

## Hacking con metasploit

- Avvio di msf console
- Search telnet\_version
- Use 1
- Set RHOSTS
- Set RPOTR
- run

```
# Name Disclosure Date Rank Check Description
-----
0 auxiliary/scanner/telnet/lantronix_telnet_version . normal No Lantronix Telnet
1 auxiliary/scanner/telnet/telnet_version . normal No Telnet Service
```

Warning: Never expose this VM to an untrusted network!

Interact with a module by name or index. For example `info 1`, `use 1` or `use auxiliary/scanner/telnet/telnet_version`

```
msf6 auxiliary(scanner/telnet/lantronix_telnet_version)> use 1
msf6 auxiliary(scanner/telnet/telnet_version)> options
```

Module options (auxiliary/scanner/telnet/telnet\_version):

- phpMyAdmin

Name	Current Setting	Required	Description
PASSWORD	W	no	The password for the specified username
RHOSTS		yes	The target host(s), see https://docs.metasploit.com/docs/using-
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 192.168.50.152
RHOSTS => 192.168.50.152
msf6 auxiliary(scanner/telnet/telnet_version)> run
```

```
[+] 192.168.50.152:23 - 192.168.50.152:23 TELNET _ _ _ _ _
_/_`/_/'_\\/_\\_/_/_`'_\\/_\\_\\_)|x0a|||_|_/||(_\\_\\)|(|_|)
|x0a      ||          |x0a|x0a|x0aWarning: Never
in/msfadmin to get started|x0a|x0ametasploitable login:
```

```
[*] 192.168.50.152:23 - Scanned 1 of 1 hosts (100% complete)
```

[illegible]

- Cambio ip kali `sudo ip addr add 192.168.1.25/24 dev eth0`
- Cambio ip metasploit `sudo ifconfig eth0 192.168.1.40 netmask 255.255.255.0`

```

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) > run

[+] 192.168.1.40:23 - 192.168.1.40:23 TELNET
Warning: Never expose this VM to an untrusted network!
Contact: m
min/msfadmin to get started
[*] 192.168.1.40:23 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
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 '^J'.

Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

metasploitable login:

```