

Configurazione IP Kali 192.168.1.25 e Meta 192.168.1.40

Accertarsi che la porta relativa al servizio Telnet, la 23, sia aperta.

```

$ nmap 192.168.1.40
Starting Nmap 7.94 ( https://nmap.org ) at 2023-06-13 08:45 EDT
Nmap scan report for 192.168.1.40
Host is up (0.00062s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown

Nmap done: 1 IP address (1 host up) scanned in 13.15 seconds

```

Avviare msfconsole, con relativo comando

```

(kali@kali)-[~]
$ msfconsole

WARNING: An internal exception occurred. This may be caused by a
WARNING: missing or broken dependency. Please report this to the
WARNING: Metasploit project.

Metasploit

[*] Metasploit v6.3.19-dev (2023-06-13)
[*] Using configured language: English
[*] Using configured framework: Metasploit
[*] Using configured payload: x64/windows/exec

[*] Metasploit v6.3.19-dev (2023-06-13)
+ -- --=[ 2318 exploits - 1215 auxiliary - 412 post ]
+ -- --=[ 1234 payloads - 46 encoders - 11 nops ]
+ -- --=[ 9 evasion ]

Metasploit tip: Use the analyze command to suggest
runnable modules for hosts
Metasploit Documentation: https://docs.metasploit.com/

msf6 >

```

Già sappiamo che andremo ad usare il modulo **auxiliary/scanner/telnet/telnet_version** ma possiamo fare una ricerca, ad esempio cerchiamo telnet version, per vedere tutti i risultati relativi. Useremo il

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

Andiamo a vedere le opzioni, e controlliamo quali settaggi sono necessari per l'esecuzione

```
msf6 auxiliary(scanner/telnet/telnet_version) > show 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/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	The username to authenticate as

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

Vediamo che è necessario settare l'RHOSTS con l'Ip della macchina target, dopo controlliamo di

```
msf6 auxiliary(scanner/telnet/telnet_version) > set RHOSTS 192.168.1.40
RHOSTS => 192.168.1.40
msf6 auxiliary(scanner/telnet/telnet_version) > show options

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

Name	Current Setting	Required	Description
PASSWORD		no	The password for the specified username
RHOSTS	192.168.1.40	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	The username to authenticate as

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

Per questo modulo non sono previsti payload, quindi procediamo a lanciare l'attacco, possiamo vedere che il modulo ha recuperato le credenziali msfamdin/msfadmin per effettuare l'accesso a Meta

[illegible]

Possiamo provare ad accedere usando quelle credenziali, e poi possiamo fare dei test per vedere se la macchina target risponde

```
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 '^]'.

metasploitable2

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 Jun 13 03:42:48 EDT 2023 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:~$ id
uid=1000(msfadmin) gid=1000(msfadmin) groups=4(adm),20(dialout),24(cdrom),25(floppy),29(audio),30(d
ip),44(video),46(plugdev),107(fuse),111(lpadmin),112(admin),119(sambashare),1000(msfadmin)
msfadmin@metasploitable:~$
```