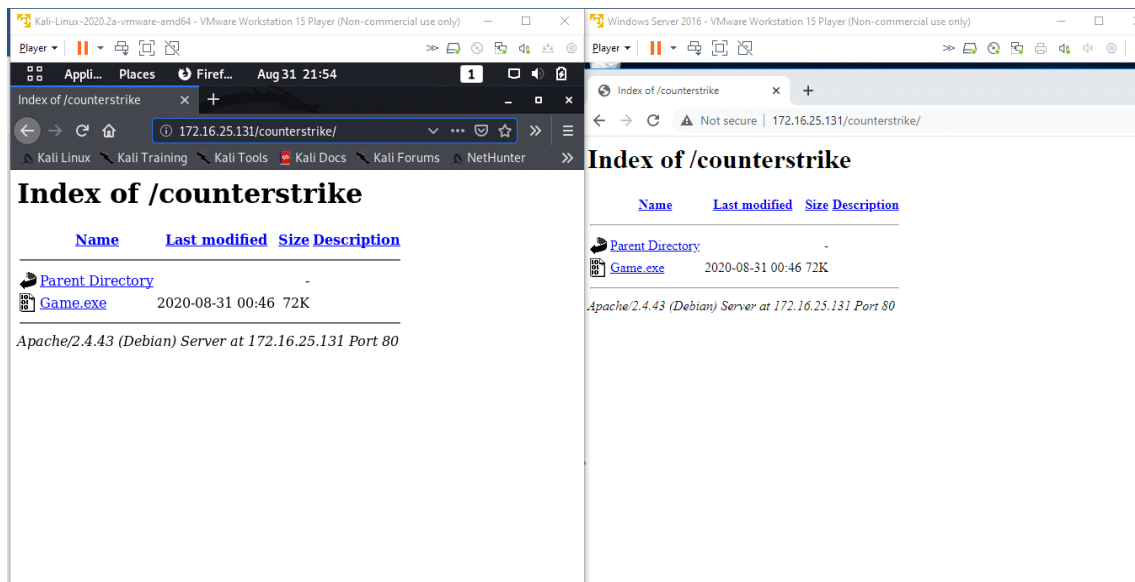


Day 6

1)

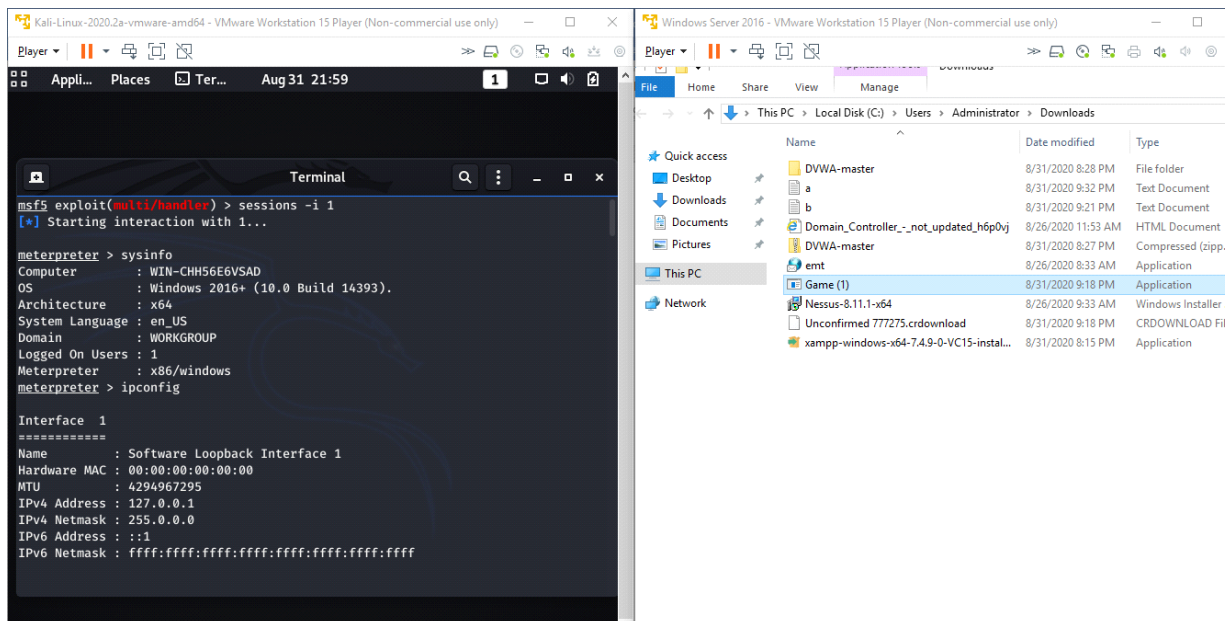
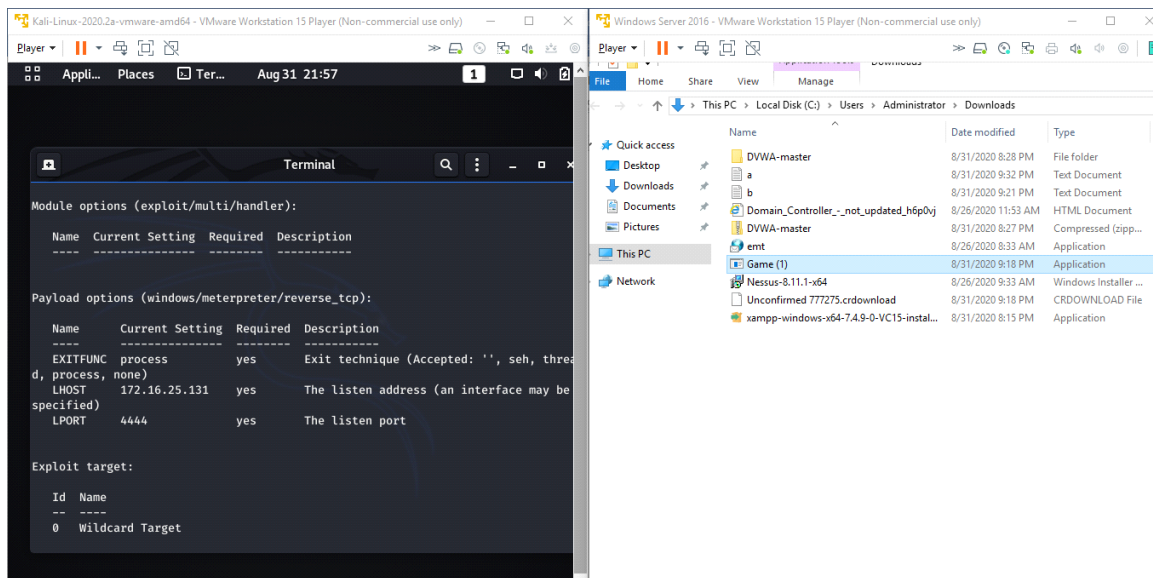
- **Create payload for windows.**
- **Transfer the payload to the victim's machine.**
- **Exploit the victim's machine.**

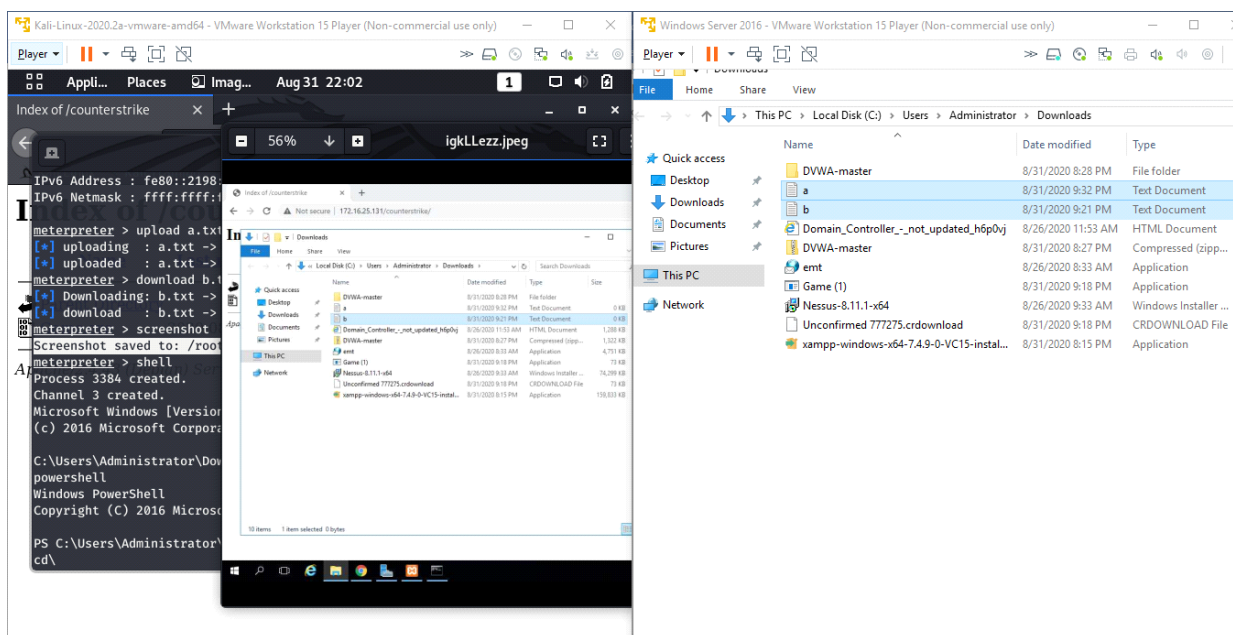
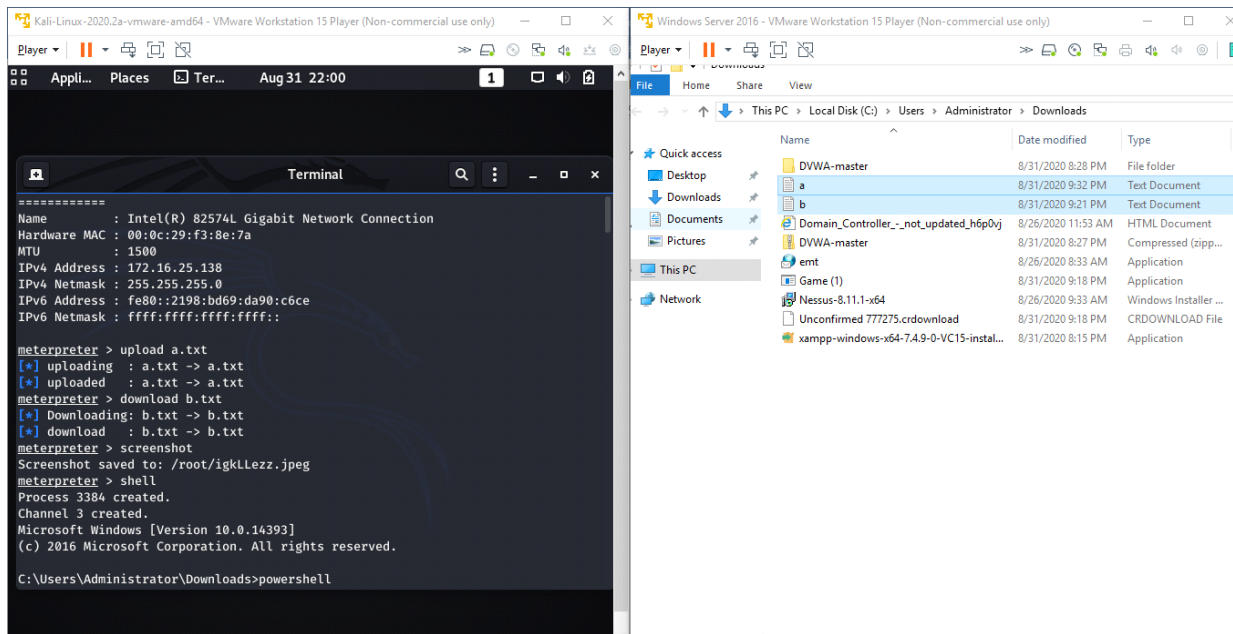


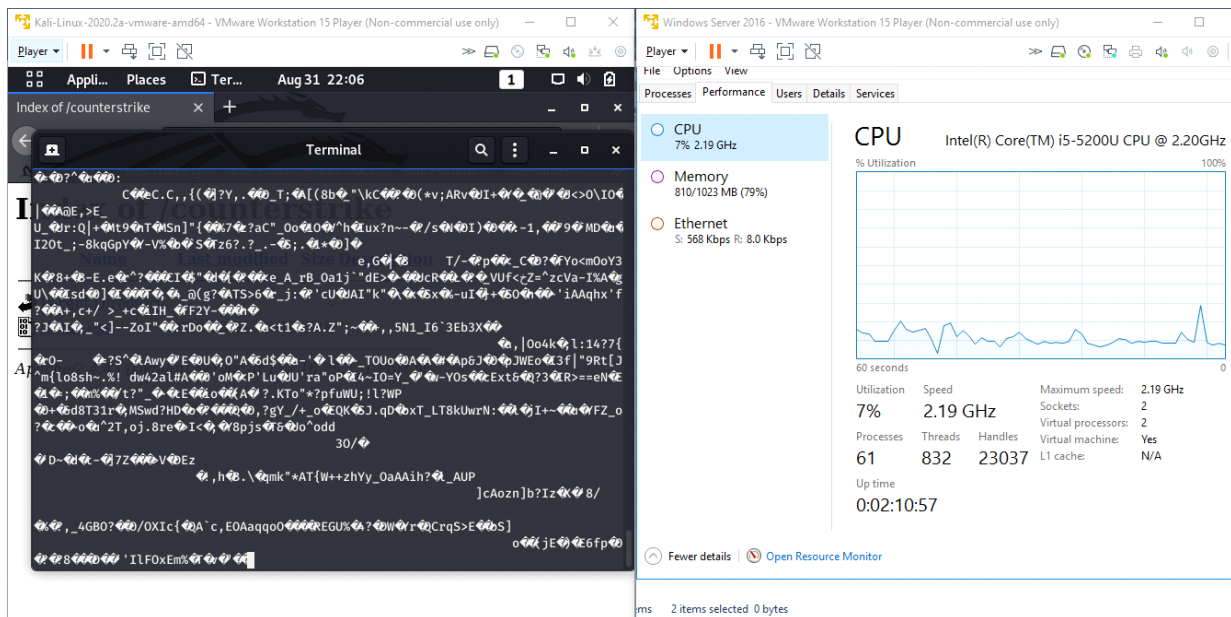
The image shows two side-by-side virtual machine windows. The left window is titled 'Kali-Linux-2020.2a-vmware-amd64 - VMware Workstation 15 Player (Non-commercial use only)' and displays a terminal window with a web browser interface. The browser shows the 'Index of /counterstrike' directory listing for the URL '172.16.25.131/counterstrike/'. The listing includes a table with columns 'Name', 'Last modified', and 'Size'. The entries are 'Parent Directory' and 'Game.exe' (2020-08-31 00:46, 72K). Below the table, it says 'Apache/2.4.43 (Debian) Server at 172.16.25.131 Port 80'. The right window is titled 'Windows Server 2016 - VMware Workstation 15 Player (Non-commercial use only)' and displays a web browser interface. The browser shows the 'Index of /counterstrike' directory listing for the URL '172.16.25.131/counterstrike/'. The listing includes a table with columns 'Name', 'Last modified', and 'Size'. The entries are 'Parent Directory' and 'Game.exe' (2020-08-31 00:46, 72K). Below the table, it says 'Apache/2.4.43 (Debian) Server at 172.16.25.131 Port 80'.

Name	Last modified	Size
Parent Directory	-	-
Game.exe	2020-08-31 00:46	72K

Apache/2.4.43 (Debian) Server at 172.16.25.131 Port 80

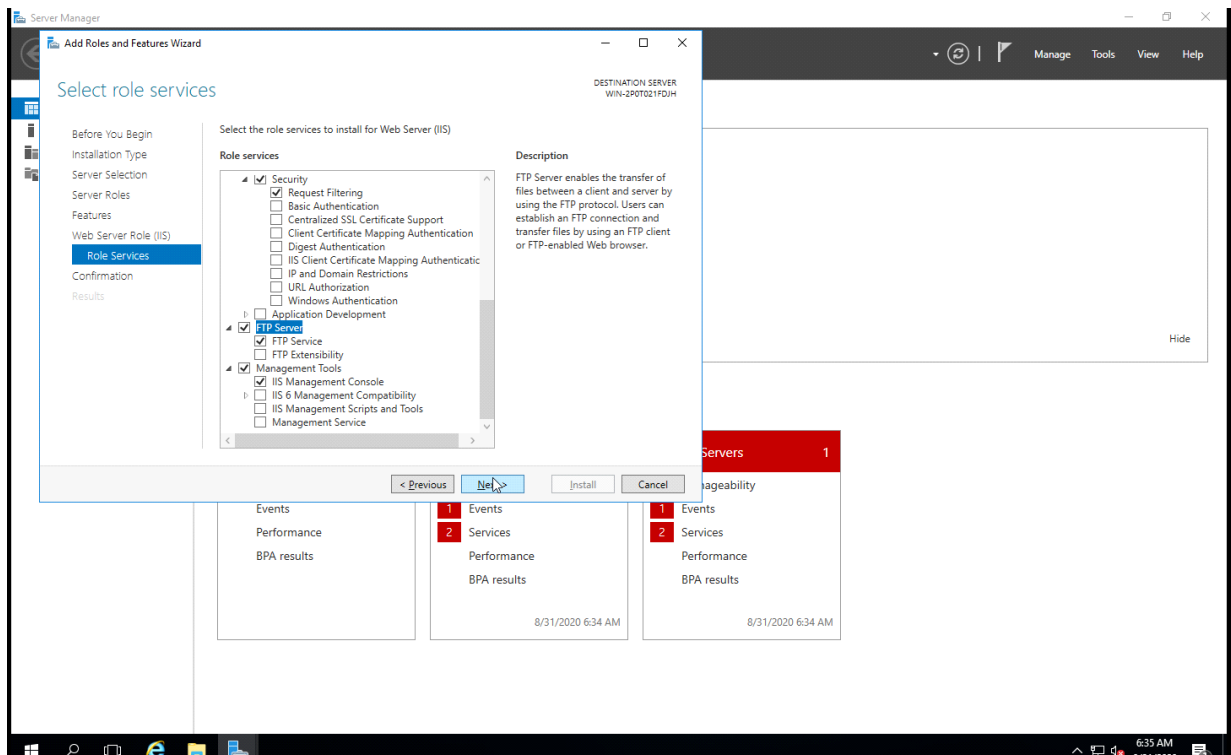
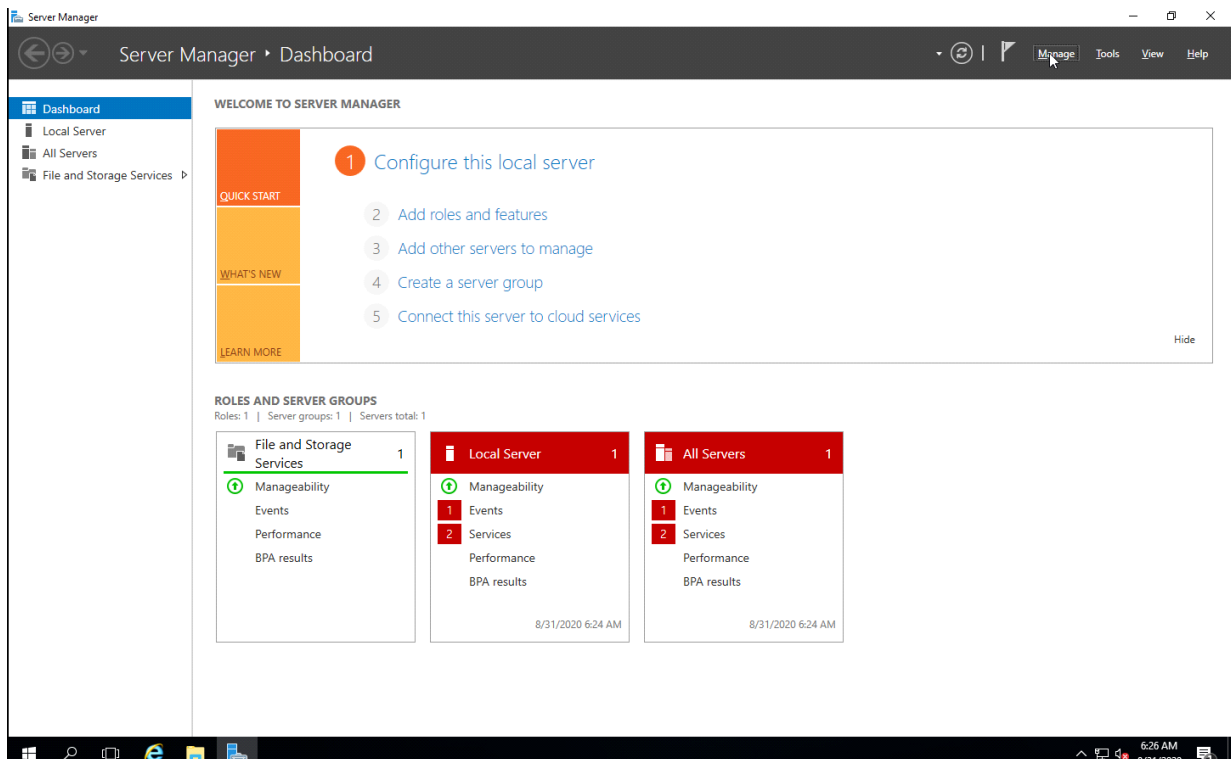


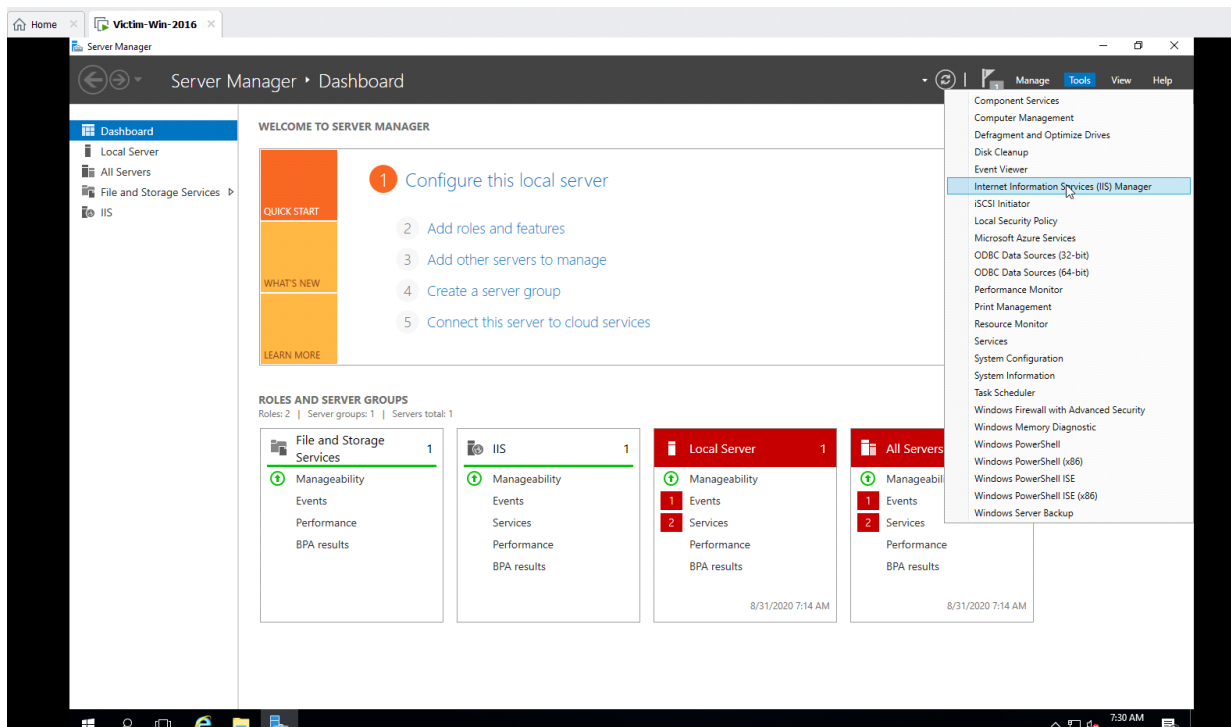
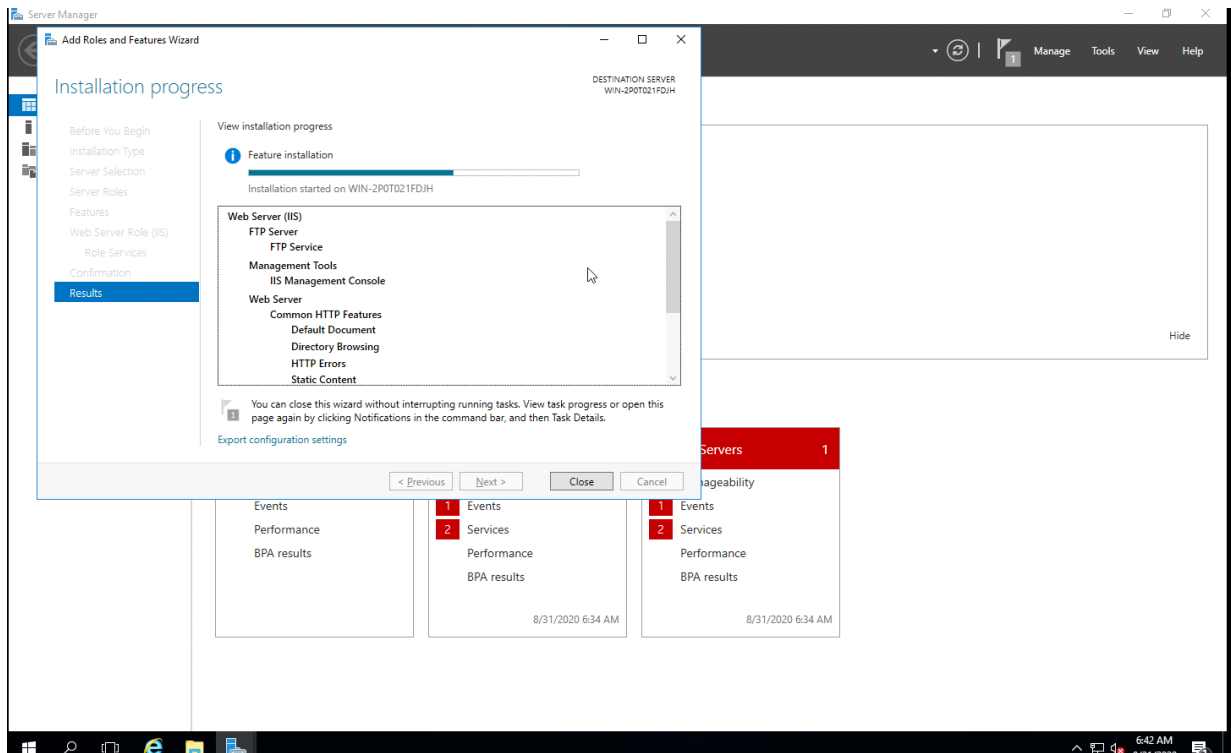


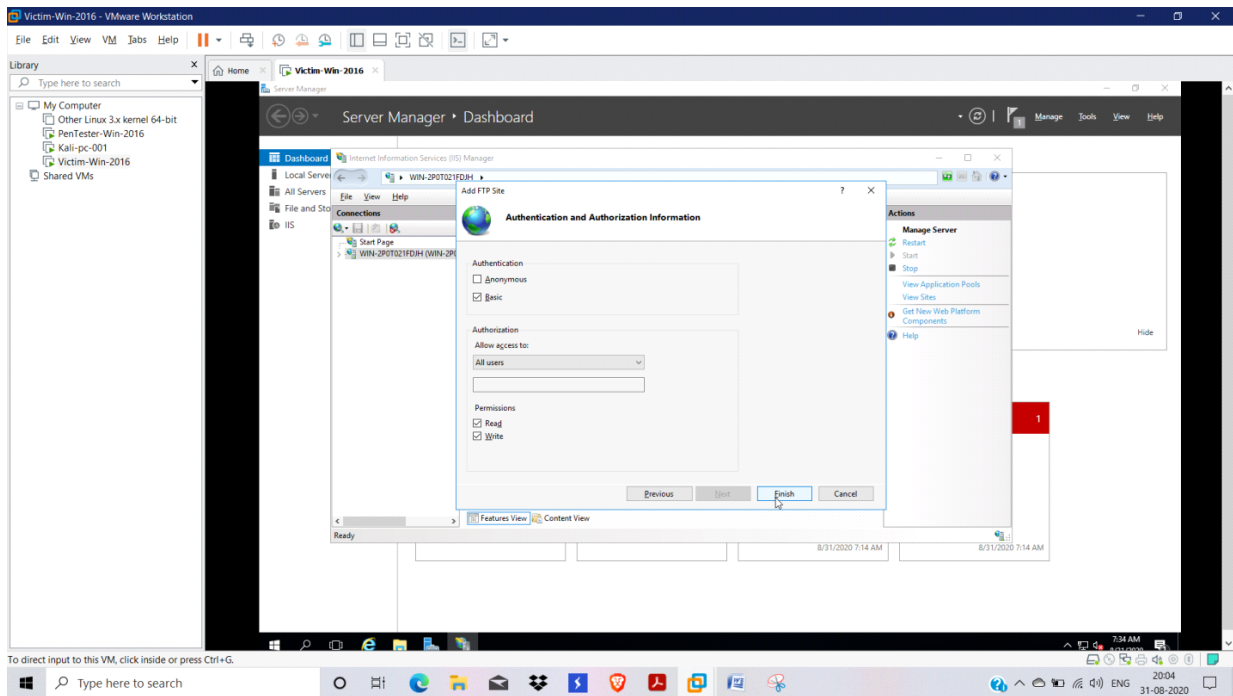
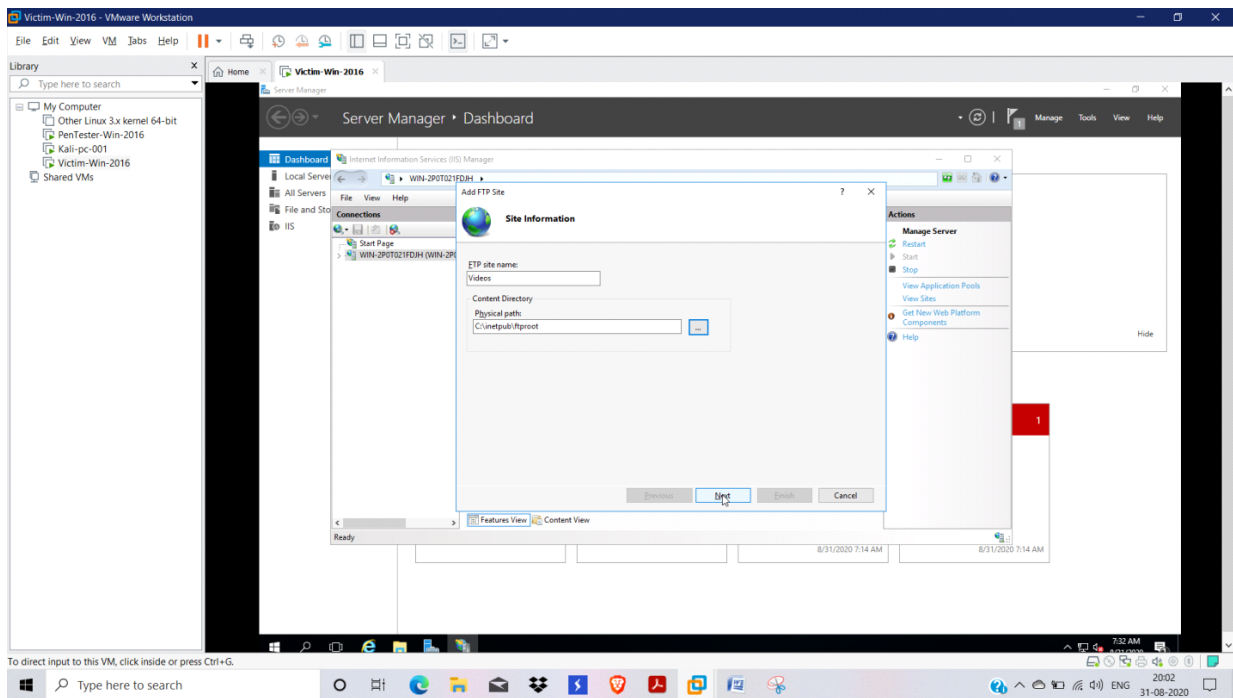


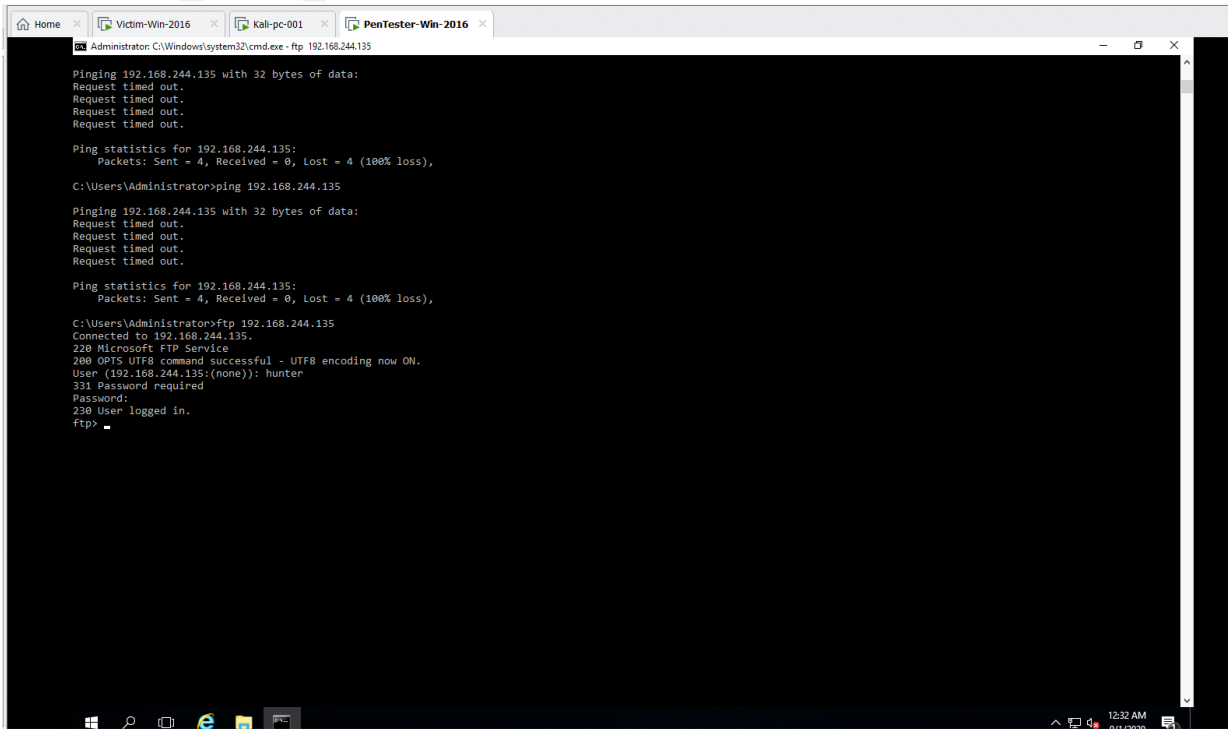
2)

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

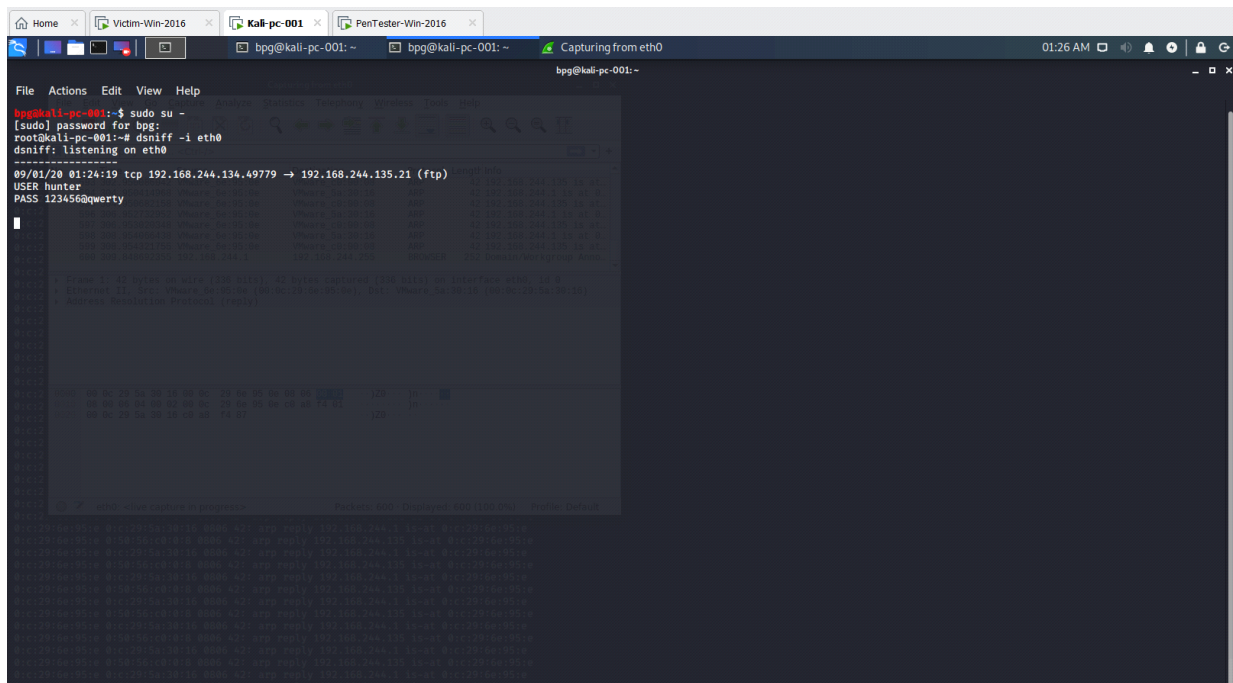








Dsniff



Wireshark

