

ESERCIZIO L7 S2 – Metasploit

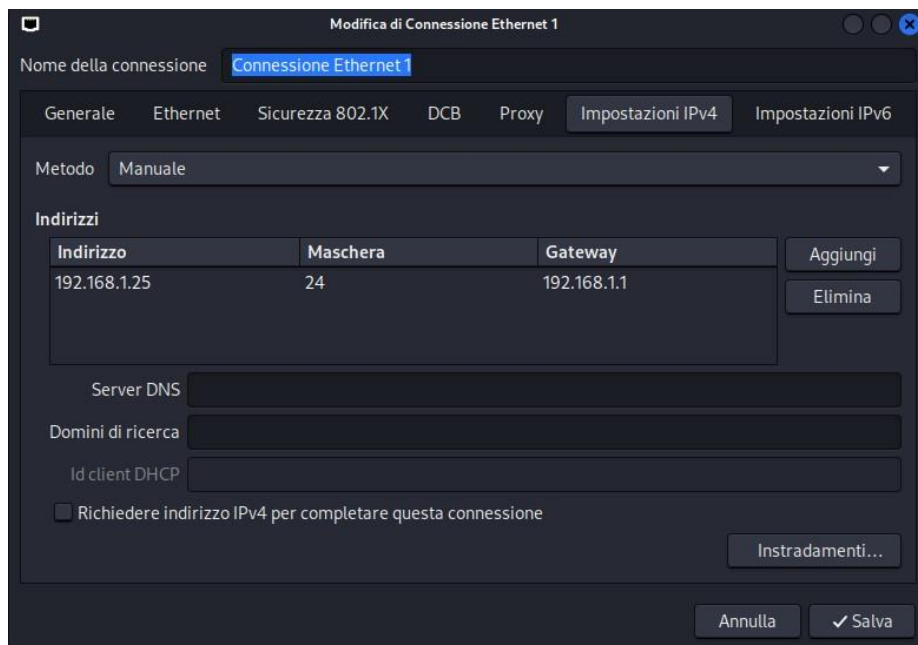
L'obiettivo di questa esercitazione è sfruttare la vulnerabilità Telnet utilizzando il modulo **auxiliary telnet_version** di Metasploit per accedere al servizio Telnet attivo sulla macchina Metasploitable.

1. Configurazione dell'ambiente

Prima di avviare l'esercitazione, ho proceduto con la configurazione della rete:

- **Kali Linux** con indirizzo IP **192.168.1.25**
- **Metasploitable** con indirizzo IP **192.168.1.40**

Kali



Metasploitable

Comandi:

- Configurazione IP e netmask: **sudo ifconfig eth0 192.168.1.40 netmask 255.255.255.0**
- Gateway: **sudo route add default gw 192.168.1.1 eth0**

Verifica che le machine sia sulla stessa subnet

```
(kali㉿kali)-[~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:48:65:cd brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.25/24 brd 192.168.1.255 scope global noprefixroute eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::6ef4:4dc9:eec9:ff8f/64 scope link noprefixroute
        valid_lft forever preferred_lft forever

(kali㉿kali)-[~]
$ sudo arp-scan -l
[sudo] password di kali:
Interface: eth0, type: EN10MB, MAC: 08:00:27:48:65:cd, IPv4: 192.168.1.25
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.1.40      08:00:27:4a:b7:b1      (Unknown)

1 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 2.016 seconds (126.98 hosts/sec). 1 responded
```

2. Avvio msfconsole

[illegible]

Con il comando **search** cerco la vulnerabilità della traccia e con il comando **use** seleziono il numero della vulnerabilità. In questo caso nr. 0

```
msf6 > search auxiliary telnet_version

Matching Modules



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



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) > 
```

Accedendo alle informazioni dell' exploit per vedere di quali opzioni a bisogno per essere eseguito tramite il comando **show options**, quindi aggiungo con il comando **set rhosts 192.168.1.40** l' indirizzo IP della macchina target.

3. Ho avviato l'exploit con il comando **run**

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

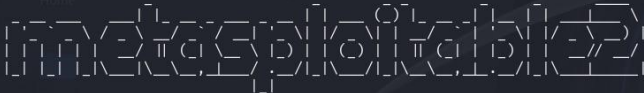
```
[+] 192.168.1.40:23 - 192.168.1.40:23 TELNET
|_ _ _ ( ) | _ _ _ | | _ _ _ | \x0a| ' ' _ / _ \ _ / _ ' / _ | ' \ | / _ \ | | _ / _ ' | '
\ | _ ) | | ( _ ) | | | | ( | | | ) | | _ // _ / \x0a| | | | | \ _ \ _ \ _ \ _ \ _ \ _ \ _ \ _ \
|_| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
Warning: Never expose this VM to an
tasploit.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
```

Questo mi ha permesso di conoscere l'username **msfadmin** e la password **msfadmin** (cerchiate in rosso)

4. Tramite il comando **telnet 192.168.1.40** ho iniziato il collegamento alla metasploit. A collegamento avviato mi ha permesso di inserire le credenziali trovate per accedere da remoto come root.

```
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 '^['.
```



```

Metasploit Framework version 6.0.0-dev
Copyright (c) 2005-2024 Rapid7 Inc. All rights reserved.
[+] http://www.metasploit.com/

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 17 08:21:43 EST 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:~$
```