

Exploit telnet

```

Interact with a module by name or index. For example info 42, use 42 or use post/windows/gather/credentials/mremote

msf6 > use auxiliary/scanner/telnet/telnet_version
msf6 auxiliary(scanner/telnet/telnet_version) > show 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 192.168.1.149
RHOSTS => 192.168.1.149
msf6 auxiliary(scanner/telnet/telnet_version) > show options

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

  Name      Current Setting  Required  Description
  --      -
PASSWORD   no               no        The password for the specified username
RHOSTS     192.168.1.149   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) > exploit

[*] 192.168.1.149:23 - 192.168.1.149:23 TELNET
[*] 192.168.1.149:23 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/telnet_version) >

```

```
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/telnet_version) > telnet 192.168.1.149
[*] exec: telnet 192.168.1.149

Trying 192.168.1.149 ...
Connected to 192.168.1.149.
Escape character is '^]'.

      _   _          _ 
     | |_| |        | |
    / ___ \|       / ___\
   / /___| \      / /___| \
  / ____ \|      / ____ \|
 / /    |  \    / /    |  \
/_/____|_\/    /_/____|_\/

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: Mon Sep 18 12:46:10 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:~$ █
```

- Come visto per il servizio vsftpd, dopo aver eseguito la scansione con nmap ed aver individuato il servizio telnet attivo sulla macchina metasploitable, ho cercato un exploit su msfconsole, e in questo caso non ho trovato un exploit, ma un modulo ausiliario che mi consente di fare banner grabbing e come in questo caso individuare le credenziali di login
- In seguito ho eseguito l'accesso tramite il comando telnet IP a cui poi è seguito l'inserimento delle credenziali trovate precedentemente