21CY681 - INTERNET PROTOCOL LAB - II

Name: Surya S Nair

Register Number: CB.EN.P2CYS22007

Date: 22th October 2022

Assignment Topic: Understanding Network Traffic Analysis using Wireshark

1. Understand PING and document it, then answer the following question: (3 marks)

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 [142.250.205.238] with 32 bytes of data:
Reply from 142.250.205.238: bytes=32 time=104ms TTL=118
Reply from 142.250.205.238: bytes=32 time=30ms TTL=118
Reply from 142.250.205.238: bytes=32 time=29ms TTL=118
Reply from 142.250.205.238: bytes=32 time=30ms TTL=118

Ping statistics for 142.250.205.238:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 29ms, Maximum = 104ms, Average = 48ms

C:\WINDOWS\system32>
```

IP address - 142.250.205.238

Time to live value - 118

Round trip time value - 48ms

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.

```
C:\WINDOWS\system32>ping -n 8 google.com

Pinging google.com [142.250.205.238] with 32 bytes of data:
Request timed out.
Request timed out.
Reply from 142.250.205.238: bytes=32 time=582ms TTL=118
Reply from 142.250.205.238: bytes=32 time=1152ms TTL=118
Reply from 142.250.205.238: bytes=32 time=686ms TTL=118
Reply from 142.250.205.238: bytes=32 time=707ms TTL=118
Reply from 142.250.205.238: bytes=32 time=235ms TTL=118
Reply from 142.250.205.238: bytes=32 time=2856ms TTL=118

Ping statistics for 142.250.205.238:
    Packets: Sent = 8, Received = 6, Lost = 2 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 235ms, Maximum = 2856ms, Average = 1036ms
```

ping -n count determines the number of echo requests to sent.By default it is 4.Here we send 8 number of packets to check the output over google.com.

c. Ping your local host. Explain what the purpose

```
C:\WINDOWS\system32>ping localhost

Pinging LAPTOP-KB8USE6Q [::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
```

If Iam facing some problems while accessing a website ,using Ping command I can diagnose my local network connectivity.Here the localhost is my computer. Localhost is useful for software testing and security purposes independent of a larger network.

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. (2 marks)

Answer the following question:

a. Try tracert over google.com

```
C:\WINDOWS\system32>tracert google.com

Tracing route to google.com [142.250.205.238]
over a maximum of 30 hops:

  1    83 ms   168 ms     *     192.168.1.1
  2     *        *        *     Request timed out.
  3   114 ms   145 ms    80 ms  172.16.1.9
  4   215 ms    99 ms   106 ms  10.1.1.10
  5    63 ms   199 ms   144 ms  72.14.212.92
  6   711 ms   550 ms   111 ms  142.251.227.217
  7   125 ms   169 ms   137 ms  142.251.60.187
  8   135 ms   162 ms   100 ms  maa05s28-in-f14.1e100.net [142.250.205.238]

Trace complete.
```

Traceroute tool (ip tracer) allows to detect the route of the ip packets to the given host.

Both IPv4 and IPv6 are supported.

Traceroute tool displays ip addresses, domains and countries of intermediate hops. If hop did not reply it will be shown as asterisk.

Traceroute tool is often used to find problems in packet routing such as unexpected hops, routes longer than expected or even loops in the route.

b. Type tracert -d google.com

```
C:\WINDOWS\system32>tracert -d google.com

Tracing route to google.com [142.250.205.238]
over a maximum of 30 hops:

  1   109 ms    36 ms    78 ms  192.168.1.1
  2     *        *        *     Request timed out.
  3    65 ms   166 ms    66 ms  172.16.1.9
  4   141 ms   122 ms   133 ms  10.1.1.10
  5   339 ms   212 ms   274 ms  72.14.212.92
  6   680 ms   415 ms   493 ms  142.251.227.217
  7   354 ms   202 ms   108 ms  142.251.60.187
  8   370 ms   289 ms   377 ms  142.250.205.238

Trace complete.
```

Using the -d option with tracert command instructs tracert not to perform a DNS lookup on each IP address so that tracert reports the IP address of the near side interface of the

routers.

1. How many hops is your machine away from google.com?

Ans : 8 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.

Ans : Round Trip Time values are different.RTT says about the time for your packet to reach that point and return to your computer. This is listed in milliseconds. There are three columns because the traceroute sends three separate signal packets. This is to display consistency, or a lack thereof, in the route.

```
C:\WINDOWS\system32>tracert -d google.com

Tracing route to google.com [142.250.205.238]
over a maximum of 30 hops:

  1    93 ms    73 ms    94 ms  192.168.1.1
  2     *        *        *     Request timed out.
  3    11 ms     *      587 ms  172.16.1.9
  4   267 ms    26 ms    51 ms  10.1.1.10
  5    33 ms    52 ms   175 ms  72.14.212.92
  6   209 ms   252 ms   124 ms  142.251.227.217
  7    38 ms   141 ms   158 ms  142.251.60.187
  8     *      252 ms    99 ms  142.250.205.238

Trace complete.
```

3. You have to read about NETSTAT from the manual page or help before answering the belowquestions: (1 mark)

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

```
C:\WINDOWS\system32>netstat -r
===========================================================================
Interface List
 15...00 ff c9 7a 6a 90 ......ExpressVPN TAP Adapter
 11...0a 00 27 00 00 0b ......VirtualBox Host-Only Ethernet Adapter
  9...82 d2 1d fb e3 f3 ......Microsoft Wi-Fi Direct Virtual Adapter
 18...c2 d2 1d fb e3 f3 ......Microsoft Wi-Fi Direct Virtual Adapter #2
 10...80 d2 1d fb e3 f3 ......Realtek RTL8822CE 802.11ac PCIe Adapter
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0      192.168.1.1      192.168.1.6     50
        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
      192.168.1.0    255.255.255.0         On-link       192.168.1.6    306
      192.168.1.6  255.255.255.255         On-link       192.168.1.6    306
    192.168.1.255  255.255.255.255         On-link       192.168.1.6    306
     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
        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       192.168.1.6    306
  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       192.168.1.6    306
===========================================================================
Persistent Routes:
  None
```

```
IPv6 Route Table
===========================================================================
Active Routes:
 If Metric Network Destination      Gateway
  1    331 ::1/128                  On-link
 11    281 fe80::/64                On-link
 10    306 fe80::/64                On-link
 11    281 fe80::5890:9542:683:4d7d/128
                                    On-link
 10    306 fe80::8181:96a9:19f3:33c4/128
                                    On-link
  1    331 ff00::/8                 On-link
 11    281 ff00::/8                 On-link
 10    306 ff00::/8                 On-link
===========================================================================
Persistent Routes:
  None

C:\WINDOWS\system32>
```

b. Use netstat to display about ethernet statistics.

```
C:\WINDOWS\system32>netstat -e
Interface Statistics

                           Received            Sent

Bytes                     738759104       185507584
Unicast packets              961680          874728
Non-unicast packets            3760            6168
Discards                          0               0
Errors                            0               0
Unknown protocols                 0

C:\WINDOWS\system32>
```

4. What is the purpose of NSLOOKUP ?

Ans : Nslookup stands for name server lookup.It is used to query a DNS server to obtain its domain name and associated IP address.It can be used with the domain name as an argument or independently.

Answer the following questions below: (3 marks)

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

Ans : 3.33.154.67 and 15.197.141.123

```
C:\Users\user>nslookup amrita.edu
Server:  dns.keralavisionisp.com
Address:  103.199.160.80

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

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

Ans :

```
C:\Users\user>nslookup -type=mx google.com
Server:  dns.keralavisionisp.com
Address:  103.199.160.80

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

c. What is the name server for amrita.edu.

Ans :

```
C:\Users\user>nslookup -type=ns google.com
Server:  dns.keralavisionisp.com
Address:  103.199.160.80

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
```

5. What are ARP and RARP?

Ans : ARP stands for Address resolution protocol and RARP for Reverse Address Resolution Protocol. The ARP retrieves the receiver's physical address in a network. The RARP retrieves a computer's logical address from its available server.

Answer the following questions below: (3 marks)

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

```
C:\Users\user>arp -a

Interface: 192.168.1.6 --- 0xa
  Internet Address      Physical Address      Type
  192.168.1.1           14-a7-2b-b5-f9-a8     dynamic
  192.168.1.255         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
  224.0.1.60            01-00-5e-00-01-3c     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 --- 0xb
  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
  224.0.1.60            01-00-5e-00-01-3c     static
  239.255.255.250       01-00-5e-7f-ff-fa     static

C:\Users\user>
```

Gateway address : 192.168.1.1

Host systems hardware address : ff-ff-ff-ff-ff-ff and 01-00-5e-00-00-16

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

Ans : Use -N flag along with the IP Address to get the arp entries for a particular interface.

c. How do delete an arp entry?

Ans : Use the -d flag along with the IP address to delete an arp entry.

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

Ans : Use -s flag along with IP address and MAC address.

6. Read about TCPDUMP tool [use manual page]. Answer the questions below: (1 marks)

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

Ans :

```
surya@surya-VirtualBox:~$ sudo tcpdump
[sudo] password for surya:
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
20:22:57.516412 IP6 surya-VirtualBox.mdns > ff02::fb.mdns: 0 PTR (QM)? _pgpkey-
hkp._tcp.local. (40)
20:22:57.516758 IP surya-VirtualBox.mdns > 224.0.0.251.mdns: 0 PTR (QM)? _pgpke
y-hkp._tcp.local. (40)
20:22:57.518633 IP surya-VirtualBox.48447 > dns.google.domain: 37070+ [1au] PTR
? b.f.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.2.0.f.f.ip6.arpa. (10
1)
20:23:02.519583 IP surya-VirtualBox.55518 > dns.keralavisionisp.com.domain: 370
70+ [1au] PTR? b.f.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.2.0.f.f.
ip6.arpa. (101)
20:23:02.542670 IP dns.keralavisionisp.com.domain > surya-VirtualBox.55518: 370
70 NXDomain 0/1/1 (165)
20:23:02.542884 IP surya-VirtualBox.55518 > dns.keralavisionisp.com.domain: 370
70+ PTR? b.f.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.2.0.f.f.ip6.ar
pa. (90)
20:23:02.556484 IP dns.keralavisionisp.com.domain > surya-VirtualBox.55518: 370
70 NXDomain 0/1/0 (154)
20:23:02.558108 IP surya-VirtualBox.45013 > dns.keralavisionisp.com.domain: 177
62+ [1au] PTR? b.c.5.5.c.4.6.0.b.7.1.b.4.1.9.5.0.0.0.0.0.0.0.0.0.0.0.0.0.8.e.f.
```

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

Ans :

```
surya@surya-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
20:50:46.266672 IP surya-VirtualBox.42954 > snapstore-content-cache-2.ps5.canon
ical.com.https: Flags [.], ack 158823786, win 65535, length 0
20:50:46.269066 IP surya-VirtualBox.50769 > dns.google.domain: 64216+ [1au] PTR
? 15.2.0.10.in-addr.arpa. (51)
20:50:46.291572 IP snapstore-content-cache-2.ps5.canonical.com.https > surya-Vi
rtualBox.42954: Flags [P.], seq 1:1441, ack 0, win 65535, length 1440
20:50:46.316890 IP snapstore-content-cache-2.ps5.canonical.com.https > surya-Vi
rtualBox.42954: Flags [P.], seq 1441:2881, ack 0, win 65535, length 1440
20:50:46.316922 IP surya-VirtualBox.42954 > snapstore-content-cache-2.ps5.canon
ical.com.https: Flags [.], ack 2881, win 65535, length 0
20:50:46.329254 IP dns.google.domain > surya-VirtualBox.50769: 64216 NXDomain 0
/0/1 (51)
20:50:46.330290 IP surya-VirtualBox.50769 > dns.google.domain: 64216+ PTR? 15.2
.0.10.in-addr.arpa. (40)
20:50:46.343177 IP snapstore-content-cache-2.ps5.canonical.com.https > surya-Vi
rtualBox.42954: Flags [P.], seq 2881:4321, ack 0, win 65535, length 1440
```

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

Use Evidence.pcapng as evidence [Provided in Teams] file to answer the below questions.

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.

```
0000  00 0c 29 67 0b d2 74 c6  3b f2 eb db 08 00 45 00   ··)g··t· ;·····E·
0010  00 24 34 f7 00 00 80 01  46 28 c0 a8 1f 10 c0 a8   ·$4····· F(····· 
0020  1f 59 00 00 d7 c6 00 00  00 00 70 61 73 73 21 40   ·Y····· ··pass!@
0030  23 24                                              #$
```

Data that is transferred in the packet is" pass!@#$ "

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

```
Source Address: 192.168.31.89
Destination Address: 192.168.31.16
```

```
0000  74 c6 3b f2 eb db 74 c6  3b f2 eb db 08 00 45 00   t·;···t· ;·····E·
0010  00 24 00 01 00 00 40 01  bb 1e c0 a8 1f 59 c0 a8   ·$····@· ·····Y··
0020  1f 10 08 00 cf c6 00 00  00 00 70 61 73 73 21 40   ···· ···· ··pass!@
0030  23 24                                              #$
```

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

```
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 36
  Identification: 0x0001 (1)
> 000. .... = Flags: 0x0
  ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 64
  Protocol: ICMP (1)
  Header Checksum: 0xbb1e [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 192.168.31.89
  Destination Address: 192.168.31.16
```

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

Protocol	Length	Info
HTTP	209	GET /1.jpg HTTP/1.1
HTTP	22234	HTTP/1.1 200 OK (JPEG JFIF image)

a. Find the name and type of file.

Ans : Name : 1.jpg

Type of file : JPEG JFIF

b. Export that file from that web traffic, then analyze the file for any secret information.

c. Find the hostname in which the file is stored : 192.168.31.113

Destination	Protocol	Length	Info
192.168.31.67	HTTP	209	GET /1.jpg HTTP/1.1
192.168.31.113	HTTP	22234	HTTP/1.1 200 OK (JPEG JFIF image)

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.

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

Ans : Password is LIMBO

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

2017/284 11:25:47.4…	12692	192.168.31.8	192.168.31.78	SIP/SDP	1325	Request: INVITE sip:1001@192.168.31.78:57332;rinstance=fc3bc219541e9861;transp
2017/284 11:25:47.4…	12703	192.168.31.78	192.168.31.8	SIP	351	Status: 100 Trying |
2017/284 11:25:47.4…	12704	192.168.31.78	192.168.31.8	SIP	477	Status: 180 Ringing |
2017/284 11:25:49.4…	13059	192.168.31.78	192.168.31.8	SIP/SDP	805	Status: 200 OK (INVITE) |
2017/284 11:25:49.4…	13060	192.168.31.78	192.168.31.8	SIP/XML	829	Request: PUBLISH sip:1001@192.168.31.8;transport=UDP |
2017/284 11:25:49.4…	13061	192.168.31.78	192.168.31.8	SIP	572	Request: SUBSCRIBE sip:1001@192.168.31.8;transport=UDP |
2017/284 11:25:49.4…	13062	192.168.31.8	192.168.31.78	SIP	474	Request: ACK sip:1001@192.168.31.78:57332 |
2017/284 11:25:49.4…	13063	192.168.31.8	192.168.31.78	SIP	508	Status: 489 Bad Event |
2017/284 11:25:49.4…	13064	192.168.31.8	192.168.31.78	SIP	589	Status: 401 Unauthorized |
2017/284 11:25:49.4…	13065	192.168.31.78	192.168.31.8	SIP	745	Request: SUBSCRIBE sip:1001@192.168.31.8;transport=UDP |
2017/284 11:25:49.4…	13066	192.168.31.8	192.168.31.78	SIP	510	Status: 489 Bad Event |
2017/284 11:25:49.5…	13073	192.168.31.78	192.168.31.8	SIP/XML	829	Request: PUBLISH sip:1001@192.168.31.8;transport=UDP |
2017/284 11:25:49.5…	13074	192.168.31.78	192.168.31.8	SIP	572	Request: SUBSCRIBE sip:1001@192.168.31.8;transport=UDP |

```
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
```

Call -ID :

```
Call-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 toyour administrator.

b. Geo locate all the endpoint of wireless devices.

c. Analyze the protocol level information transfer between wireless devices.