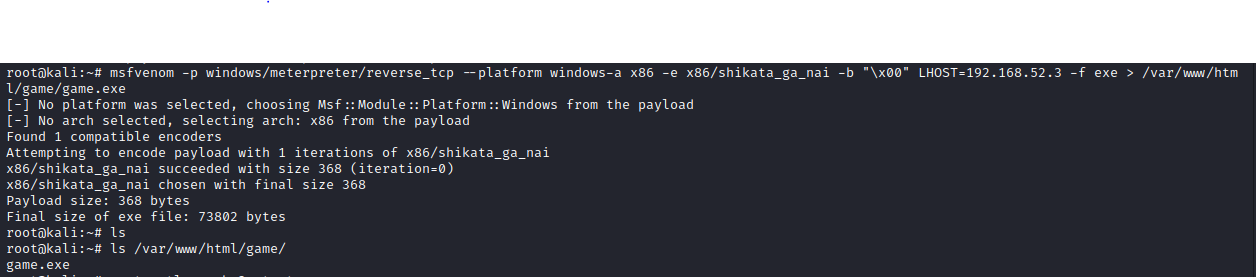
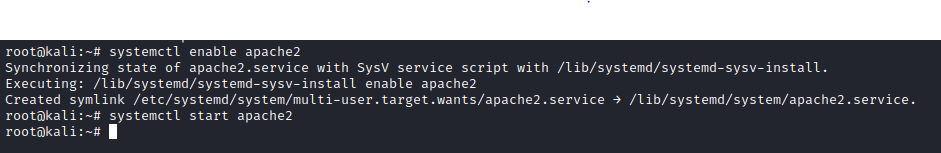
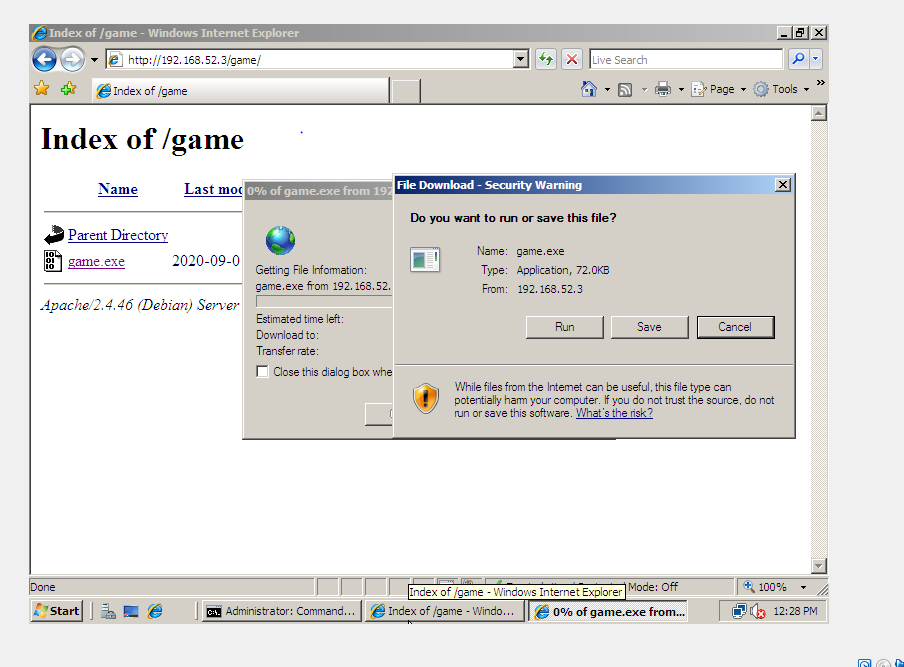
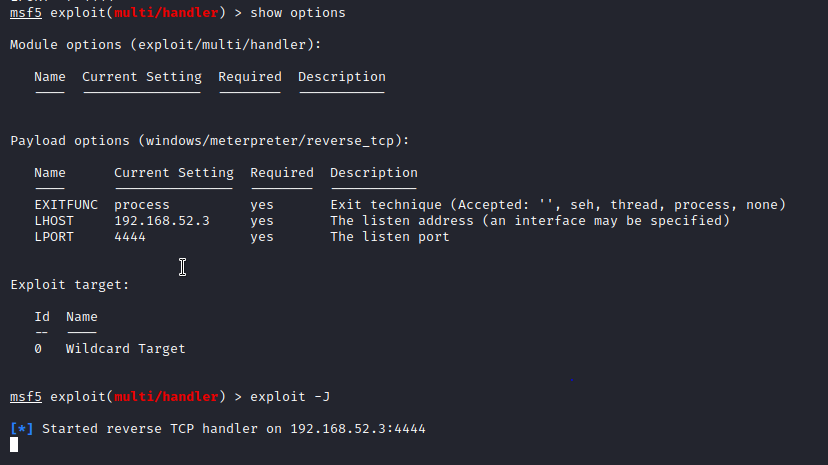
Question 1: Create payload for windows.

Windows payload created in the name of game and saved in /var/www/html/game/game.exe in kali.

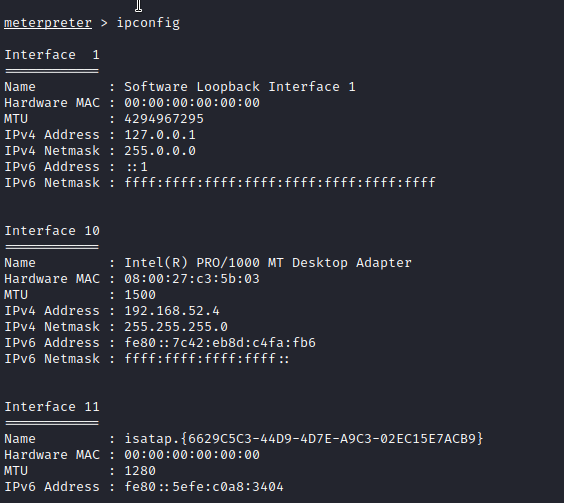
LHOST: 192.168.52.3 (Kali machine IP address)

Enable and start apache2 server in kali.Transfer the payload to the victim's machine. From Windows machine assessing and running payload. 

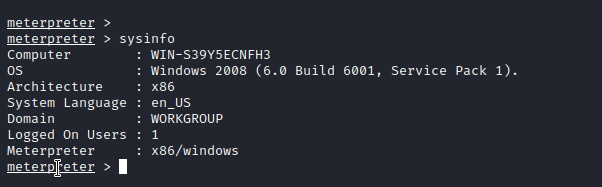
Running Multihandler to receive payload connection.



Checking Victim (Windows) IP address:192.168.52.4

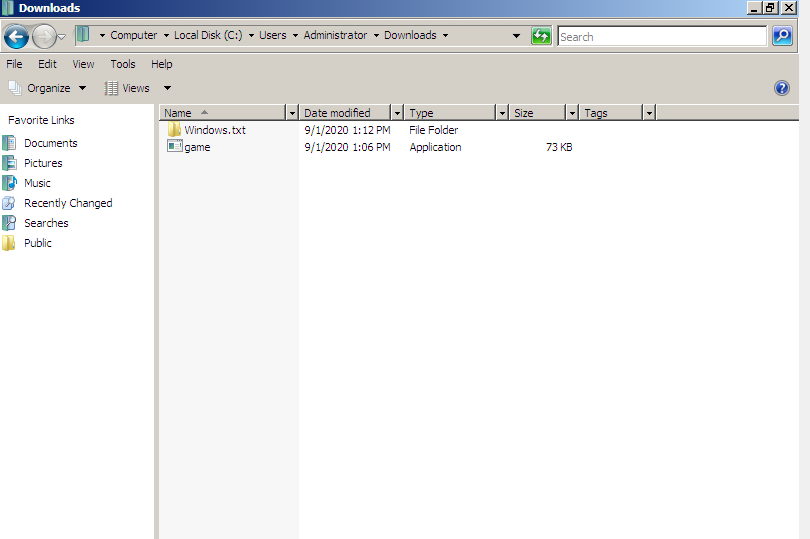


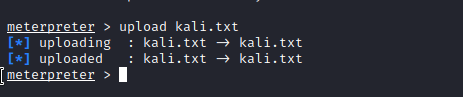
Checking Windows system information

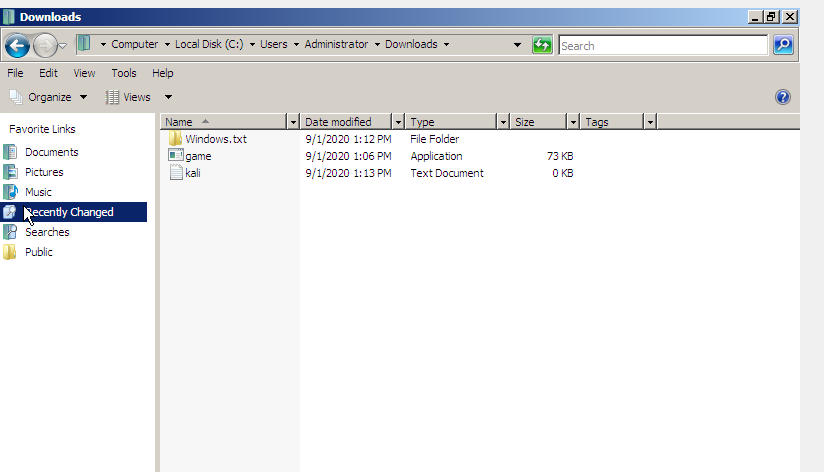


Exploit the victim's machine:

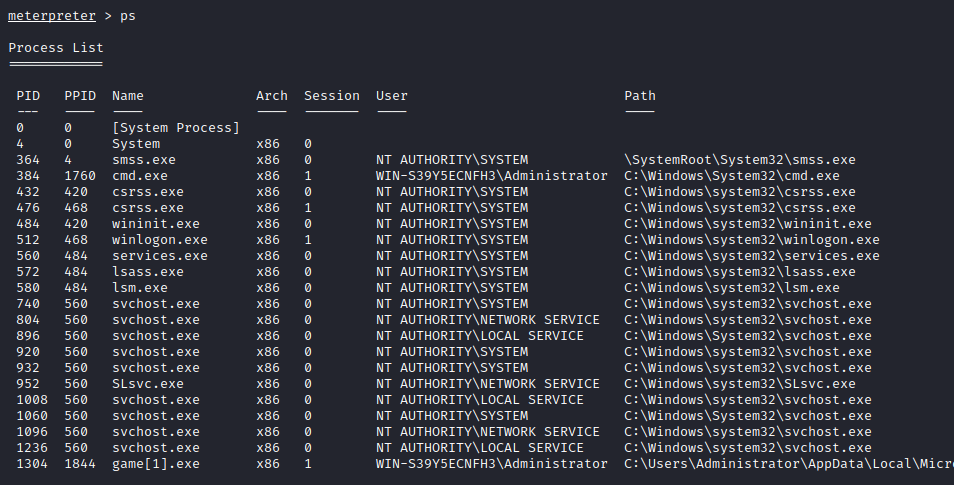
Uploading Files from Attacker Machine (Kali) to Victim (Windows) Machine.







Checking Windows Process.



Question 2:Create an FTP server.

Installing FTP server in Windows Server.

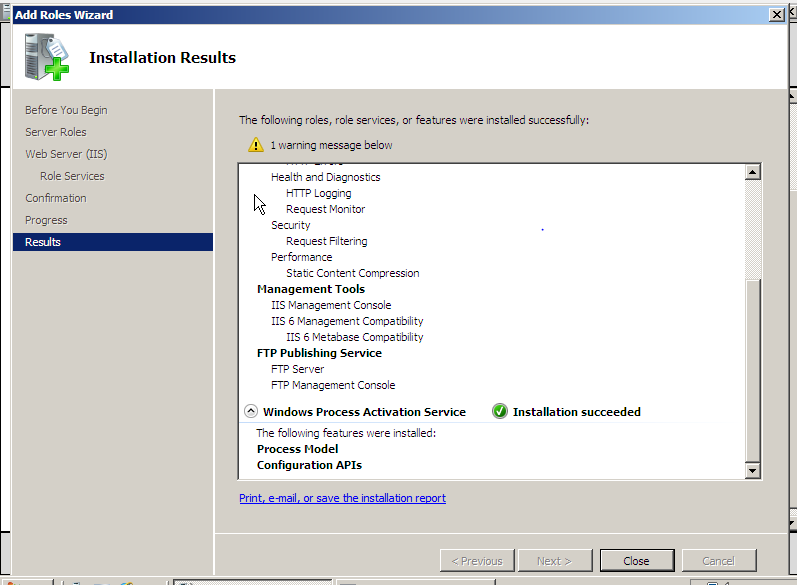
FTP server IP Address: 192.168.52.4

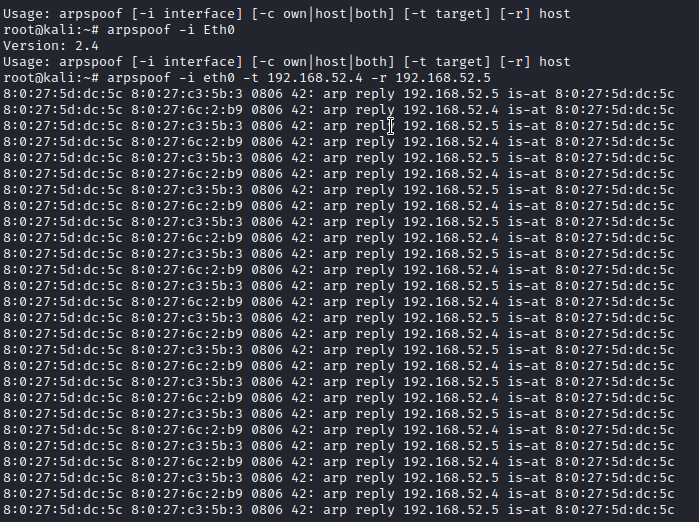
User Name: Administrator

Password: Server2008

Client IP address: 192.168.52.5

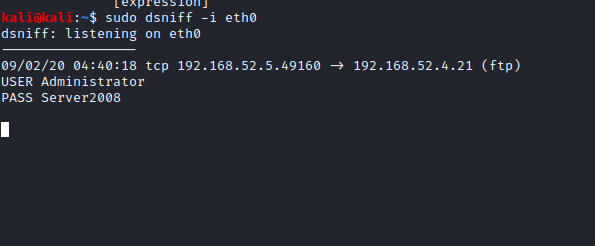
Attacker IP Address: 192.168.52.3



MITM attack using DSNIFF TOOL :Performing APRSPOOFING.

Accessing FTP server (192.168.52.4) from Windows (192.168.52.5) Command prompt:



Doing MITM attack using DSNIFF tool.Capturing FTP server user name and password.

Doing MITM attack using WireShark tool.Capturing FTP server user name and password.