

# HACKING CON METASPLOIT

**Completare una sessione di hacking sulla macchina Metasploitable con il modulo auxiliary telnet\_version**

**Con il comando `sudo nano`  
`/etc/network/interfaces`, andiamo a  
configurare le macchine kali e  
metasploitable con gli indirizzi ip richiesti**

# HACKING CON METASPLOIT

```
(kali@kali)-[~]
└─$ msfconsole
Metasploit tip: Use the 'capture' plugin to start multiple authentication-capturing and poisoning services
```

# Avviamo metasploit con il comando **msfconsole**

# Cerchiamo gli exploit presenti per telnet

```
msf6 > search telnet
```

Matching Modules

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/linux/misc/asus_infosvr_auth_bypass_exec	2015-01-04	excellent	No	ASUS infosvr Auth Bypass Command E
1	exploit/linux/http/asuswrt_lan_rce	2018-01-22	excellent	No	AsusWRT LAN Unauthenticated Remote
2	auxiliary/server/capture/telnet		normal	No	Authentication Capture: Telnet
3	auxiliary/scanner/telnet/brocade_enable_login		normal	No	Brocade Enable Login Check Scanner
4	exploit/windows/proxy/ccproxy_telnet_ping	2004-11-11	average	Yes	CCProxy Telnet Proxy Ping Overflow
5	auxiliary/dos/cisco/ios_telnet_rocem	2017-03-17	normal	No	Cisco IOS Telnet Denial of Service
6	auxiliary/admin/http/dlink_dir_300_600_exec_noauth	2013-02-04	normal	No	D-Link DIR-600 / DIR-300 Unauthent
33	exploit/linux/http/tp_link_sc2020n_authenticated_telnet_injection	2015-12-20	excellent	No	TP-Link SC2020n Authenticated Tel
34	auxiliary/scanner/telnet/telnet_login		normal	No	Telnet Login Check Scanner
35	auxiliary/scanner/telnet/telnet_version		normal	No	Telnet Service Banner Detection
36	auxiliary/scanner/telnet/telnet_encrypt_overflow		normal	No	Telnet Service Encryption Key ID
37	payload/cmd/unix/bind_busybox_telnetd		normal	No	Unix Command Shell, Bind TCP (via
38	payload/cmd/unix/reverse		normal	No	Unix Command Shell, Double Revers
39	payload/cmd/unix/reverse_ssl_double_telnet		normal	No	Unix Command Shell, Double Revers
40	payload/cmd/unix/reverse_bash_telnet_ssl		normal	No	Unix Command Shell, Reverse TCP S
41	exploit/linux/ssh/vyos_restricted_shell_privesc	2018-11-05	great	Yes	VyOS restricted-shell Escape and
42	post/windows/gather/credentials/mremote		normal	No	Windows Gather mRemote Saved Pass

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

Con il comando **use** e il nome dell'exploit lo andiamo a selezionare

# HACKING CON METASPLOIT

Con il comando **show options** andiamo a vedere la configurazione del nostro attacco e con il comando **set**, effettuiamo le modifiche.

## RHOSTS: l'indirizzo IP della macchina target.

**RPORT:** la porta sulla macchina target dove il servizio è in ascolto

```
msf6 auxiliary(scanner/telnet/telnet_version) > set RHOSTS 192.168.1.40
RHOSTS => 192.168.1.40
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   | 192.168.1.40    | yes      | The target host(s), see <a href="https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html</a> |
| 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) > exploit

[+] 192.168.1.40:23 - 192.168.1.40:23 TELNET
Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started
metasploitable login:

[*] 192.168.1.40:23 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/telnet_version) >
```

**Effettuiamo l'attacco con `exploit` e notiamo che ci mostra le credenziali di accesso del servizio telnet**

# HACKING CON METASPLOIT

[illegible]

**Verifichiamo le credenziali  
riportate dall'attacco e  
riusciamo effettivamente ad  
accedere alla macchina  
metasploitable**