

Adrian.Amarfii 06/12/2022

Report

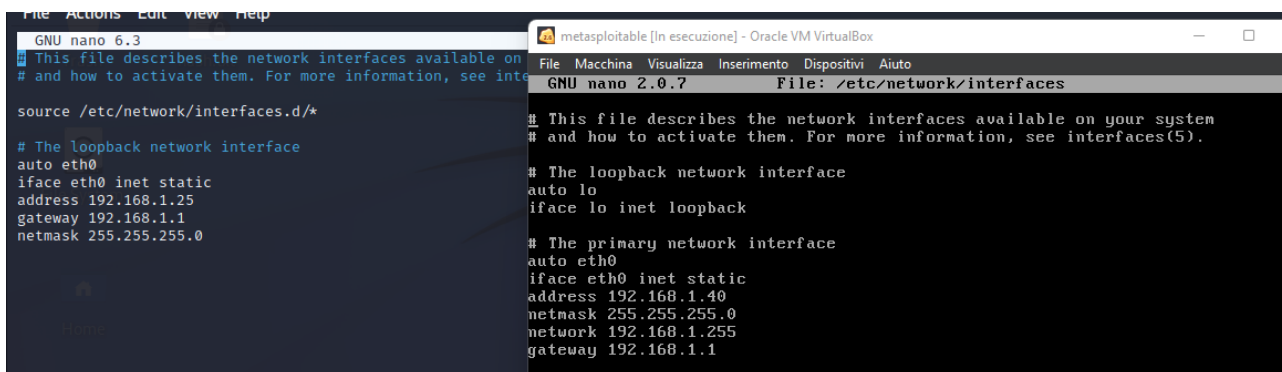
Task

Traccia:

Sulla base dell'esercizio visto in lezione teorica, utilizzare Metasploit 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

Nel esercizio di oggi ci viene chiesto di fare una prova con Metasploit, in particolare prendendo come esempio la prova fatta oggi nella parte di teoria ci viene detto di usare EXPLOIT TELNET CON AUXILIARY. Partiamo subito a cambiare l'IP sia a Kali che a Metasploitable. Comando `sudo nano /etc/network/interfaces` su entrambe le macchine e modifichiamo con i IP richiesti Kali=192.168.1.25 META=192.168.1.40.



```
File Actions Edit view Help
GNU nano 6.3
# This file describes the network interfaces available on
# and how to activate them. For more information, see inter
source /etc/network/interfaces.d/*

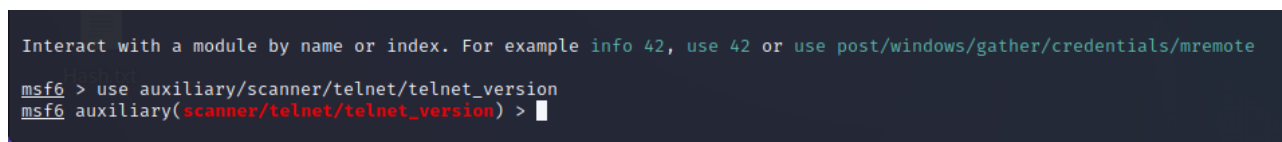
# The loopback network interface
auto eth0
iface eth0 inet static
address 192.168.1.25
gateway 192.168.1.1
netmask 255.255.255.0

metasploitable [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
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 static
address 192.168.1.40
netmask 255.255.255.0
network 192.168.1.255
gateway 192.168.1.1
```

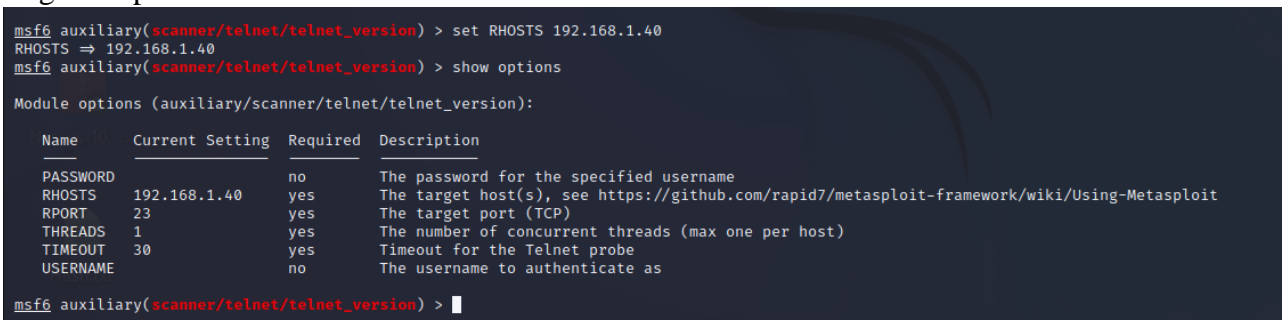
Aviamo su Kali msfconsole. E Partiamo subito con la scelta del modulo per l'esercizio .In questo caso è:



```
Interact with a module by name or index. For example info 42, use 42 or use post/windows/gather/credentials/mremote

msf6 > use auxiliary/scanner/telnet/telnet_version
msf6 auxiliary(scanner/telnet/telnet_version) > █
```

Sci come non bisogna selezionare il payload si lascia quello di default .Comando show options apriamo le impostazioni e vediamo quale dato ci viene chiesto e lo impostiamo per esempio ip target e ip local. Con il comando `set` :



```
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  192.168.1.40    yes       The password for the specified username
  RHOSTS    23              yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
  RPORT     1               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

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

Dopo aver impostato tutto si parte con il comando Exploit.

```
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:
[*] 192.168.1.40:23 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/telnet_version) >
```

Ci viene fornito anche le credenziali di accesso che in questo caso e msfadmin sia come password sia come username. Con il comando telnet IpMeta abbiamo una ulteriore conferma :

```
File Actions Edit View Help
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 '^]'.

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: Tue Dec 6 06:13:09 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:
```

```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:ef:f8:31
          inet addr:192.168.1.40  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:feef:f831/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:98 errors:0 dropped:0 overruns:0 frame:0
          TX packets:176 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:7082 (6.9 KB)  TX bytes:16686 (16.2 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:167 errors:0 dropped:0 overruns:0 frame:0
          TX packets:167 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:46579 (45.4 KB)  TX bytes:46579 (45.4 KB)

msfadmin@metasploitable:~$
```