

METASPLOIT

Telnet Attack



Michelangelo **Borromeo**

hacking **METASPLOITABLE 2**

(impostazione Mtsp2)

iniziamo con la configurazione della metasploitable2 con ip: 192.168.1.40/24

loggiamo in metasploitable2 (user: msfadmin – password: msfadmin) e diamo il comando:

sudo nano /etc/network/interfaces

```
msfadmin@metasploitable:~$ sudo nano /etc/network/interfaces_
```

dopo di che si aprirà un file dove possiamo immettere l'indirizzo statico da noi scelto in questo caso:

IP: 192.168.1.40

Netmask: 255.255.255.0

Network: 192.168.1.255

Broadcast: 192.168.1.255

Gateway 192.168.1.1

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet static

address 192.168.1.40
netmask 255.255.255.0
network 192.168.1.0
broadcast 192.168.1.255
gateway 192.168.1.1
```

Facciamo un riavvio della scheda di rete su metasploitable 2:

sudo /etc/init.d/networking restart

```
msfadmin@metasploitable:~$ sudo /etc/init.d/networking restart
* Reconfiguring network interfaces... [ OK ]
msfadmin@metasploitable:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:1f:c3:22 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.40/24 brd 192.168.1.255 scope global eth0
    inet6 fe80::a00:27ff:fe1f:c322/64 scope link
        valid_lft forever preferred_lft forever
msfadmin@metasploitable:~$
```

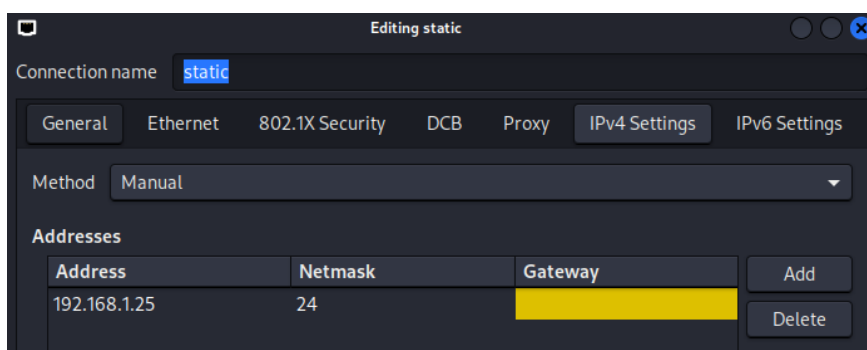
hacking **METASPLOITABLE 2**

(impostazione Kali)

Ricordiamoci di impostare la Kali all'interno della stessa rete della Metasploitable2
Altrimenti non pingano a vicenda.

Andiamo su scheda di rete ipv4 della kali e andiamo ad impostare ip:

192.168.1.25 /24



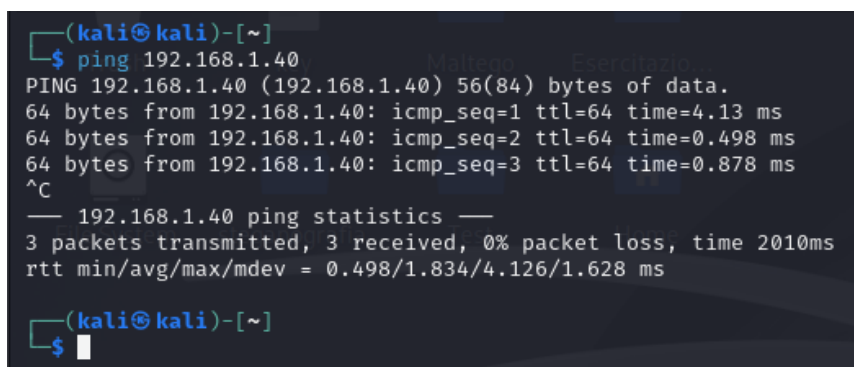
E clicchiamo su salva.

E restartiamo la scheda di rete:

```
sudo /etc/init.d/networking restart
```

Per verificare che si pingano, apriamo una linea di comando dalla kali ed immettiamo ip della metasploitable2

ping 192.168.1.40



hacking **METASPLOITABLE 2**

(Avvio Nmap, ricerca servizio telnet)

Per verificare le porte aperte su una rete, dalla kali, eseguiamo il comando:

`nmap 192.168.1.0/24`

```
(kali@kali)-[~]
$ nmap -p- 192.168.1.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-09 11:19 CEST
```

Da qui usciranno tutti gli indirizzi Ip della rete con le porte aperte e i loro servizi:

```
Nmap scan report for 192.168.1.26
Host is up (0.0020s latency).
Not shown: 65526 closed tcp ports (conn-refused)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
49152/tcp  open  unknown
49153/tcp  open  unknown
49154/tcp  open  unknown
49155/tcp  open  unknown
49156/tcp  open  unknown
49157/tcp  open  unknown

Nmap scan report for 192.168.1.40
Host is up (0.0074s latency).
Not shown: 65509 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
513/tcp   open  login
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
3632/tcp  open  distccd
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
6697/tcp  open  ircs-u
8787/tcp  open  msgsrvr
44851/tcp open  unknown
45101/tcp open  unknown
48891/tcp open  unknown
59672/tcp open  unknown

Nmap done: 256 IP addresses (3 hosts up) scanned in 47.14 seconds
```

hacking **METASPLOITABLE 2**

(Avvio Nmap, ricerca servizio ftp)

Ciò che interessa a noi è l'indirizzo ip della Metasploitable2:

192.168.1.40

```
Nmap scan report for 192.168.1.40
Host is up (0.0074s latency).
Not shown: 65509 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
513/tcp   open  login
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
3632/tcp  open  distccd
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
6697/tcp  open  ircs-u
8787/tcp  open  msgsrvr
44851/tcp open  unknown
45101/tcp open  unknown
48891/tcp open  unknown
59672/tcp open  unknown

Nmap done: 256 IP addresses (3 hosts up) scanned in 47.14 seconds
```

Andiamo a ricercare la porta Telnet che vogliamo andare ad hackerare

```
23/tcp    open  telnet
```

Ora abbiamo la porta e la tipologia di collegamento

23/tcp telnet

hacking **METASPLOITABLE 2**

(Avvio Metasploit, ricerca Exploit Telnet)

Avviamo Metasploit con il seguente comando:
msfconsole

```
(kali@kali)-[~]
└─$ msfconsole
Metasploit tip: You can upgrade a shell to a Meterpreter session on many
platforms using sessions -u <session_id>

3Kom SuperHack II Logon

User Name: [ security ]
Password: [ ]

[ OK ]

https://metasploit.com

+ -- ==[ metasploit v6.3.55-dev ]
+ -- ==[ 2397 exploits - 1235 auxiliary - 422 post ]
+ -- ==[ 1391 payloads - 46 encoders - 11 nops ]
+ -- ==[ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/
```

Dopo di che possiamo fare una piccola ricerca riguardo il servizio che vorremo hackerare:

search telnet

```
search telnetmsf6 > 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 Execution
1 exploit/linux/http/asuswrt_lan_rce 2018-01-22 excellent No AsusWRT LAN Unauthenticated Remote Code Execution
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 average Yes CCProxy telnet Proxy Ping Overflow
5 auxiliary/dos/cisco_ios_telnet_rccom 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 Unauthenticated Remote Comma
nd Execution
7 exploit/linux/http/dlink_diagnostic_exec_noauth 2013-03-05 excellent No D-Link DIR-645 / DIR-815 diagnostic.php Command Executi
on
8 exploit/linux/http/dlink_dir300_exec_telnet 2013-04-22 excellent No D-Link Devices Unauthenticated Remote Command Executi
on
9 exploit/unix/webapp/dogfood_spell_exec 2009-03-03 excellent Yes Dogfood CRM spell.php Remote Command Execution
10 exploit/freebsd/telnet/telnet_encrypt_keyid 2011-12-23 great No FreeBSD telnet Service Encryption Key ID Buffer Overf
low
11 exploit/windows/telnet/gamsoft_telnet_username 2000-07-17 average Yes GAMSoft TelSrv 1.5 Username Buffer Overflow
12 exploit/windows/telnet/goodtech_telnet 2005-03-15 average No GoodTech telnet Server Buffer Overflow
13 exploit/linux/misc/hp_jetdirect_path_traversal 2017-04-05 normal No HP Jetdirect Path Traversal Arbitrary Code Execution
14 exploit/linux/http/huawei_hg532n_cmdinject 2017-04-15 excellent Yes Huawei HG532n Command Injection
15 exploit/linux/misc/igel_command_injection 2021-02-25 excellent Yes Igel OS Secure VNC/Terminal Command Injection RCE
16 auxiliary/scanner/ssh/juniper_backdoor 2015-12-20 normal No Juniper SSH Backdoor Scanner
17 auxiliary/scanner/telnet/lantronix_telnet_password normal No Lantronix telnet Password Recovery
18 auxiliary/scanner/telnet/lantronix_telnet_version normal No Lantronix telnet Service Banner Detection
19 exploit/linux/telnet/telnet_encrypt_keyid 2011-12-23 great No Linux BSD-derived telnet Service Encryption Key ID Bu
ffer Overflow
20 auxiliary/dos/windows/ftp/iis75_ftpd_iac_bof 2010-12-21 normal No Microsoft IIS FTP Server Encoded Response Overflow Tr
igger
21 exploit/linux/telnet/netgear_telnetenable 2009-10-30 excellent Yes NETGEAR telnetenable
22 auxiliary/admin/http/netgear_pnpx_getsharefolderlist_auth_bypass 2021-09-06 normal Yes Netgear PNXP_GetShareFolderList Authentication Bypass
23 auxiliary/admin/http/netgear_r7000_pass_reset 2020-06-15 normal Yes Netgear R6700v3 Unauthenticated LAN Admin Password Re
set
24 auxiliary/admin/http/netgear_r7000_backup.cgi_heap_overflow_rce 2021-04-21 normal Yes Netgear R7000 backup.cgi Heap Overflow RCE
25 exploit/unix/misc/polycom_hdx_auth_bypass 2013-01-18 normal Yes Polycom Command Shell Authorization Bypass
26 exploit/unix/misc/polycom_hdx_traceroute_exec 2017-11-12 excellent Yes Polycom Shell HDX Series Traceroute Command Execution
27 exploit/freebsd/ftp/proftpd_telnet_iac 2010-11-01 great Yes ProFTPD 1.3.2rc3 - 1.3.3b telnet IAC Buffer Overflow
(FreeBSD)
28 exploit/linux/ftp/proftpd_telnet_iac 2010-11-01 great Yes ProFTPD 1.3.2rc3 - 1.3.3b telnet IAC Buffer Overflow
(Linux)
29 auxiliary/scanner/telnet/telnet_ruggedcom normal No RuggedCom telnet Password Generator
30 auxiliary/scanner/telnet/telnet_satel_cmd_exec normal No Satel Iberia SenNet Data Logger and Electricity Meter
Command Injection Vulnerability
```

hacking **METASPLOITABLE 2**

(hacking telnet)

```
35 auxiliary/scanner/telnet/telnet_version
```

Abbiamo trovato qualche modulo, ma quello che interessa a noi è

telnet auxiliary/scanner/telnet/telnet_version

Per andarlo ad utilizzare inseriamo:

use 35

```
msf6 > use 35
msf6 auxiliary(scanner/telnet/telnet_version) > █
```

Ricordiamoci di dare:

Show options

Per controllare ciò che ci richiede

```
msf6 auxiliary(scanner/telnet/telnet_version) > show options
```

```
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/docs/using-metasploit/basics/using-metasploit.html
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) > █
```

Ci richiede RHOST, il target, che lo andiamo ad impostare con:

set rhost 192.168.1.40

```
msf6 auxiliary(scanner/telnet/telnet_version) > set rhost 192.168.1.40
rhost => 192.168.1.40
msf6 auxiliary(scanner/telnet/telnet_version) > █
```

hacking **METASPLOITABLE 2**

(Run / exploit)

L'exploit in particolare non richiede un payload, di conseguenza possiamo andarlo ad eseguire direttamente con:

run o exploit

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

Attendiamo qualche secondo e ci apparirà questa seguente schermata, un accesso diretto verso il server da noi scelto come target, utilizzando la porta:

23/tcp telnet

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

Leggendo attentamente ci darà username e password che andremo ad inserire durante il log remoto, per verificare ciò, possiamo procedere con la connessione.

```
.com\x0a\x0aLogin with msfadmin/msfadmin to get star
```

Username: msfadmin

Password: msfadmin

hacking **METASPLOITABLE 2**

(verifica connessione con credenziali ottenute)

Possiamo procedere con la connessione alla porta 23/tcp telnet inserendo:

```
telnet 192.168.1.40
```

apparirà il menù del server alla quale stiamo accedendo (Metasploitable2)

```
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](mailto:msfdev[at]metasploit.com)

Login with msfadmin/msfadmin to get started

metasploitable login: █

Ora inseriamo le credenziali che abbiamo recuperato in precedenza

User: msfadmin

Pass: msfadmin

E diamo invio.

```
metasploitable login: msfadmin
Password:
Last login: Tue Jul 9 03:12:28 EDT 2024 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:~$
```

Dunque siamo riusciti ad accedere ad un server recuperando le credenziali da una porta aperta (23/tcp telnet) sfruttando l' `Exploit auxiliary/scanner/telnet/telnet_version`.

hacking **METASPLOITABLE 2**

(test)

verifichiamo la connessione avvenuta spulciando e muovendoci all'interno della Metasploitable2:

ifconfig

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:1f:c3:22
          inet addr:192.168.1.40  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe1f:c322/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:66877  errors:0  dropped:0  overruns:0  frame:0
          TX packets:65848  errors:0  dropped:0  overruns:0  carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:5212090 (4.9 MB)  TX bytes:3575397 (3.4 MB)
          Base address:0xd020  Memory:f0200000-f0220000
```

Whoami

```
msfadmin@metasploitable:~$ whoami
msfadmin
```

Id

```
msfadmin@metasploitable:~$ id
uid=1000(msfadmin) gid=1000(msfadmin)
```

Ls

```
msfadmin@metasploitable:~$ ls
test_metasploit  vulnerable
```