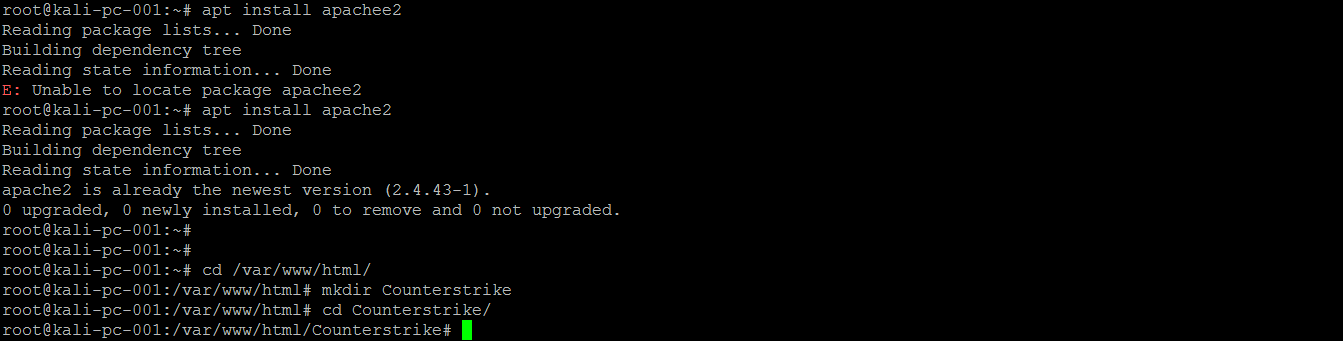
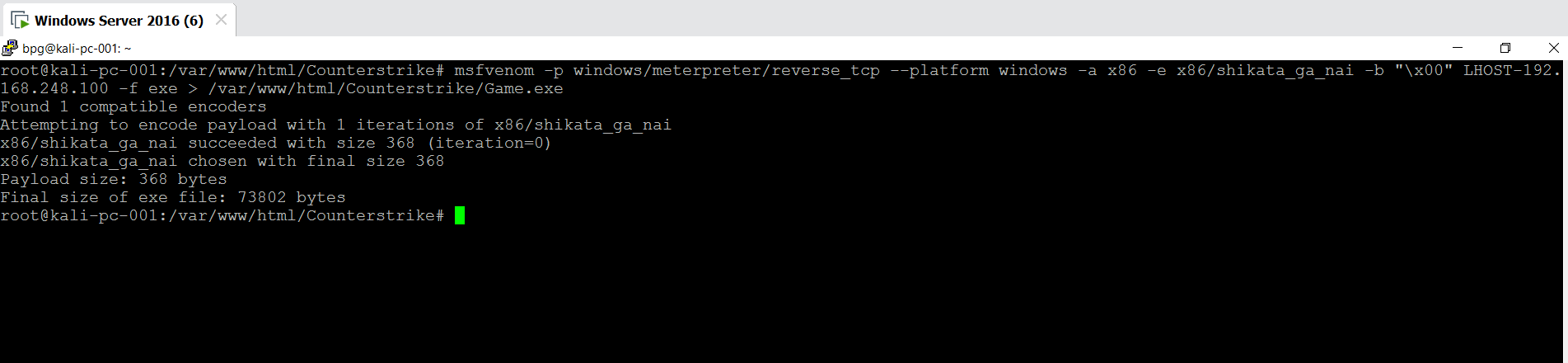
**Assignment Day 6**

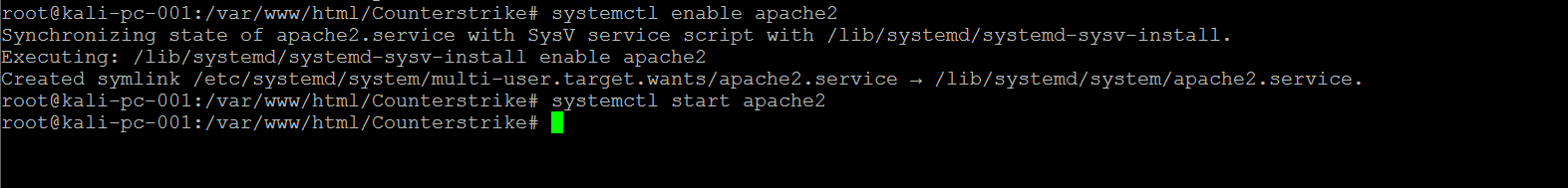
**Question 1:**

1. **Create payload for windows**

**Install apache taking remote of kali in victim machine using either SSH or GIT**

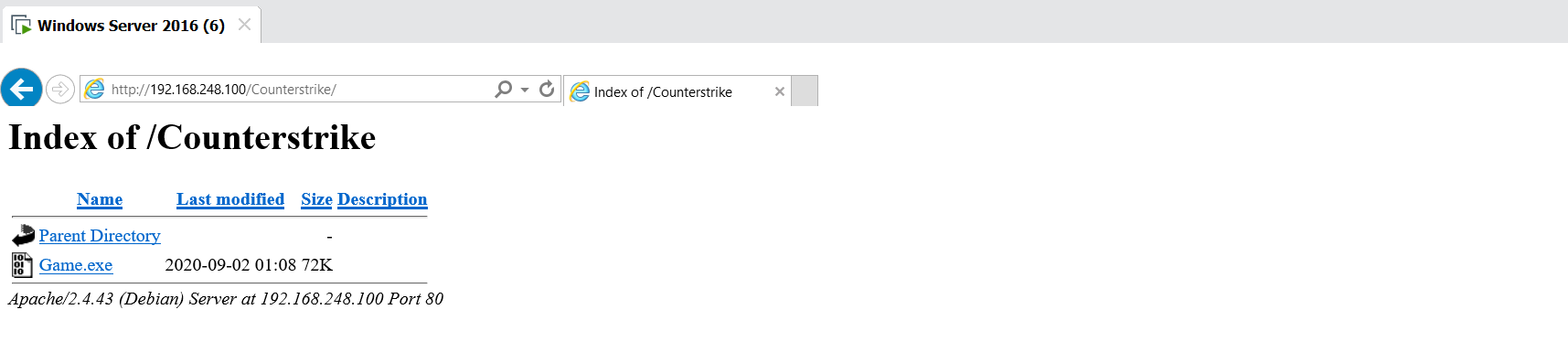
****

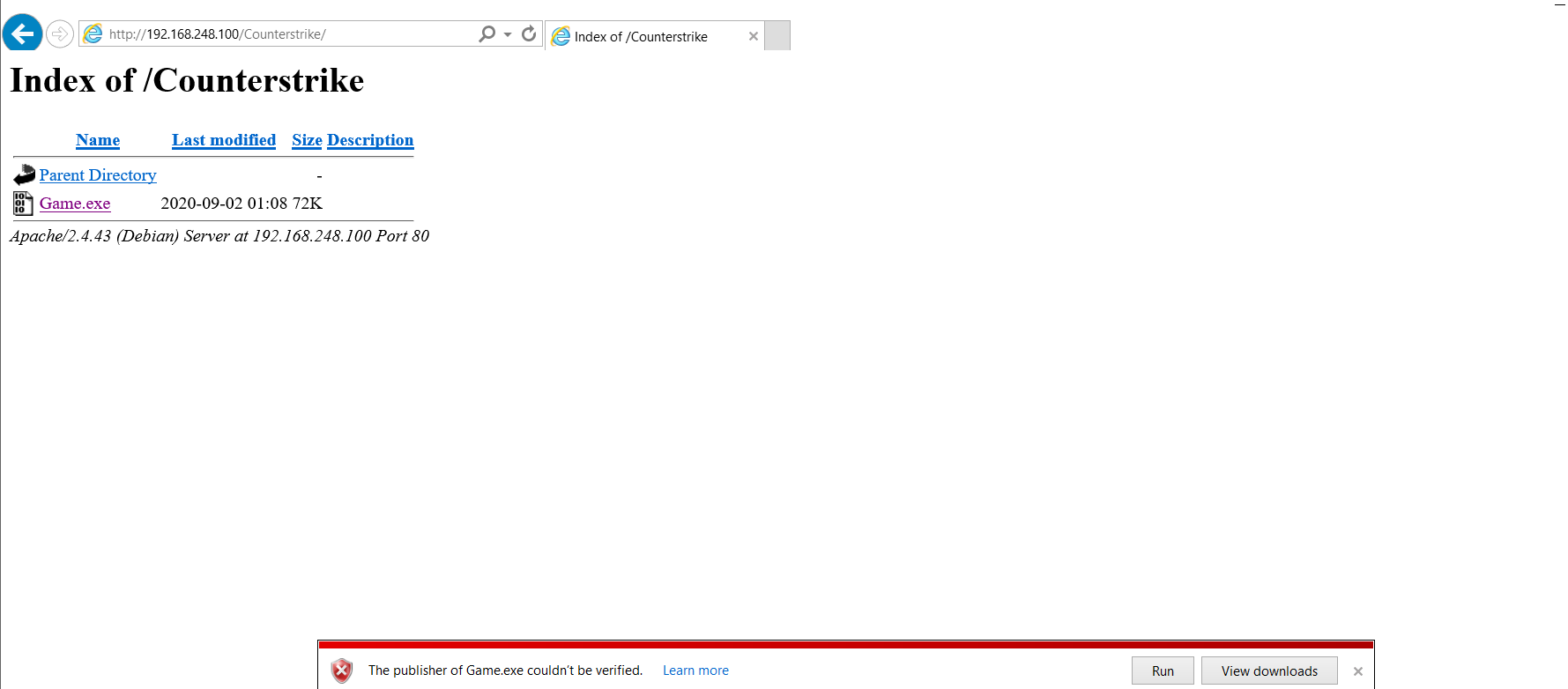
****

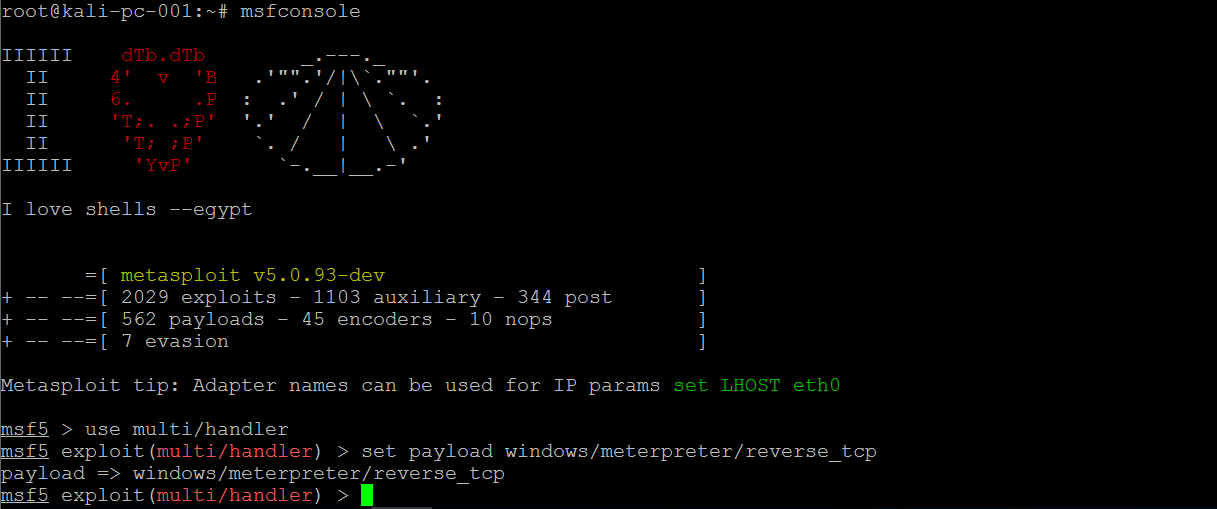
****

1. **Transfer payload to victim’s machine**

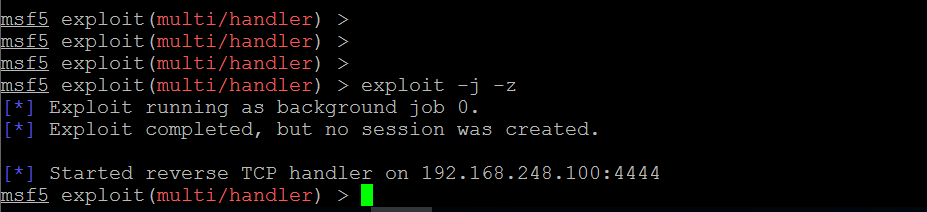
**We are entering here Kali machine IP address**

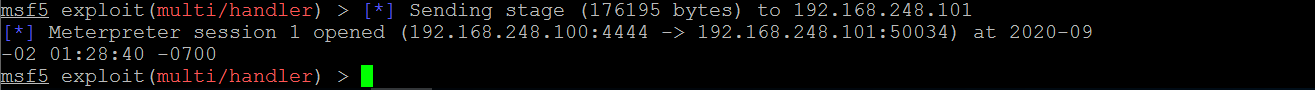
****

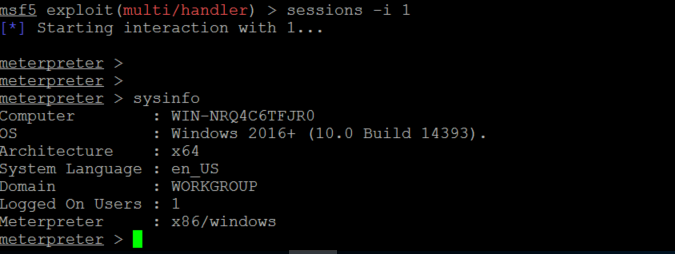
****

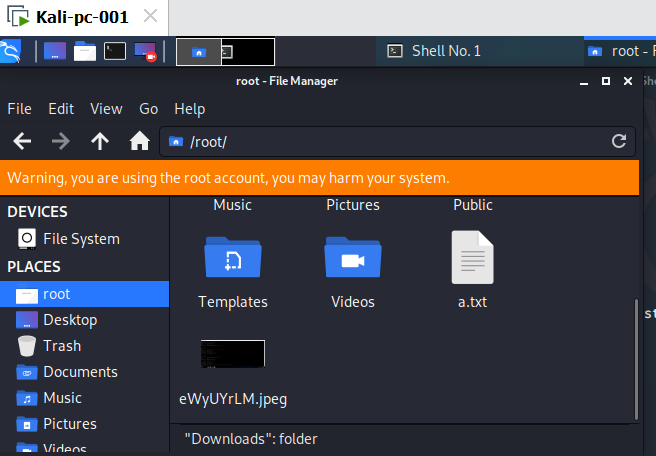
****

1. **Exploit the victim machine**

****

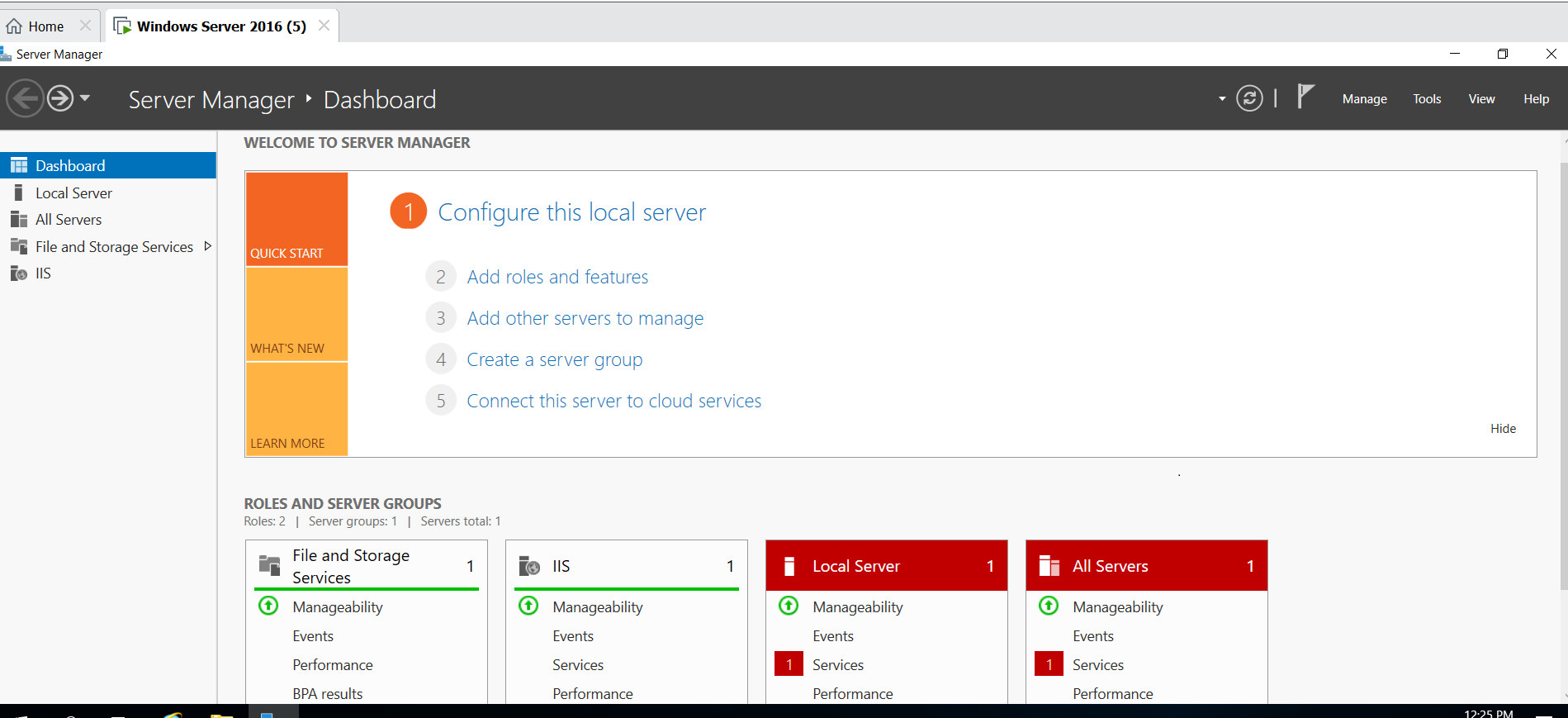
****

****

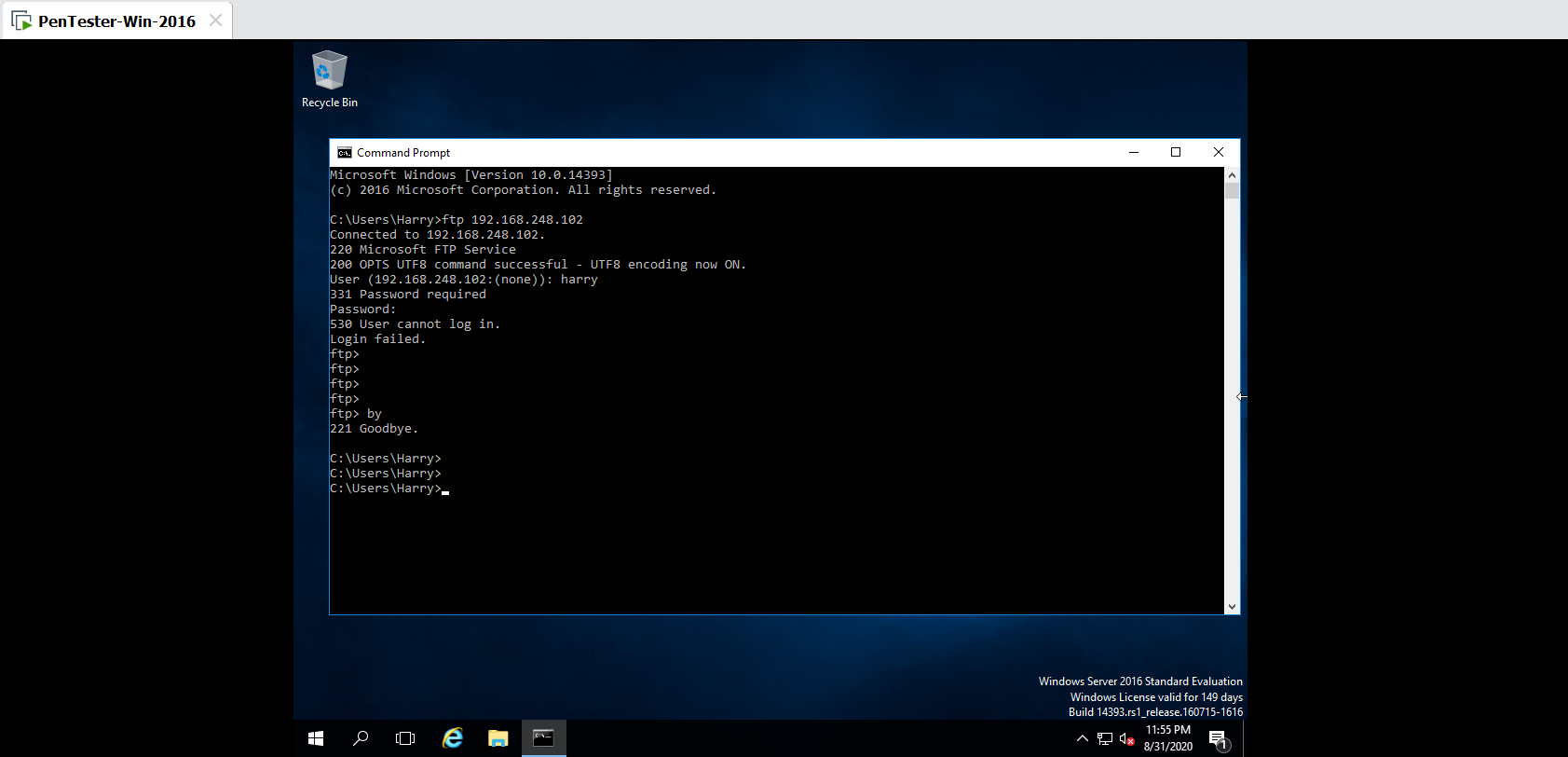
****

**Question 2:**

1. **Create FTP Server**



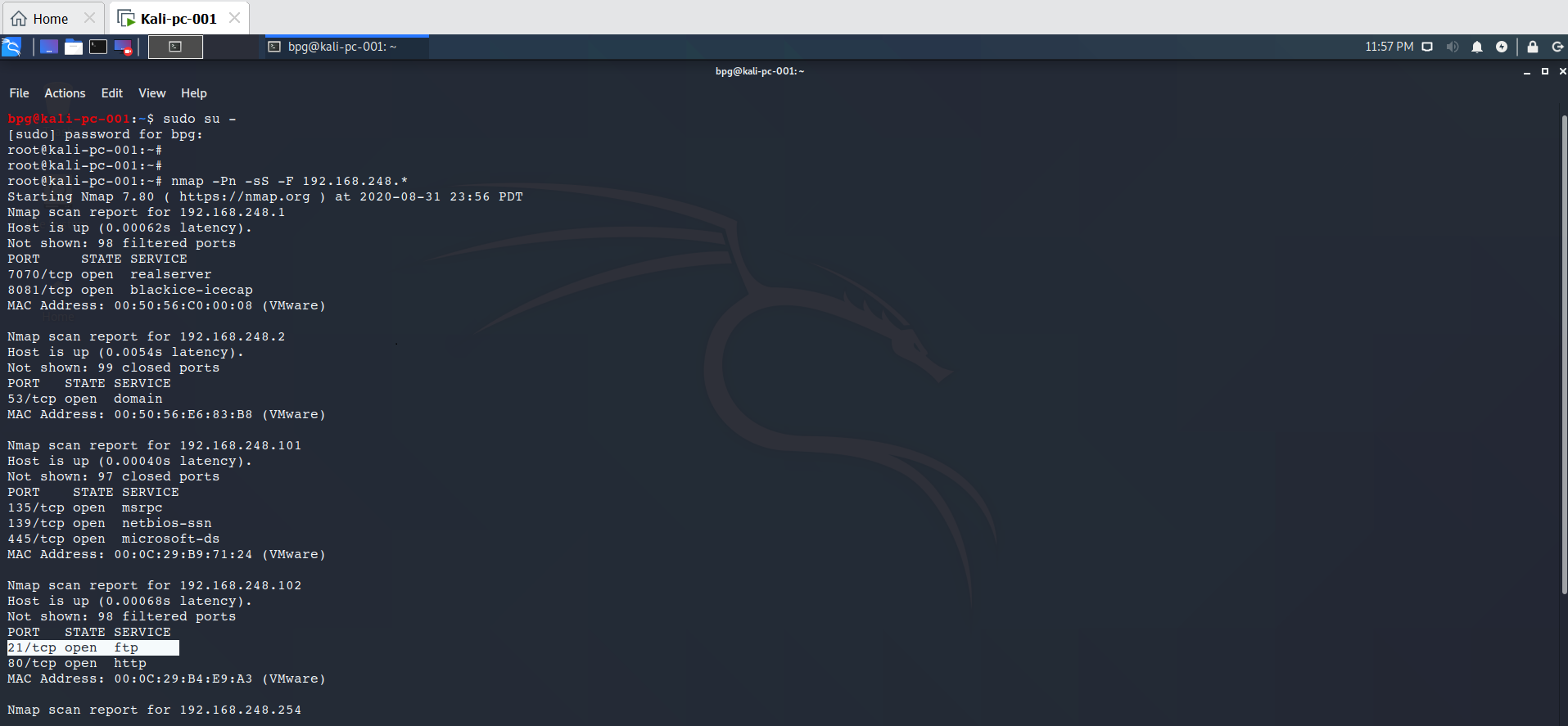
1. **Access FTP server from windows command prompt**



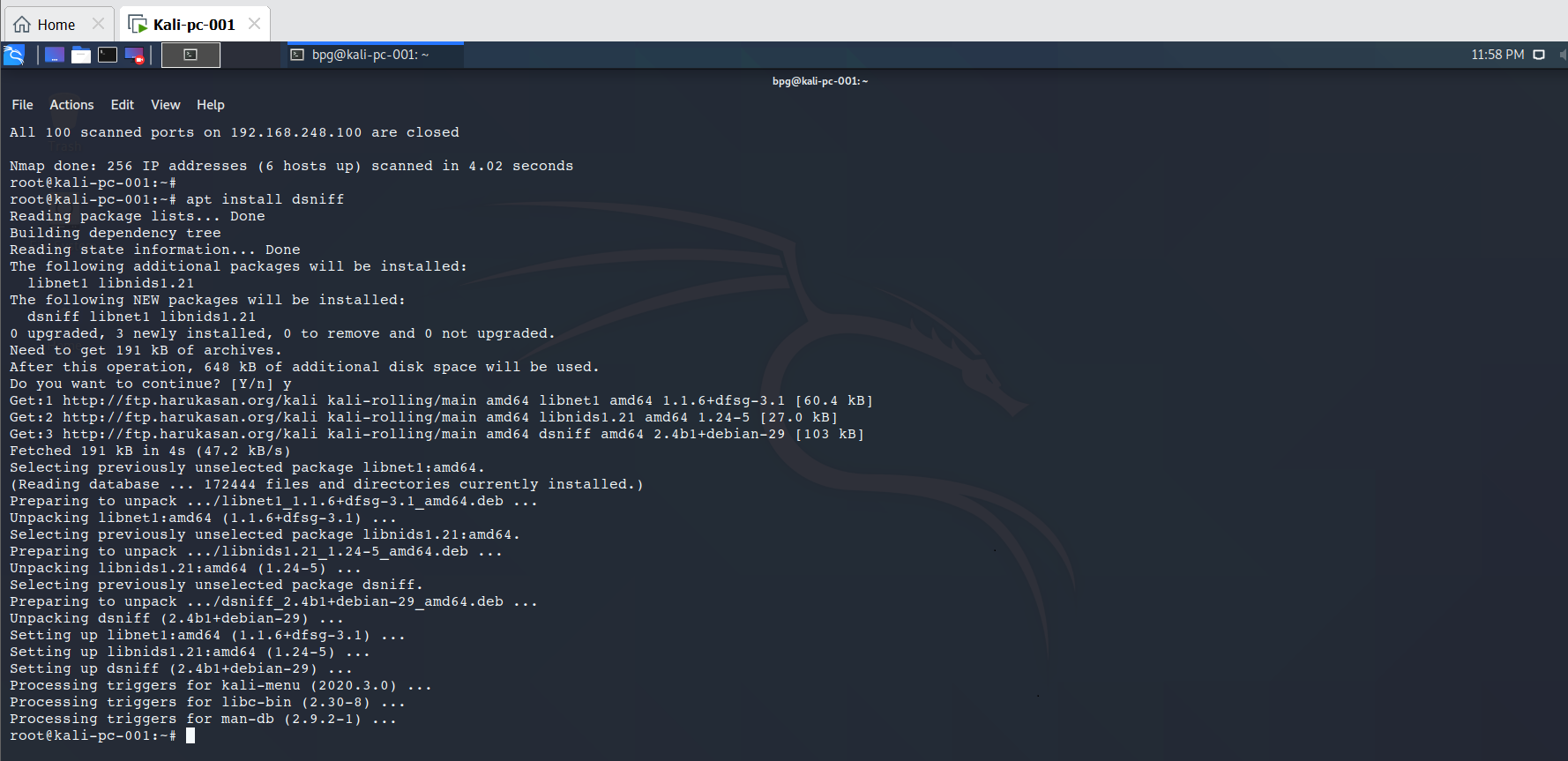
1. **Do mitm of username & password of FTP transaction using dsniff & wireshark**

Use below commands:

1. nmap –Pn –sS –F 192.168.248.\*



1. apt install dsniff (Installs dsniff)
2. echo 1 > /proc/sys/net/ipv4/ip\_forward (enables routing)
3. sysctl -w net.ipv4.ip\_forward=1 (Assigns variable 1)
4. check again the open ports



In Pentest machine try with ftp 192.168.248.102 (ftp server ip)

In Kali machine, you will be able to catch the username & password through dsniff & wireshark

