CY681 -IP LAB EXPERIMENT – 2

NAME: KARTHIKA P **DATE:22-10-22**

ROLL NO: CB.EN.P2CYS22001

1)PING

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].

from the fig:1,

ip address:8.8.8.8

ttl:111

round trip time average=95

```
C:\Users\Administrator>ping google.com

Pinging google.com [2404:6800:4009:80a::200e] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 2404:6800:4009:80a::200e:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\Administrator>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=115ms TTL=111
Reply from 8.8.8.8: bytes=32 time=103ms TTL=111
Reply from 8.8.8.8: bytes=32 time=88ms TTL=111
Reply from 8.8.8.8: bytes=32 time=76ms TTL=111

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 76ms, Maximum = 115ms, Average = 95ms
```

Fig :1

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.

Setting a higher number of packets, the ping to continue to run as a way of gathering more data or checking responsiveness.

```
C:\Users\Administrator> ping -n 8 google.com

Pinging google.com [2404:6800:4007:813::200e] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 2404:6800:4007:813::200e:
    Packets: Sent = 8, Received = 0, Lost = 8 (100% loss),
```

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

we have pinged local host in which we can know the network connectivity and discover any performance issues.

```
C:\Users\Administrator>ping 192.168.56.1

Pinging 192.168.56.1 with 32 bytes of data:
Reply from 192.168.56.1: bytes=32 time<1ms TTL=128
Reply from 192.168.56.1: bytes=32 time<1ms TTL=128
Reply from 192.168.56.1: bytes=32 time<1ms TTL=128
Reply from 192.168.56.1: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.56.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

```
C:\Users\Administrator>ping localhost

Pinging karthumbi [::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
```

2)TRACERT

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.

a) Try tracert over google.com

```
C:\Users\Administrator>tracert 8.8.8.8

Tracing route to dns.google [8.8.8.8]
over a maximum of 30 hops:

  1     4 ms     2 ms     2 ms  192.168.185.101
  2     *        *        *     Request timed out.
  3    58 ms    50 ms    37 ms  56.8.74.113
  4   237 ms    55 ms    75 ms  192.168.92.24
  5    66 ms    36 ms    45 ms  192.168.92.29
  6    55 ms    41 ms    41 ms  172.26.100.7
  7    45 ms    42 ms    62 ms  172.26.100.18
  8   132 ms    26 ms    38 ms  192.168.83.22
  9     *        *        *     Request timed out.
 10     *        *        *     Request timed out.
 11    50 ms    35 ms    47 ms  74.125.51.4
 12    37 ms    45 ms    55 ms  209.85.142.173
 13   179 ms   145 ms    46 ms  142.251.55.63
 14    46 ms    53 ms    96 ms  dns.google [8.8.8.8]

Trace complete.
```

B) Type tracert -d google.com

```
C:\Users\Administrator>tracert -d 8.8.8.8

Tracing route to 8.8.8.8 over a maximum of 30 hops

  1    24 ms     1 ms     1 ms  192.168.60.206
  2     *        *        *     Request timed out.
  3    41 ms    36 ms    34 ms  10.72.51.18
  4    58 ms    65 ms    35 ms  192.168.47.38
  5    65 ms    56 ms    47 ms  172.26.75.37
  6    39 ms    55 ms    35 ms  172.26.75.67
  7    46 ms    43 ms    47 ms  192.168.47.18
  8     *        *        *     Request timed out.
  9     *        *        *     Request timed out.
 10    61 ms    59 ms    57 ms  74.125.50.202
 11    73 ms    67 ms    55 ms  216.239.43.133
 12    71 ms    48 ms    59 ms  172.253.73.35
 13    56 ms    68 ms    57 ms  8.8.8.8

Trace complete.
```

How many hops is your machine away from google.com? 13 hops.

3)NETSTAT

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

A)netstat –r: used to display routing table.

```
C:\Users\Administrator>netstat -r
===========================================================================
Interface List
 10...0a 00 27 00 00 0a ......VirtualBox Host-Only Ethernet Adapter
  9...84 3a 4b d9 8f 55 ......Microsoft Wi-Fi Direct Virtual Adapter
 18...86 3a 4b d9 8f 54 ......Microsoft Wi-Fi Direct Virtual Adapter #2
  4...84 3a 4b d9 8f 54 ......Intel(R) Centrino(R) Advanced-N 6205
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0      10.11.128.1     10.11.139.62     40
      10.11.128.0    255.255.224.0         On-link      10.11.139.62    296
     10.11.139.62  255.255.255.255         On-link      10.11.139.62    296
    10.11.159.255  255.255.255.255         On-link      10.11.139.62    296
        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    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      10.11.139.62    296
  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      10.11.139.62    296
===========================================================================
Persistent Routes:
  None
```

```
IPv6 Route Table
===========================================================================
Active Routes:
 If Metric Network Destination      Gateway
  1    331 ::1/128                  On-link
 10    281 fe80::/64                On-link
  4    296 fe80::/64                On-link
 10    281 fe80::9083:a407:164a:9c9b/128
                                   On-link
  4    296 fe80::bd96:9920:2810:3daa/128
                                   On-link
  1    331 ff00::/8                 On-link
 10    281 ff00::/8                 On-link
  4    296 ff00::/8                 On-link
===========================================================================
Persistent Routes:
  None
```

b) netstat -s to display about ethernet statistics

```
C:\Users\Administrator>netstat -s

IPv4 Statistics

  Packets Received                    = 973869
  Received Header Errors              = 0
  Received Address Errors             = 2520
  Datagrams Forwarded                 = 0
  Unknown Protocols Received          = 0
  Received Packets Discarded          = 362733
  Received Packets Delivered          = 966162
  Output Requests                     = 517155
  Routing Discards                    = 0
  Discarded Output Packets            = 1020
  Output Packet No Route              = 285
  Reassembly Required                 = 9343
  Reassembly Successful               = 1715
  Reassembly Failures                 = 0
  Datagrams Successfully Fragmented   = 1027
  Datagrams Failing Fragmentation     = 0
  Fragments Created                   = 4108

IPv6 Statistics

  Packets Received                    = 271594
  Received Header Errors              = 0
  Received Address Errors             = 0
  Datagrams Forwarded                 = 0
  Unknown Protocols Received          = 0
  Received Packets Discarded          = 121689
  Received Packets Delivered          = 273185
  Output Requests                     = 79973
  Routing Discards                    = 0
  Discarded Output Packets            = 4
  Output Packet No Route              = 11
  Reassembly Required                 = 0
  Reassembly Successful               = 0
  Reassembly Failures                 = 0
  Datagrams Successfully Fragmented   = 0
  Datagrams Failing Fragmentation     = 0
  Fragments Created                   = 0

ICMPv4 Statistics
```

```
TCP Statistics for IPv4

  Active Opens                        = 8799
  Passive Opens                       = 338
  Failed Connection Attempts          = 998
  Reset Connections                   = 1130
  Current Connections                 = 105
  Segments Received                   = 501412
  Segments Sent                       = 450820
  Segments Retransmitted              = 17076

TCP Statistics for IPv6

  Active Opens                        = 1705
  Passive Opens                       = 794
  Failed Connection Attempts          = 389
  Reset Connections                   = 178
  Current Connections                 = 2
  Segments Received                   = 88933
  Segments Sent                       = 70368
  Segments Retransmitted              = 1520

UDP Statistics for IPv4

  Datagrams Received    = 604515
  No Ports              = 21053
  Receive Errors        = 342333
  Datagrams Sent        = 23829

UDP Statistics for IPv6

  Datagrams Received    = 263160
  No Ports              = 1855
  Receive Errors        = 17216
  Datagrams Sent        = 30163
```

4)NSLOOKUP:

What is the purpose of NSLOOKUP ? Answer the following questions below:

nslookup: It is used to obtain dns records.

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

```
C:\Users\Administrator>nslookup amrita.edu
Server:  prithvi.amritanet.edu
Address:  172.17.18.2

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

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

```
C:\Users\Administrator>nslookup -q=mx google.com
Server:  prithvi.amritanet.edu
Address:  172.17.18.2

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

smtp.google.com internet address = 74.125.68.27
smtp.google.com internet address = 142.250.4.26
smtp.google.com internet address = 74.125.24.26
smtp.google.com internet address = 74.125.24.27
smtp.google.com internet address = 142.250.4.27
smtp.google.com AAAA IPv6 address = 2404:6800:4003:c03::1b
smtp.google.com AAAA IPv6 address = 2404:6800:4003:c06::1b
smtp.google.com AAAA IPv6 address = 2404:6800:4003:c02::1a
smtp.google.com AAAA IPv6 address = 2404:6800:4003:c06::1a
```

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

```
C:\Users\Administrator>nslookup -type=ns amrita.edu
Server:  UnKnown
Address:  192.168.60.206

Non-authoritative answer:
amrita.edu      nameserver = ns2.amrita.edu
amrita.edu      nameserver = ns1.amrita.edu
amrita.edu      nameserver = ns4.amrita.edu
amrita.edu      nameserver = ns3.amrita.edu

ns1.amrita.edu  internet address = 14.139.187.131
ns2.amrita.edu  internet address = 117.193.77.232
ns3.amrita.edu  internet address = 103.10.24.200
ns4.amrita.edu  internet address = 115.243.144.130
ns4.amrita.edu  internet address = 103.5.112.81
```

5) ARP AND RARP:

What are ARP and RARP? Answer the following questions below

ARP: mapping dynamic IP address to the permanent physical machine in the local area network.It will request packet to all the machines on LAN and ask if any of the machine are using particular ip address.The ARP command is used to manipulate ARP tables. **RARP**: physical machine in a local area network (LAN) can use to request its IP address'

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

Gateway address:192.168.60.206**,**Host system hardware address:6e-8676-0f-da-7e

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

Interface: 192.168.60.197 --- 0x4
  Internet Address      Physical Address      Type
  192.168.60.206        6e-86-76-0f-da-7e     dynamic
  192.168.60.255        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
  239.255.102.18        01-00-5e-7f-66-12     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 --- 0xa
  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
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

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

The arp –a command is used to find arp entry for particular interface.

C)How do delete an arp entry?

To delete an arp entry arp /d *Inetaddr* command is used

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

arp-s command is used to add an arp entry in arpcache.

6) TCPDUMP:

Read about TCPDUMP tool [use manual page]. Answer the questions below

The tcpdump is used to captures and dumps the network traffic passing through a given server's or node's network interfaces .

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

```
karthika@karthika-VirtualBox:~$ sudo tcpdump
[sudo] password for karthika:
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on enp0s3, link-type EN10MB (Ethernet), snapshot length 262144 bytes
19:23:27.252828 IP karthika-VirtualBox.50203 > prod-ntp-3.ntp4.ps5.canonical.co
m.ntp: NTPv4, Client, length 48
19:23:27.320441 IP karthika-VirtualBox.52330 > 192.168.60.206.domain: 22226+ PT
R? 56.190.125.185.in-addr.arpa. (45)
19:23:27.446001 IP prod-ntp-3.ntp4.ps5.canonical.com.ntp > karthika-VirtualBox.
50203: NTPv4, Server, length 48
19:23:27.998588 IP 192.168.60.206.domain > karthika-VirtualBox.52330: 22226 2/0
/0 PTR prod-ntp-3.ntp4.ps5.canonical.com., PTR prod-ntp-3.ntp1.ps5.canonical.co
m. (122)
19:23:27.999367 IP karthika-VirtualBox.48268 > 192.168.60.206.domain: 29653+ PT
R? 15.2.0.10.in-addr.arpa. (40)
19:23:28.005283 IP 192.168.60.206.domain > karthika-VirtualBox.48268: 29653 NXD
omain 0/0/0 (40)
19:23:28.007375 IP karthika-VirtualBox.58945 > 192.168.60.206.domain: 25335+ PT
R? 206.60.168.192.in-addr.arpa. (45)
19:23:28.049765 IP 192.168.60.206.domain > karthika-VirtualBox.58945: 25335 NXD
omain* 0/1/0 (104)
19:23:28.145277 IP6 karthika-VirtualBox > ip6-allrouters: ICMP6, router solicit
ation, length 8
19:23:28.711129 IP karthika-VirtualBox.39560 > blackcat.canonical.com.https: Fl
ags [S], seq 1790245870, win 64240, options [mss 1460,sackOK,TS val 1472253095
ecr 0,nop,wscale 7], length 0
19:23:28.773688 IP karthika-VirtualBox.57146 > 192.168.60.206.domain: 5201+ PTR
? 49.91.189.91.in-addr.arpa. (43)
19:23:29.003366 IP blackcat.canonical.com.https > karthika-VirtualBox.39560: Fl
```

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

```
karthika@karthika-VirtualBox:~$ sudo tcpdump -i enp0s3
[sudo] password for karthika:
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on enp0s3, link-type EN10MB (Ethernet), snapshot length 262144 bytes
22:00:11.619109 IP karthika-VirtualBox.45457 > 192.168.60.206.domain: 58505+ A?
 connectivity-check.ubuntu.com. (47)
22:00:11.672314 IP 192.168.60.206.domain > karthika-VirtualBox.45457: 58505 3/0
/0 A 35.232.111.17, A 34.122.121.32, A 35.224.170.84 (95)
22:00:11.675587 IP karthika-VirtualBox.40966 > 17.111.232.35.bc.googleuserconte
nt.com.http: Flags [S], seq 3688208186, win 64240, options [mss 1460,sackOK,TS
val 3132217862 ecr 0,nop,wscale 7], length 0
22:00:11.677061 IP karthika-VirtualBox.52563 > 192.168.60.206.domain: 7427+ PTR
? 206.60.168.192.in-addr.arpa. (45)
22:00:11.681792 IP 192.168.60.206.domain > karthika-VirtualBox.52563: 7427 NXDo
main 0/0/0 (45)
22:00:11.684237 IP karthika-VirtualBox.46129 > 192.168.60.206.domain: 11057+ PT
R? 15.2.0.10.in-addr.arpa. (40)
22:00:11.738134 IP 192.168.60.206.domain > karthika-VirtualBox.46129: 11057 NXD
omain* 0/1/0 (99)
22:00:11.775847 IP karthika-VirtualBox.33607 > 192.168.60.206.domain: 61666+ PT
R? 17.111.232.35.in-addr.arpa. (44)
22:00:11.982183 IP 17.111.232.35.bc.googleusercontent.com.http > karthika-Virtu
alBox.40966: Flags [S.], seq 71680001, ack 3688208187, win 65535, options [mss
1460], length 0
22:00:11.982326 IP karthika-VirtualBox.40966 > 17.111.232.35.bc.googleuserconte
nt.com.http: Flags [.], ack 1, win 64240, length 0
22:00:11.983112 IP karthika-VirtualBox.40966 > 17.111.232.35.bc.googleuserconte
```

7)wireshark:

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

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

a)find the data transferred?

The data transferred is pass!@#$

```
0 a8 1f 10 c0 a8    ·$4····· F(·····
0 61 73 73 21 40    ·Y····· ··pass!@
                    #$
```

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

```
Source Address: 192.168.31.89
<Source or Destination Address: 192.168.31.89>
<[Source Host: 192.168.31.89]>
<[Source or Destination Host: 192.168.31.89]>
Destination Address: 192.168.31.16
<Source or Destination Address: 192.168.31.16>
<[Destination Host: 192.168.31.16]>
<[Source or Destination Host: 192.168.31.16]>
```

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

```
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 36
Identification: 0x34f7 (13559)
000. .... = Flags: 0x0
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 128
Protocol: ICMP (1)
Header Checksum: 0x4628 [validation disabled]
[Header checksum status: Unverified]
```

Data length : 36 and 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

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

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.

192.168.31.67	80	HTTP	209	GET /1.jpg HTTP/1.1	
192.168.31.113	59380	HTTP	22234	HTTP/1.1 200 OK	(JPEG JFIF image)

HOSTNAME: 192.168.31.113

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.

The password is LIMBO.

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

udp.stream eq 0

No.	Time	Source	source port	Destination	destination port	Protocol	Length	Info
12692	-714.128824	192.168.31.8	5060	192.168.31.78	57332	SIP/SDP	1325	Request: INVITE sip:1001@192.168.31.78:57332;rinstance=fc3
12703	-714.045167	192.168.31.78	57332	192.168.31.8	5060	SIP	351	Status: 100 Trying |
12704	-714.045064	192.168.31.78	57332	192.168.31.8	5060	SIP	477	Status: 180 Ringing |
13059	-712.108976	192.168.31.78	57332	192.168.31.8	5060	SIP/SDP	805	Status: 200 OK (INVITE) |
13060	-712.108845	192.168.31.78	57332	192.168.31.8	5060	SIP/XML	829	Request: PUBLISH sip:1001@192.168.31.8;transport=UDP |
13061	-712.108775	192.168.31.78	57332	192.168.31.8	5060	SIP	572	Request: SUBSCRIBE sip:1001@192.168.31.8;transport=UDP |
13062	-712.102800	192.168.31.8	5060	192.168.31.78	57332	SIP	474	Request: ACK sip:1001@192.168.31.78:57332 |
13063	-712.102799	192.168.31.8	5060	192.168.31.78	57332	SIP	508	Status: 489 Bad Event |
13064	-712.102798	192.168.31.8	5060	192.168.31.78	57332	SIP	589	Status: 401 Unauthorized |
13065	-712.099558	192.168.31.78	57332	192.168.31.8	5060	SIP	745	Request: SUBSCRIBE sip:1001@192.168.31.8;transport=UDP |
13066	-712.092662	192.168.31.8	5060	192.168.31.78	57332	SIP	510	Status: 489 Bad Event |
13073	-711.986522	192.168.31.78	57332	192.168.31.8	5060	SIP/XML	829	Request: PUBLISH sip:1001@192.168.31.8;transport=UDP |
13074	-711.986320	192.168.31.78	57332	192.168.31.8	5060	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
```