

# ESERCITAZIONE W16D1(1)



**Esercizio**  
Traccia

## Traccia:

Sulla base dell'esercizio visto in lezione teorica, utilizzare Kali per sfruttare la vulnerabilità relativa a Telnet con il modulo auxiliary telnet\_version sulla macchina Metasploitable.

**Requisito:** Seguire gli step visti in lezione teorica. Prima, configurate l'IP della vostra Kali con 192.168.1.25 e l'IP della vostra Metasploitable con 192.168.1.40

- 1) Configuro gli IP delle macchine come mostra la traccia:

```
kali@kali: ~  
File Actions Edit View Help  
  
(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:feeb:7ef5 prefixlen 64 scopeid 0<link>  
    ether 08:00:27:cb:7e:f5 txqueuelen 1000 (Ethernet)  
    RX packets 64 bytes 6048 (5.9 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 32 bytes 5525 (5.3 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
    inet 127.0.0.1 netmask 255.0.0.0  
    inet6 ::1 prefixlen 128 scopeid 0<host>  
    loop txqueuelen 1000 (Local Loopback)  
    RX packets 4 bytes 240 (240.0 B)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 4 bytes 240 (240.0 B)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
(kali@kali)-[~]  
$  
  
metasploitable [In esecuzione] - Oracle VM VirtualBox  
File Macchina Visualizza Inserimento Dispositivi Aiuto  
msfadmin@metasploitable:~$ ifconfig  
eth0: Link encap:Ethernet HWaddr 08:00:27:96:7a:21  
    inet addr:192.168.1.40 Bcast:192.168.1.255 Mask:255.255.255.0  
    inet6 addr: fe80::a00:27ff:fe96:7a21/64 Scope:Link  
    UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1  
    RX packets:10 errors:0 dropped:0 overruns:0 frame:0  
    TX packets:68 errors:0 dropped:0 overruns:0 carrier:0  
    collisions:0 txqueuelen:1000  
    RX bytes:944 (944.0 B) TX bytes:5368 (5.2 KB)  
    Base address:0xd020 Memory:f0200000-f0220000  
  
lo: Link encap:Local Loopback  
    inet addr:127.0.0.1 Mask:255.0.0.0  
    inet6 addr: ::1/128 Scope:Host  
    UP LOOPBACK RUNNING MTU:16436 Metric:1  
    RX packets:113 errors:0 dropped:0 overruns:0 frame:0  
    TX packets:113 errors:0 dropped:0 overruns:0 carrier:0  
    collisions:0 txqueuelen:0  
    RX bytes:24749 (24.1 KB) TX bytes:24749 (24.1 KB)  
  
msfadmin@metasploitable:~$
```

- 2) Avvio msfconsole, e cerco il modulo auxiliary scanner/telnet/telnet\_version.

```
kali@kali: ~  
File Actions Edit View Help  
msf6 > search auxiliary scanner telnet  
  
Matching Modules  
  
# Name                                     Disclosure Date  
Rank Check Description  
- - - - -  
0 auxiliary/scanner/telnet/brocade_enable_login 2015-12-20  
normal No Brocade Enable Login Check Scanner  
1 auxiliary/scanner/ssh/juniper_backdoor  
normal No Juniper SSH Backdoor Scanner  
2 auxiliary/scanner/telnet/lantronix_telnet_password  
normal No Lantronix Telnet Password Recovery  
3 auxiliary/scanner/telnet/lantronix_telnet_version  
normal No Lantronix Telnet Service Banner Detection  
4 auxiliary/admin/http/netgear_pnp_getsharefolderlist_auth_bypass 2021-09-06  
normal Yes Netgear PNPX_GetShareFolderList Authentication Bypass  
5 auxiliary/scanner/telnet/telnet_ruggedcom  
normal No RuggedCom Telnet Password Generator  
6 auxiliary/scanner/telnet/satel_cmd_exec 2017-04-07  
normal No Satel Iberia SenNet Data Logger and Electricity Meters Command Injecti  
on Vulnerability  
7 auxiliary/scanner/telnet/telnet_login  
normal No Telnet Login Check Scanner  
8 auxiliary/scanner/telnet/telnet_version  
normal No Telnet Service Banner Detection  
9 auxiliary/scanner/telnet/telnet_encrypt_overflow  
normal No Telnet Service Encryption Key ID Overflow Detection  
  
Interact with a module by name or index. For example info 9, use 9 or use auxiliary/sca  
nner/telnet/telnet_encrypt_overflow  
  
msf6 > use 8  
msf6 auxiliary(scanner/telnet/telnet_version) > 
```

- 3) Configuro i parametri che mi chiede, in questo caso l'IP:

```

kali@kali: ~
File Actions Edit View Help

Name      Current Setting  Required  Description
PASSWORD
RHOSTS    yes             The password for the specified username
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) > show options

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

Name      Current Setting  Required  Description
PASSWORD
RHOSTS    192.168.1.40    yes       The password for the specified username
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.

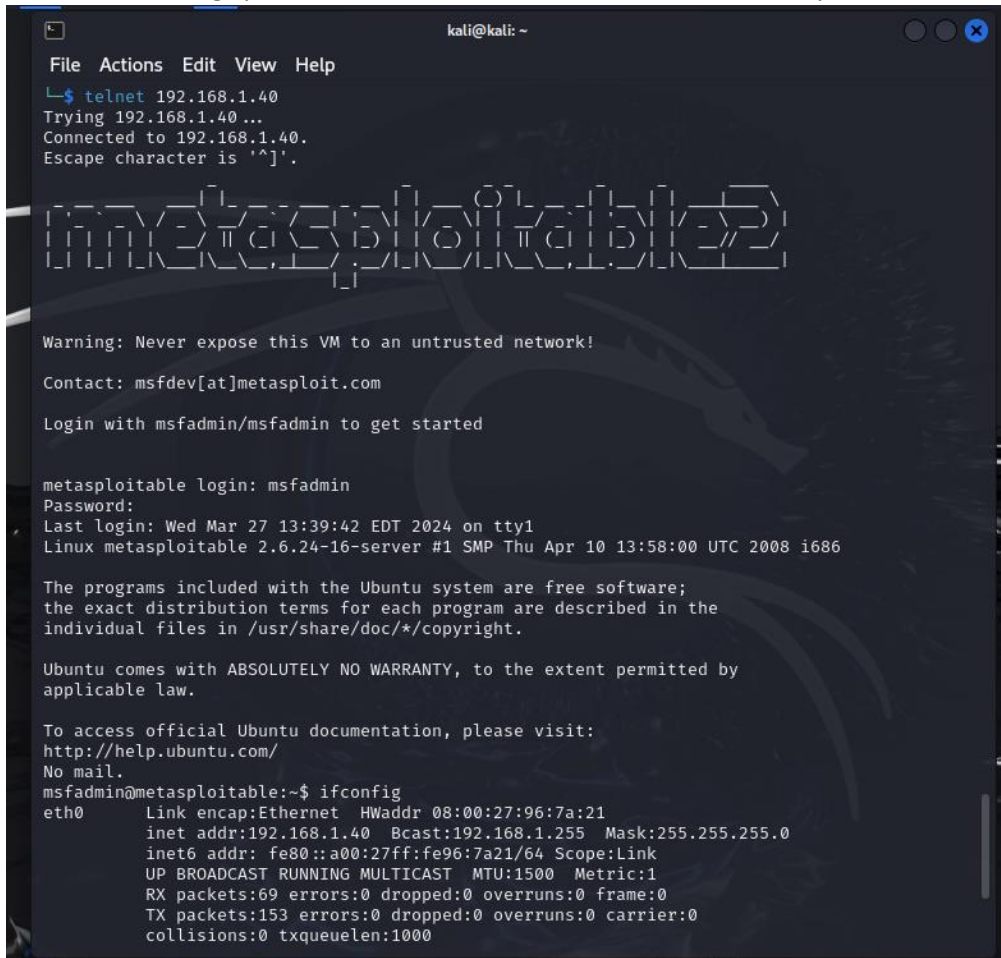
msf6 auxiliary(scanner/telnet/telnet_version) >

```

- 4) Avvio l'attacco e recupero login e password per accedere alla macchina dal servizio Telnet

[illegible]

- 5) Infine avvio il servizio telnet, inserisco le credenziali ottenute precedentemente ed eseguo il comando “ifconfig” per verificare se sono dentro la macchina Metasploitable



```
kali@kali: ~  
File Actions Edit View Help  
$ telnet 192.168.1.40  
Trying 192.168.1.40 ...  
Connected to 192.168.1.40.  
Escape character is '^J'.  
  
Metasploitable  
  
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: Wed Mar 27 13:39:42 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:~$ ifconfig  
eth0      Link encap:Ethernet  HWaddr 08:00:27:96:7a:21  
          inet addr:192.168.1.40  Bcast:192.168.1.255  Mask:255.255.255.0  
          inet6 addr: fe80::a00:27ff:fe96:7a21/64 Scope:Link  
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
          RX packets:69 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:153 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:1000
```

Come si può vedere dall'immagine sopra l'IP corrisponde alla macchina Metasploitable.