

```
msf6 exploit(multi/http/tomcat_mgr_upload) > 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

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

```
msf6 exploit(multi/http/tomcat_mgr_upload) > 
```

Per prima cosa , come suggerito dalla traccia ho utilizzato il comando **"search telnet version"** per cercare il modulo interessato.

Successivamente vado a scrivere **“Use 1”** per utilizzare il modulo richiesto dalla traccia.

Dopo aver fatto ciò posso utilizzare “options” per verificare cosa richiede il modulo per essere eseguito

```
msf6 exploit(multi/http/tomcat_mgr_upload) > use 1
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 <a href="https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html</a> |
| 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) > 
```

**RHOSTS** risulta in stato Required quindi andremo a valorizzarla con l'ip della macchina destinataria tramite il comando **"set rhosts ..."**

```
msf6 auxiliary(scanner/telnet/telnet_version) > set rhosts 192.168.50.151
rhosts => 192.168.50.151
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   | 192.168.50.151  | yes      | The target host(s), see <a href="https://docs.metasploit.com/docs/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit.html</a> |
| 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) >
```

Eseguo l'auxiliary e confermo una connessione alla macchina tramite telnet.

```

msf5 auxiliary (msf5auxiliary) > run

[*] 192.168.58.151:23 - 192.168.58.151:23 TELNET
[*] 192.168.58.151:23 - 192.168.58.151:23 TELNET
[*] Compiling host headers for msf5auxiliary/stealable login
[*] 192.168.58.151:23 Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary (msf5auxiliary) > telnet 192.168.58.151
[*] exec telnet 192.168.58.151

Trying 192.168.58.151...
Connected to 192.168.58.151.
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 Sep 24 03:13:57 EDT 2024 on tty1
msf5 metasploitable 2-24-25 server # 390 Tue Aug 18 21:54:00 UTC 2008 1666

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/
or mail:
msf5 metasploitable2 >

```