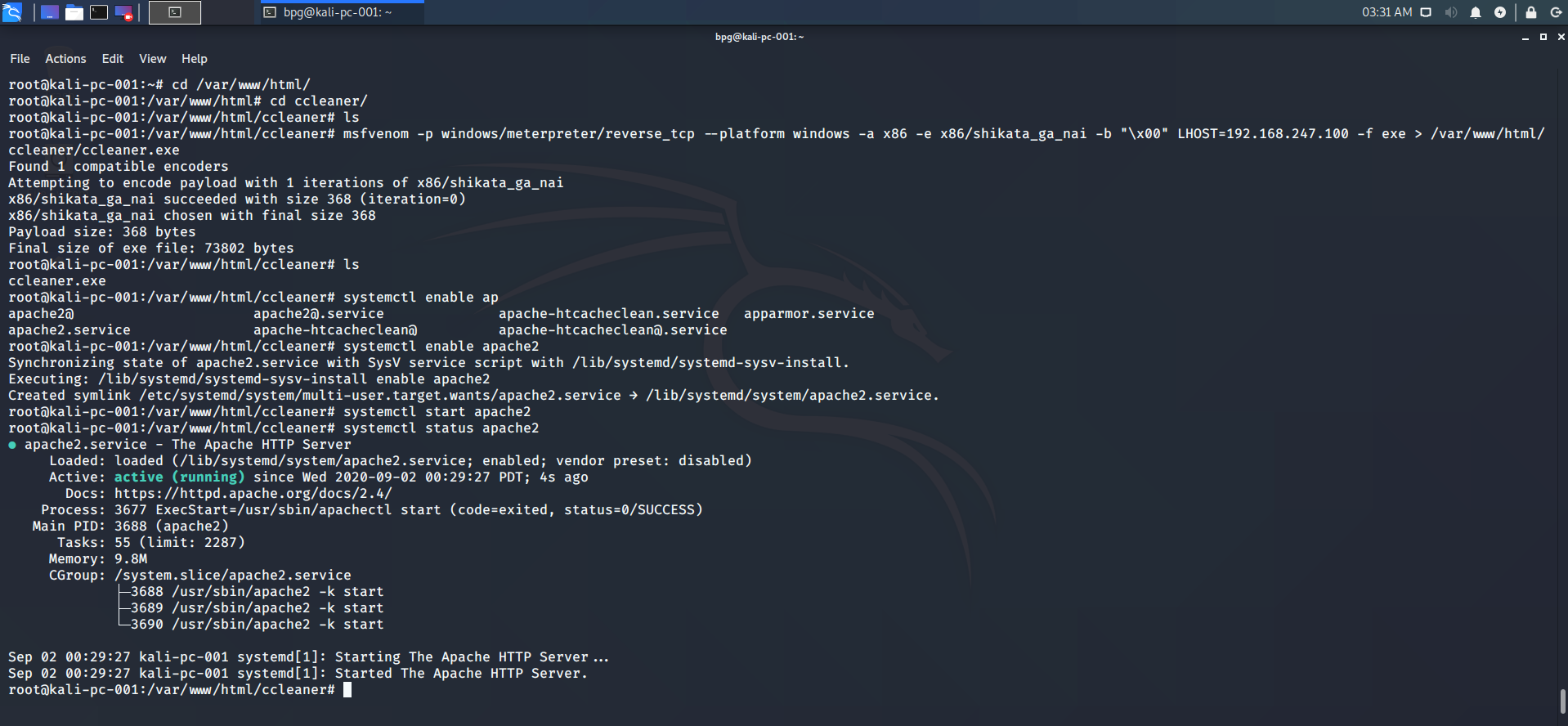
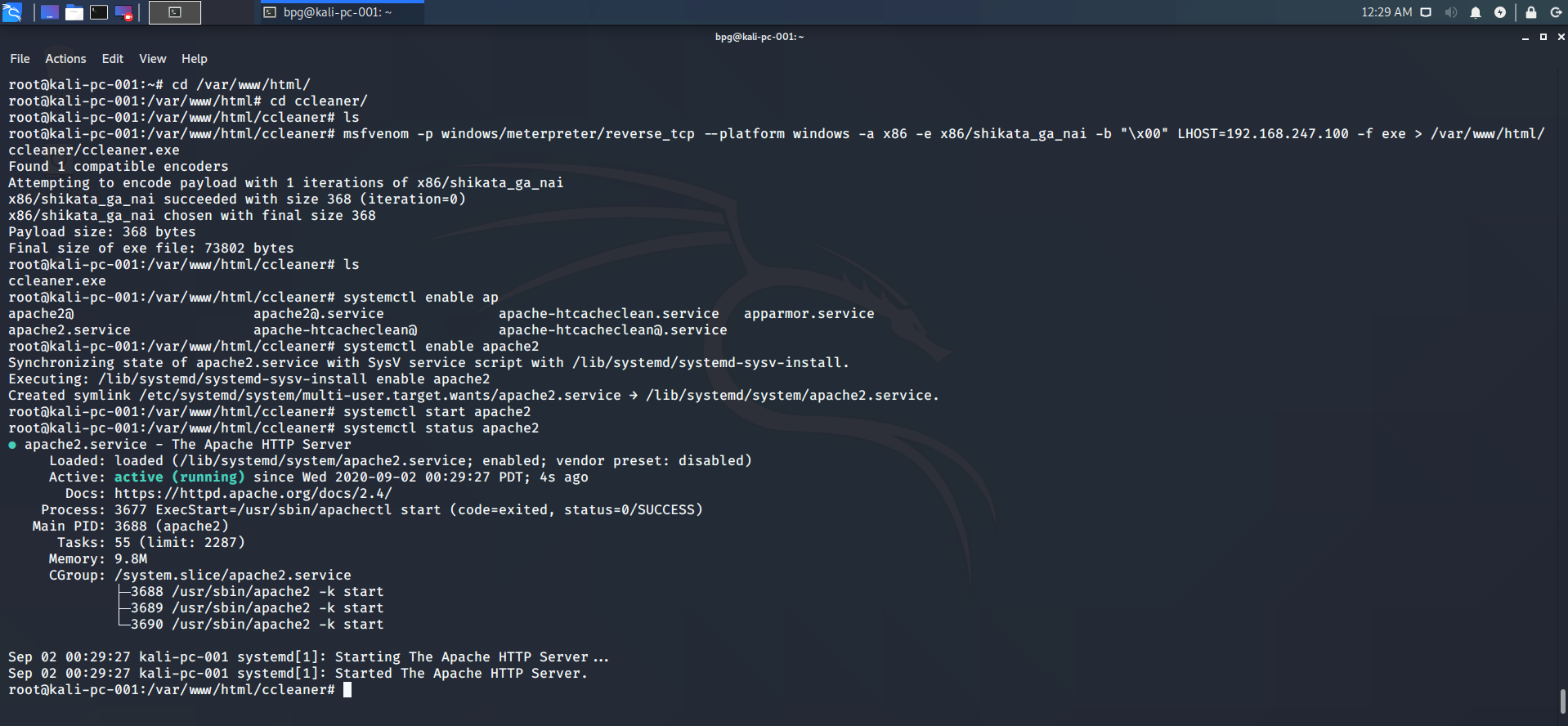
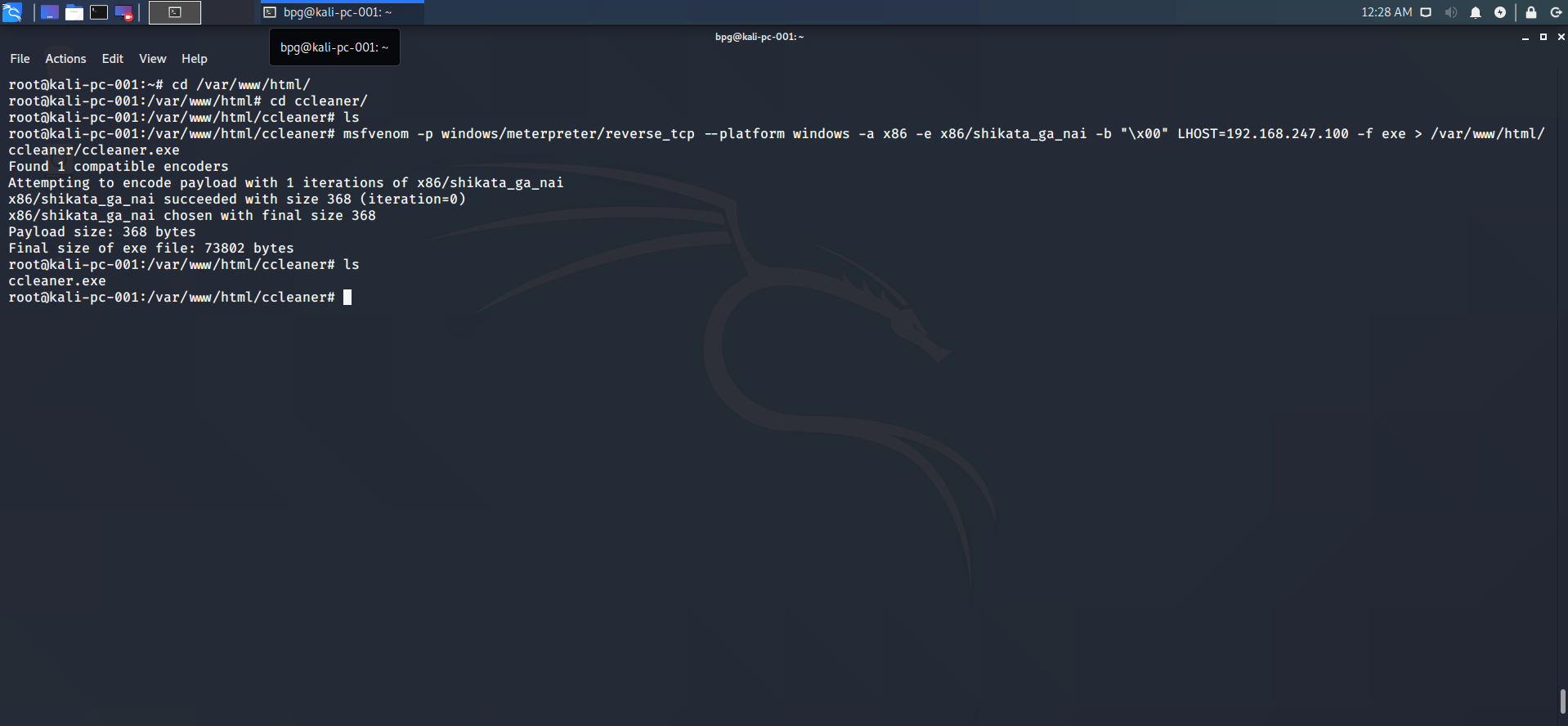
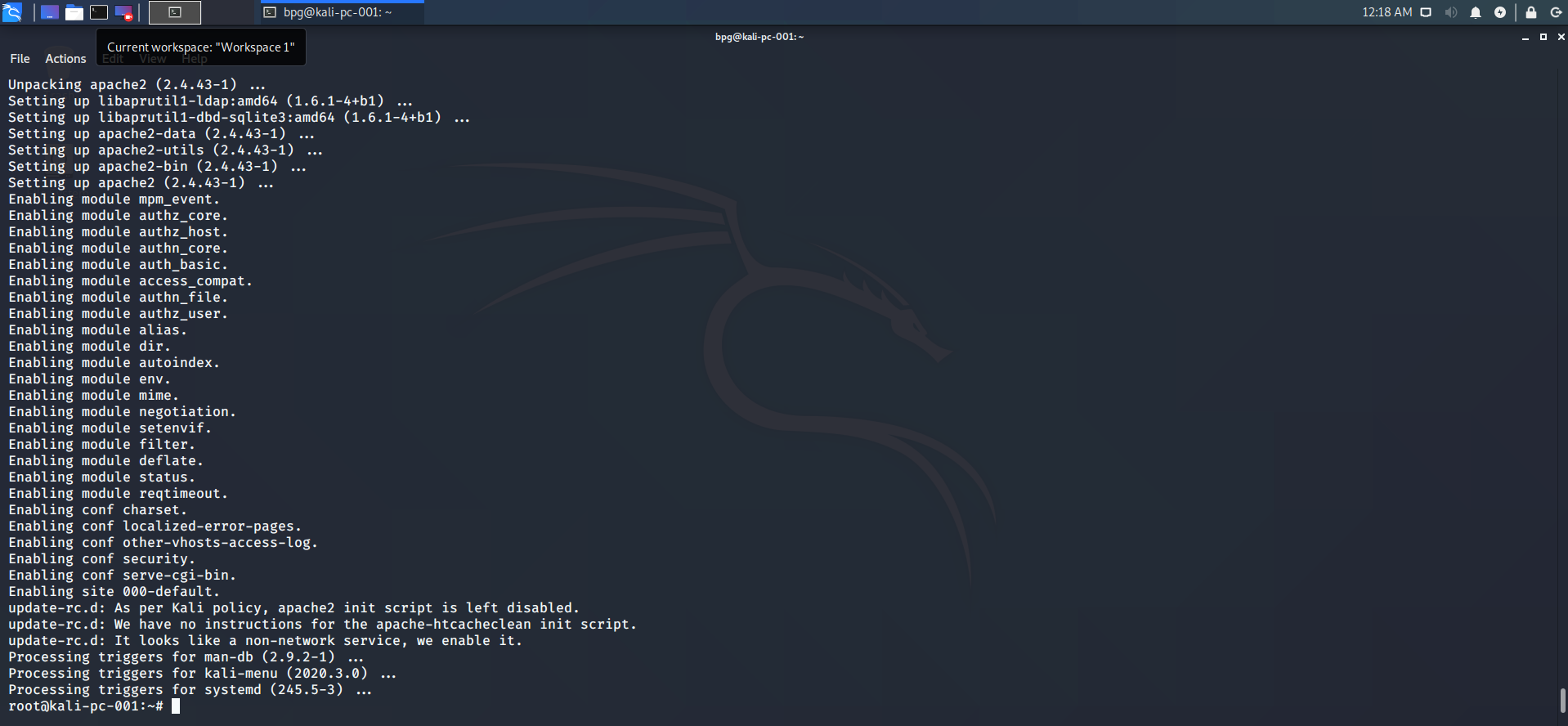
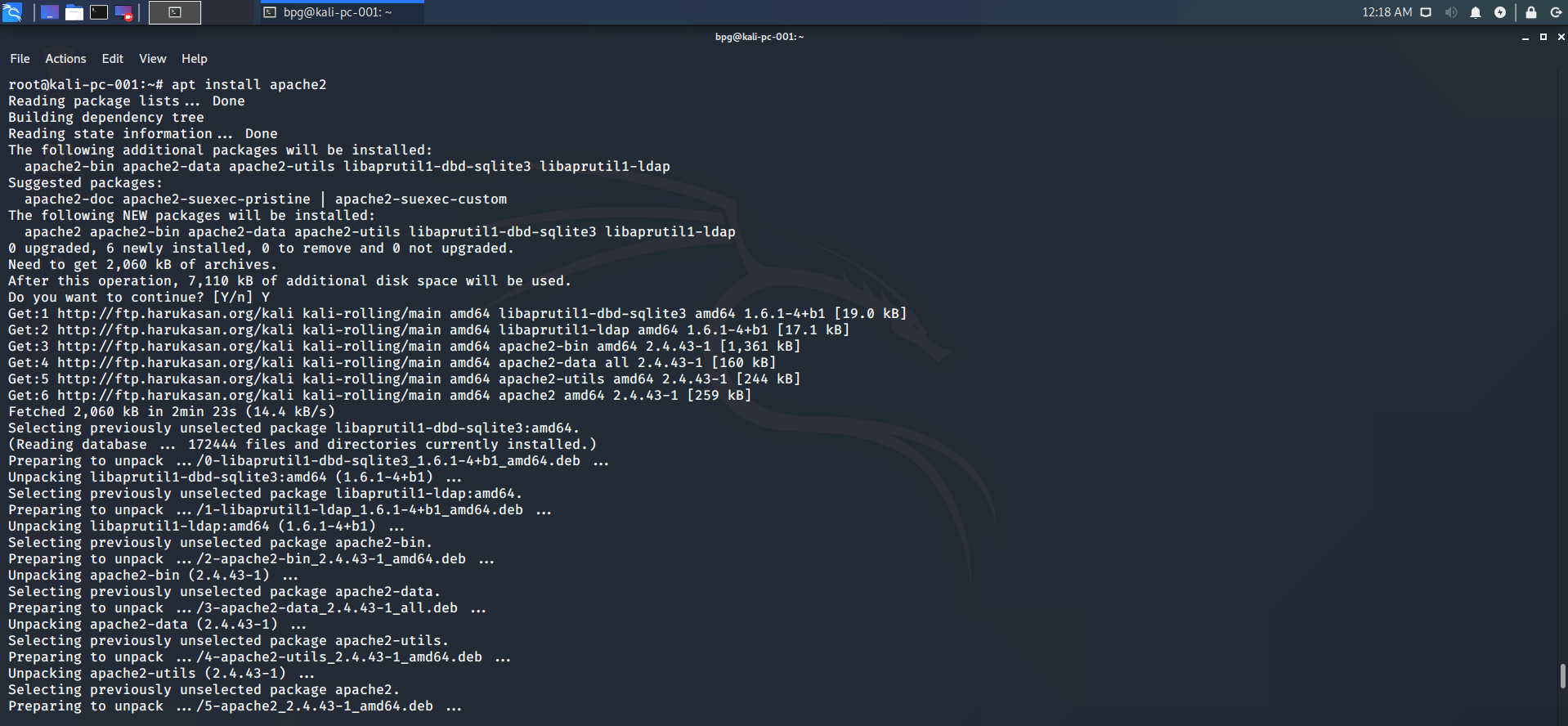
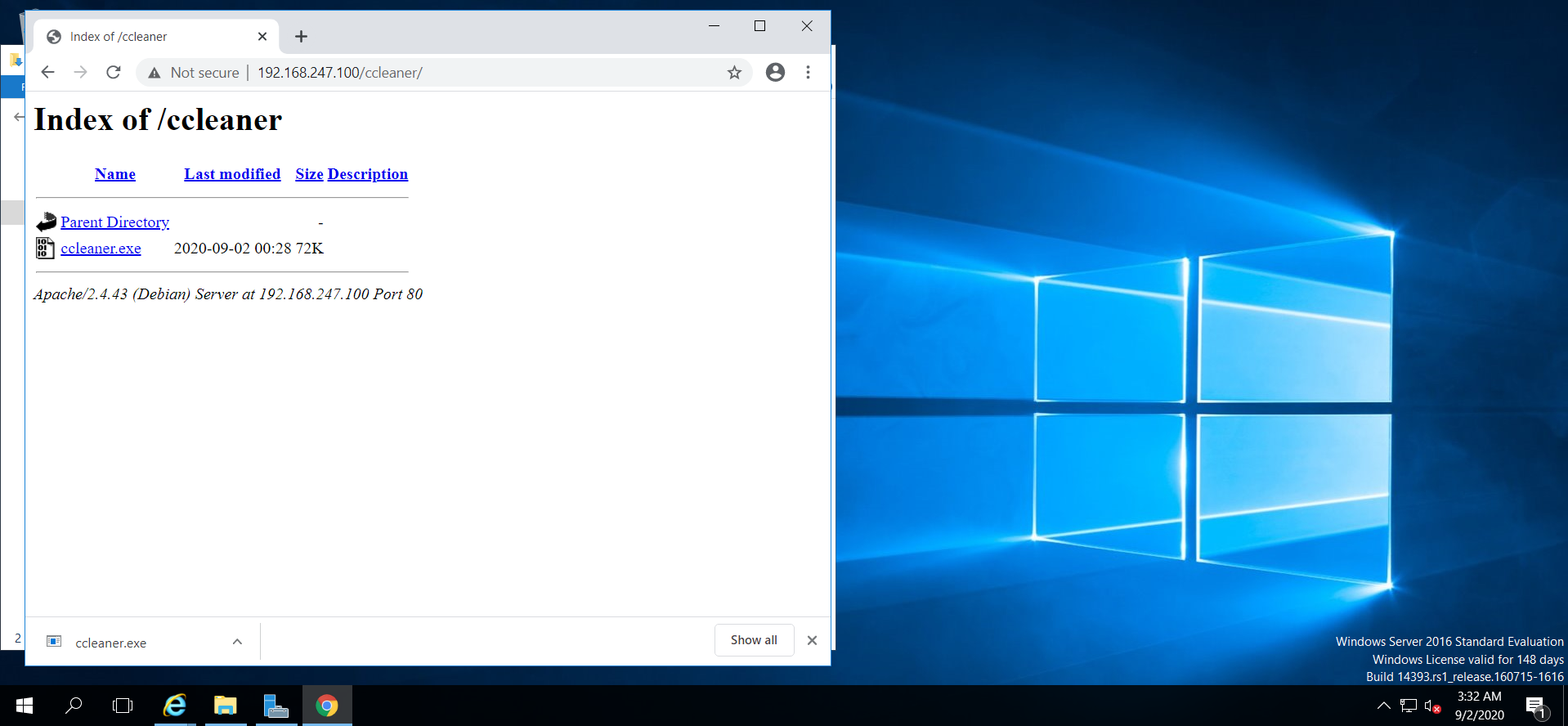
Question 1:

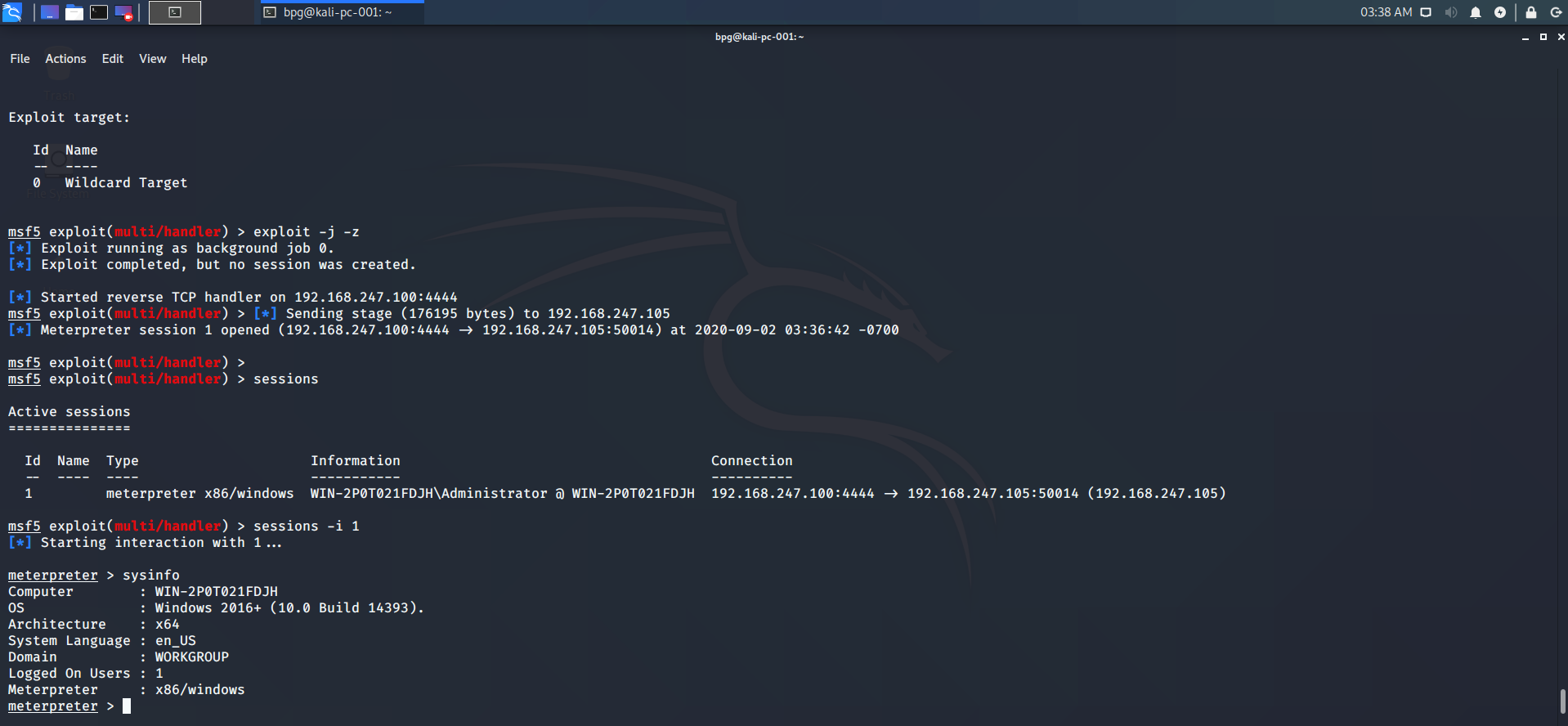
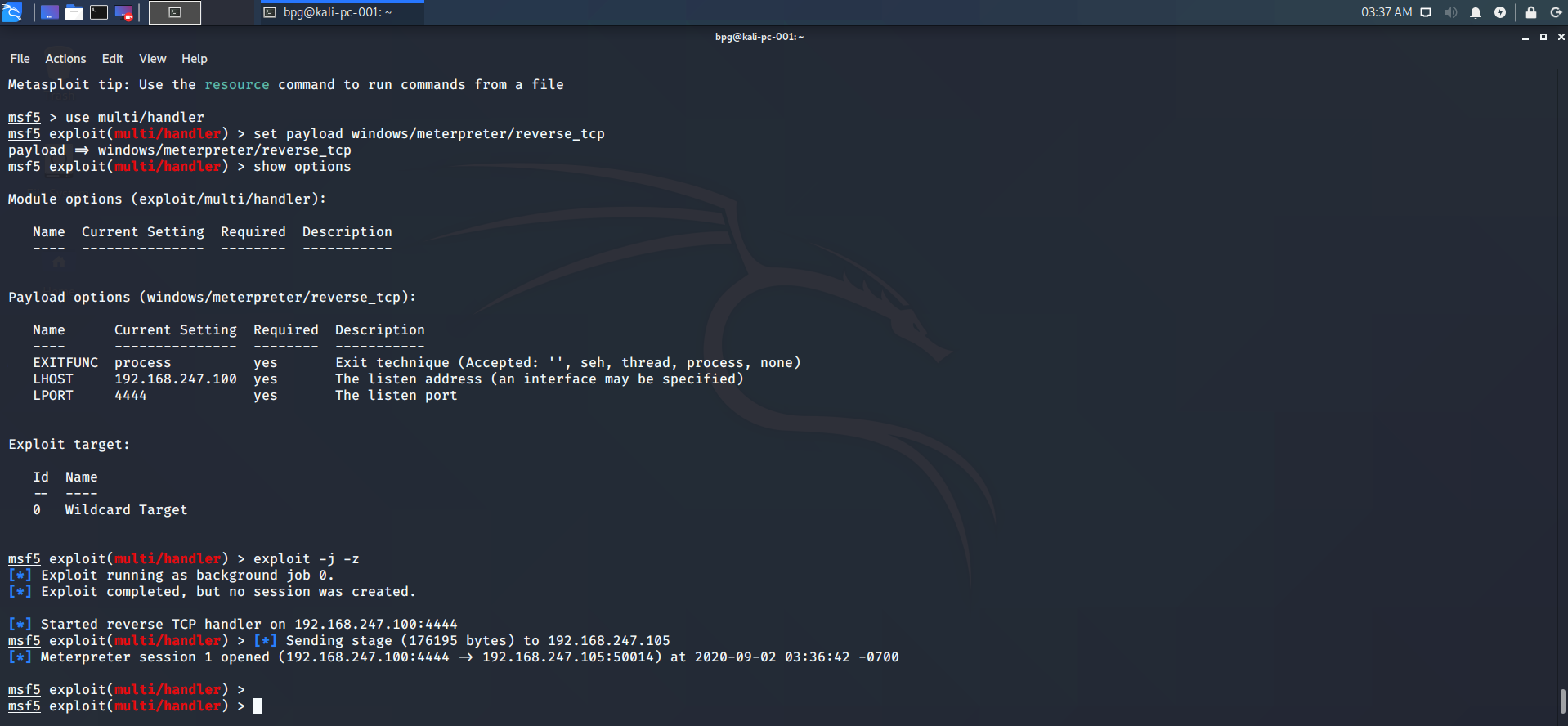
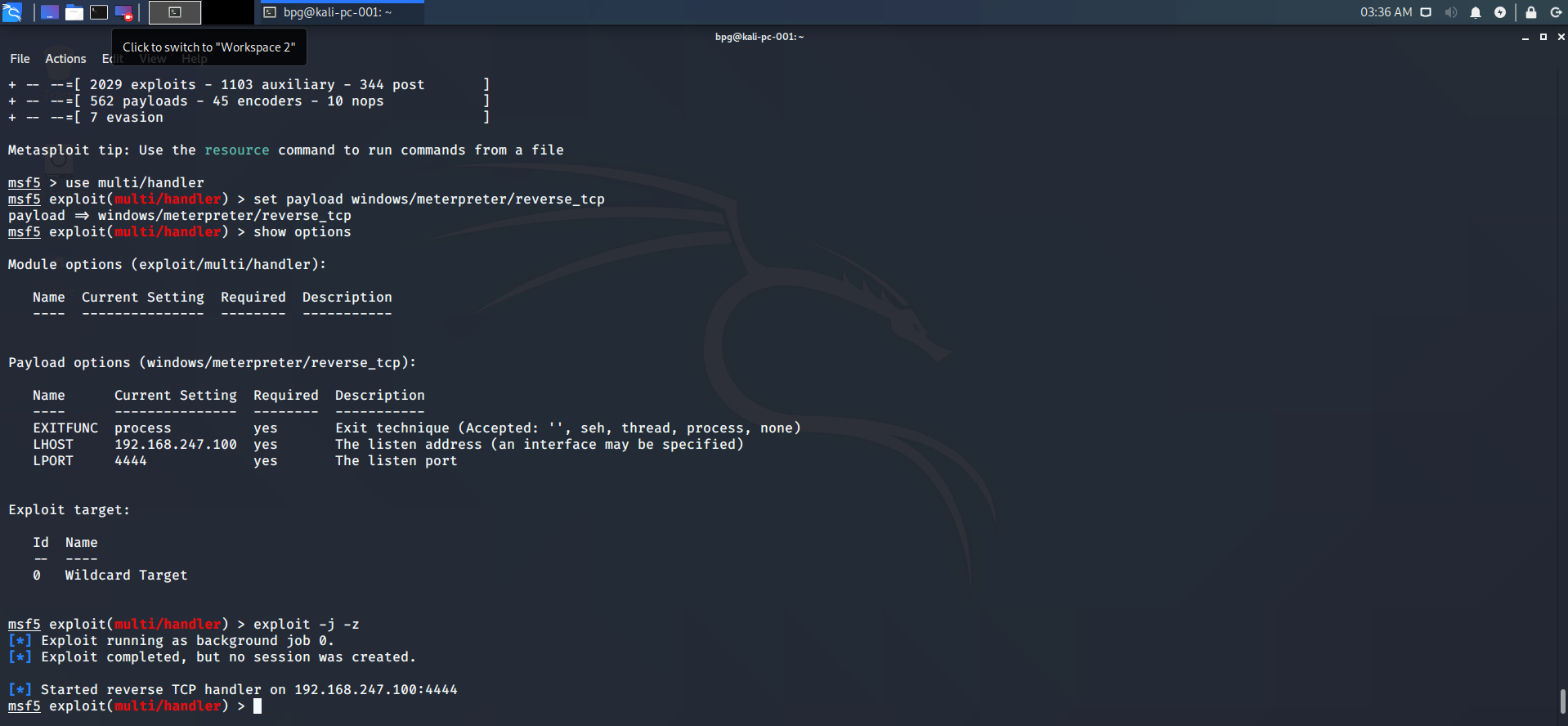
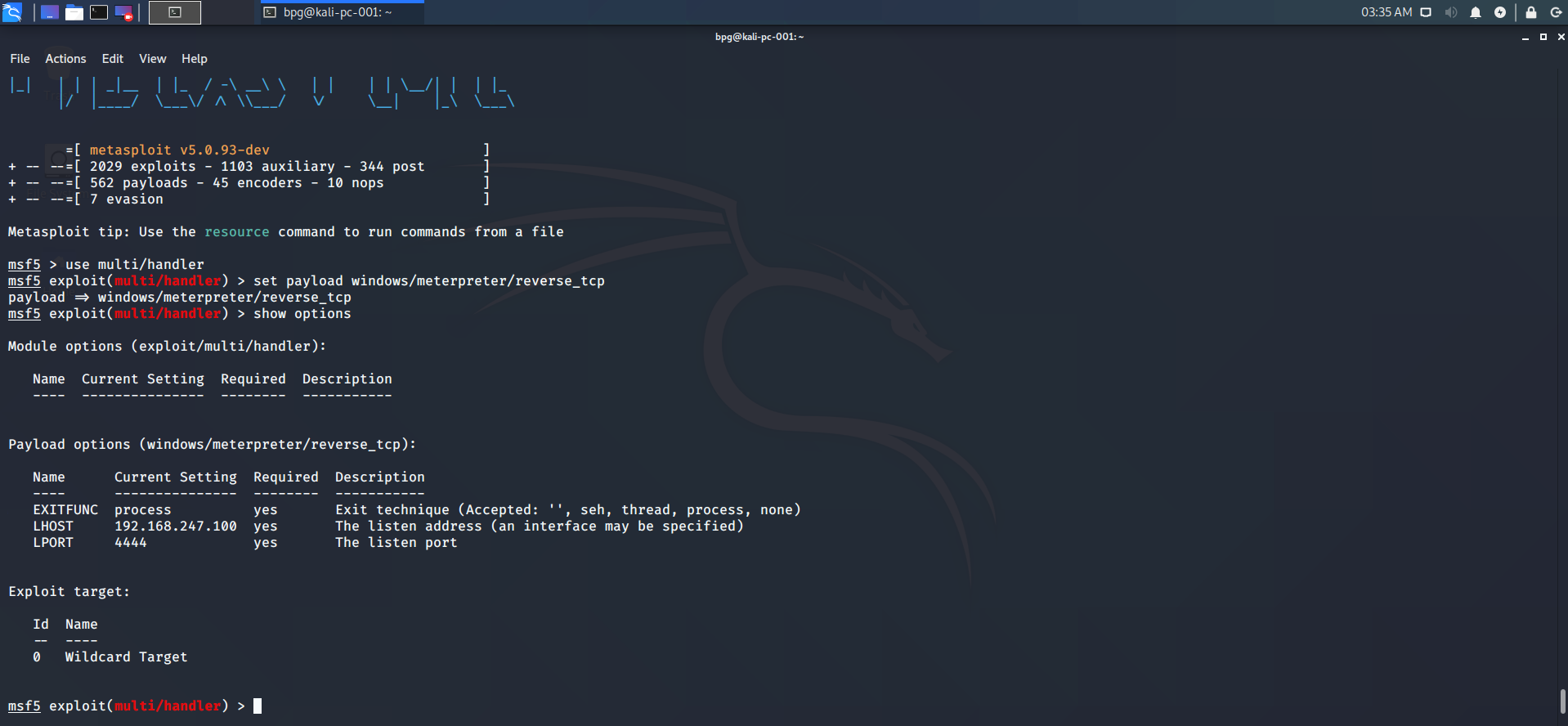
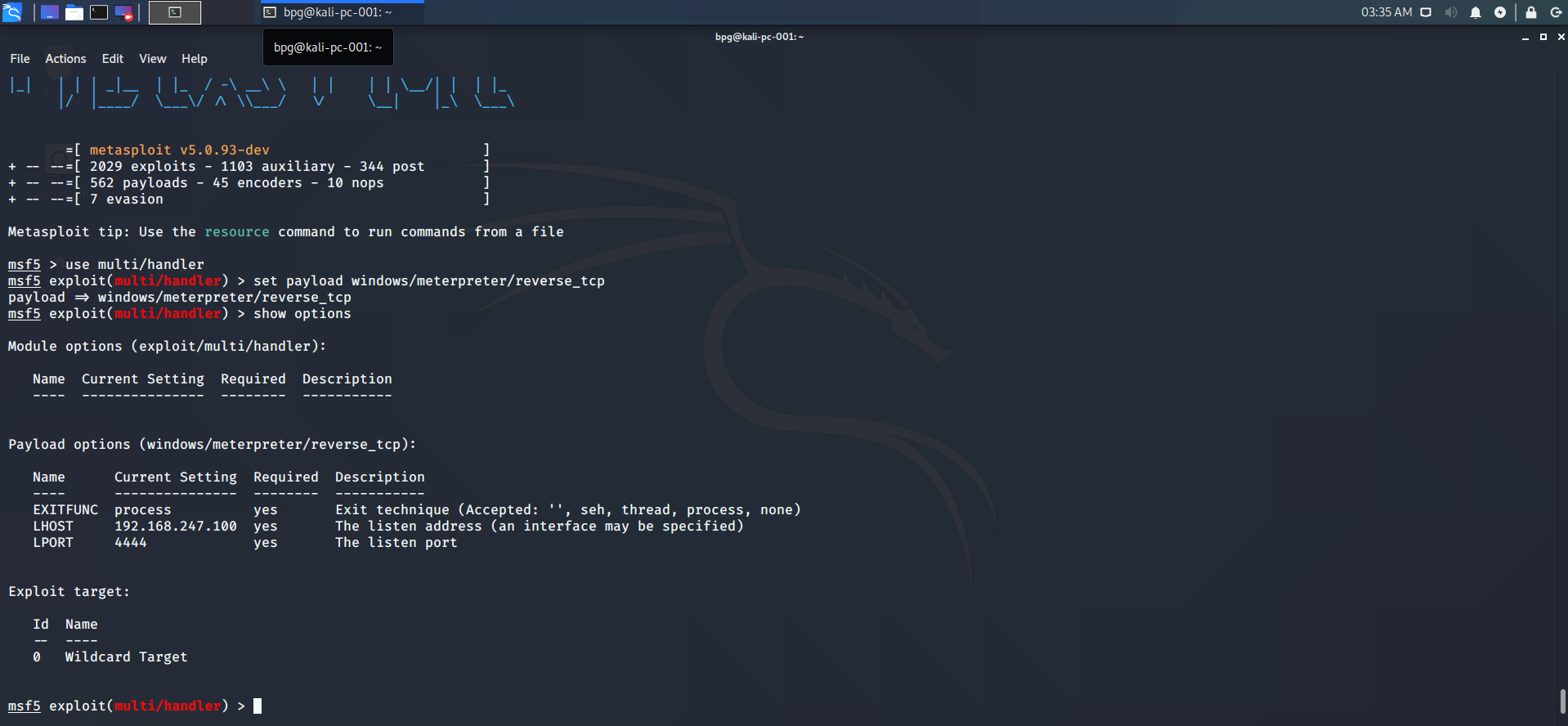
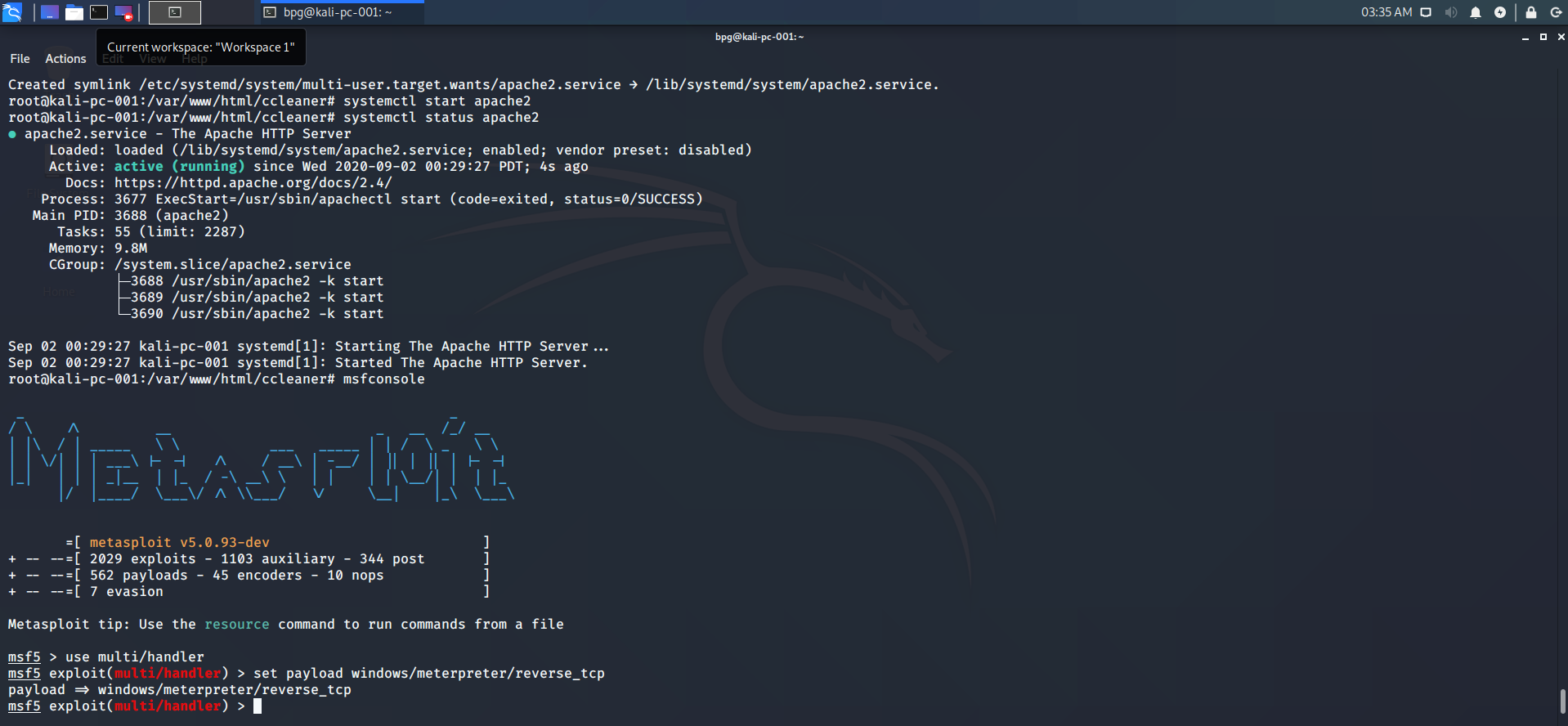
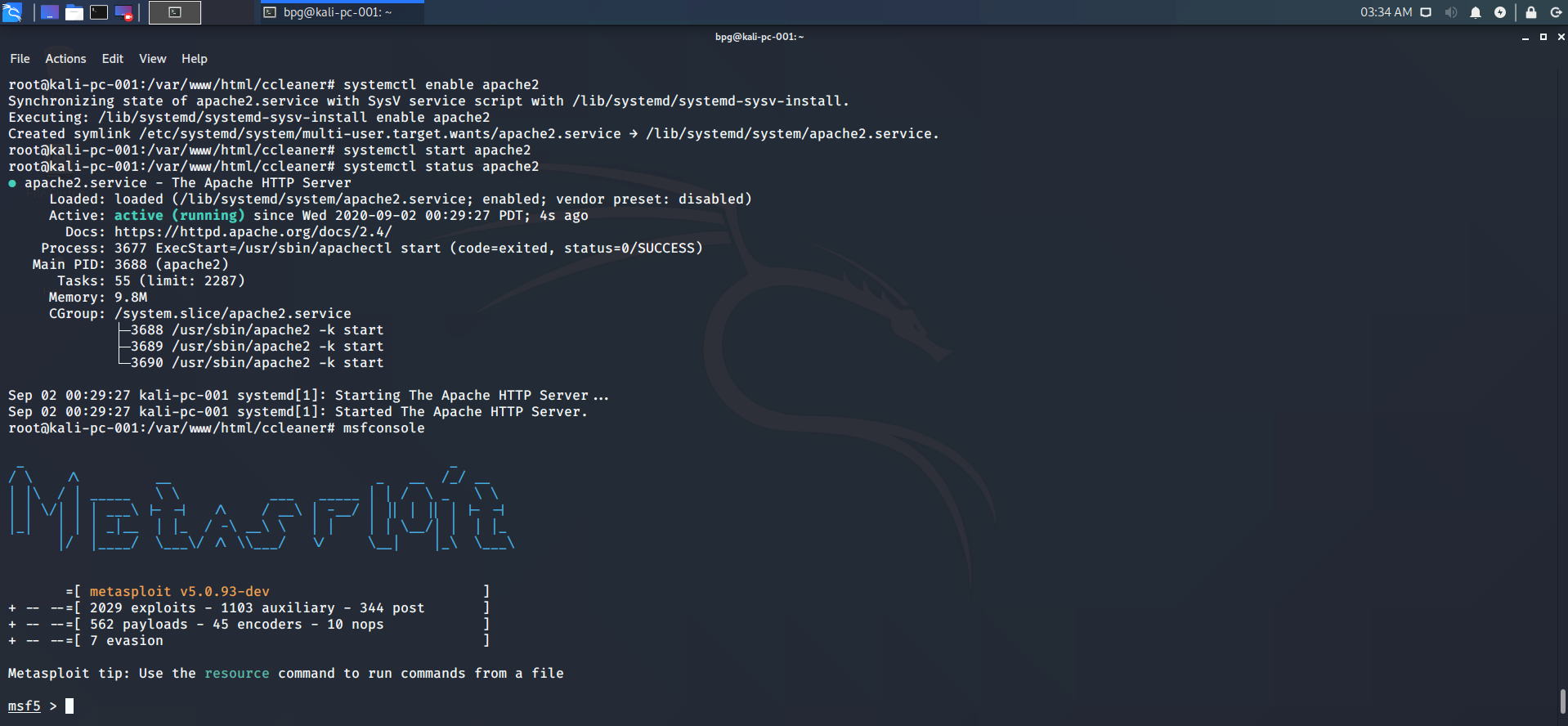
Create payload for windows .

****

Transfer the payload to the victim's machine.

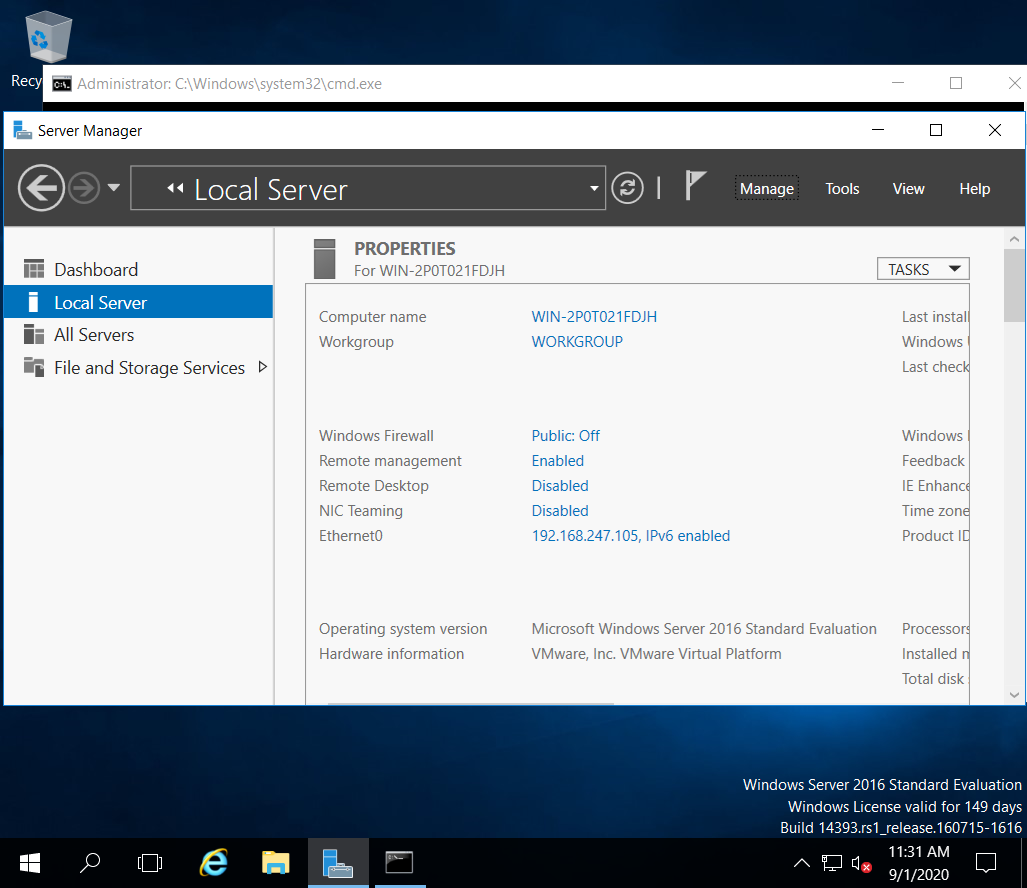
****

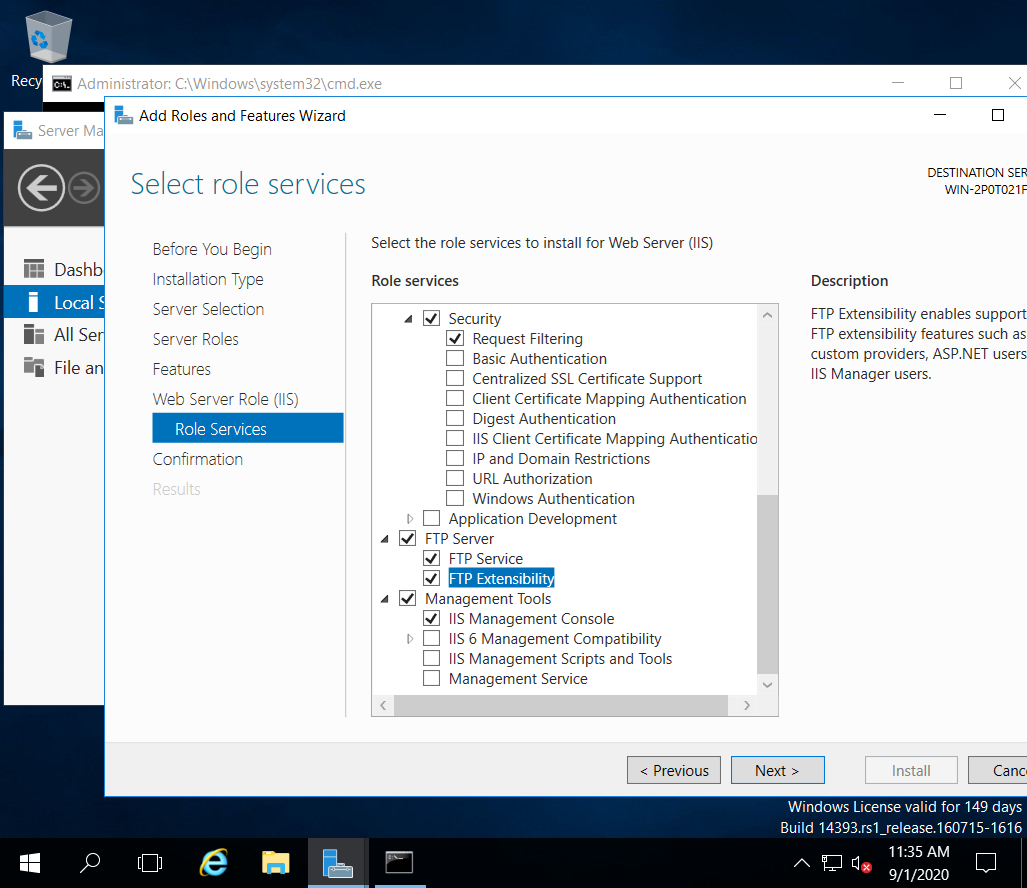
Exploit the victim's machine.

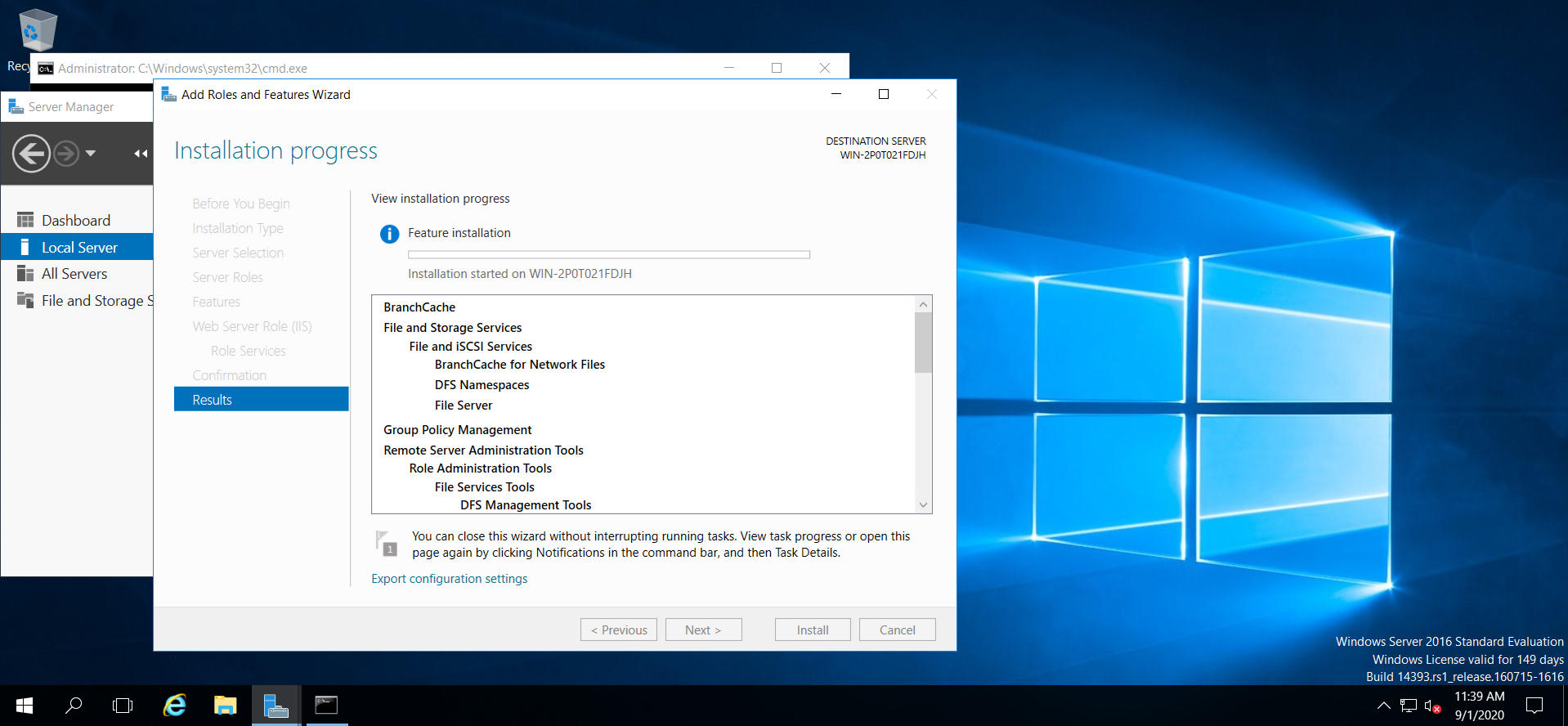
****

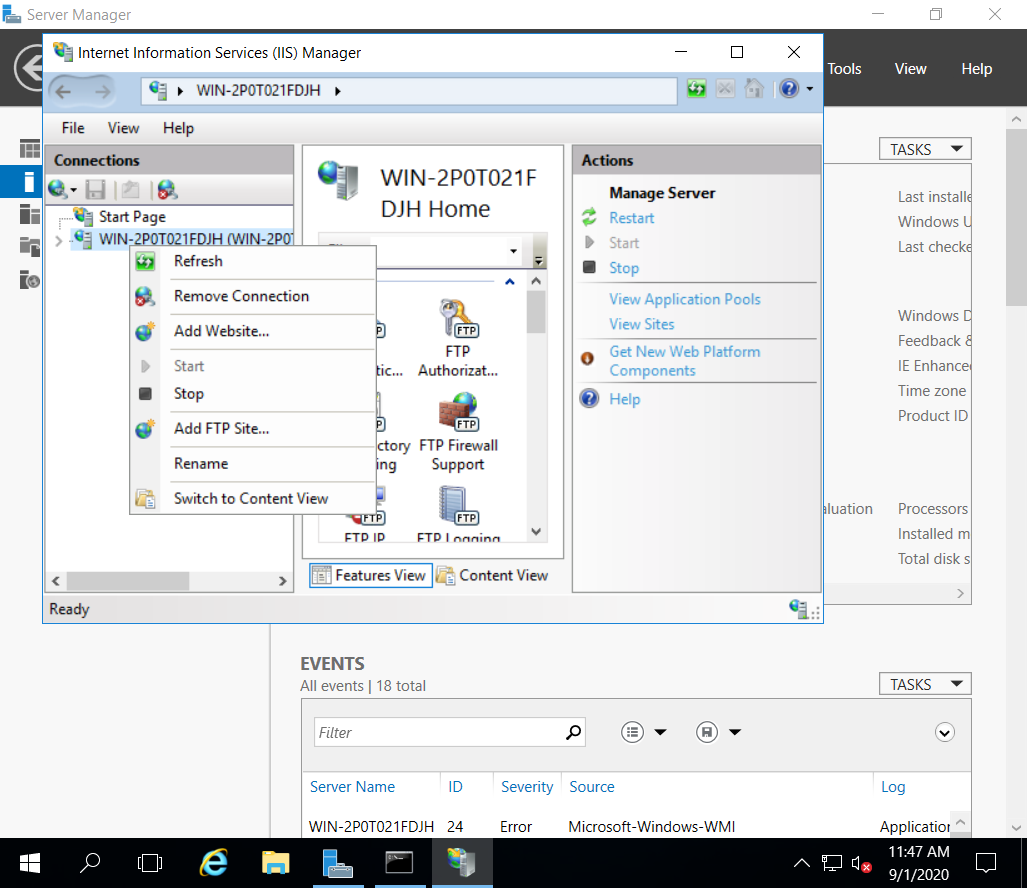
Question 2:

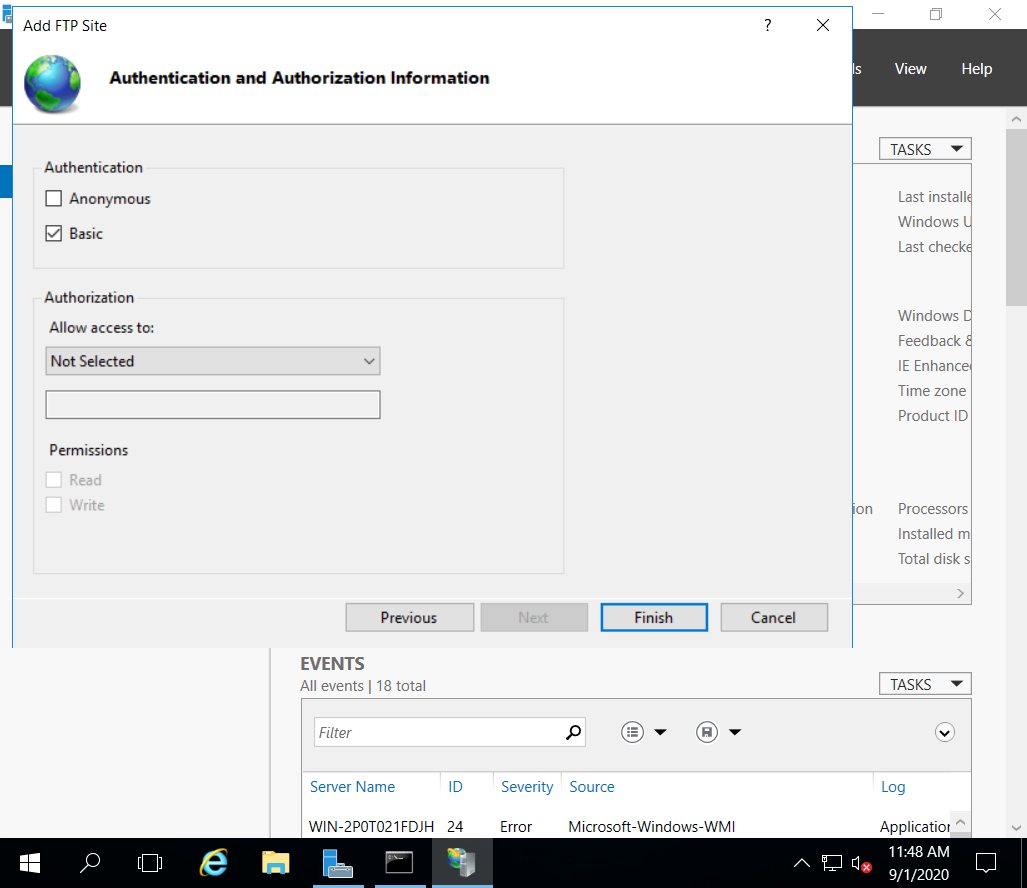
Create an FTP server.



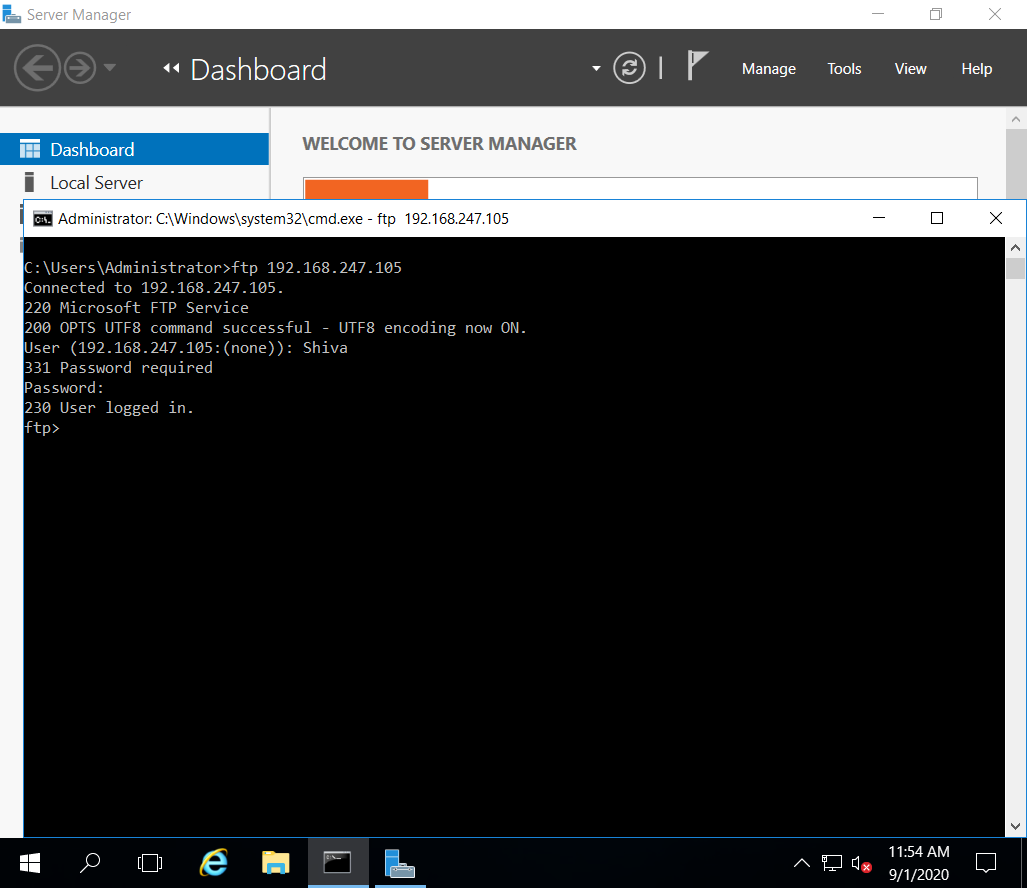




****

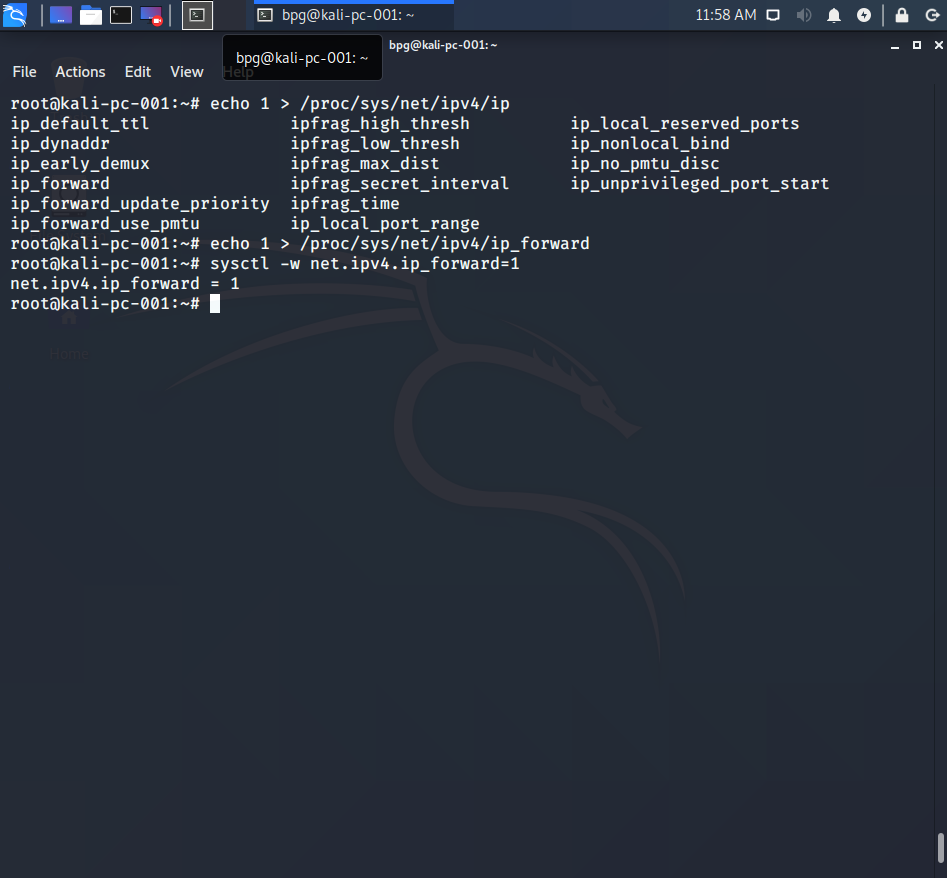
****FTP Server Installed and Configured.

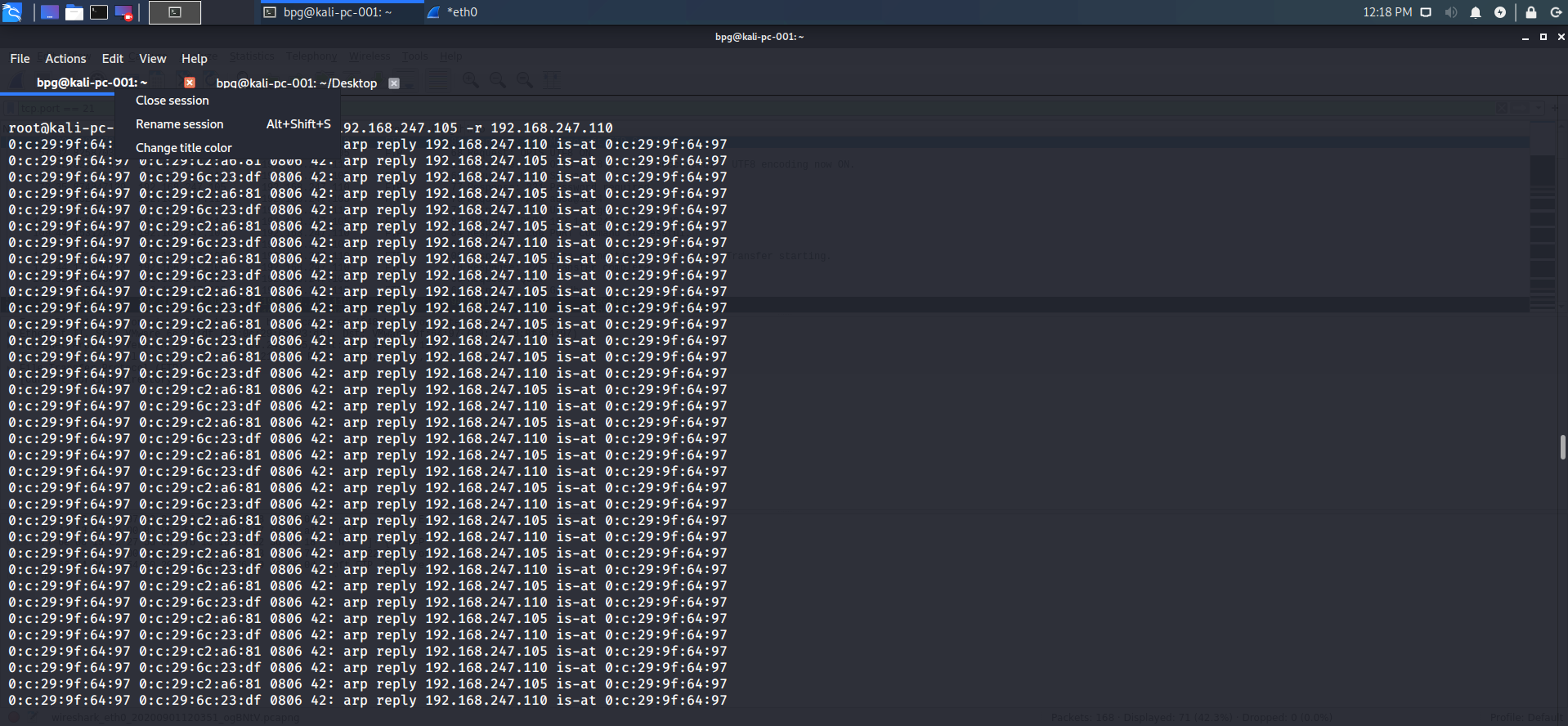
On Machine with IP -192.168.247.105

Access FTP server from windows command prompt

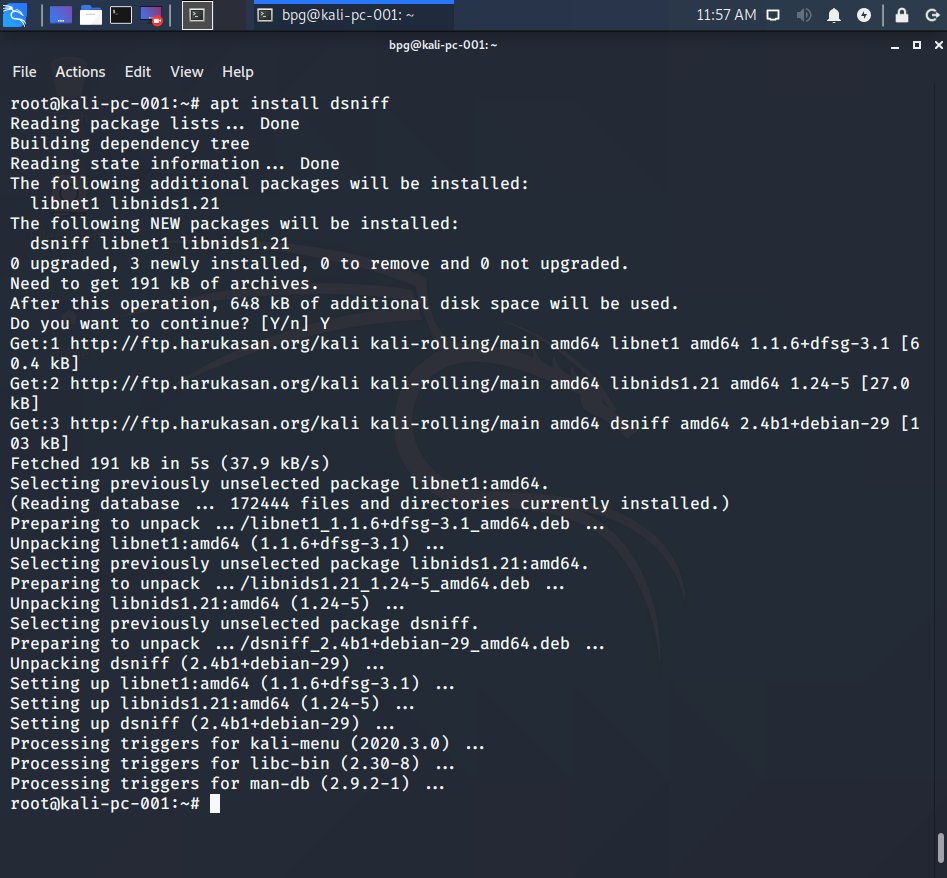
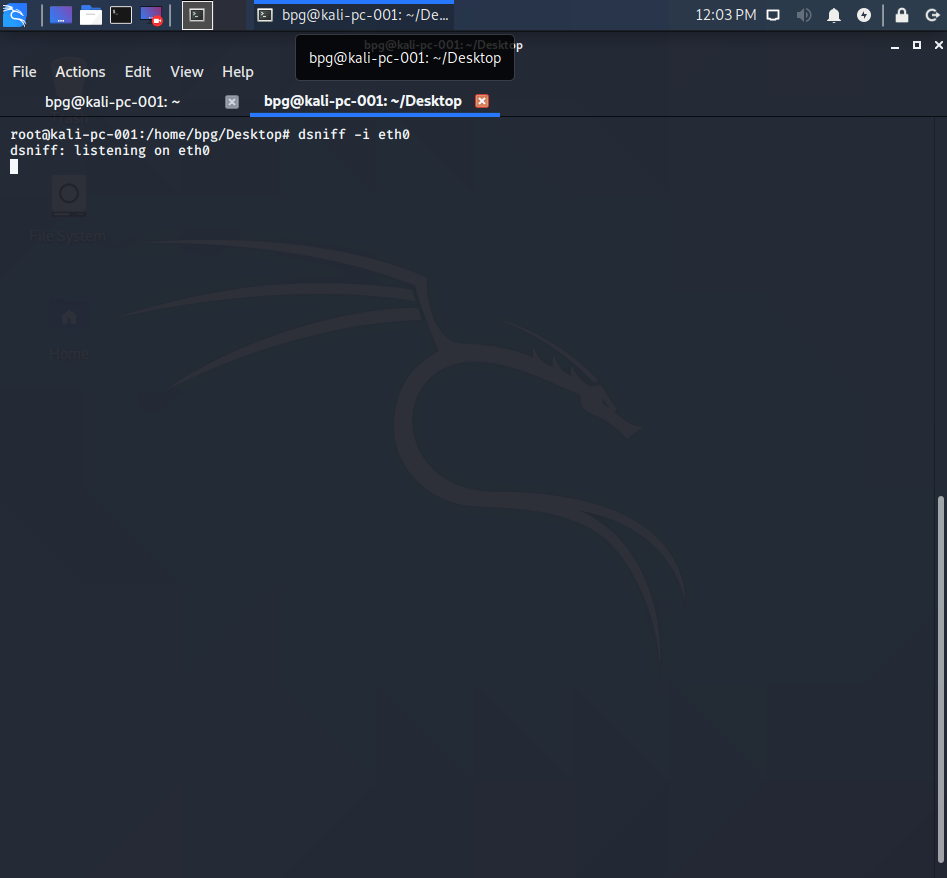
**FTP Server logged in from Machine 192.168.247.110 and logged in Successfully**

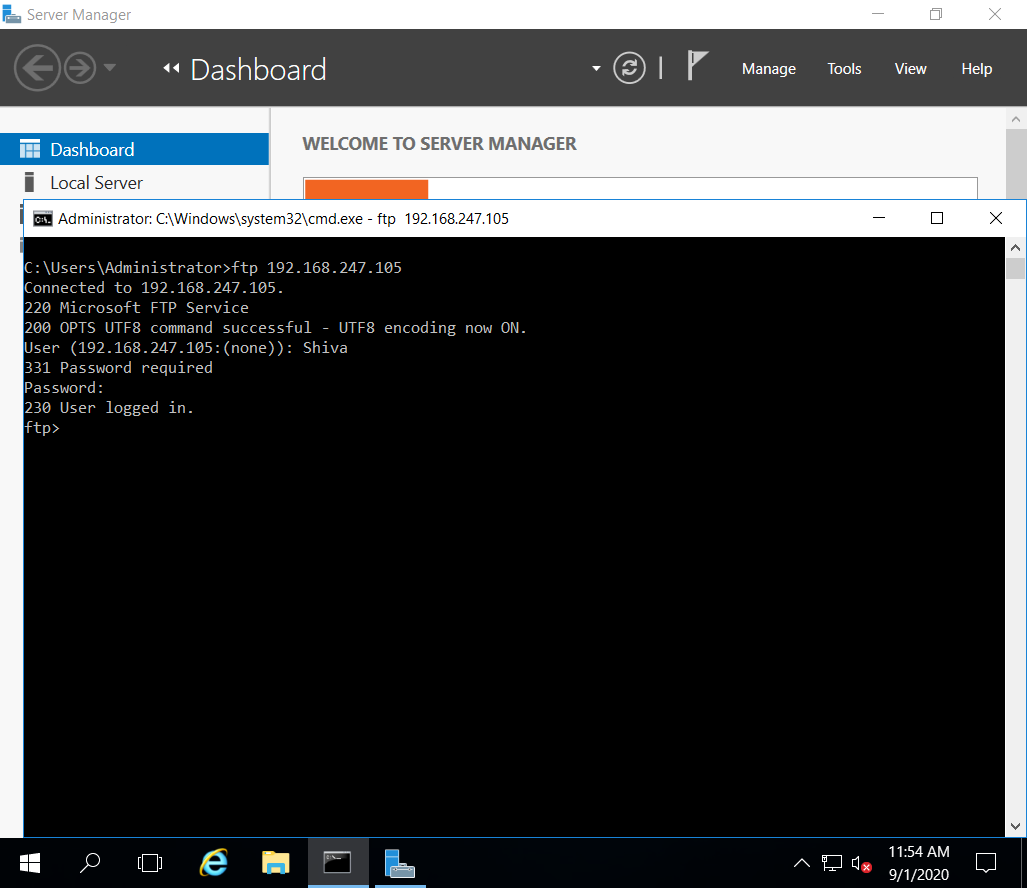
Do an mitm and username and password of FTP transaction using wireshark and dsniff

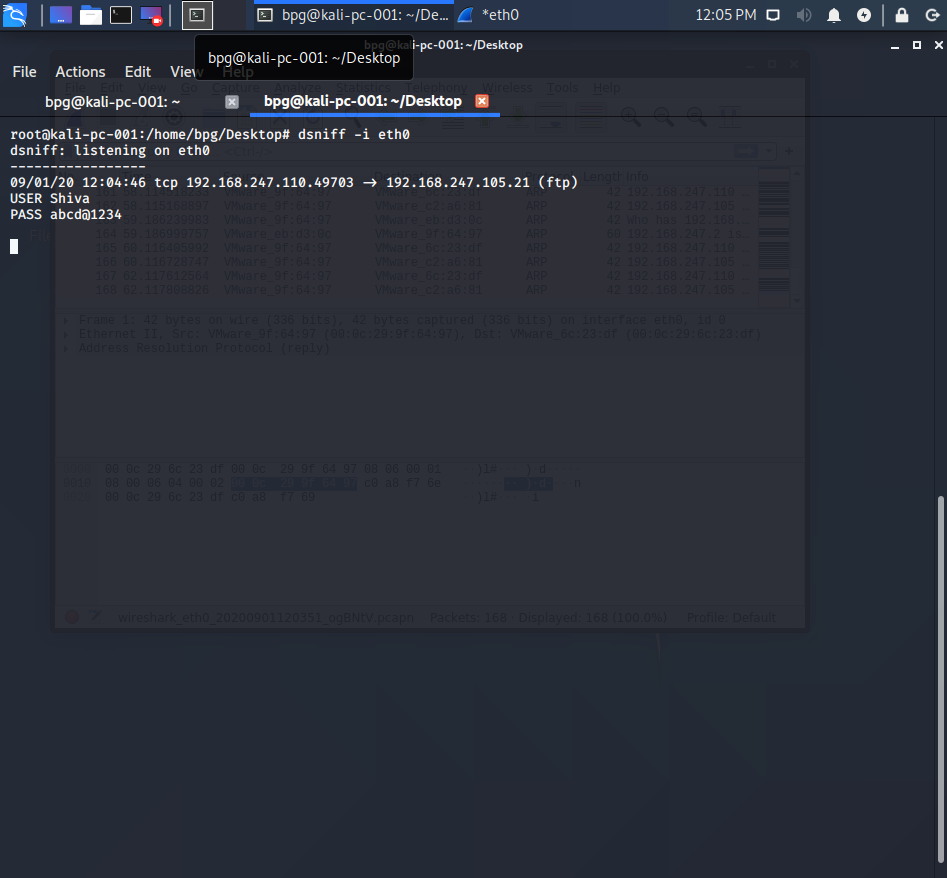
IP forwarding configured on Kali Machine 192.168.247.100****

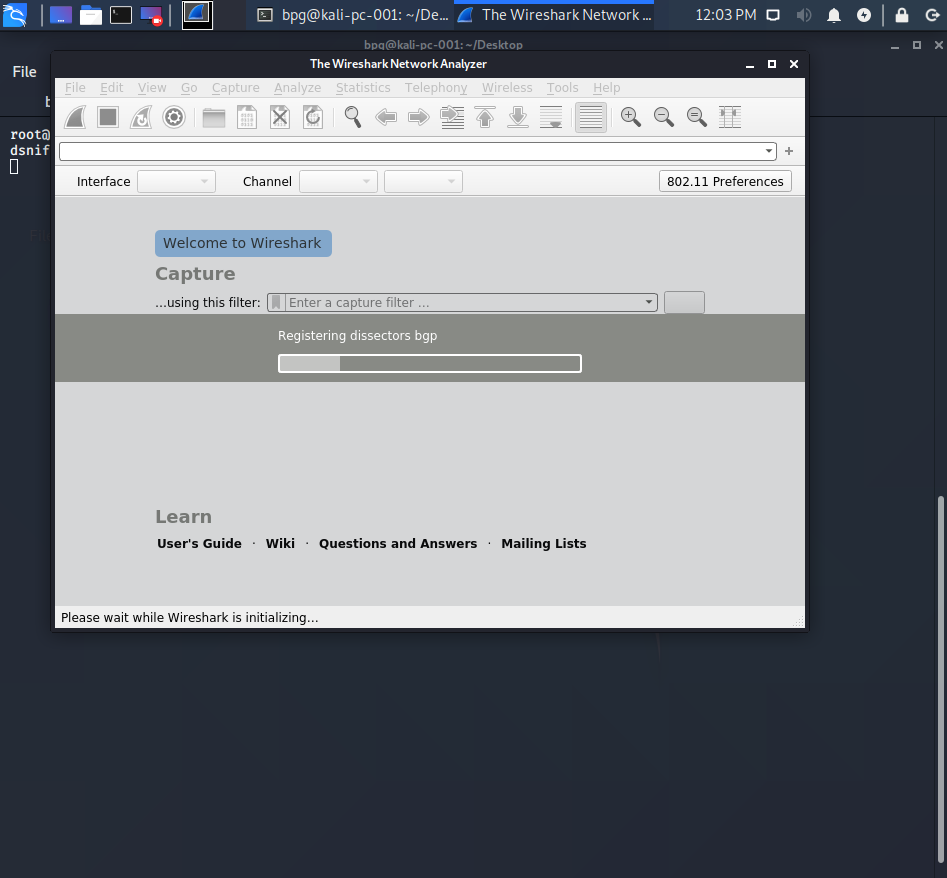


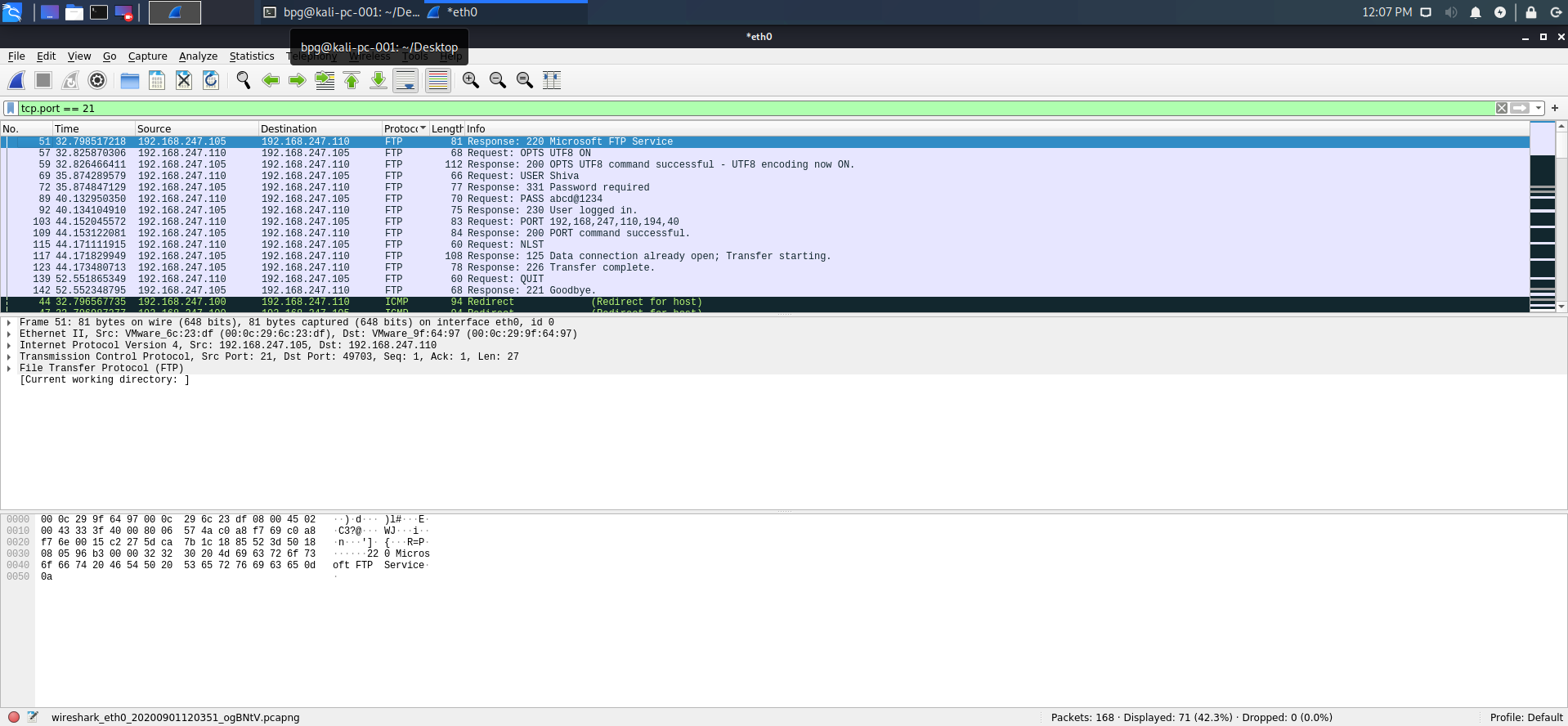
**ARP Spoofing started**

**Dsniff installed and command executed on interface eth0**

**FTP Server logged in to capture the credentials  
**

**Dsniff captured the credentials**





**Started wireshark and filtered FTP Protocol and got Username and Password of FTP User**