

Telnet

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

```
msf6 > search telnet_version
```

Matching Modules

#	Name	Disclosure Date	Rank	Check	Description
0	auxiliary/scanner/telnet/lantronix_telnet_version		normal	No	Lantronix Telnet Service Banner Detection
1	auxiliary/scanner/telnet/telnet_version		normal	No	Telnet Service Banner Detection

Dopo l'avvio di **mfconsole**, faccio **search talent_version** per la ricerca di **auxiliary/scanner/telnet/telnet_version**

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

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

In questa fase faccio l'utilizzo del **auxiliary/scanner/telnet/telnet_version**

```
msf6 auxiliary(scanner/telnet/telnet_version) > set rhosts 192.168.161.81
rhosts => 192.168.161.81
msf6 auxiliary(scanner/telnet/telnet_version) > show options

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

  Name      Current Setting  Required  Description
  ----      -
  PASSWORD  192.168.161.81  no        The password for the specified username
  RHOSTS    192.168.161.81  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  192.168.161.81  no        The username to authenticate as

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

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

Configurazione dell'indirizzo IP target (**RHOSTS**) con quello della macchina Metasploitable.

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

[*] 192.168.161.81:23 - 192.168.161.81:23 TELNET
[*] 192.168.161.81:23 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed

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

Lancio del modulo con **exploit** per effettuare la scansione. Il risultato è: trova le credenziale per effettuare il login

```
└─$ telnet 192.168.161.81
Trying 192.168.161.81 ... telnet/lantronix_telnet_version
Connected to 192.168.161.81. telnet/lantronix_telnet_version
Escape character is '^]'.

Interact with a module by name or index. For example:
msf5 > use auxiliary/scanner/telnet/telnet_version
msf5 auxiliary/scanner/telnet/telnet_version >

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

Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com      The password for the specified user
RHOSTS                                yes      The target host(s), see https://docs
Login with msfadmin/msfadmin to get started target port (TCP)
THREADS                                yes      The number of concurrent threads
TIMEOUT                                yes      Timeout for the Telnet probe
metasploitable login: msfadmin         The username to authenticate as
```

In questa fase, con il comando **telnet ip**, per avviare nel terminale di kali meta, e di conseguenza effettuare il login.

```
msfadmin@metasploitable:~$ whoami 192.168.161.81:23 TELNET
msfadmin
msfadmin@metasploitable:~$ mkdir nuovo Warning: Never expose this VM to an untrusted network!
msfadmin@metasploitable:~$ ls scanned 1 of 1 hosts (100% complete)
nuovo vulnerable ls execution completed
msfadmin@metasploitable:~$
```

Dopo il login effettuato, ho provato a fare solo delle prove, come creare una directory.

```
RX packets:91 errors:0
TX packets:91 errors:0
collisions:0 txqueuelen:1000
RX bytes:19301 (18.8 KiB)

msfadmin@metasploitable:~$
msfadmin@metasploitable:~$ ls
nuovo vulnerable
msfadmin@metasploitable:~$
```

Infatti appare pure nella macchina di meta.