

Dopo aver cambiato gli ip delle macchine le testo

```
(kali㉿kali)-[~]
$ ping 192.168.1.40
PING 192.168.1.40 (192.168.1.40) 56(84) bytes of data.
64 bytes from 192.168.1.40: icmp_seq=1 ttl=64 time=1.27 ms
64 bytes from 192.168.1.40: icmp_seq=2 ttl=64 time=1.02 ms
64 bytes from 192.168.1.40: icmp_seq=3 ttl=64 time=0.550 ms
^C
— 192.168.1.40 ping statistics —
3 packets transmitted, 3 received, 0% packet loss, time 2163ms
rtt min/avg/max/mdev = 0.550/0.946/1.269/0.298 ms

(kali㉿kali)-[~]
$
```

Cerco l'exploit descritto nella teoria

```
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
```

Imposto l'host della macchina target

```
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 <a href="https://docs.metasploit.com/docs/using-the-framework/000-what-is-the-metasploit-framework.html">https://docs.metasploit.com/docs/using-the-framework/000-what-is-the-metasploit-framework.html</a> |
| RPORT    | 23              | yes      | The target port (TCP)                                                                                                                                                                                                               |
| THREADS  | 1               | yes      | The number of concurrent threads (max one times the number of processors)                                                                                                                                                           |
| 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) >
```

In seguito notiamo che possiamo prendere le credenziali di msfadmin

[illegible]