms  76 ms  2404:6800:4007:82b::200e

Trace complete.

C:\Windows\System32>
```

It prevents tracert from resolving IP to Hostnames and often resulting in much faster results. So each time when we run tracert command with google, it gives us different path ie, No of hops is different.

3. You have to read about NETSTAT from the manual page or help before answering the below questions:

a . Use netstat to display information about the routing table.

```
Administrator: Command Prompt
C:\Windows\System32>netstat -r

=====
Interface List
=====
41...0a 00 27 00 00 29 .....VirtualBox Host-Only Ethernet Adapter
17...f4 46 37 9f 81 d5 .....Microsoft Wi-Fi Direct Virtual Adapter
13...f6 46 37 9f 81 d4 .....Microsoft Wi-Fi Direct Virtual Adapter #2
8...f4 46 37 9f 81 d4 .....Intel(R) Wi-Fi 6 AX201 160MHz
1.....Software Loopback Interface 1
=====

IPv4 Route Table
=====
Active Routes:
Network Destination        Netmask          Gateway           Interface        Metric
0.0.0.0                    0.0.0.0          192.168.251.49    192.168.251.101   55
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
192.168.56.0               255.255.255.0    On-link           192.168.56.1      330
192.168.56.1               255.255.255.255  On-link           192.168.56.1      330
192.168.56.255             255.255.255.255  On-link           192.168.56.1      330
192.168.251.0              255.255.255.0    On-link           192.168.251.101   311
192.168.251.101            255.255.255.255  On-link           192.168.251.101   311
192.168.251.255            255.255.255.255  On-link           192.168.251.101   311
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      330
224.0.0.0                  240.0.0.0        On-link           192.168.251.101   311
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      330
255.255.255.255            255.255.255.255  On-link           192.168.251.101   311
=====

Persistent Routes:
None

IPv6 Route Table
=====
Active Routes:
If Metric Network Destination      Gateway
8         71 ::/0 fe80::9429:44ff:feb7:f5fa
1         331 ::1/128 On-link
```

b. Use netstat to display about ethernet statistics.

```
C:\Windows\System32>netstat -e
Interface Statistics


```

	Received	Sent
Bytes	153656296	32462424
Unicast packets	173488	77392
Non-unicast packets	184	1816
Discards	0	0
Errors	0	0
Unknown protocols	0	0

```
C:\Windows\System32>_
```

4. What is the purpose of NSLOOKUP?

Name server lookup (nslookup) is a command-line tool that lets you find the internet protocol address or DNS record of a specific hostname.

Answer the following questions below:

- Use nslookup to find out the internet address of the domain amrita.edu.

ans: 3.33.154.67 and 15.197.141.123

```
C:\Windows\System32>nslookup amrita.edu
Server: UnKnown
Address: 192.168.251.49

Non-authoritative answer:
Name: amrita.edu
Addresses: 15.197.141.123
          3.33.154.67

C:\Windows\System32>
```

- What is the mail exchanger for the domain google.com.

```
C:\Windows\System32>nslookup -type=mx google.com
Server: UnKnown
Address: 192.168.251.49

Non-authoritative answer:
google.com MX preference = 10, mail exchanger = smtp.google.com

C:\Windows\System32>_
```

ans: smtp.google.com

c. What is the name server for amrita.edu

```
Administrator: Command Prompt
Errors 0
Unknown protocols 0

C:\Windows\System32>nslookup amrita.edu
Server: Unknown
Address: 192.168.251.49

Non-authoritative answer:
Name: amrita.edu
Addresses: 15.197.141.123
          3.33.154.67

C:\Windows\System32>nslookup -type=mx google.com
Server: Unknown
Address: 192.168.251.49

Non-authoritative answer:
google.com MX preference = 10, mail exchanger = smtp.google.com

C:\Windows\System32>nslookup -type=ns google.com
Server: Unknown
Address: 192.168.251.49

Non-authoritative answer:
google.com nameserver = ns4.google.com
google.com nameserver = ns2.google.com
google.com nameserver = ns3.google.com
google.com nameserver = ns1.google.com

ns2.google.com internet address = 216.239.34.10
ns2.google.com AAAA IPv6 address = 2001:4860:4802:34::a
ns3.google.com internet address = 216.239.36.10
ns3.google.com AAAA IPv6 address = 2001:4860:4802:36::a
ns1.google.com internet address = 216.239.32.10
ns1.google.com AAAA IPv6 address = 2001:4860:4802:32::a
ns4.google.com internet address = 216.239.38.10
ns4.google.com AAAA IPv6 address = 2001:4860:4802:38::a

C:\Windows\System32>
```

ans:ns4.google.com,ns2.google.com,ns3.google.com,ns1.google.com

5. What are ARP and RARP?

ARP stands for Address Resolution protocol .It retrieves the receiver's physical address in a network. RARP stands for Reverse Address Resolution Protocol . It retrieves logical address for a computer from the server.

a. Use arp command to find the gateway address and host systems hardware address.

```
C:\Windows\System32>arp -a

Interface: 192.168.251.101 --- 0x8
Internet Address Physical Address Type
192.168.251.49 96-29-44-b7-f5-fa dynamic
224.0.0.22 01-00-5e-00-00-16 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
255.255.255.255 ff-ff-ff-ff-ff-ff static

Interface: 192.168.56.1 --- 0x29
Internet Address Physical Address Type
192.168.56.255 ff-ff-ff-ff-ff-ff static
224.0.0.22 01-00-5e-00-00-16 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

C:\Windows\System32>
```

The gateway address is 192.168.251.49 & the hardware address of the host systems are 96-29-44-b7-f5-fa

b. How do you find the arp entries for a particular interface?

To find the arp entries for a particular interface we need to use the **-N** flag along with the ip address.

c. How do delete an arp entry?

To delete an arp entry, we need to use the **-d flag** along with the ip address . To delete all the entries we need to use the wildcard flag(*) .

d. How do you add an arp entry in arpcache?

To add an arp entry we need to use **-s** flag along with IP address and MAC address.

EXAMPLE - `arp -s 192.168.43.160 00-aa-00-62-c6-09`

6. Read about TCPDUMP tool [use manual page].

a. Using tcpdump, get the information about the general incoming network traffic with names.

```
ramya@ramya-VirtualBox:~$ sudo tcpdump
[sudo] password for ramya:
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
22:06:06.947439 IP snapstore-content-cache-2.ps5.canonical.com.https > ramya-VirtualBox.58024: Flags [P.],
seq 23991373:23995483, ack 2200155358, win 65535, length 4110
22:06:06.948168 IP ramya-VirtualBox.58024 > snapstore-content-cache-2.ps5.canonical.com.https: Flags [.], a
ck 4110, win 65535, length 0
22:06:06.950221 IP ramya-VirtualBox.49753 > 192.168.251.49.domain: 46362+ PTR? 15.2.0.10.in-addr.arpa. (40)
22:06:06.950550 IP snapstore-content-cache-2.ps5.canonical.com.https > ramya-VirtualBox.58024: Flags [P.],
seq 4110:6850, ack 1, win 65535, length 2740
22:06:06.950581 IP snapstore-content-cache-2.ps5.canonical.com.https > ramya-VirtualBox.58024: Flags [P.],
seq 6850:8220, ack 1, win 65535, length 1370
22:06:06.954642 IP 192.168.251.49.domain > ramya-VirtualBox.49753: 46362 NXDomain 0/0/0 (40)
22:06:06.958465 IP ramya-VirtualBox.58024 > snapstore-content-cache-2.ps5.canonical.com.https: Flags [.], a
ck 8220, win 65535, length 0
22:06:06.960562 IP ramya-VirtualBox.58338 > 192.168.251.49.domain: 23673+ PTR? 49.251.168.192.in-addr.arpa.
(45)
22:06:06.963138 IP snapstore-content-cache-2.ps5.canonical.com.https > ramya-VirtualBox.58024: Flags [P.],
seq 8220:9590, ack 1, win 65535, length 1370
22:06:06.965060 IP snapstore-content-cache-2.ps5.canonical.com.https > ramya-VirtualBox.58024: Flags [P.],
seq 9590:12330, ack 1, win 65535, length 2740
22:06:06.965384 IP ramya-VirtualBox.58024 > snapstore-content-cache-2.ps5.canonical.com.https: Flags [.], a
```

b. Using tcpdump, get the information about the general incoming network traffic with ip address on specific interface.

```
ramya@ramya-VirtualBox:~$ sudo tcpdump -i enp0s3
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
22:09:22.174596 IP ramya-VirtualBox.36359 > prod-ntp-5.ntp4.ps5.canonical.com.ntp: NTPv4, Client, length 48
22:09:22.180758 IP ramya-VirtualBox.41677 > 192.168.251.49.domain: 54704+ PTR? 15.2.0.10.in-addr.arpa. (40)
22:09:22.238313 IP 192.168.251.49.domain > ramya-VirtualBox.41677: 54704 NXDomain 0/0/0 (40)
22:09:22.244450 IP ramya-VirtualBox.51063 > 192.168.251.49.domain: 26619+ PTR? 49.251.168.192.in-addr.arpa.
(45)
22:09:22.254565 IP 192.168.251.49.domain > ramya-VirtualBox.51063: 26619 NXDomain 0/0/0 (45)
22:09:22.813866 IP prod-ntp-5.ntp4.ps5.canonical.com.ntp > ramya-VirtualBox.36359: NTPv4, Server, length 48
22:09:27.362900 ARP, Request who-has _gateway tell ramya-VirtualBox, length 28
22:09:27.364816 ARP, Reply _gateway is-at 52:54:00:12:35:02 (oui Unknown), length 46
22:09:27.367710 IP ramya-VirtualBox.50395 > 192.168.251.49.domain: 21956+ PTR? 2.2.0.10.in-addr.arpa. (39)
22:09:27.498154 IP 192.168.251.49.domain > ramya-VirtualBox.50395: 21956 NXDomain 0/0/0 (39)
22:09:54.924223 IP ramya-VirtualBox.54234 > prod-ntp-5.ntp4.ps5.canonical.com.ntp: NTPv4, Client, length 48
```

7. Use Wireshark (Latest version) to solve the below scenarios:

1. You, as a SOC analyst noted that someone try to send information (PING) to unknown IP address and you are suspecting some malicious information might transferred in it. Analyze the log file.

a. Find the data transferred. – The data that is transferred in the packet is “pass!@#\$”

Wireshark packet capture showing an ICMP Echo (ping) request. The packet list shows packet 20016 as the target. The packet details pane shows the ICMP Echo request with data length 8 bytes. The packet bytes pane shows the raw data: 70 61 73 73 21 40, which corresponds to the ASCII string 'pass!@'.

b. Find the source and destination IP of that log.

Wireshark packet details for the ICMP Echo request. The packet list shows packet 20016. The packet details pane shows the ICMP Echo request with source address 192.168.31.89 and destination address 192.168.31.16. The packet bytes pane shows the raw data: 70 61 73 73 21 40, which corresponds to the ASCII string 'pass!@'.

Source IP = 192.168.31.89, Destination IP = 192.168.31.16

c. Find the Data length (Bytes) and verify the checksum status on destination.

Wireshark packet details for the Ethernet II frame. The packet list shows packet 20016. The packet details pane shows the Ethernet II frame with source MAC address 74:c6:3b:f2:eb:db and destination MAC address 74:c6:3b:f2:eb:db. The packet bytes pane shows the raw data: 74 c6 3b f2 eb db 74 c6 3b f2 eb db 08 00, which corresponds to the ASCII string 'pass!@'.


```

Identification: 0x0001 (1)
> 000. .... = Flags: 0x0
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 64
Protocol: ICMP (1)
Header Checksum: 0xbble [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.31.89
Destination Address: 192.168.31.16
> Internet Control Message Protocol

```

```

0010 00 24 00 01 00 00 40 01 bb 1e c0 a8 1f 59 c0 a8 .$.---@:---Y--
0020 1f 10 08 00 cf c6 00 00 00 00 70 61 73 73 21 40 .....pass!@
0030 23 24                                     #$.

```

ans - The data length is 36 bytes and the header checksum status is unverified

2. Now you have found that some kind of file is been downloaded by insider in unencrypted web traffic. Your task is to

- Find the name and type of file: Name = 1.jpg , Type of file = JPEG JFIF
- Export that file from that web traffic, then analyze the file for any secret information.
- Find the hostname in which the file is stored. – 192.168.31.113

The image shows a Wireshark packet capture. The top pane displays a list of packets. Packet 21175 is an HTTP GET request for /1.jpg from 192.168.31.113 to 192.168.31.67. Packet 21259 is the corresponding HTTP 200 OK response. The bottom pane shows the details of packet 21175, including Ethernet II, Internet Protocol Version 4, and TCP details. The TCP details show the source port as 5060 and the destination port as 80.

3. Based upon their activities, auditing team has started investigation against them and found that the insider passed some sensitive information via call to someone. The traffic is been captured.

- Analyze the traffic and find those conversations and extract the sensitive information in it.

Ans - The password is “LIMBO”

- Find the call-ID when the status of the call is ringing.

The image shows a Wireshark packet capture of SIP traffic. The top pane displays a list of packets. Packet 12692 is a SIP INVITE message from 192.168.31.8 to 192.168.31.78. Packet 12703 is a SIP 180 Ringing response from 192.168.31.78 to 192.168.31.8. The bottom pane shows the details of packet 12703, including SIP details and the 180 Ringing status.

```
INVITE sip:1001@192.168.31.78:57332;rinstance=fc3bc219541e9861;transport=UDP SIP/2.0
Via: SIP/2.0/UDP 192.168.31.8:5060;branch=z9hG4bK30e63862
Max-Forwards: 70
From: "1002" <sip:1002@192.168.31.8>;tag=as1d95fb93
To: <sip:1001@192.168.31.78:57332;rinstance=fc3bc219541e9861;transport=UDP>
Contact: <sip:1002@192.168.31.8:5060>
Call-ID: 01caab9b53b12efe00d3493a67ff695d@192.168.31.8:5060
CSeq: 102 INVITE
User-Agent: FPBX-2.11.0(11.13.0)
Date: Tue, 10 Oct 2017 16:25:46 GMT
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY, INFO, PUBLISH, MESSAGE
Supported: replaces, timer
Content-Type: application/sdp
Content-Length: 627
```

CALLER-ID = 01caab9b53b12efe00d3493a67ff695d@192.168.31.8:5060

4. On further investigation, you have a suspect on some wireless device communications. List out the Bluetooth devices communications from this traffic and find the details about native Bluetooth adapter.
 - a. Analyze the captured WPA handshake from this traffic and report in detail about it to your administrator.
 - b. Geo locate all the endpoint of wireless devices.
 - c. Analyze the protocol level information transfer between wireless devices