VIT®

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

SCHOOL OF INFORMATION TECHNOLOGY AND ENGINEERING

DIGITAL ASSIGNMENT 2 - WINTER SEMESTER 2023-24

Course: Information Security Management

Lab Course Code: BCSE354E

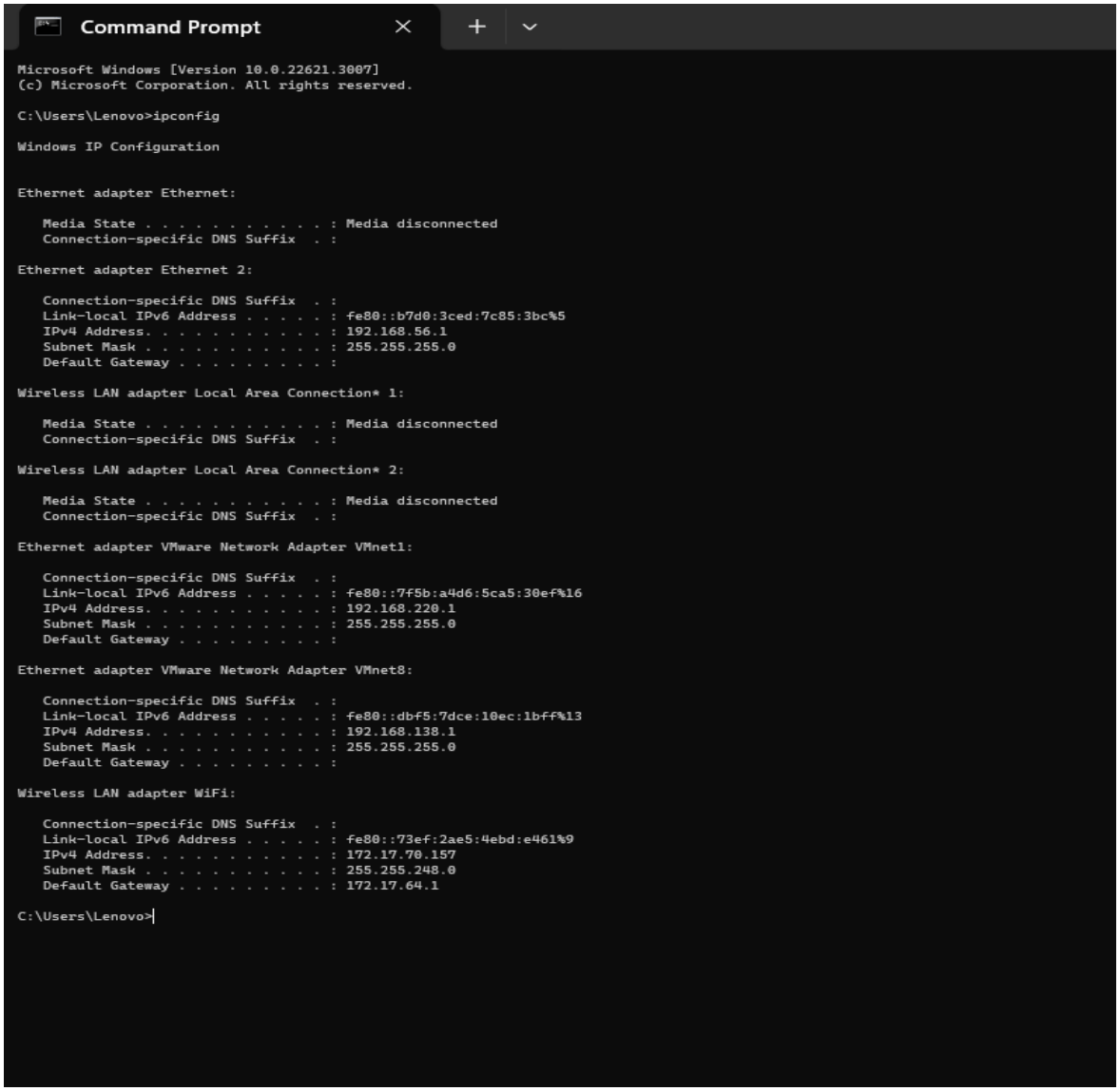
Deadline: 31-Jan-2024

Name: Poli Vardhini Reddy

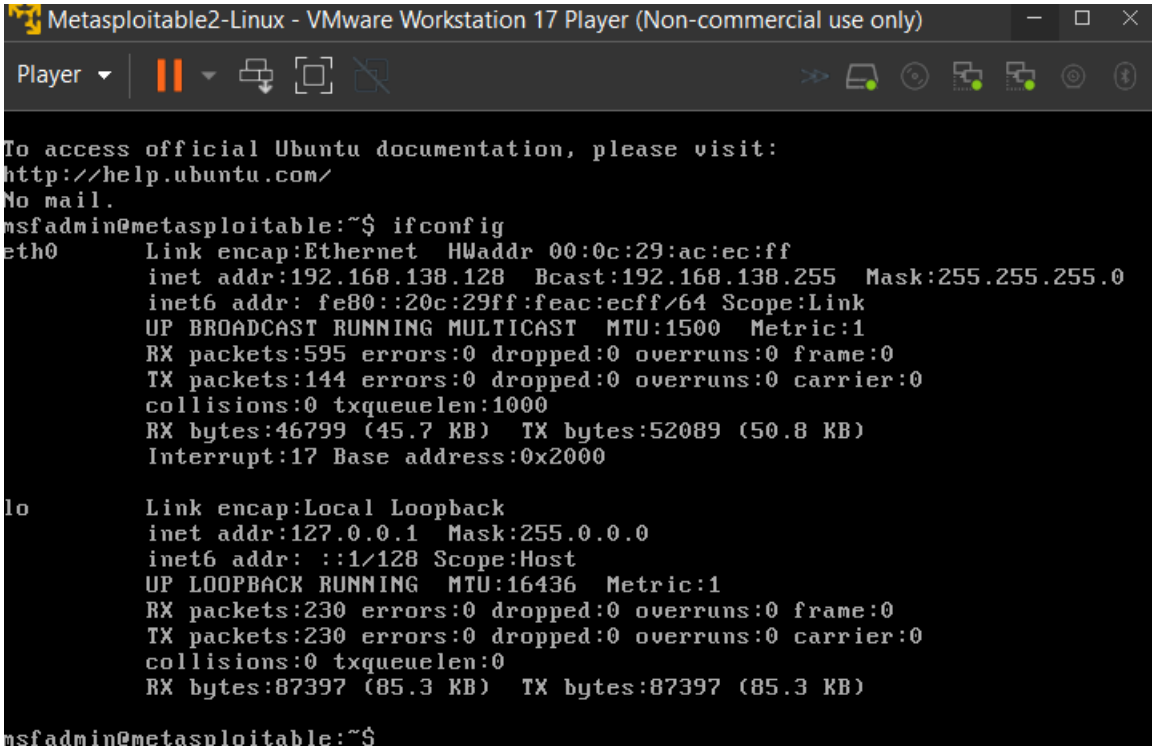
Register number: 21BIT0382

Give screenshot of System IP, Kali Linux IP and Metasploitable IP

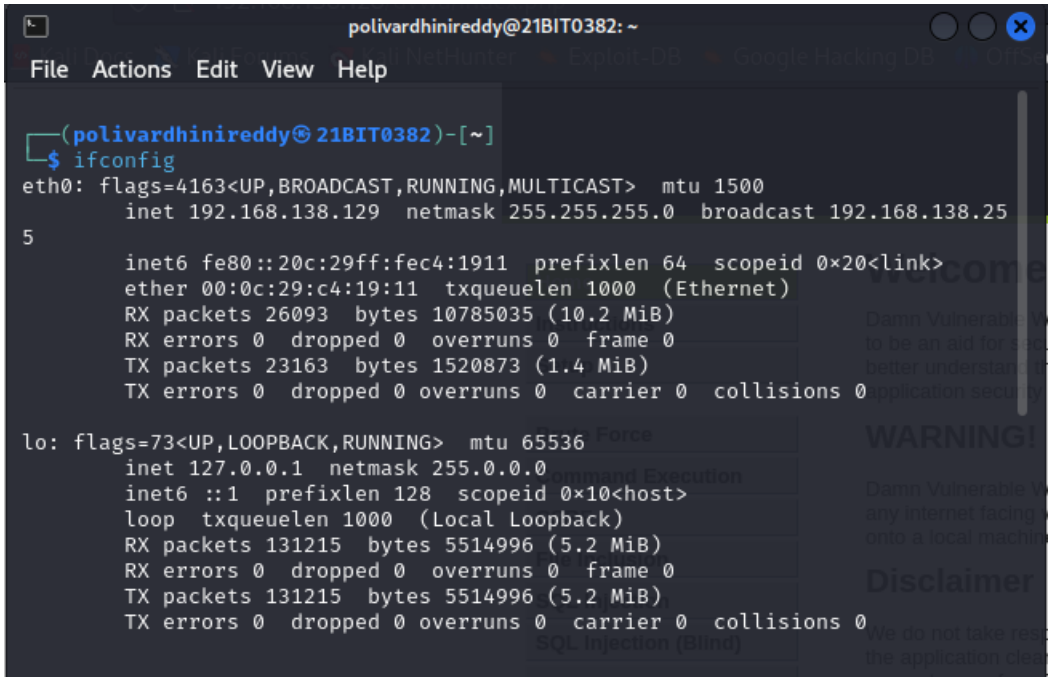
System IP



Metasploitable IP



Kali Linux IP



Question 1 [5 Marks] Marks : 10

Perform the following scans and give the purpose of each of the commands listed below: Take screenshot of each scans. (the ipaddr can be of your wireless gateway or your system ip address)

1. nmap –sS ipaddr

```
┌──(root㉿21BIT0382)-[~]
└─# nmap -sS 172.17.70.157
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-31 20:20 IST
Nmap scan report for 172.17.70.157
Host is up (0.0016s latency).
Not shown: 994 filtered tcp ports (no-response)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
902/tcp  open  iss-realsecure
1521/tcp open  oracle
6881/tcp open  bittorrent-tracker

Nmap done: 1 IP address (1 host up) scanned in 4.87 seconds

┌──(root㉿21BIT0382)-[~]
```

Purpose: It is used for TCP SYN port scan (Default)

2. nmap --script http-enum ipaddr

Purpose: The command nmap --script http-enum ipaddr scans the target IP address for HTTP service details using Nmap's http-enum script.

```
┌──(root㉿21BIT0382)-[~]
└─# nmap --script http-enum 172.17.70.157
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-31 20:22 IST
Nmap scan report for 172.17.70.157
Host is up (0.0034s latency).
Not shown: 993 filtered tcp ports (no-response)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
902/tcp  open  iss-realsecure
912/tcp  open  apex-mesh
1521/tcp open  oracle
6881/tcp open  bittorrent-tracker

Nmap done: 1 IP address (1 host up) scanned in 9.90 seconds
```

3. nmap -p 80,443 ipaddr (which port is open and closed)

```
┌──(root㉿21BIT0382)-[~]
└─# nmap -p 80,443 172.17.70.157
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-31 20:24 IST
Nmap scan report for 172.17.70.157
Host is up (0.00087s latency).

PORT    STATE    SERVICE
80/tcp  filtered http
443/tcp filtered https

Nmap done: 1 IP address (1 host up) scanned in 1.37 seconds
```

Purpose: The command nmap -p 80,443 ipaddr scans ports 80 and 443 on the specified IP address to identify open HTTP and HTTPS services.

Typically, open ports are displayed with the "open" status, and closed ports may be marked as "closed" or "filtered" depending on the response received during the scan.

Port 80/tcp – closed

Port 443/tcp - closed

4. nmap -p T:8888,443 ipaddr (what is the service name which is closed on 8888)

```
┌──(root㉿21BIT0382)-[~]
└─# nmap -p T:8888,443 172.17.70.157
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-31 20:26 IST
Nmap scan report for 172.17.70.157
Host is up (0.0012s latency).

PORT     STATE    SERVICE
443/tcp  filtered https
8888/tcp filtered sun-answerbook

Nmap done: 1 IP address (1 host up) scanned in 1.35 seconds
```

The service name is sun-answerbook which is closed on 8888

Purpose: The command nmap -p T:8888,443 ipaddr scans for open ports 8888 and 443 on the specified IP address using TCP SYN scan to identify potential HTTP and HTTPS services.

5. nmap Chennai.vit.ac.in (determine the rdns record value and which are open and closed ports)

```
┌──(root㉿21BIT0382)-[~]
└─# nmap Chennai.vit.ac.in
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-31 20:28 IST
Nmap scan report for Chennai.vit.ac.in (122.187.117.186)
Host is up (0.0034s latency).
Other addresses for Chennai.vit.ac.in (not scanned): 115.240.194.16
rDNS record for 122.187.117.186: nsg-corporate-186.117.187.122.airtel.in
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE
21/tcp  open  ftp
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 4.95 seconds
```

Purpose: The command nmap Chennai.vit.ac.in is used to perform a network scan on the domain Chennai.vit.ac.in to identify open ports and services.

rDns record for 122.187.117.186: nsg-corporate-186.117.187.122.airtel.in

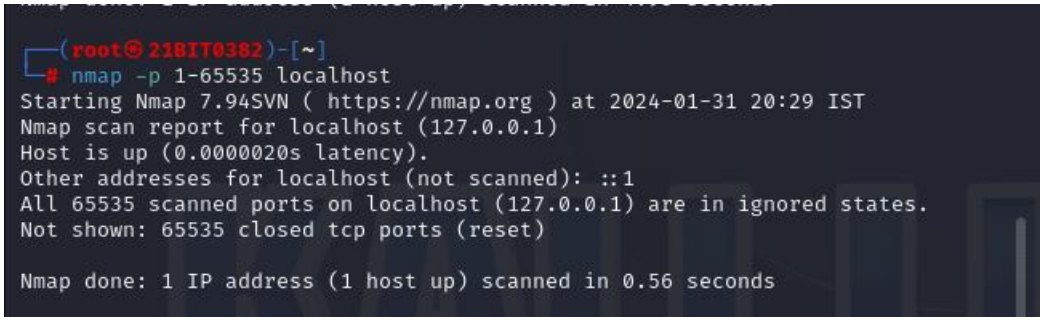
21/tcp – open

80/tcp – open

443/tcp – open

997 closed tcp ports

6. nmap -p 1-65535 localhost (which are the open and known ports)

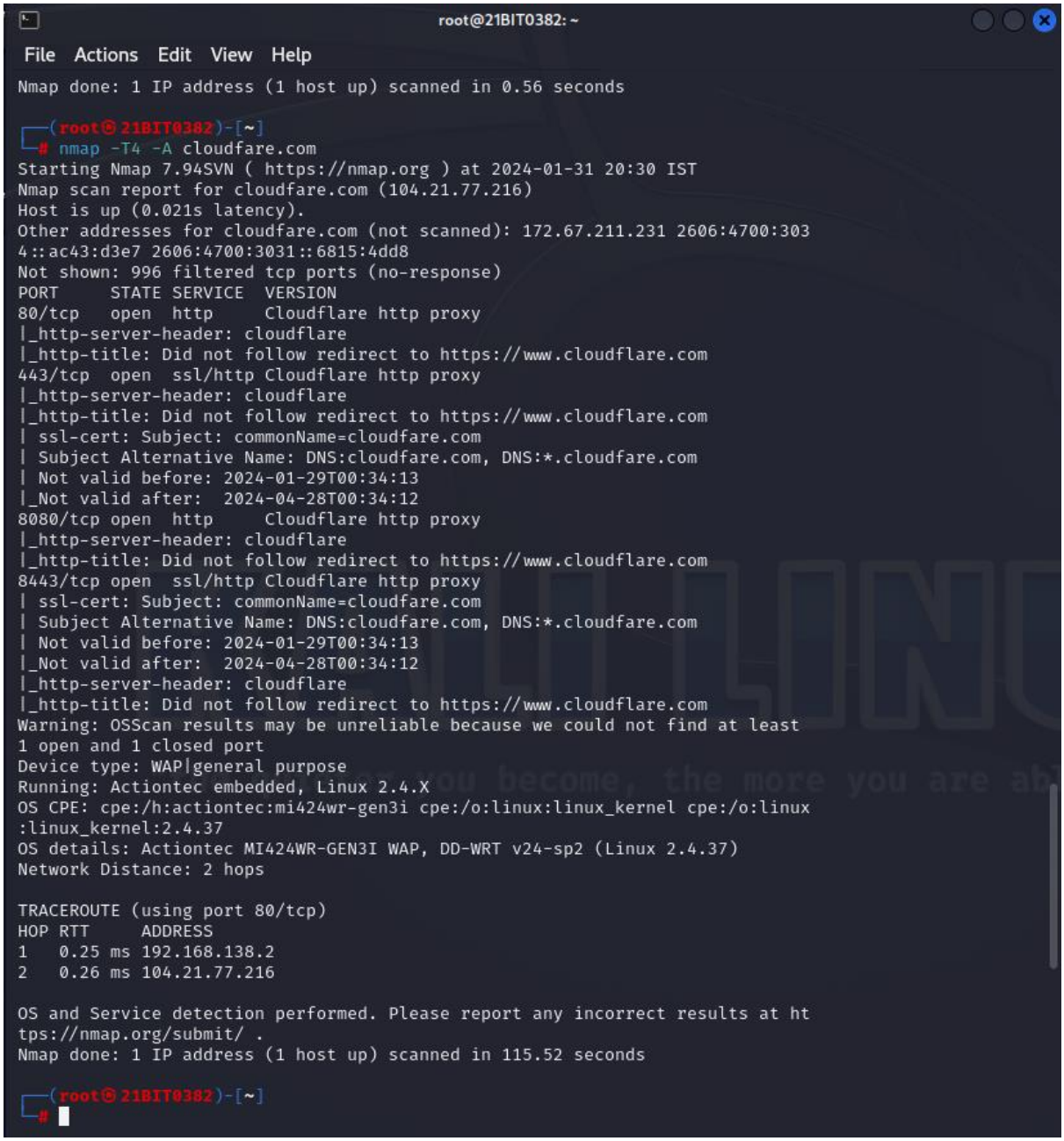


65535 closed tcp ports

purpose: The command nmap -p 1-65535 localhost scans all TCP ports (1 through 65535) on the local machine to identify open ports and services.

7. nmap -T4 -A cloudflare.com (from the complete output, give only the trace route result)

Purpose: The command nmap -T4 -A cloudflare.com performs an aggressive scan with increased timing against the domain cloudflare.com to gather detailed information about the target's operating system, services, and versions.



Traceroute result:

```
TRACEROUTE (using port 80/tcp)
HOP RTT     ADDRESS
1   0.25 ms 192.168.138.2
2   0.26 ms 104.21.77.216

OS and Service detection performed. Please report any incorrect results at ht
tps://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 115.52 seconds
```

8. nmap -Pn --script vuln ipaddr (how many ports are filtered)

```
┌──(root㉿21BIT0382)-[~]
└─# nmap -Pn --script vuln 172.17.70.157
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-31 20:38 IST
Nmap scan report for 172.17.70.157
Host is up (0.0015s latency).
Not shown: 994 filtered tcp ports (no-response)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
902/tcp  open  iss-realsecure
912/tcp  open  apex-mesh
1521/tcp open  oracle

Host script results:
|_smb-vuln-ms10-061: Could not negotiate a connection:SMB: Failed to receive bytes: ERROR
|_samba-vuln-cve-2012-1182: Could not negotiate a connection:SMB: Failed to receive bytes: ERROR
|_smb-vuln-ms10-054: false

Nmap done: 1 IP address (1 host up) scanned in 33.40 seconds
```

994 filtered tcp ports

Purpose: The command nmap -Pn --script vuln ipaddr scans the specified IP address while skipping host discovery and runs Nmap's vulnerability scripts to identify potential security vulnerabilities on the target system.

9. nmap -A ipaddr

```
┌──(root㉿21BIT0382)-[~]
└─# nmap -A 172.17.70.157
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-31 20:40 IST
Nmap scan report for 172.17.70.157
Host is up (0.0013s latency).
Not shown: 993 filtered tcp ports (no-response)
PORT     STATE SERVICE             VERSION
135/tcp  open  msrpc               Microsoft Windows RPC
139/tcp  open  netbios-ssn         Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
902/tcp  open  ssl/vmware-auth     VMware Authentication Daemon 1.10 (Uses VNC, SOAP)
912/tcp  open  vmware-auth         VMware Authentication Daemon 1.0 (Uses VNC, SOAP)
1521/tcp open  oracle-tns          Oracle TNS Listener 10.2.0.3.0 (for 32-bit Windows)
6881/tcp open  bittorrent-tracker?
| fingerprint-strings:
|   Kerberos:
|     N?'"o
|     hE4E
|     X+6;
|     {9C5
|     116cq
|     0~ed
|   TLSSessionReq:
|     'nra
|     #Q\xd2'
|_    EGJN/
1 service unrecognized despite returning data. If you know the service/version, please submit the f
ollowing fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port6881-TCP:V=7.94SVN%I=7%D=1/31%Time=65BA633A%P=x86_64-pc-linux-gnu%r
SF:(TLSSessionReq,1D1,"\x8b\xa1Dz6\xd3\xf3\xefCDf\xc3\xf9\xe3\$\*\xcd\xb4\
SF:xeb\xe4!\xb2\?z\x01\xcfL\xbe\x88y\x8b\x04\|c\xb7\xdc&V\xdc\xfbclD\xeeY\
SF:.\xd0/\xd5\xd2W\x99w\xd4\xfa4\xd8\xd7\xb0F\xd5:\xd9\x87M\xb2\$MQ\xd5\xd
SF:8\|\0nA\xd1F\xd22\xceqG\x82:\x8e\$r\0\xb5ee\xba\xfbc\(x\x08\x95M\xd8\xa
SF:d\x83\[\xd9S\x88\xc4\xc9u\xdbk'\t\xb5!\x9a@u,\xae\xae\x92\xe9e\xe6=\xde
SF:tr\x82-\t\xd6\)\x8e\x16\xd6\xc7K7\xd7\xc4\x8c\xc7'nra\x08\^\xd23\xff\(\
SF:xae\x06\xc0h-\xf3X\xb4\xa5\x0fB\xea}X\x12\x9ej\xfb\x98G<\x1cN\x0e\xcf\x
SF:15\xd1\x140\xee\n\xb9N\0\xec\x03D\x88W\xd0#\x8d\x8dB\n\xafe>\xa2_\xf3\x
SF:cc\xa5o\x86\xf5bp-\xb9G\n\xe1\x82P\x04\xe6\x0b\x9a\\2\xd2\xe3\xe7\xe4\x
SF:91\xc9\xda\x11\x8c\xe9\x80\xa43WI\xa1t\x0eHjI\xc0\xa28\xb8\xec\xa4\x07-
SF:N\x80\xa6#\xa6\x9e\n\x03\xb1\x9a\xfe\x14\xa0N\xa6\xd1\xe3_\xf5Z\xa5\t\x
SF:96\xcc\xccd~@\xce\x82\xac\xc3\xab\xfd\xd7\r\xdb\x80#Q\\\xd2'\xa2\xf4\xa
SF:f_\x16p@!\\0\xd1<\xdeU\x87\x13\xc7\x92,\x0e\^3\x82\x20\xb4\xc7\x0f4\0\x
SF:8a\xd7\x18\xcb\xe2}\x8a\xc9\xab\x0b=\xd0\xb1\xe8t\xd7\xdd\xe5\xa70\x94\
SF:x124\xd3}\xa6\x20\xc4EGJN/\x9cN\x80\xd3\x02\xa2\xa2\xa05N\xc0F1\x84\xa5
SF:\rv@\xfa\xdcZ\xbco\xbd\xe8\xaf@\x9a\xb5\xb9\$\xbb\)\xf4\xba\n\xc9\x97=,
SF:\x8d\x9b\xab>Xm\xef\.\xe0G\xc7Od\x08Z\x8a\x9b\xfe@\xab\x84#%;\xa3\xe7\x
SF:85{\xedL\xf9\x96\x9b\xdc>VR\xee\xd0c\xd0\xd1\xd3\x1e\|\x96\x11\^\xe1x\x
SF:ec&\x96HEg\x205\xfa\xb5\xa5\xf4\xce\x195\xbe")%r(Kerberos,11A,"N\?'\"o\
```

```
SF:15\xd1\x14O\xee\n\xb9N\0\xec\x03D\x88W\xd0#\x8d\x8dB\n\xafe>\xa2_\xf3\x
SF:cc\xa5o\x86\xf5bp-\xb9G\n\xe1\x82P\x04\xe6\x0b\x9a\\2\xd2\xe3\xe7\xe4\x
SF:91\xc9\xda\x11\x8c\xe9\x80\xa43WI\xa1t\x0eHjI\xc0\xa28\xb8\xec\xa4\x07-
SF:N\x80\xa6#\xa6\x9e\n\x03\xb1\x9a\xfe\x14\xa0N\xa6\xd1\xe3_\xf5Z\xa5\t\x
SF:96\xcc\xccd~@\xce\x82\xac\xc3\xab\xfd\xd7\r\xdb\x80#Q\\\xd2'\xa2\xf4\xa
SF:f_\x16p@!\\0\xd1<\xdeU\x87\x13\xc7\x92,\x0e\^3\x82\x20\xb4\xc7\x0f4\0\x
SF:8a\xd7\x18\xcb\xe2}\x8a\xc9\xab\x0b=\xd0\xb1\xe8t\xd7\xdd\xe5\xa70\x94\
SF:x124\xd3}\xa6\x20\xc4EGJN/\x9cN\x80\xd3\x02\xa2\xa2\xa05N\xc0F1\x84\xa5
SF:\rv@\xfa\xdcZ\xbco\xbd\xe8\xaf@\x9a\xb5\xb9\$\xbb\)\xf4\xba\n\xc9\x97=,
SF:\x8d\x9b\xab>Xm\xef\.\xe0G\xc7Od\x08Z\x8a\x9b\xfe@\xab\x84#%;\xa3\xe7\x
SF:85{\xedL\xf9\x96\x9b\xdc>VR\xee\xd0c\xd0\xd1\xd3\x1e\|\x96\x11\^\xe1x\x
SF:ec&\x96HEg\x205\xfa\xb5\xa5\xf4\xce\x195\xbe")%r(Kerberos,11A,"N\?'\"o\
SF:x91\xa1w\xb2\xdfbY\(\xa3\x18\?\xda\xd7s\xae7k\xc2\x83\xdb\xd4\x9e\xdfu\
SF:xef\xef\x8b\xe6P\xd8\xe7\xbc\xe3pY\x92\xd3J\+}\xe6hE4E\xd2\.\+\x11\xe7\
SF:xb7\t\xf5@\xea\xfd\xf6\xd4\x94\xac2\xd9\x88\x88L\x979ym\x14\xdd-\xf8\x0
SF:5\xd3\xcf\x88h\x04v\x1cW\[\xbb\x07\xb6\x9d\xe1X\+6;\xf2\x19\x0f\xe1TC\x
SF:92\xea\xcd\xda\xdb{9C5\xc3\xee\xb3\0&h\xcf\xb5kD\xce116cq\xe7\|\x80\x85
SF:\xb9\$\x96\x12\x0c\xcb\xa3\xfeL\xc8\xe8\x94\x8ep\x82\\'\xcfi\x06\xb4\x8
SF:4>\xd4\x16~p\xf2\x87\xfb\xe9j\x8e\xdd\x12\xefZ\xd9D\xfd\xb8R\)\xe1\x80\
SF:x12\xcaL\xa5\x16\xbe\xda\xdd\x82xP\xaa\x16F\xc5'\x8a\x83\x983\xa1\xaf\x
SF:c9O\t7s\xb8\x8c\xc2\xf0\x18>\xcd\x90V\xdc/\xfe\x7fR\xa0x\x93\x8bY\xa90~
SF:ed\xe1\x9b<\xdd\x9feK\x99\x99\x8b\+\x9bG\x07\|=\xc0\xdc\xc4\xee\+s\0\xb
SF:5\xb4y\xa0'\]\x94\xe0\xb8\x08x\x84\x8c\xaf\x7f\xd7\xdc\?\xfeQ\xdb\x80\x
SF:e0\xf7\n\x8cB\]p\x9a7");
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed po
rt
Device type: general purpose
Running: Microsoft Windows XP|7|2012
OS CPE: cpe:/o:microsoft:windows_xp::sp3 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_server
_2012
OS details: Microsoft Windows XP SP3 or Windows 7 or Windows Server 2012
Network Distance: 2 hops
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2024-01-31T15:13:29
|_  start_date: N/A
|_clock-skew: -1s

TRACEROUTE (using port 445/tcp)
HOP RTT     ADDRESS
1   0.95 ms 192.168.138.2
2   1.07 ms 172.17.70.157

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/
 .
Nmap done: 1 IP address (1 host up) scanned in 180.43 seconds
```

Purpose: The command nmap -A ipaddr performs an aggressive scan on the specified IP address, providing detailed information about the target's operating system, services, and versions.

10. What is the command to scan ipv6 address?

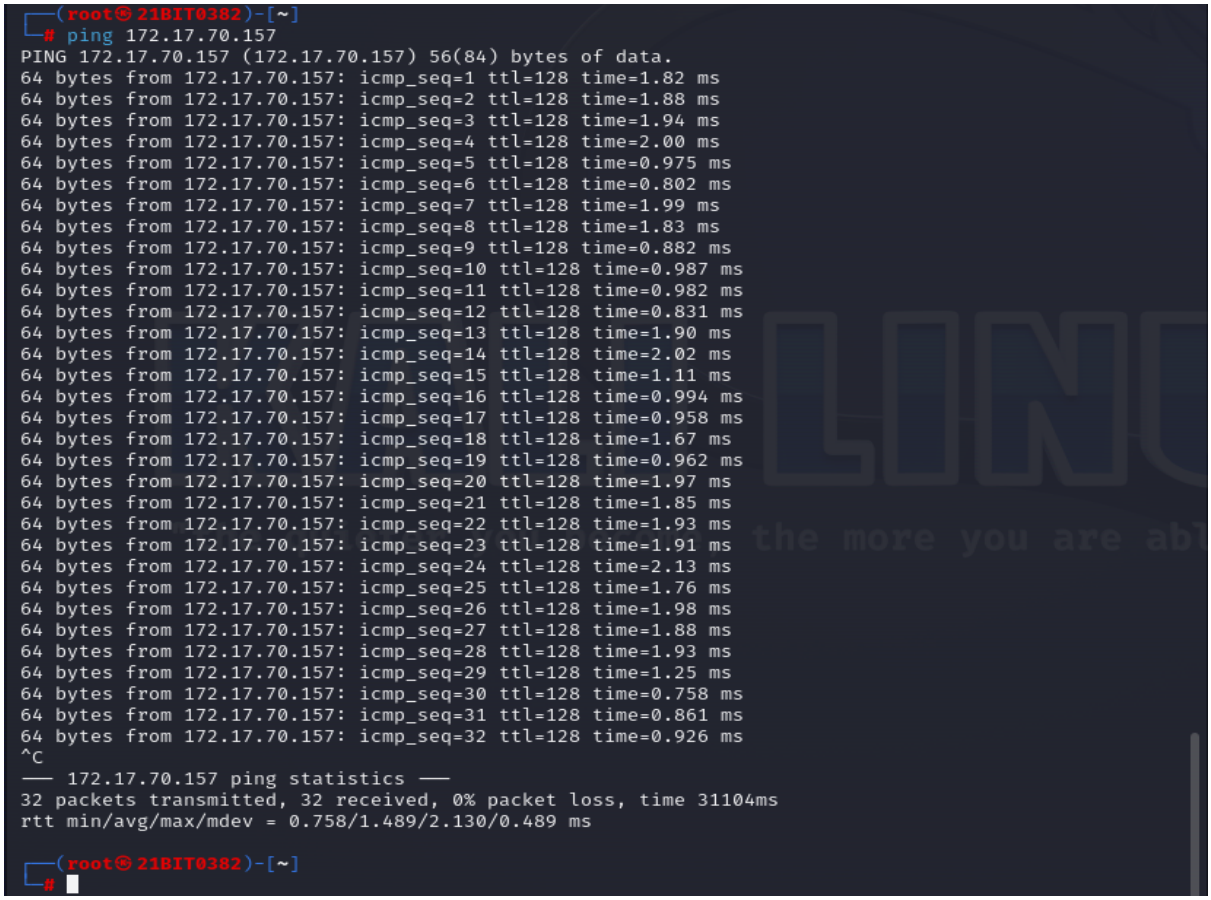
```
┌──(root㉿21BIT0382)-[~]
└─# nmap -6 fe80::20c:29ff:fec4:1911
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-31 21:29 IST
Nmap scan report for fe80::20c:29ff:fec4:1911
Host is up (0.000014s latency).
All 1000 scanned ports on fe80::20c:29ff:fec4:1911 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in 0.21 seconds
```

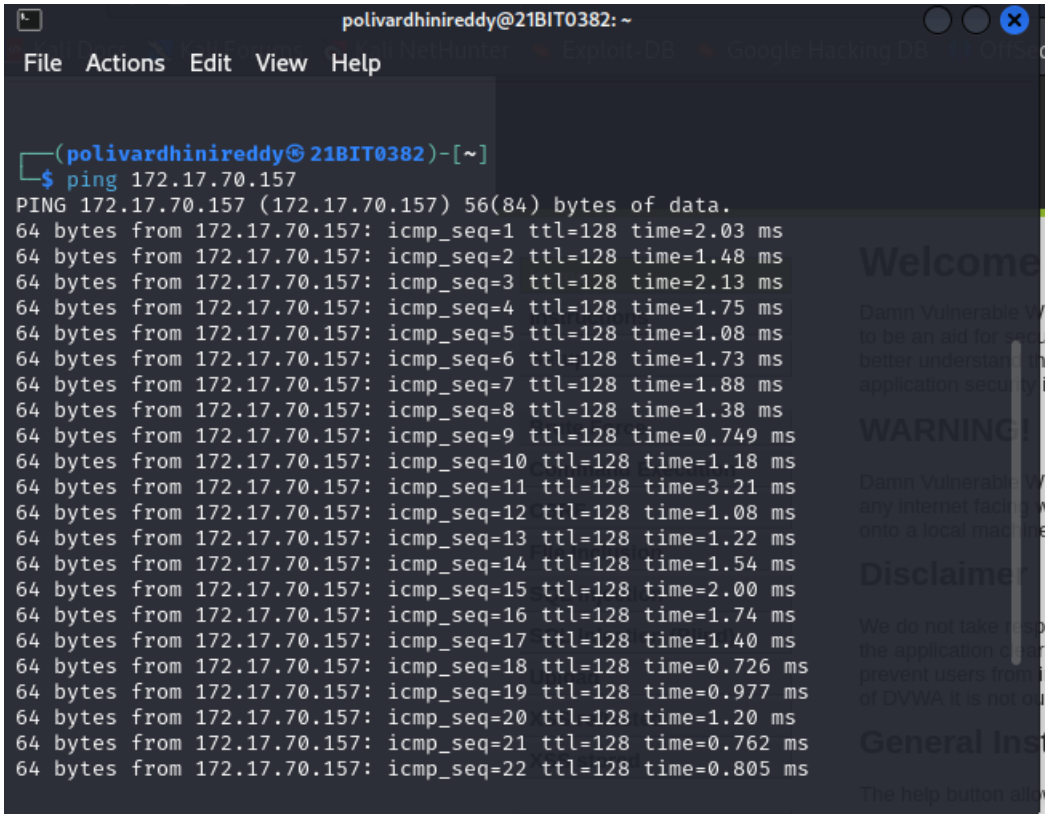
Purpose: These commands help manage and troubleshoot IPv6-related configurations on network devices. If you have a specific aspect of IPv6 commands you are inquiring about, please provide more details for a more accurate response.

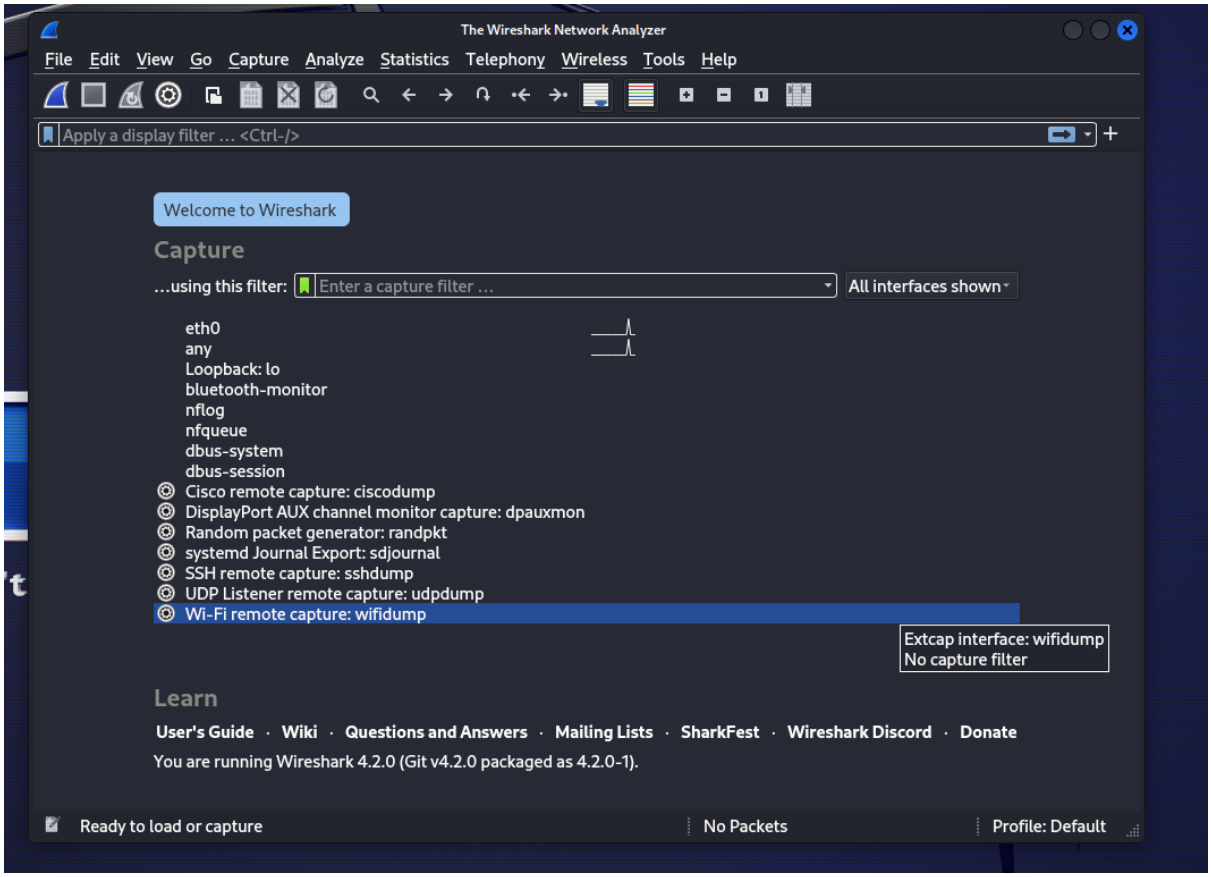
Question 2 [2 Marks]

Perform a Ping of Metaploitable IP on Kali Linux command and observe the packets in Wireshark. Give 2 screenshots one for pinging to metasploitable IP and another for wireshark capturing request and response packets to metasploitable IP.

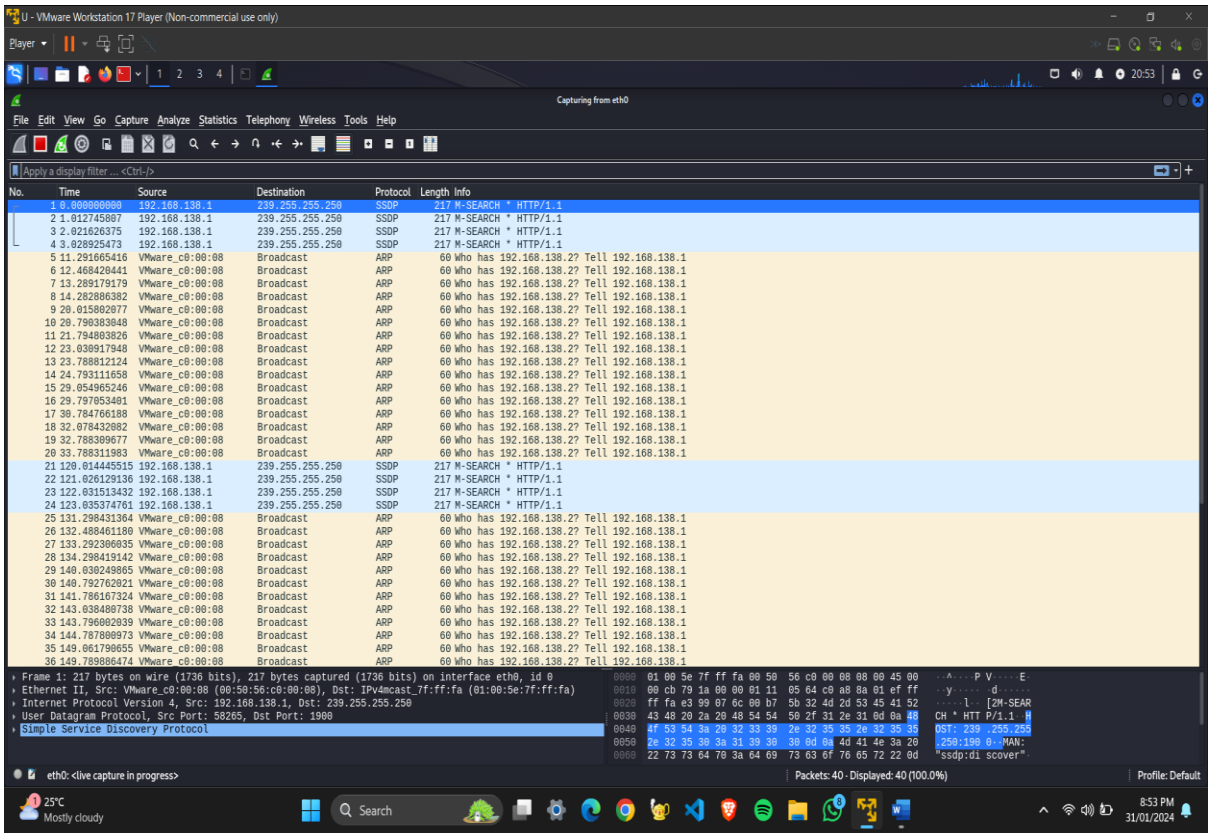
Performing ping of metasploatable ip on kali linux

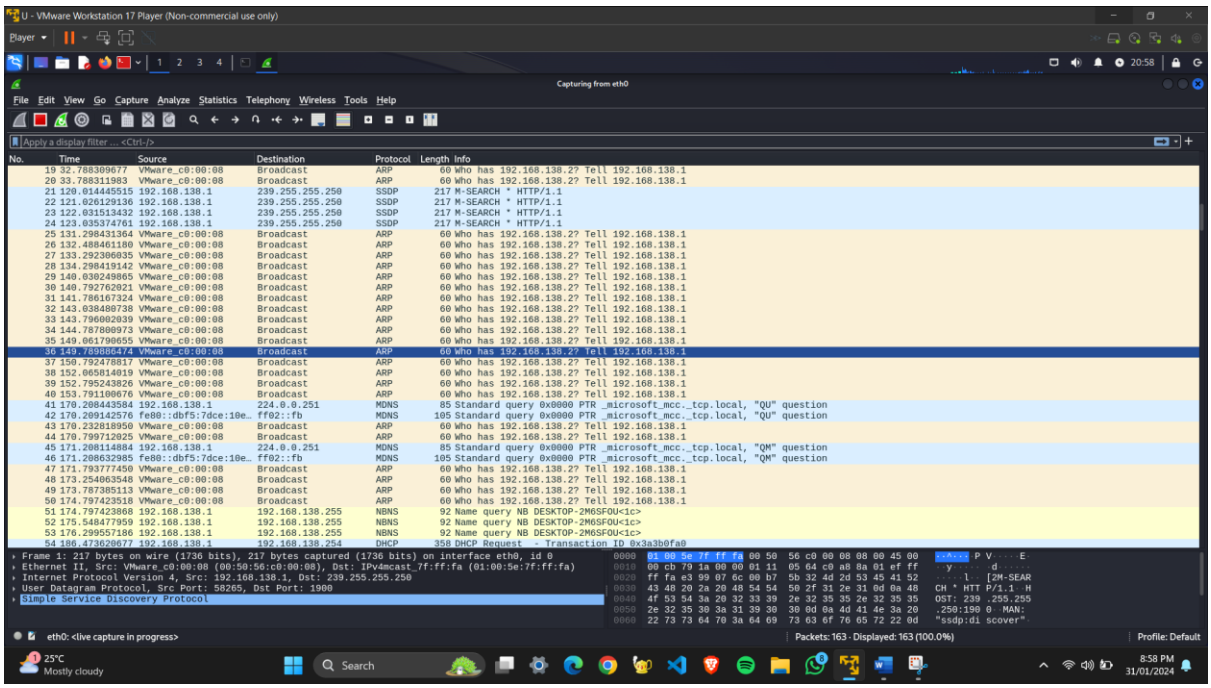


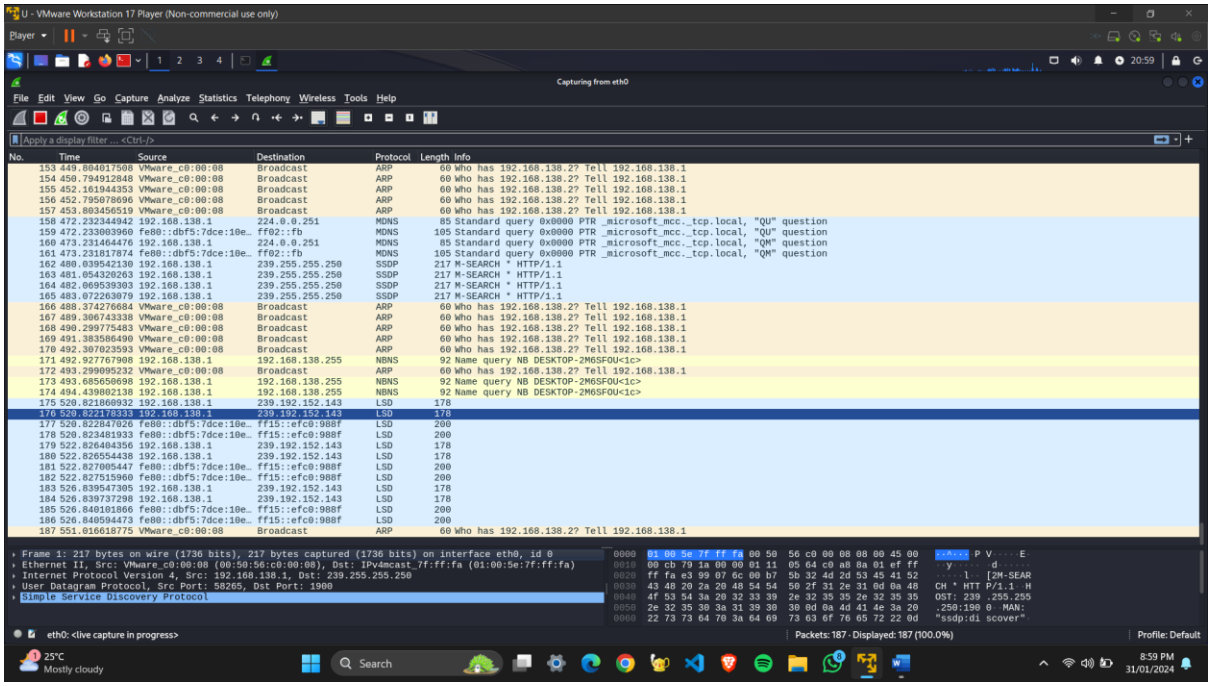

polivardhinireddy@21BIT0382: ~
File Actions Edit View Help
(polivardhinireddy㉿21BIT0382)-[~]
$ ping 172.17.70.157
PING 172.17.70.157 (172.17.70.157) 56(84) bytes of data.
64 bytes from 172.17.70.157: icmp_seq=1 ttl=128 time=2.03 ms
64 bytes from 172.17.70.157: icmp_seq=2 ttl=128 time=1.48 ms
64 bytes from 172.17.70.157: icmp_seq=3 ttl=128 time=2.13 ms
64 bytes from 172.17.70.157: icmp_seq=4 ttl=128 time=1.75 ms
64 bytes from 172.17.70.157: icmp_seq=5 ttl=128 time=1.08 ms
64 bytes from 172.17.70.157: icmp_seq=6 ttl=128 time=1.73 ms
64 bytes from 172.17.70.157: icmp_seq=7 ttl=128 time=1.88 ms
64 bytes from 172.17.70.157: icmp_seq=8 ttl=128 time=1.38 ms
64 bytes from 172.17.70.157: icmp_seq=9 ttl=128 time=0.749 ms
64 bytes from 172.17.70.157: icmp_seq=10 ttl=128 time=1.18 ms
64 bytes from 172.17.70.157: icmp_seq=11 ttl=128 time=3.21 ms
64 bytes from 172.17.70.157: icmp_seq=12 ttl=128 time=1.08 ms
64 bytes from 172.17.70.157: icmp_seq=13 ttl=128 time=1.22 ms
64 bytes from 172.17.70.157: icmp_seq=14 ttl=128 time=1.54 ms
64 bytes from 172.17.70.157: icmp_seq=15 ttl=128 time=2.00 ms
64 bytes from 172.17.70.157: icmp_seq=16 ttl=128 time=1.74 ms
64 bytes from 172.17.70.157: icmp_seq=17 ttl=128 time=1.40 ms
64 bytes from 172.17.70.157: icmp_seq=18 ttl=128 time=0.726 ms
64 bytes from 172.17.70.157: icmp_seq=19 ttl=128 time=0.977 ms
64 bytes from 172.17.70.157: icmp_seq=20 ttl=128 time=1.20 ms
64 bytes from 172.17.70.157: icmp_seq=21 ttl=128 time=0.762 ms
64 bytes from 172.17.70.157: icmp_seq=22 ttl=128 time=0.805 ms

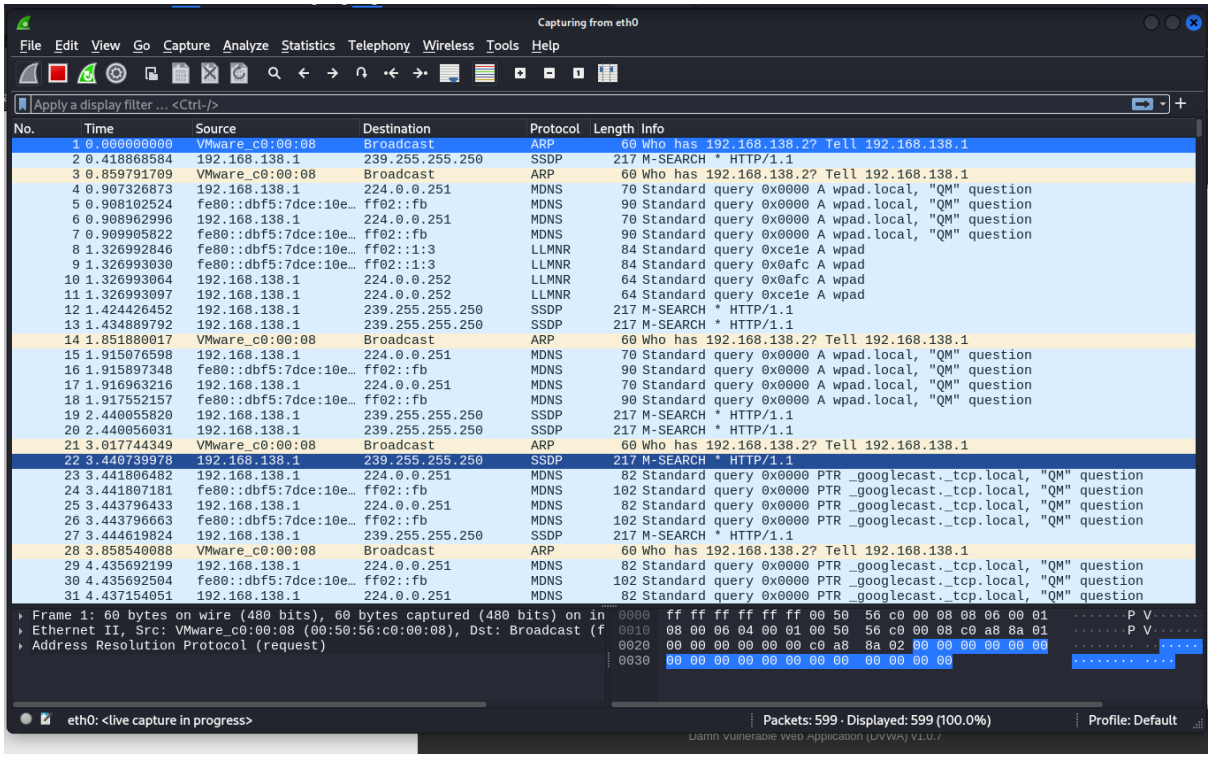

The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Welcome to Wireshark
Capture
...using this filter: Enter a capture filter ...
All interfaces shown
eth0
any
Loopback: lo
bluetooth-monitor
nflog
nfqueue
dbus-system
dbus-session
Cisco remote capture: ciscodump
DisplayPort AUX channel monitor capture: dpauxmon
Random packet generator: randpkt
systemd Journal Export: sdjournal
SSH remote capture: sshdump
UDP Listener remote capture: udpdump
Wi-Fi remote capture: wifidump
Extcap interface: wifidump
No capture filter
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord · Donate
You are running Wireshark 4.2.0 (Git v4.2.0 packaged as 4.2.0-1).
Ready to load or capture
No Packets
Profile: Default

Observing packets in WireShark.





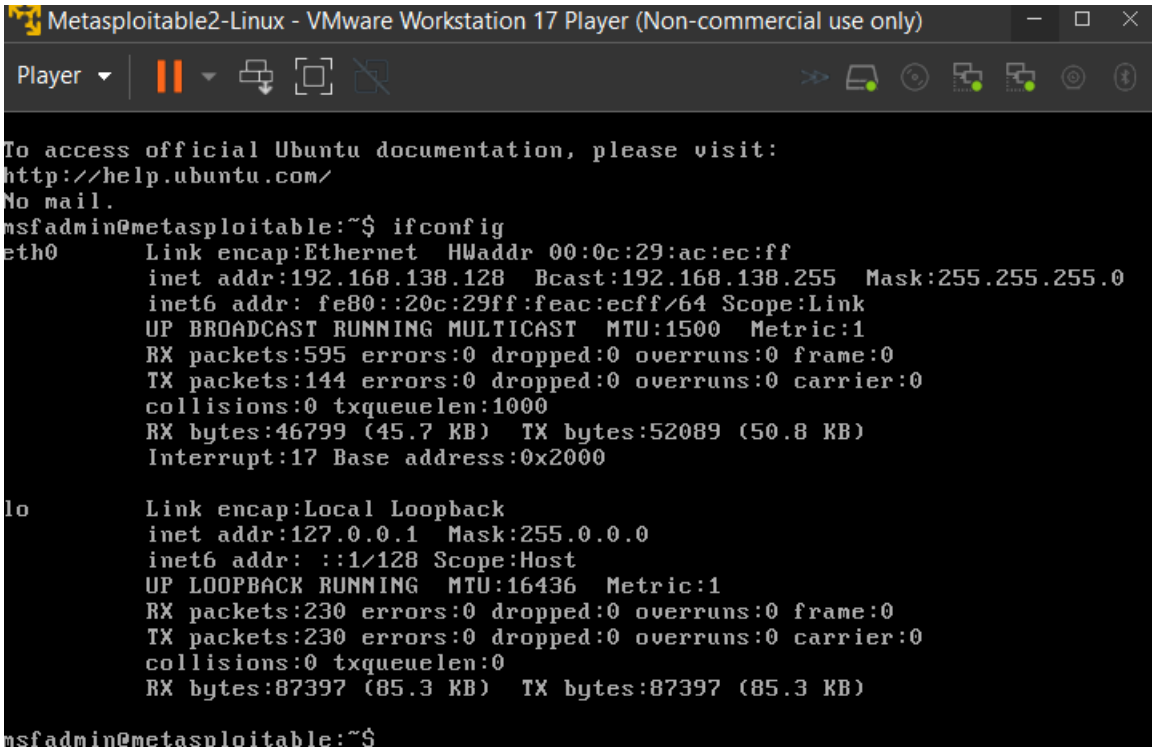


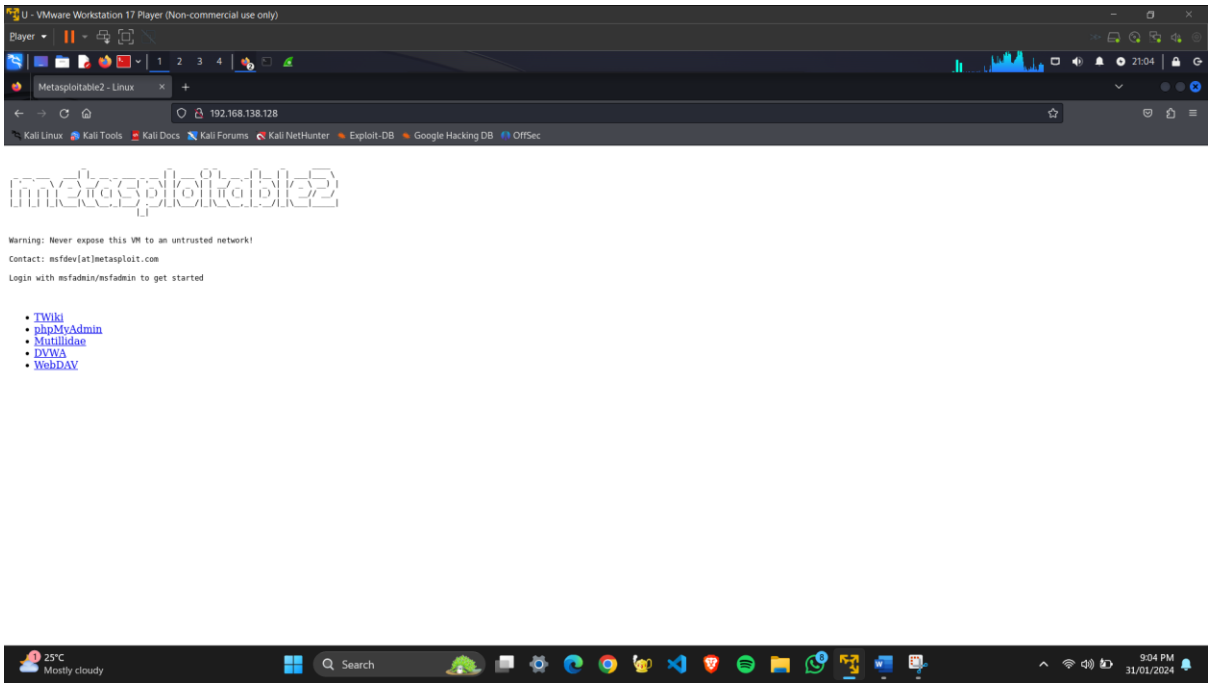


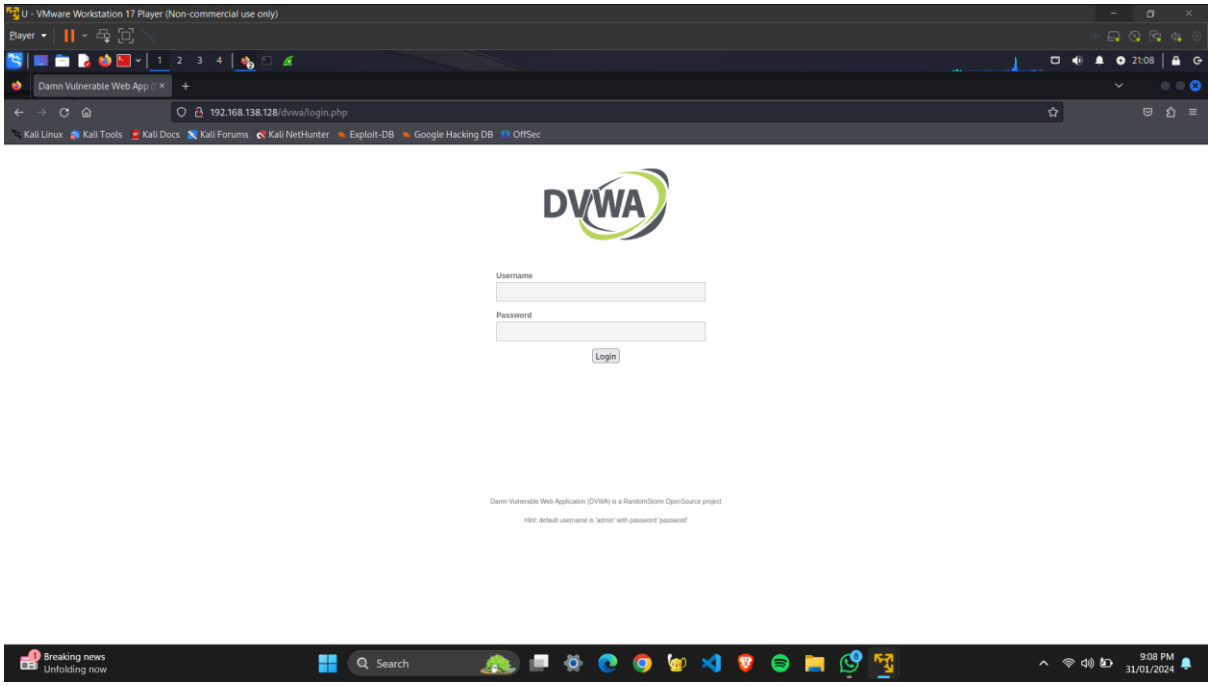
Question 3 [3 Marks]

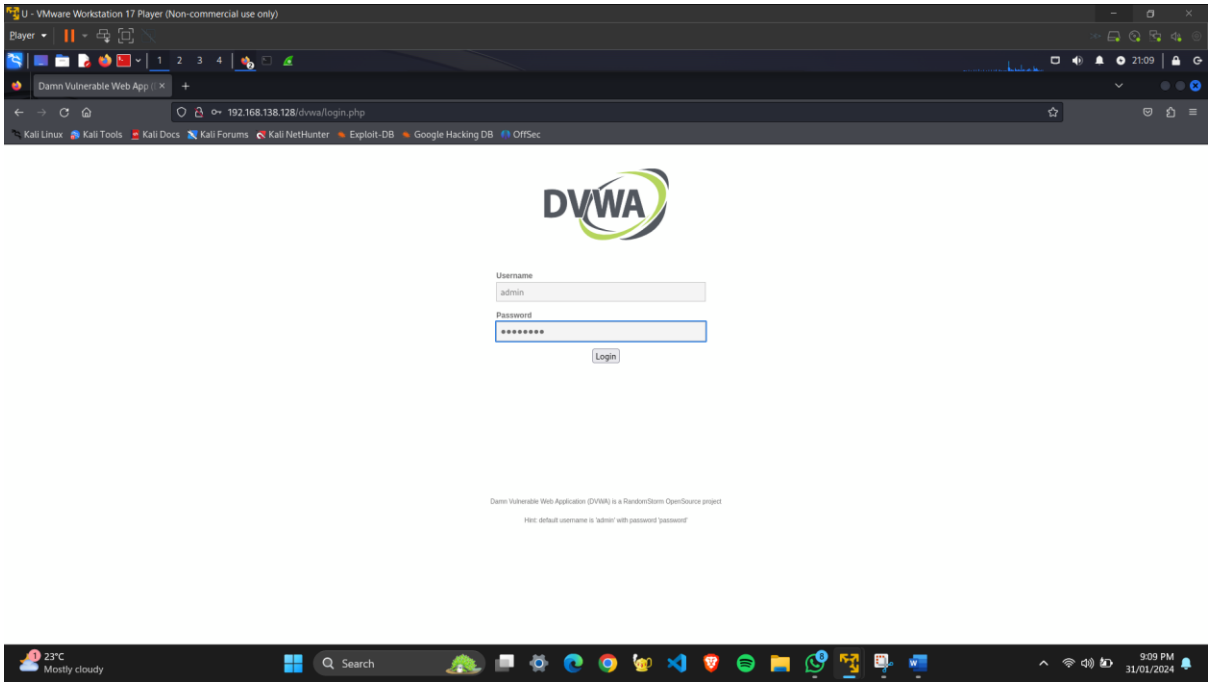
Open Wireshark and start capturing packets. Open Metasploitable IP from Kali Linux browser and visit DVWA website. Go to login page and login with the given credentials in the website. Perform a password sniffing on Wireshark after login. Also give the screenshot of flow graph and perform an HTTP analysis.

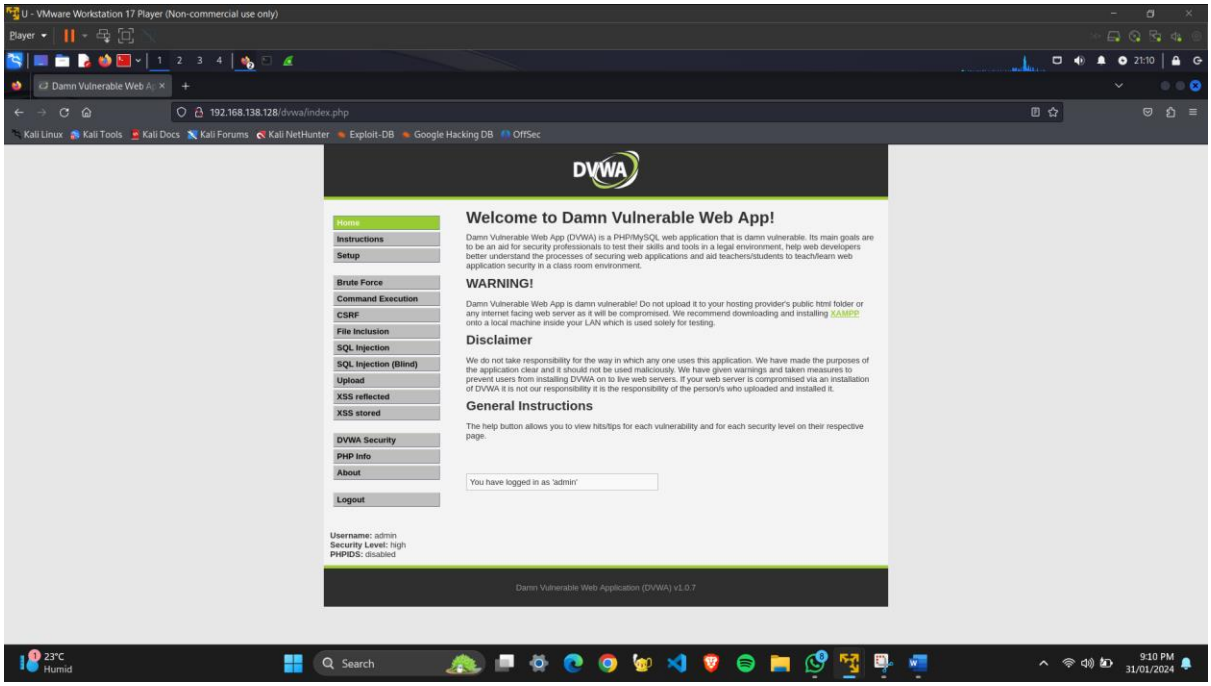
Opening Metasploitable IP from Kali Linux browser and visiting DVWA website



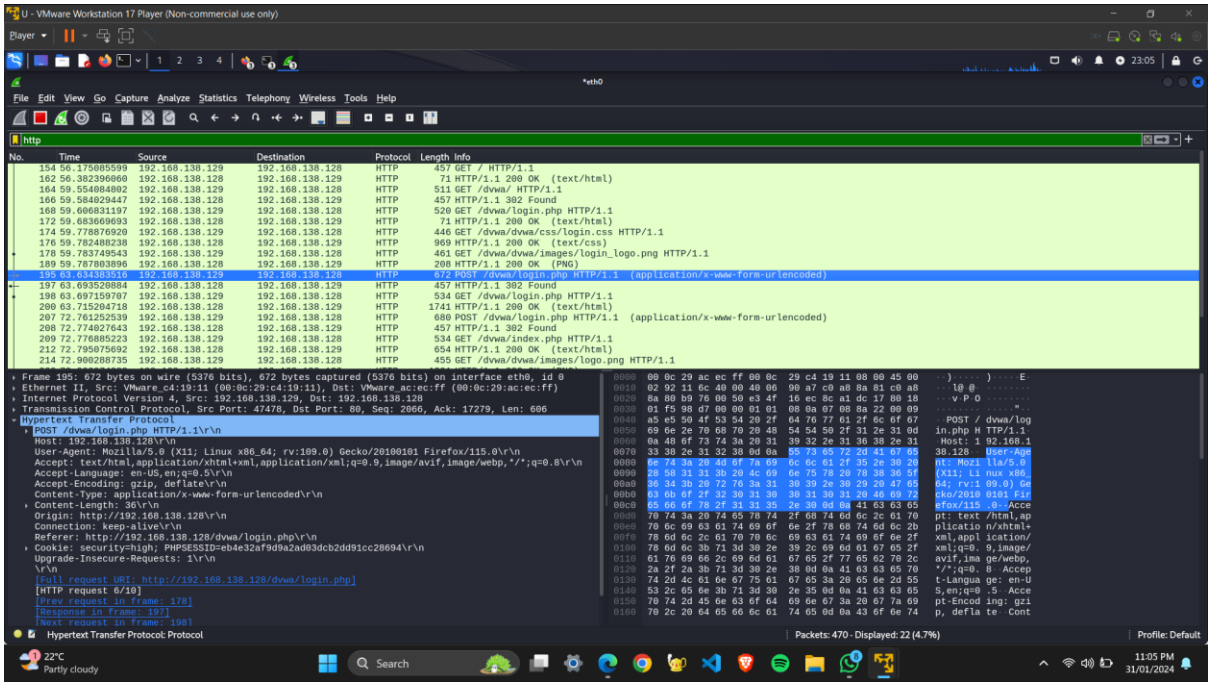



U - VMware Workstation 17 Player (Non-commercial use only)
Player
Damn Vulnerable Web App
192.168.138.128/dvwa/login.php
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
DVWA
Username
Password
Login
Damn Vulnerable Web Application (DVWA) is a RandomStorm OpenSource project
Hint: default username is 'admin' with password 'password'
Breaking news
Unfolding now
Search
9:08 PM
31/01/2024

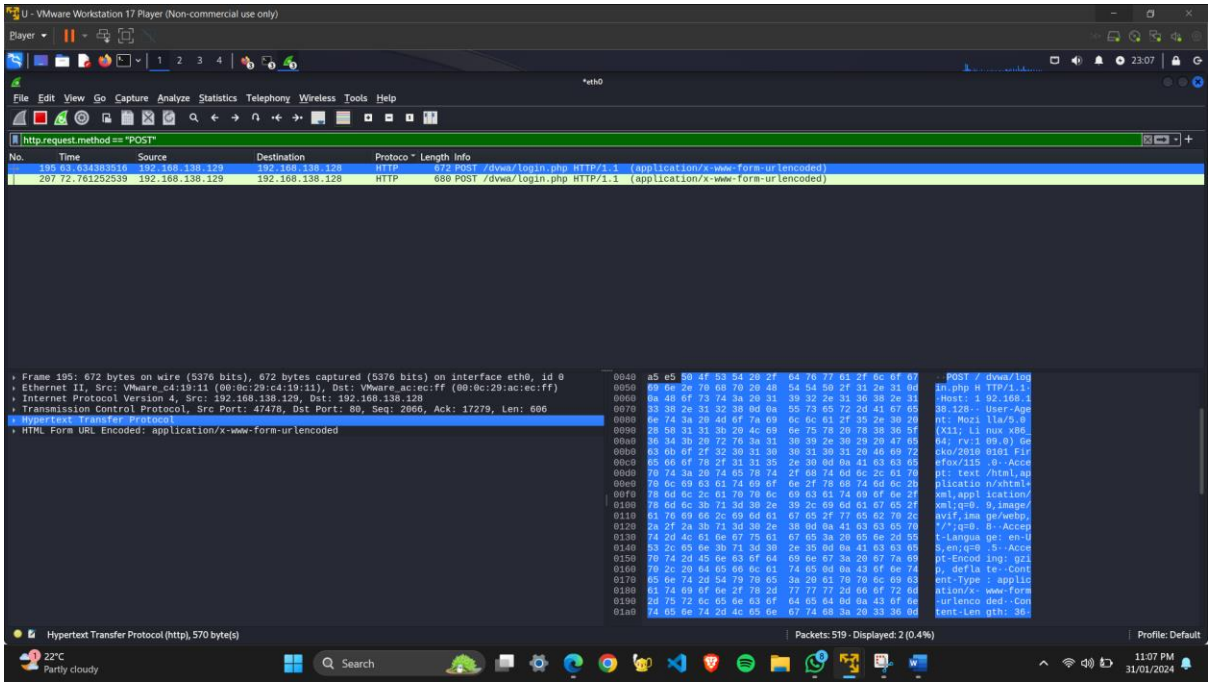

U - VMware Workstation 17 Player (Non-commercial use only)
Player
Damn Vulnerable Web App
192.168.138.128/dvwa/login.php
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
DVWA
Username
admin
Password
Login
Damn Vulnerable Web Application (DVWA) is a RandomStorm OpenSource project
Hint: default username is 'admin' with password 'password'
23°C
Mostly cloudy
Search
9:09 PM
31/01/2024

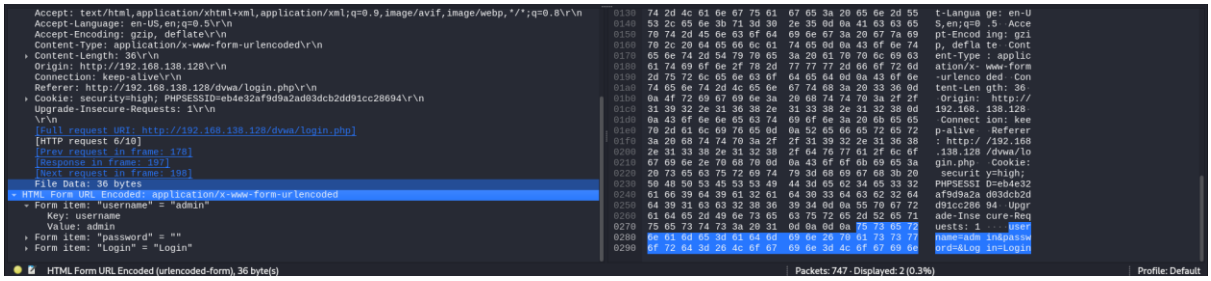


Screenshot of packets captured in Wireshark.

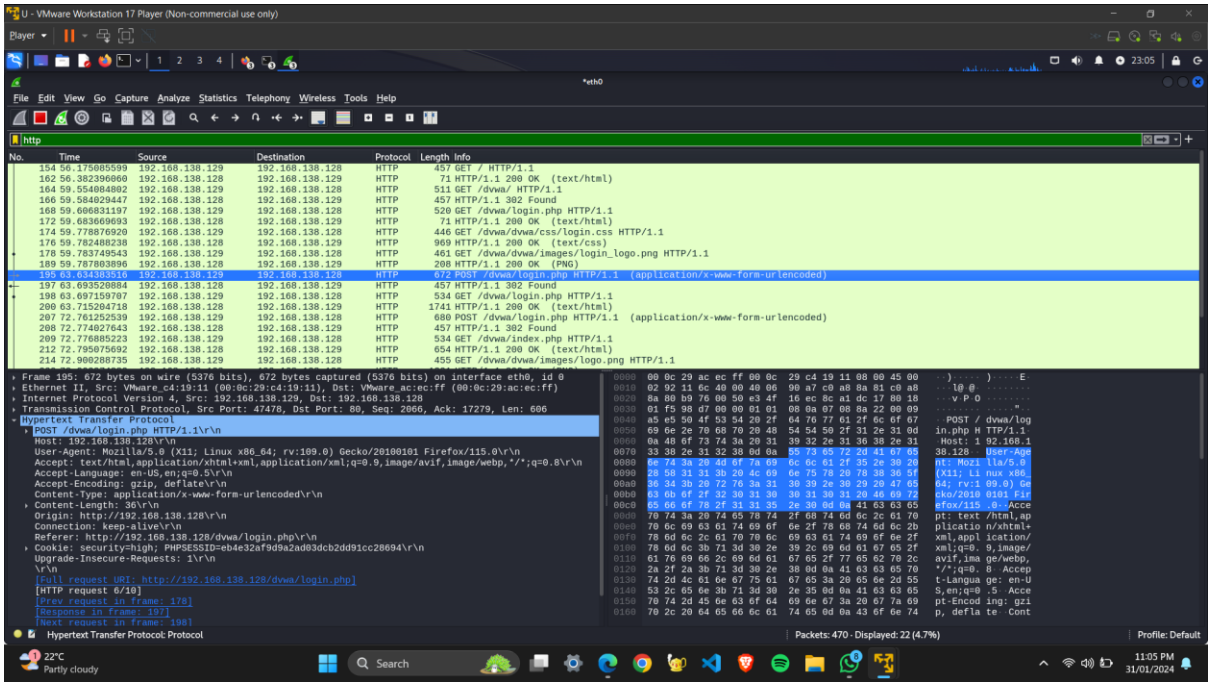


Password Sniffing

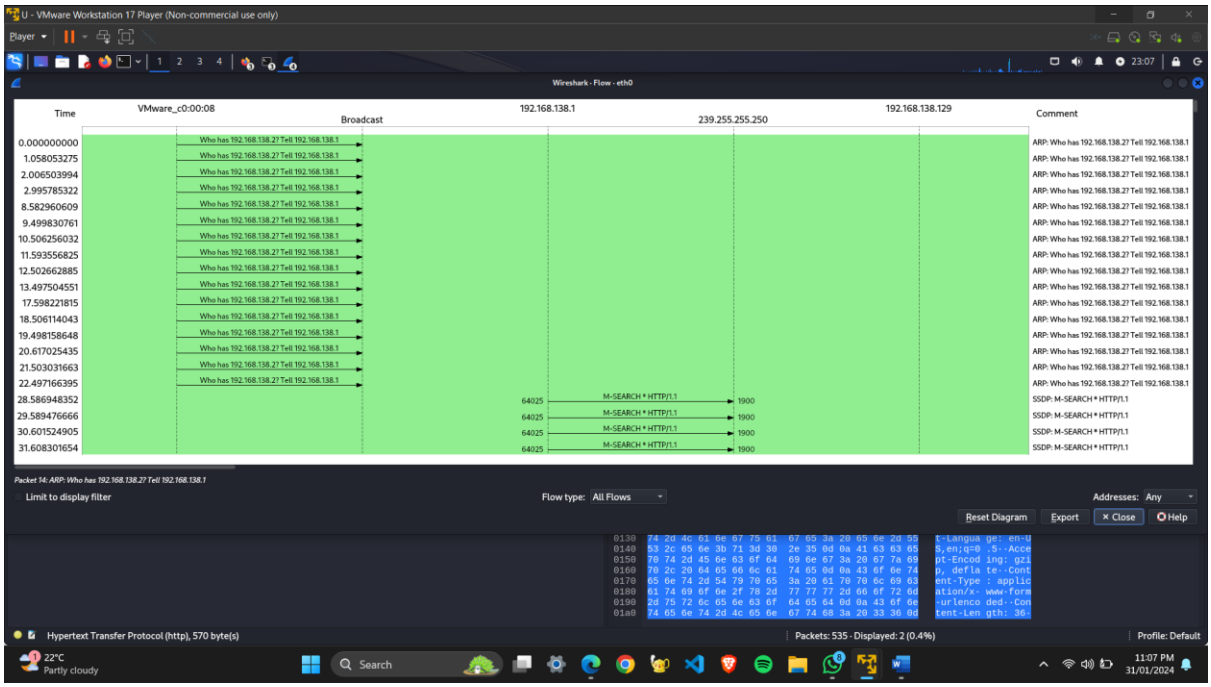


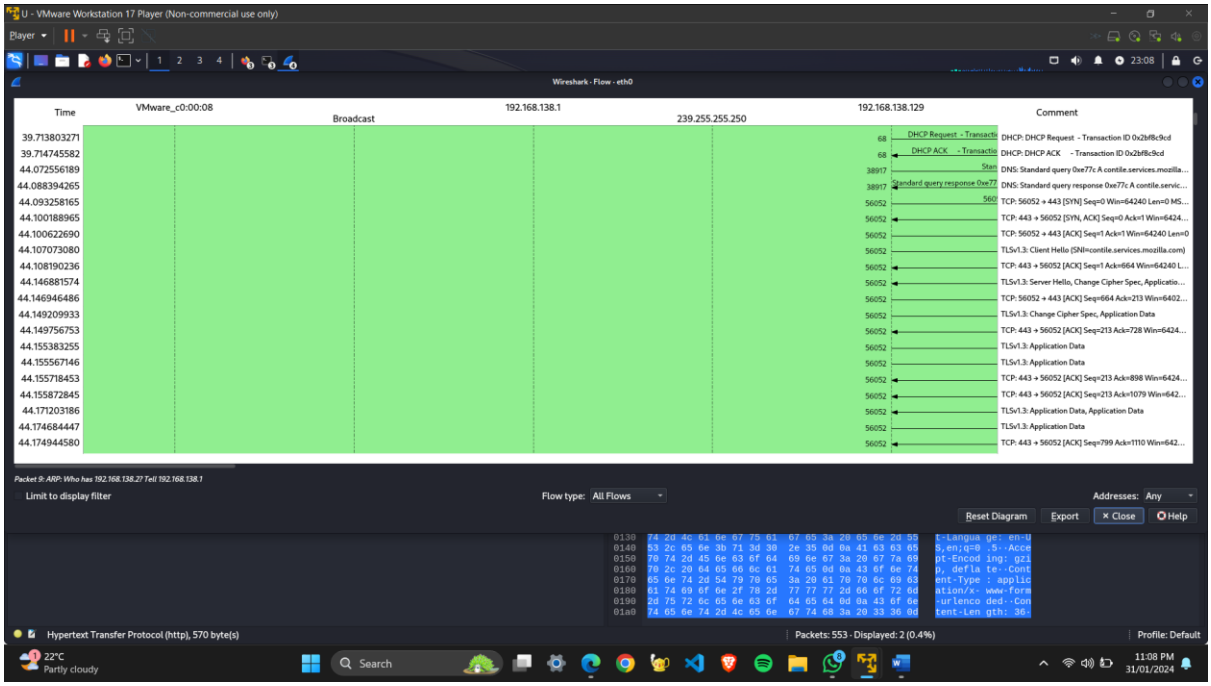


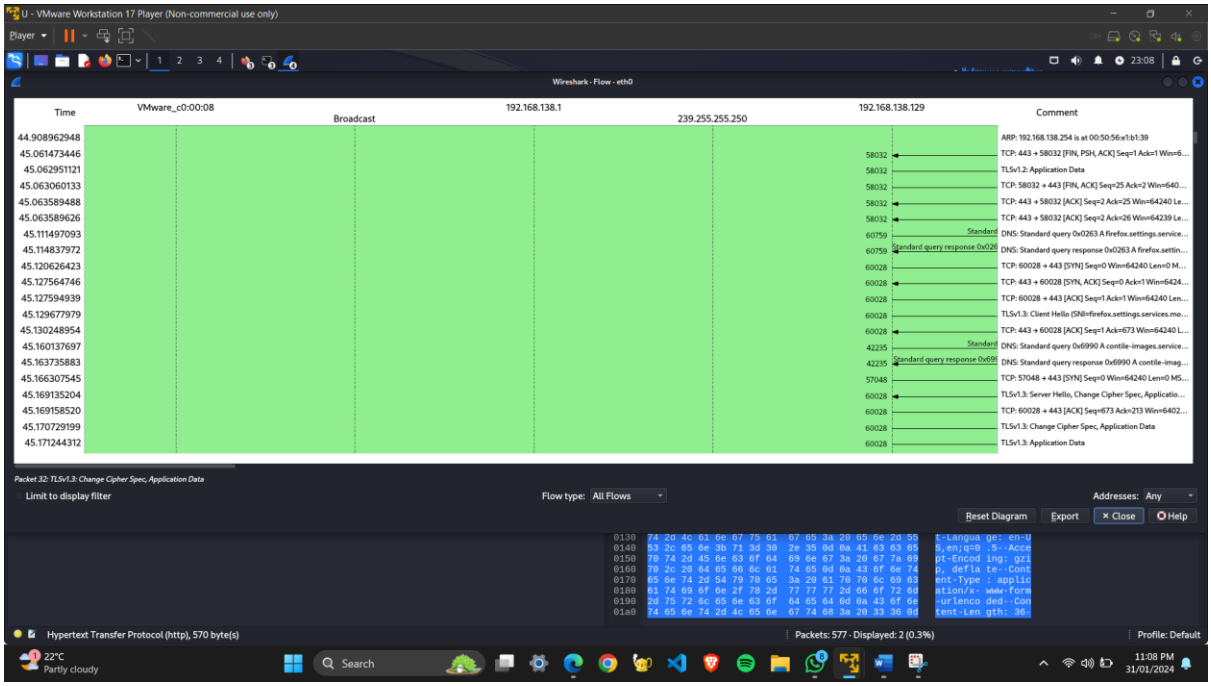
HTTP Analysis



Flow Graph


U - VMware Workstation 17 Player (Non-commercial use only)
Wireshark - Flow - eth0
Time
VMware_c0:00:08
Broadcast
192.168.138.1
239.255.255.250
192.168.138.129
Comment
Who has 192.168.138.2? Tell 192.168.138.1
ARP: Who has 192.168.138.2? Tell 192.168.138.1
M-SEARCH * HTTP/1.1
SSDP: M-SEARCH * HTTP/1.1
Limit to display filter
Flow type: All Flows
Addresses: Any
Reset Diagram
Export
Close
Help
Hypertext Transfer Protocol (http), 570 byte(s)
Packets: 535 · Displayed: 2 (0.4%)
Profile: Default
22°C
Partly cloudy
Search
11:07 PM
31/01/2024


U - VMware Workstation 17 Player (Non-commercial use only)
Wireshark - Flow - eth0
Time
VMware_c0:00:08
Broadcast
192.168.138.1
239.255.255.250
192.168.138.129
Comment
DHCP: DHCP Request - Transaction ID 0x2bf8c9cd
DHCP: DHCP ACK - Transaction ID 0x2bf8c9cd
TCP: 56052 → 443 [SYN] Seq=0 Win=64240 Len=0 MS...
TCP: 443 → 56052 [SYN, ACK] Seq=0 Ack=1 Win=6424...
TCP: 56052 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
TLSv1.3: Client Hello (SNI=contile.services.mozilla.com)
TCP: 443 → 56052 [ACK] Seq=1 Ack=664 Win=64240 L...
TLSv1.3: Server Hello, Change Cipher Spec, Applicatio...
TCP: 56052 → 443 [ACK] Seq=664 Ack=213 Win=6402...
TLSv1.3: Change Cipher Spec, Application Data
TCP: 443 → 56052 [ACK] Seq=213 Ack=728 Win=6424...
TLSv1.3: Application Data
TLSv1.3: Application Data
TCP: 443 → 56052 [ACK] Seq=213 Ack=898 Win=6424...
TCP: 443 → 56052 [ACK] Seq=213 Ack=1079 Win=642...
TLSv1.3: Application Data, Application Data
TLSv1.3: Application Data
TCP: 443 → 56052 [ACK] Seq=799 Ack=1110 Win=642...
Limit to display filter
Flow type: All Flows
Addresses: Any
Reset Diagram
Export
Close
Help
Hypertext Transfer Protocol (http), 570 byte(s)
Packets: 553 · Displayed: 2 (0.4%)
Profile: Default
22°C
Partly cloudy
Search
11:08 PM
31/01/2024


U - VMware Workstation 17 Player (Non-commercial use only)
Player
Wireshark · Flow · eth0
Time
VMware_c0:00:08
Broadcast
192.168.138.1
239.255.255.250
192.168.138.129
Comment
44.908962948 ARP: 192.168.138.254 is at 00:50:56:e1:b1:39
45.061473446 58032 TCP: 443 → 58032 [FIN, PSH, ACK] Seq=1 Ack=1 Win=6...
45.062951121 58032 TLSv1.2: Application Data
45.063060133 58032 TCP: 58032 → 443 [FIN, ACK] Seq=25 Ack=2 Win=640...
45.063589488 58032 TCP: 443 → 58032 [ACK] Seq=2 Ack=25 Win=64240 Le...
45.063589626 58032 TCP: 443 → 58032 [ACK] Seq=2 Ack=26 Win=64239 Le...
45.111497093 60759 Standard DNS: Standard query 0x0263 A firefox.settings.service...
45.114837972 60759 Standard query response 0x026 DNS: Standard query response 0x0263 A firefox.settin...
45.120626423 60028 TCP: 60028 → 443 [SYN] Seq=0 Win=64240 Len=0 M...
45.127564746 60028 TCP: 443 → 60028 [SYN, ACK] Seq=0 Ack=1 Win=6424...
45.127594939 60028 TCP: 60028 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len...
45.129677979 60028 TLSv1.3: Client Hello (SNI=firefox.settings.services.mo...
45.130248954 60028 TCP: 443 → 60028 [ACK] Seq=1 Ack=673 Win=64240 L...
45.160137697 42235 Standard DNS: Standard query 0x6990 A contile-images.service...
45.163735883 42235 Standard query response 0x69 DNS: Standard query response 0x6990 A contile-imag...
45.166307545 57048 TCP: 57048 → 443 [SYN] Seq=0 Win=64240 Len=0 MS...
45.169135204 60028 TLSv1.3: Server Hello, Change Cipher Spec, Applicatio...
45.169158520 60028 TCP: 60028 → 443 [ACK] Seq=673 Ack=213 Win=6402...
45.170729199 60028 TLSv1.3: Change Cipher Spec, Application Data
45.171244312 60028 TLSv1.3: Application Data
Packet 32: TLSv1.3: Change Cipher Spec, Application Data
Limit to display filter
Flow type: All Flows
Addresses: Any
Reset Diagram
Export
Close
Help
0130 74 2d 4c 61 6e 67 75 61 67 65 3a 20 65 6e 2d 55 t-Langua ge: en-U
0140 53 2c 65 6e 3b 71 3d 30 2e 35 0d 0a 41 63 63 65 S,en;q=0 .5··Acce
0150 70 74 2d 45 6e 63 6f 64 69 6e 67 3a 20 67 7a 69 pt-Encod ing: gzi
0160 70 2c 20 64 65 66 6c 61 74 65 0d 0a 43 6f 6e 74 p, defla te··Cont
0170 65 6e 74 2d 54 79 70 65 3a 20 61 70 70 6c 69 63 ent-Type : applic
0180 61 74 69 6f 6e 2f 78 2d 77 77 77 2d 66 6f 72 6d ation/x- www-form
0190 2d 75 72 6c 65 6e 63 6f 64 65 64 0d 0a 43 6f 6e -urlenco ded··Con
01a0 74 65 6e 74 2d 4c 65 6e 67 74 68 3a 20 33 36 0d tent-Len gth: 36·
Hypertext Transfer Protocol (http), 570 byte(s)
Packets: 577 · Displayed: 2 (0.3%)
Profile: Default
22°C
Partly cloudy
Search
11:08 PM
31/01/2024