SCHOOL OF INFORMATION TECHNOLOGY AND

ENGINEERING

DIGITAL ASSIGNMENT 1

WINTER SEMESTER 2022-23

Course : Information Security Management Lab

Marks :10

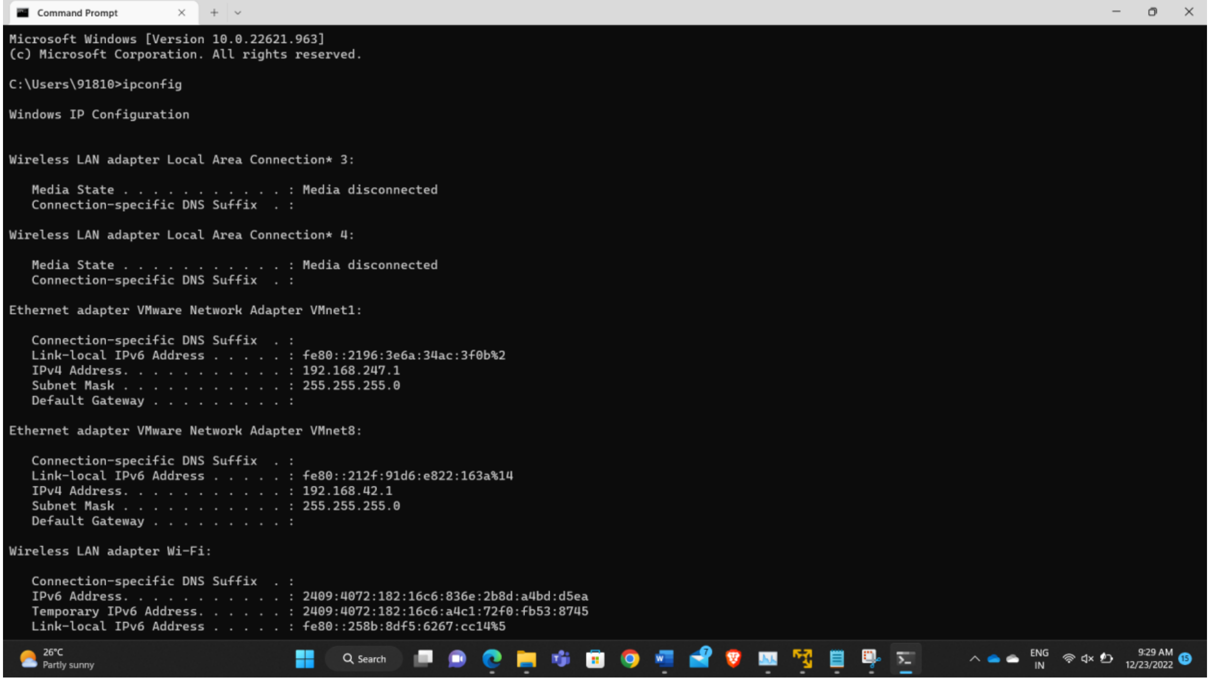
Course Code : CSE3502

Slot : L25+26

Name : Chavan Mukul Manish

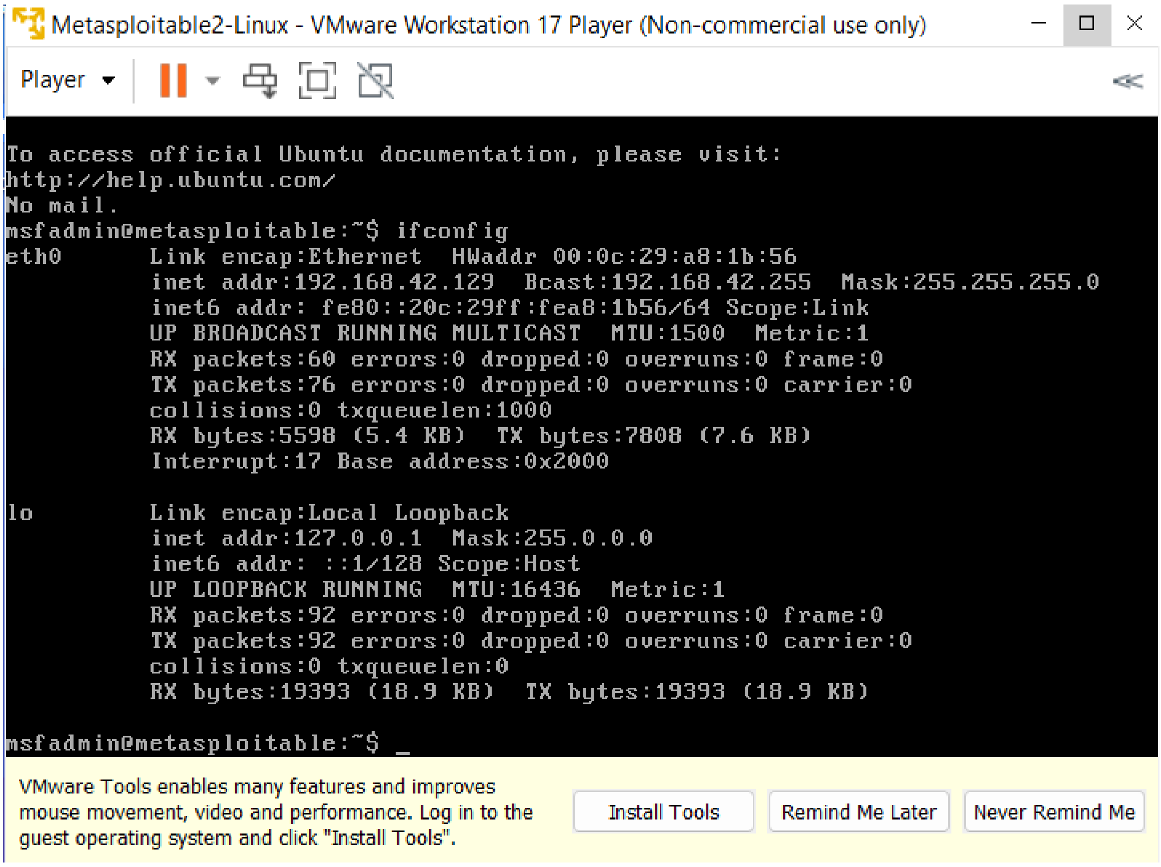
Reg no: 20BIT0238

System IP



```
Microsoft Windows [Version 10.0.22621.963]
(c) Microsoft Corporation. All rights reserved.

C:\Users\91810>ipconfig

Windows IP Configuration


Wireless LAN adapter Local Area Connection* 3:

   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::2196:3e6a:34ac:3f0b%2
   IPv4 Address. . . . . . . . . . . : 192.168.247.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Ethernet adapter VMware Network Adapter VMnet8:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::212f:91d6:e822:163a%14
   IPv4 Address. . . . . . . . . . . : 192.168.42.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2409:4072:182:16c6:836e:2b8d:a4bd:d5ea
   Temporary IPv6 Address. . . . . . : 2409:4072:182:16c6:a4c1:72f0:fb53:8745
   Link-local IPv6 Address . . . . . : fe80::258b:8df5:6267:cc14%5
```

Metasploitable IP (192.168.42.129)

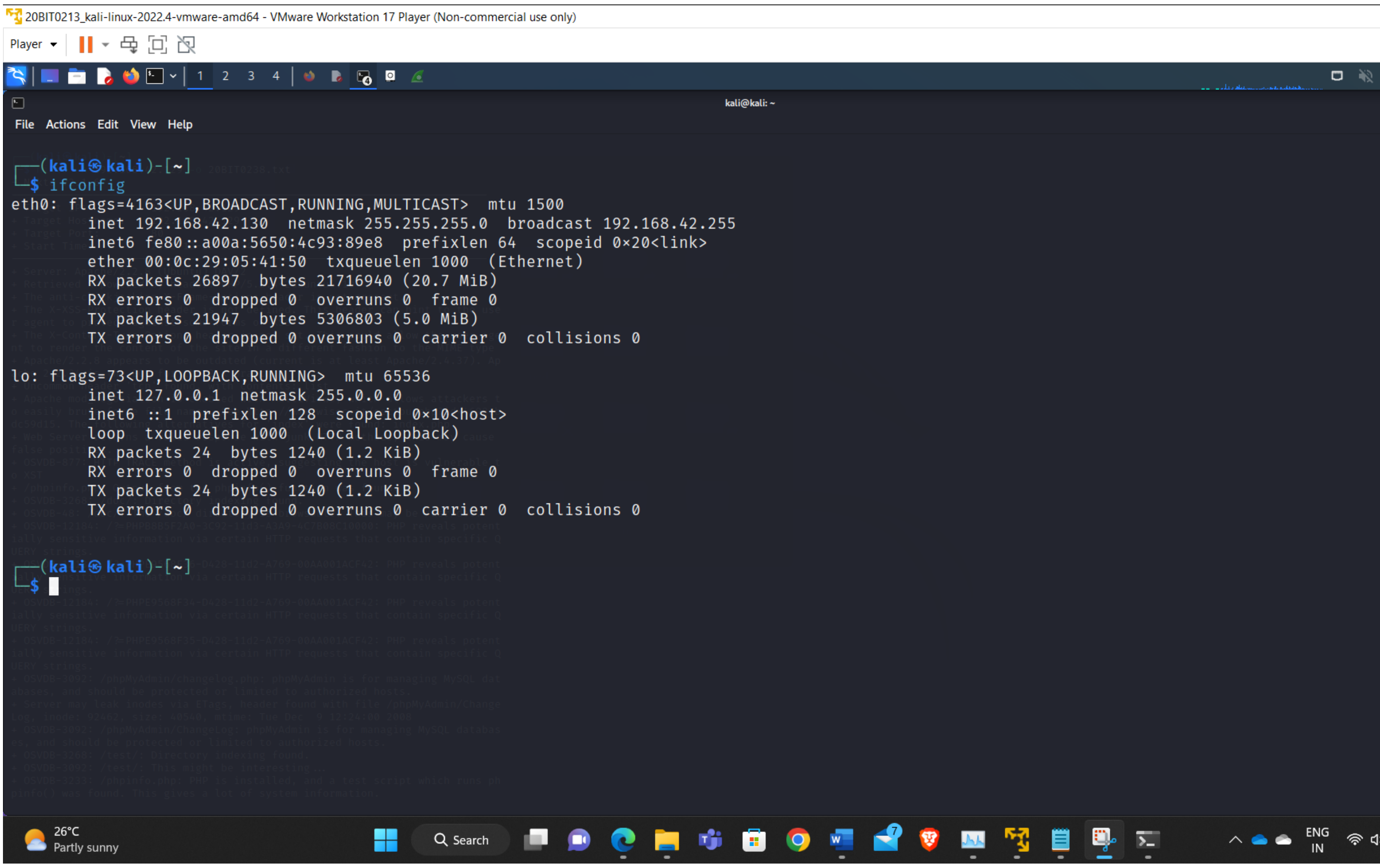


Metasploitable2-Linux - VMware Workstation 17 Player (Non-commercial use only)
Player

```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:a8:1b:56
          inet addr:192.168.42.129  Bcast:192.168.42.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fea8:1b56/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:60 errors:0 dropped:0 overruns:0 frame:0
          TX packets:76 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:5598 (5.4 KB)  TX bytes:7808 (7.6 KB)
          Interrupt:17 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:92 errors:0 dropped:0 overruns:0 frame:0
          TX packets:92 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:19393 (18.9 KB)  TX bytes:19393 (18.9 KB)

msfadmin@metasploitable:~$ _
```

VMware Tools enables many features and improves mouse movement, video and performance. Log in to the guest operating system and click "Install Tools".

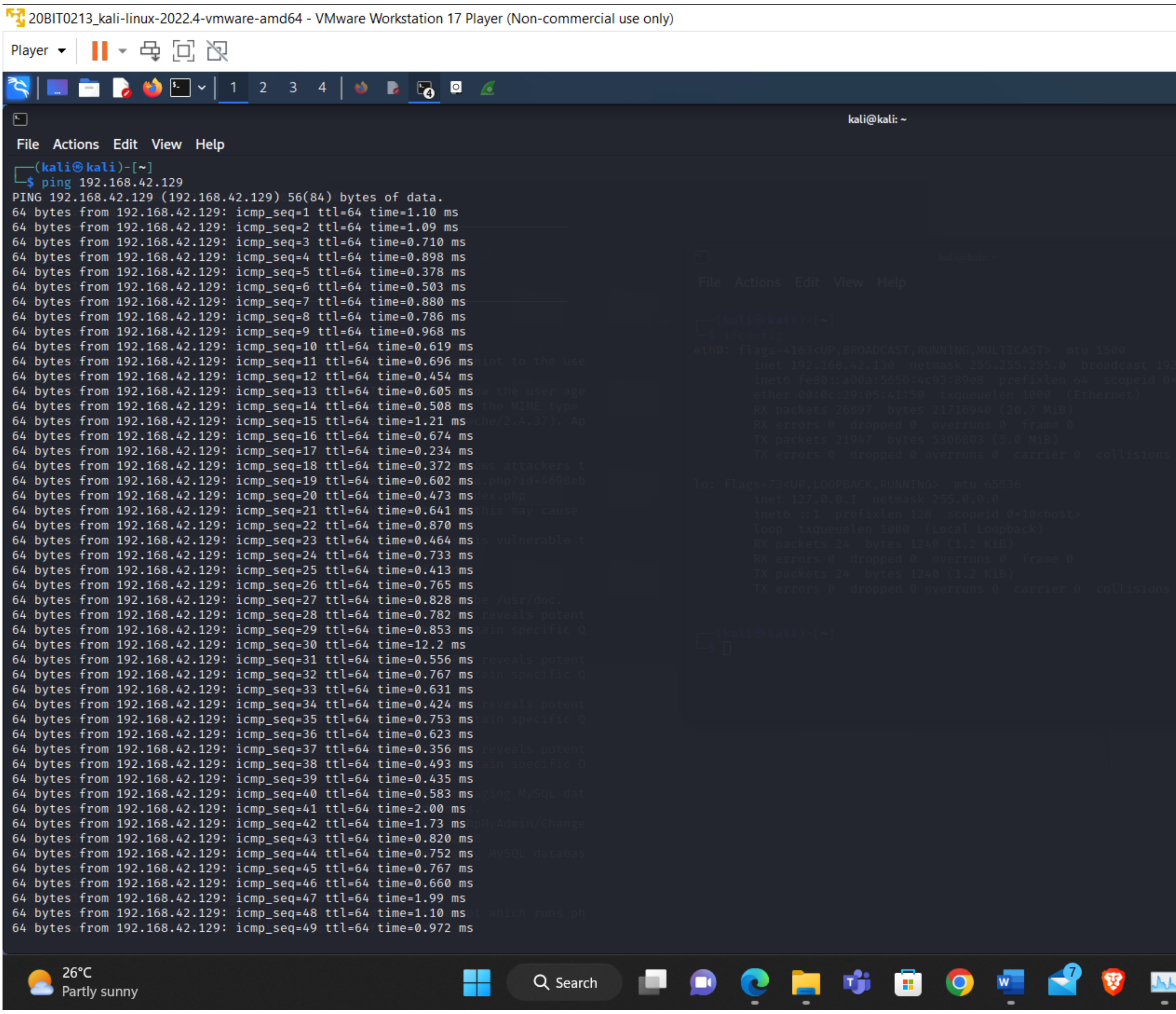
Kali linux IP (192.168.42.130)



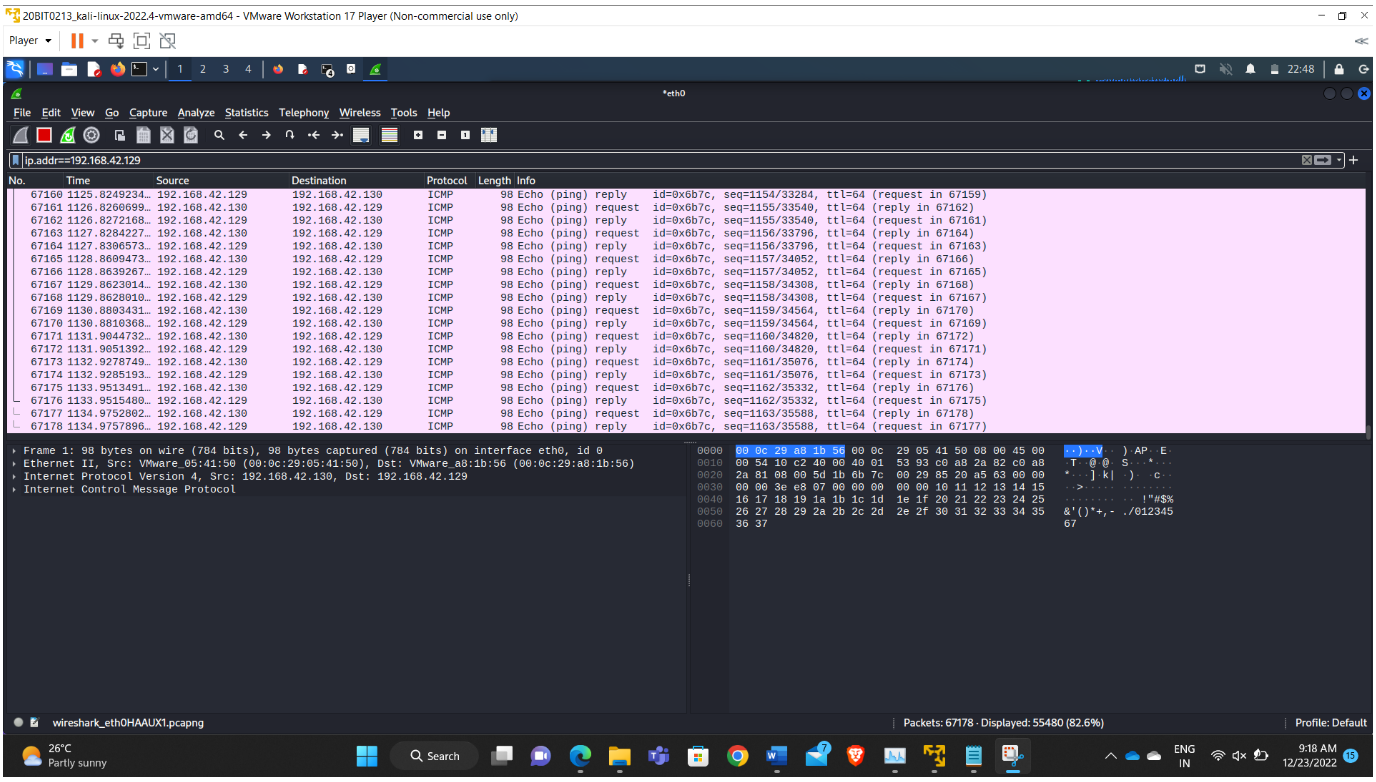
20BIT0213_kali-linux-2022.4-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)

```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.42.130  netmask 255.255.255.0  broadcast 192.168.42.255
        inet6 fe80::a00a:5650:4c93:89e8  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:05:41:50  txqueuelen 1000  (Ethernet)
        RX packets 26897  bytes 21716940 (20.7 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 21947  bytes 5306803 (5.0 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 24  bytes 1240 (1.2 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 24  bytes 1240 (1.2 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

┌──(kali㉿kali)-[~]
└─$ 
```

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


20BIT0213_kali-linux-2022.4-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
1 2 3 4
kali@kali: ~
File Actions Edit View Help
26°C
Partly sunny
Search

```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.42.129
PING 192.168.42.129 (192.168.42.129) 56(84) bytes of data.
64 bytes from 192.168.42.129: icmp_seq=1 ttl=64 time=1.10 ms
64 bytes from 192.168.42.129: icmp_seq=2 ttl=64 time=1.09 ms
64 bytes from 192.168.42.129: icmp_seq=3 ttl=64 time=0.710 ms
64 bytes from 192.168.42.129: icmp_seq=4 ttl=64 time=0.898 ms
64 bytes from 192.168.42.129: icmp_seq=5 ttl=64 time=0.378 ms
64 bytes from 192.168.42.129: icmp_seq=6 ttl=64 time=0.503 ms
64 bytes from 192.168.42.129: icmp_seq=7 ttl=64 time=0.880 ms
64 bytes from 192.168.42.129: icmp_seq=8 ttl=64 time=0.786 ms
64 bytes from 192.168.42.129: icmp_seq=9 ttl=64 time=0.968 ms
64 bytes from 192.168.42.129: icmp_seq=10 ttl=64 time=0.619 ms
64 bytes from 192.168.42.129: icmp_seq=11 ttl=64 time=0.696 ms
64 bytes from 192.168.42.129: icmp_seq=12 ttl=64 time=0.454 ms
64 bytes from 192.168.42.129: icmp_seq=13 ttl=64 time=0.605 ms
64 bytes from 192.168.42.129: icmp_seq=14 ttl=64 time=0.508 ms
64 bytes from 192.168.42.129: icmp_seq=15 ttl=64 time=1.21 ms
64 bytes from 192.168.42.129: icmp_seq=16 ttl=64 time=0.674 ms
64 bytes from 192.168.42.129: icmp_seq=17 ttl=64 time=0.234 ms
64 bytes from 192.168.42.129: icmp_seq=18 ttl=64 time=0.372 ms
64 bytes from 192.168.42.129: icmp_seq=19 ttl=64 time=0.602 ms
64 bytes from 192.168.42.129: icmp_seq=20 ttl=64 time=0.473 ms
64 bytes from 192.168.42.129: icmp_seq=21 ttl=64 time=0.641 ms
64 bytes from 192.168.42.129: icmp_seq=22 ttl=64 time=0.870 ms
64 bytes from 192.168.42.129: icmp_seq=23 ttl=64 time=0.464 ms
64 bytes from 192.168.42.129: icmp_seq=24 ttl=64 time=0.733 ms
64 bytes from 192.168.42.129: icmp_seq=25 ttl=64 time=0.413 ms
64 bytes from 192.168.42.129: icmp_seq=26 ttl=64 time=0.765 ms
64 bytes from 192.168.42.129: icmp_seq=27 ttl=64 time=0.828 ms
64 bytes from 192.168.42.129: icmp_seq=28 ttl=64 time=0.782 ms
64 bytes from 192.168.42.129: icmp_seq=29 ttl=64 time=0.853 ms
64 bytes from 192.168.42.129: icmp_seq=30 ttl=64 time=12.2 ms
64 bytes from 192.168.42.129: icmp_seq=31 ttl=64 time=0.556 ms
64 bytes from 192.168.42.129: icmp_seq=32 ttl=64 time=0.767 ms
64 bytes from 192.168.42.129: icmp_seq=33 ttl=64 time=0.631 ms
64 bytes from 192.168.42.129: icmp_seq=34 ttl=64 time=0.424 ms
64 bytes from 192.168.42.129: icmp_seq=35 ttl=64 time=0.753 ms
64 bytes from 192.168.42.129: icmp_seq=36 ttl=64 time=0.623 ms
64 bytes from 192.168.42.129: icmp_seq=37 ttl=64 time=0.356 ms
64 bytes from 192.168.42.129: icmp_seq=38 ttl=64 time=0.493 ms
64 bytes from 192.168.42.129: icmp_seq=39 ttl=64 time=0.435 ms
64 bytes from 192.168.42.129: icmp_seq=40 ttl=64 time=0.583 ms
64 bytes from 192.168.42.129: icmp_seq=41 ttl=64 time=2.00 ms
64 bytes from 192.168.42.129: icmp_seq=42 ttl=64 time=1.73 ms
64 bytes from 192.168.42.129: icmp_seq=43 ttl=64 time=0.820 ms
64 bytes from 192.168.42.129: icmp_seq=44 ttl=64 time=0.752 ms
64 bytes from 192.168.42.129: icmp_seq=45 ttl=64 time=0.767 ms
64 bytes from 192.168.42.129: icmp_seq=46 ttl=64 time=0.660 ms
64 bytes from 192.168.42.129: icmp_seq=47 ttl=64 time=1.99 ms
64 bytes from 192.168.42.129: icmp_seq=48 ttl=64 time=1.10 ms
64 bytes from 192.168.42.129: icmp_seq=49 ttl=64 time=0.972 ms
```



20BIT0213_kali-linux-2022.4-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
1 2 3 4
22:48
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
wireshark_eth0HAAUX1.pcapng
Profile: Default
26°C
Partly sunny
Search
ENG
IN
9:18 AM
12/23/2022

```
ip.addr==192.168.42.129
```

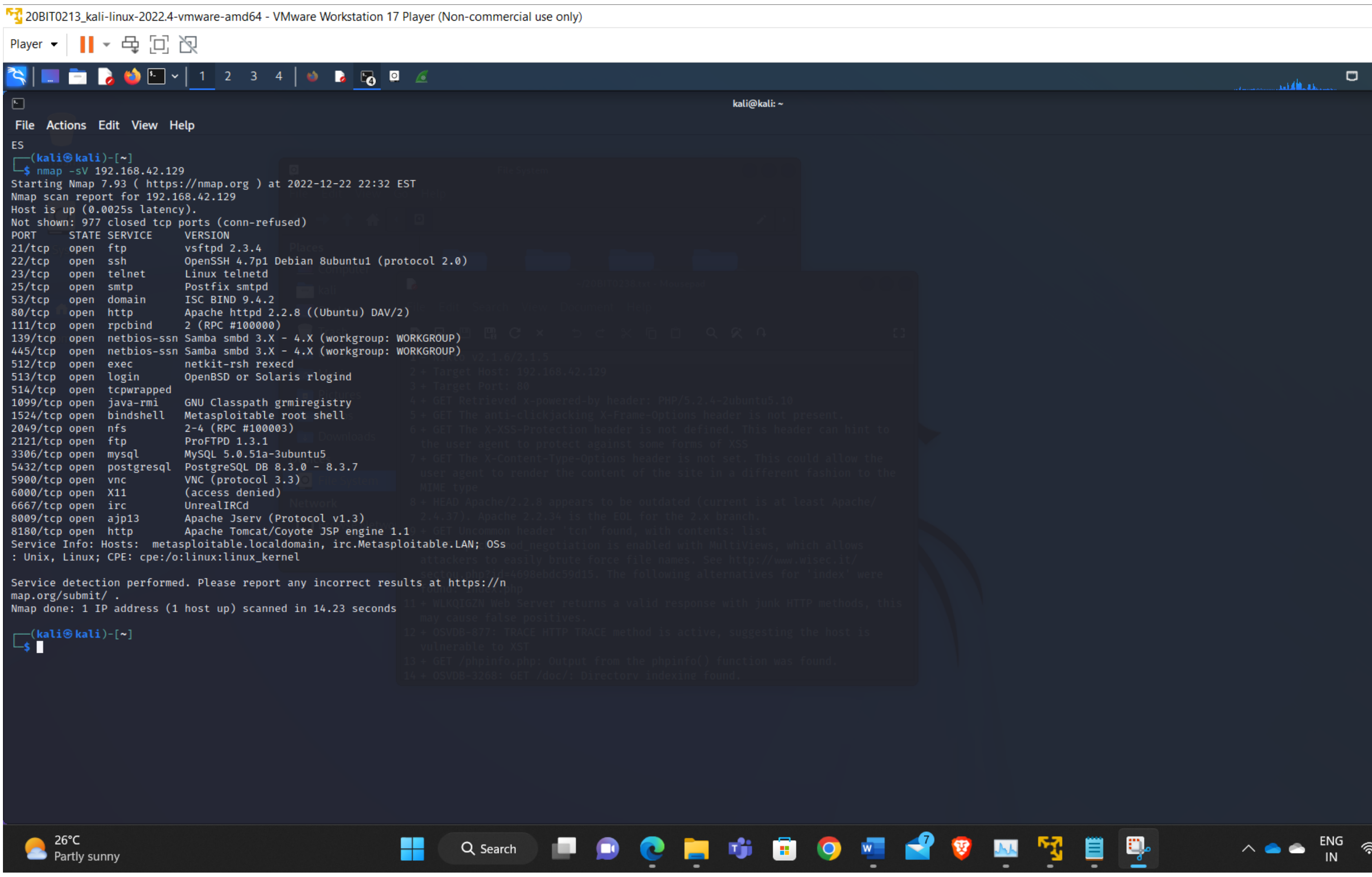
```
No.   Time          Source          Destination     Protocol Length Info
67160 1125.8249234… 192.168.42.129  192.168.42.130  ICMP     98 Echo (ping) reply    id=0x6b7c, seq=1154/33284, ttl=64 (request in 67159)
67161 1126.8260699… 192.168.42.130  192.168.42.129  ICMP     98 Echo (ping) request  id=0x6b7c, seq=1155/33540, ttl=64 (reply in 67162)
67162 1126.8272168… 192.168.42.129  192.168.42.130  ICMP     98 Echo (ping) reply    id=0x6b7c, seq=1155/33540, ttl=64 (request in 67161)
67163 1127.8284227… 192.168.42.130  192.168.42.129  ICMP     98 Echo (ping) request  id=0x6b7c, seq=1156/33796, ttl=64 (reply in 67164)
67164 1127.8306573… 192.168.42.129  192.168.42.130  ICMP     98 Echo (ping) reply    id=0x6b7c, seq=1156/33796, ttl=64 (request in 67163)
67165 1128.8609473… 192.168.42.130  192.168.42.129  ICMP     98 Echo (ping) request  id=0x6b7c, seq=1157/34052, ttl=64 (reply in 67166)
67166 1128.8639267… 192.168.42.129  192.168.42.130  ICMP     98 Echo (ping) reply    id=0x6b7c, seq=1157/34052, ttl=64 (request in 67165)
67167 1129.8623014… 192.168.42.130  192.168.42.129  ICMP     98 Echo (ping) request  id=0x6b7c, seq=1158/34308, ttl=64 (reply in 67168)
67168 1129.8628010… 192.168.42.129  192.168.42.130  ICMP     98 Echo (ping) reply    id=0x6b7c, seq=1158/34308, ttl=64 (request in 67167)
67169 1130.8803431… 192.168.42.130  192.168.42.129  ICMP     98 Echo (ping) request  id=0x6b7c, seq=1159/34564, ttl=64 (reply in 67170)
67170 1130.8810368… 192.168.42.129  192.168.42.130  ICMP     98 Echo (ping) reply    id=0x6b7c, seq=1159/34564, ttl=64 (request in 67169)
67171 1131.9044732… 192.168.42.130  192.168.42.129  ICMP     98 Echo (ping) request  id=0x6b7c, seq=1160/34820, ttl=64 (reply in 67172)
67172 1131.9051392… 192.168.42.129  192.168.42.130  ICMP     98 Echo (ping) reply    id=0x6b7c, seq=1160/34820, ttl=64 (request in 67171)
67173 1132.9278749… 192.168.42.130  192.168.42.129  ICMP     98 Echo (ping) request  id=0x6b7c, seq=1161/35076, ttl=64 (reply in 67174)
67174 1132.9285193… 192.168.42.129  192.168.42.130  ICMP     98 Echo (ping) reply    id=0x6b7c, seq=1161/35076, ttl=64 (request in 67173)
67175 1133.9513491… 192.168.42.130  192.168.42.129  ICMP     98 Echo (ping) request  id=0x6b7c, seq=1162/35332, ttl=64 (reply in 67176)
67176 1133.9515480… 192.168.42.129  192.168.42.130  ICMP     98 Echo (ping) reply    id=0x6b7c, seq=1162/35332, ttl=64 (request in 67175)
67177 1134.9752802… 192.168.42.130  192.168.42.129  ICMP     98 Echo (ping) request  id=0x6b7c, seq=1163/35588, ttl=64 (reply in 67178)
67178 1134.9757896… 192.168.42.129  192.168.42.130  ICMP     98 Echo (ping) reply    id=0x6b7c, seq=1163/35588, ttl=64 (request in 67177)
```

```
› Frame 1: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface eth0, id 0
› Ethernet II, Src: VMware_05:41:50 (00:0c:29:05:41:50), Dst: VMware_a8:1b:56 (00:0c:29:a8:1b:56)
› Internet Protocol Version 4, Src: 192.168.42.130, Dst: 192.168.42.129
› Internet Control Message Protocol
```

```
0000  00 0c 29 a8 1b 56 00 0c  29 05 41 50 08 00 45 00   ··)··V·· )·AP··E·
0010  00 54 10 c2 40 00 40 01  53 93 c0 a8 2a 82 c0 a8   ·T··@·@· S···*···
0020  2a 81 08 00 5d 1b 6b 7c  00 29 85 20 a5 63 00 00   *···]·k| ·)· ·c··
0030  00 00 3e e8 07 00 00 00  00 00 10 11 12 13 14 15   ··>····· ········
0040  16 17 18 19 1a 1b 1c 1d  1e 1f 20 21 22 23 24 25   ········ ·· !"#$%
0050  26 27 28 29 2a 2b 2c 2d  2e 2f 30 31 32 33 34 35   &'()*+,- ./012345
0060  36 37                                              67
```

Packets: 67178 · Displayed: 55480 (82.6%)

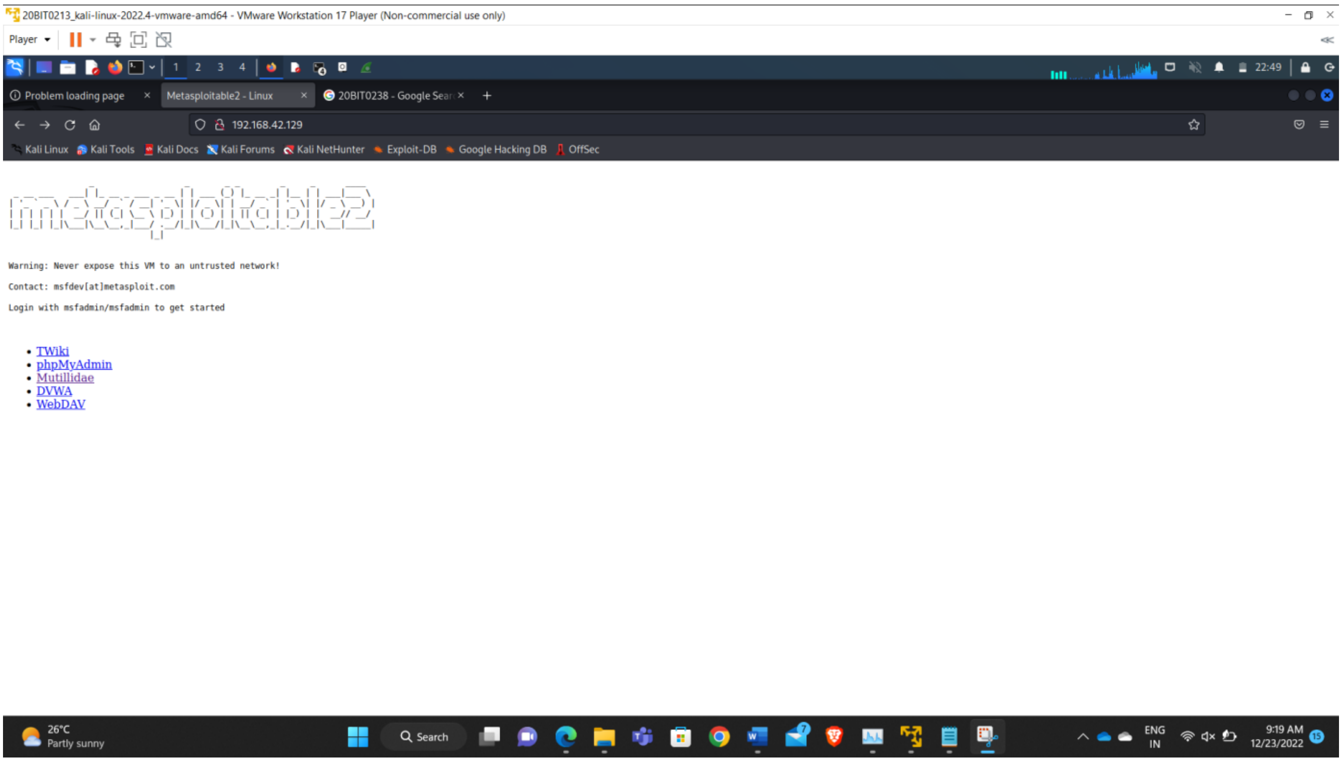
2. Perform a NMAP scan of determining the version of the services running in metasploitable IP. Give snapshot of the same. (2 Marks)’



20BIT0213_kali-linux-2022.4-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
1 2 3 4
kali@kali: ~
File Actions Edit View Help
26°C
Partly sunny
Search
ENG
IN

```
ES
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.42.129
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-22 22:32 EST
Nmap scan report for 192.168.42.129
Host is up (0.0025s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs
: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.23 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

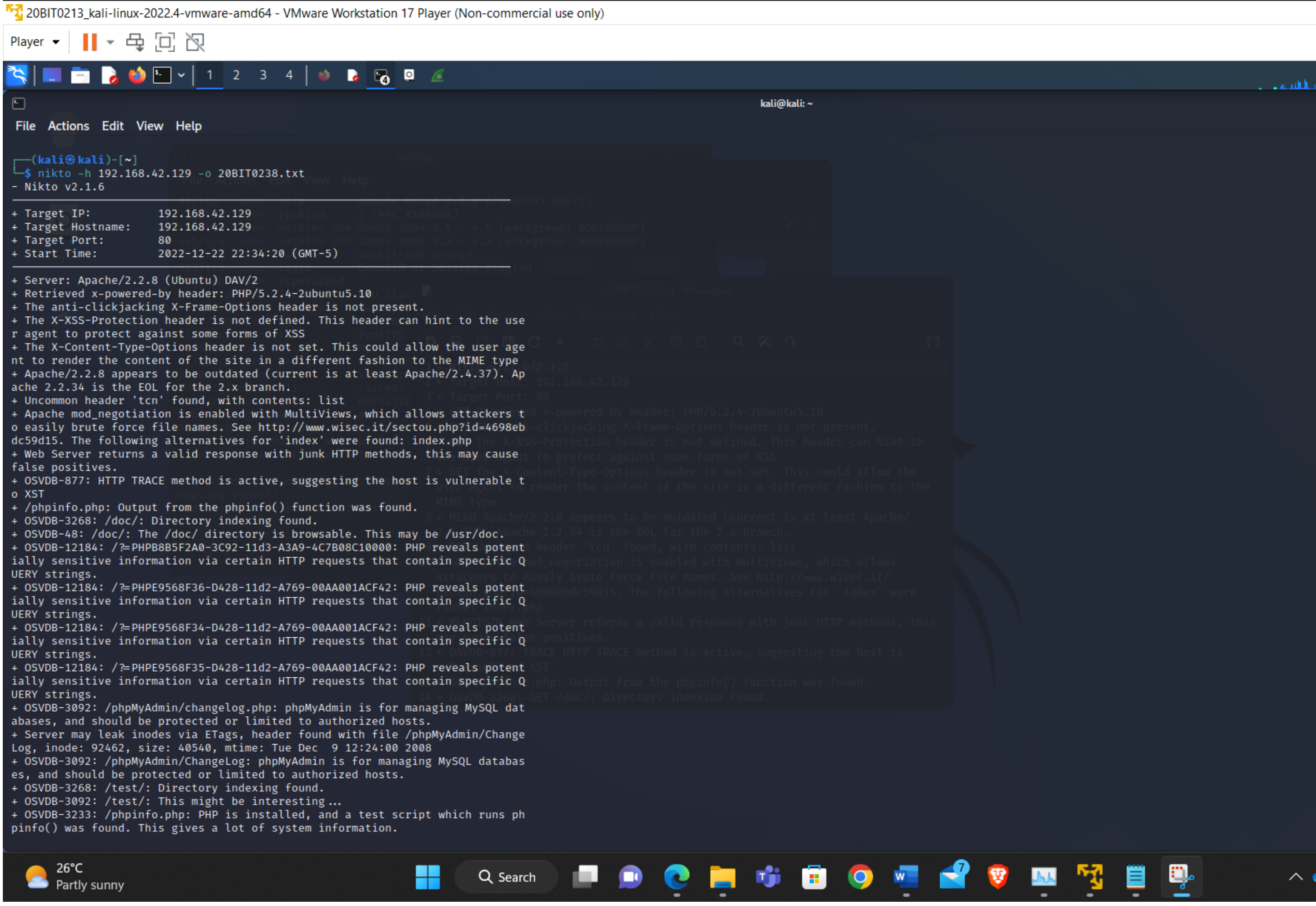
3. Run metasploitable IP in firefox browser of Kali. Give Snapshot (2 Marks)



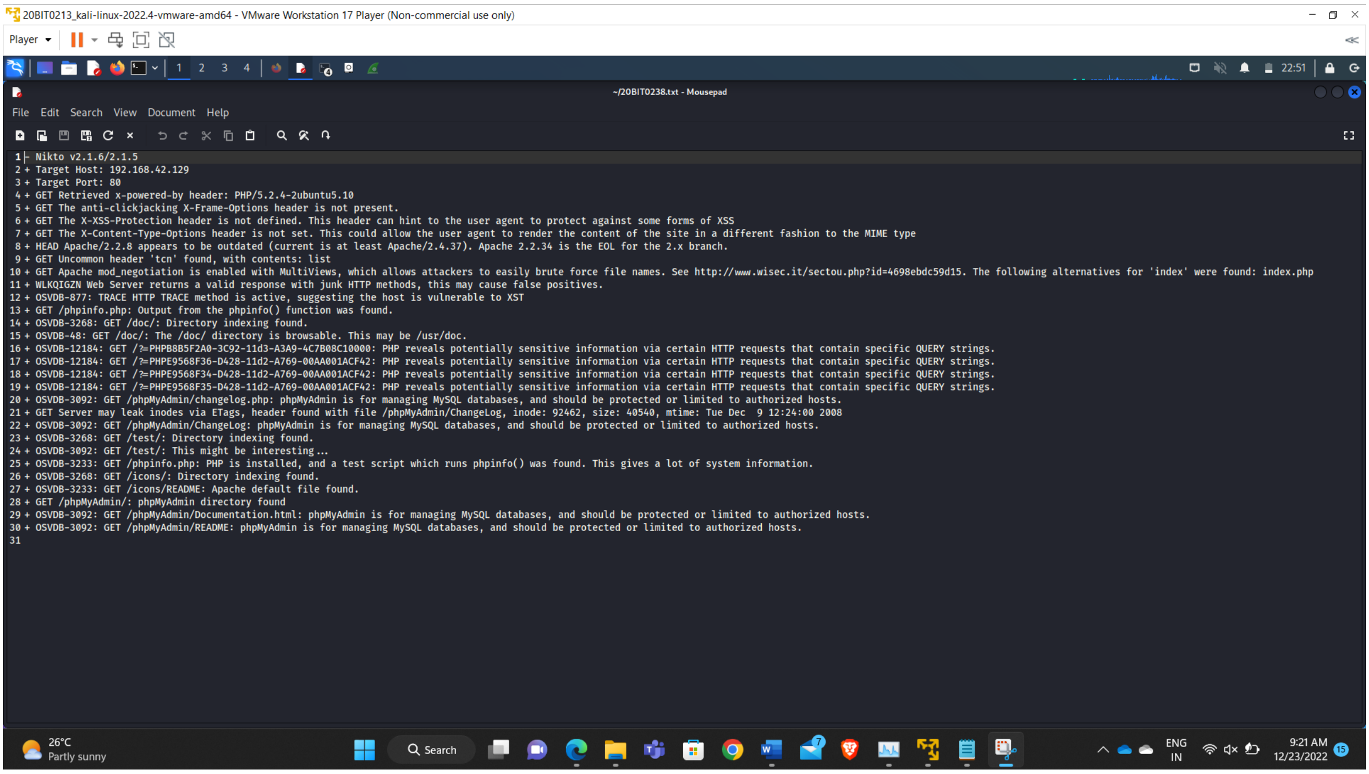
```
Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started
```

- TWiki
- phpMyAdmin
- Mutillidae
- DVWA
- WebDAV

4. Perform a Nikto Scan of metasploitable IP. Give snapshot and save the results in a text file. Save the text file in google drive link and share the link in the document.


20BIT0213_kali-linux-2022.4-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
kali@kali: ~
File Actions Edit View Help
26°C
Partly sunny
Search

```
┌──(kali㉿kali)-[~]
└─$ nikto -h 192.168.42.129 -o 20BIT0238.txt
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.42.129
+ Target Hostname:    192.168.42.129
+ Target Port:        80
+ Start Time:         2022-12-22 22:34:20 (GMT-5)
---------------------------------------------------------------------------
+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the use
r agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user age
nt to render the content of the site in a different fashion to the MIME type
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.37). Ap
ache 2.2.34 is the EOL for the 2.x branch.
+ Uncommon header 'tcn' found, with contents: list
+ Apache mod_negotiation is enabled with MultiViews, which allows attackers t
o easily brute force file names. See http://www.wisec.it/sectou.php?id=4698eb
dc59d15. The following alternatives for 'index' were found: index.php
+ Web Server returns a valid response with junk HTTP methods, this may cause
false positives.
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable t
o XST
+ /phpinfo.php: Output from the phpinfo() function was found.
+ OSVDB-3268: /doc/: Directory indexing found.
+ OSVDB-48: /doc/: The /doc/ directory is browsable. This may be /usr/doc.
+ OSVDB-12184: /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potent
ially sensitive information via certain HTTP requests that contain specific Q
UERY strings.
+ OSVDB-12184: /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potent
ially sensitive information via certain HTTP requests that contain specific Q
UERY strings.
+ OSVDB-12184: /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potent
ially sensitive information via certain HTTP requests that contain specific Q
UERY strings.
+ OSVDB-12184: /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potent
ially sensitive information via certain HTTP requests that contain specific Q
UERY strings.
+ OSVDB-3092: /phpMyAdmin/changelog.php: phpMyAdmin is for managing MySQL dat
abases, and should be protected or limited to authorized hosts.
+ Server may leak inodes via ETags, header found with file /phpMyAdmin/Change
Log, inode: 92462, size: 40540, mtime: Tue Dec  9 12:24:00 2008
+ OSVDB-3092: /phpMyAdmin/ChangeLog: phpMyAdmin is for managing MySQL databas
es, and should be protected or limited to authorized hosts.
+ OSVDB-3268: /test/: Directory indexing found.
+ OSVDB-3092: /test/: This might be interesting...
+ OSVDB-3233: /phpinfo.php: PHP is installed, and a test script which runs ph
pinfo() was found. This gives a lot of system information.
```


20BIT0213_kali-linux-2022.4-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
22:51
~/20BIT0238.txt - Mousepad
File Edit Search View Document Help
26°C
Partly sunny
Search
ENG
IN
9:21 AM
12/23/2022

```
- Nikto v2.1.6/2.1.5
+ Target Host: 192.168.42.129
+ Target Port: 80
+ GET Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10
+ GET The anti-clickjacking X-Frame-Options header is not present.
+ GET The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ GET The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ HEAD Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ GET Uncommon header 'tcn' found, with contents: list
+ GET Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. See http://www.wisec.it/sectou.php?id=4698ebdc59d15. The following alternatives for 'index' were found: index.php
+ WLKQIGZN Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ OSVDB-877: TRACE HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ GET /phpinfo.php: Output from the phpinfo() function was found.
+ OSVDB-3268: GET /doc/: Directory indexing found.
+ OSVDB-48: GET /doc/: The /doc/ directory is browsable. This may be /usr/doc.
+ OSVDB-12184: GET /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: GET /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: GET /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: GET /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-3092: GET /phpMyAdmin/changelog.php: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ GET Server may leak inodes via ETags, header found with file /phpMyAdmin/ChangeLog, inode: 92462, size: 40540, mtime: Tue Dec  9 12:24:00 2008
+ OSVDB-3092: GET /phpMyAdmin/ChangeLog: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ OSVDB-3268: GET /test/: Directory indexing found.
+ OSVDB-3092: GET /test/: This might be interesting...
+ OSVDB-3233: GET /phpinfo.php: PHP is installed, and a test script which runs phpinfo() was found. This gives a lot of system information.
+ OSVDB-3268: GET /icons/: Directory indexing found.
+ OSVDB-3233: GET /icons/README: Apache default file found.
+ GET /phpMyAdmin/: phpMyAdmin directory found
+ OSVDB-3092: GET /phpMyAdmin/Documentation.html: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ OSVDB-3092: GET /phpMyAdmin/README: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
```

Google Drive link : https://drive.google.com/file/d/18-dM8z5-rI-NzQxwxhLlEaGo-wI_7Nr1/view?usp=sharing