Relazione sull'Exploit di un Server Metasploitable tramite Kali Linux

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

Impostazione dell'IP su Kali Linux

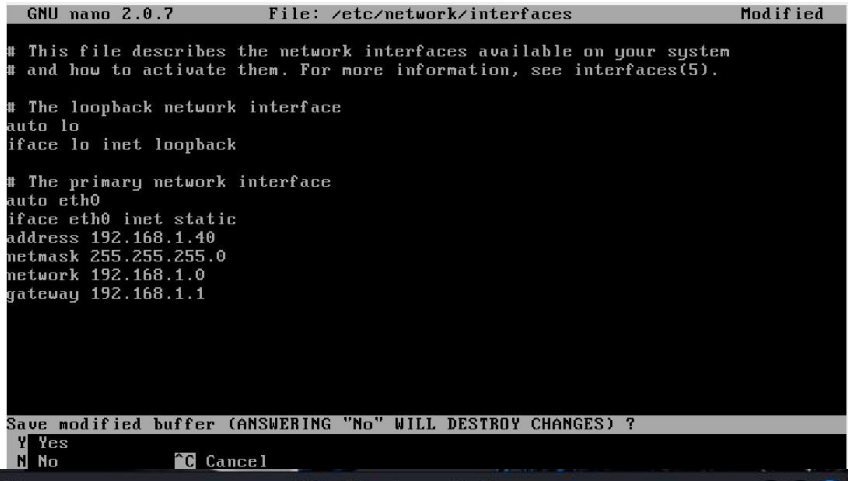
Ho usato l'edit connections da kali per settare la macchina sulla rete richiesta

Impostazione dell'IP su Metasploitable

Per settare la Meta sull'IP richiesto bisogna modificare un file con il seguente comando:

```
sudo nano
/etc/network/interfaces
```

settando l'IP a 192.168.1.40

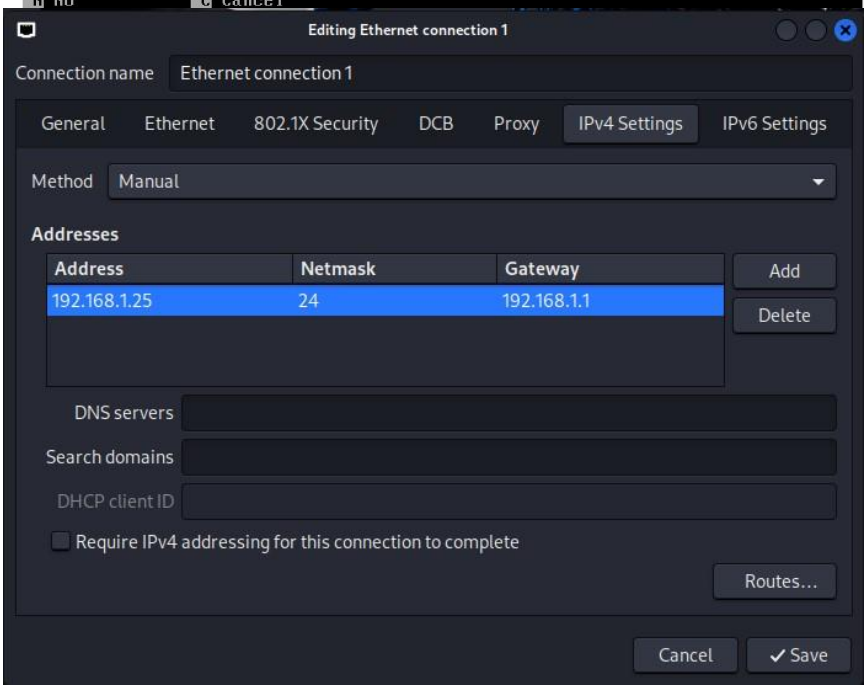


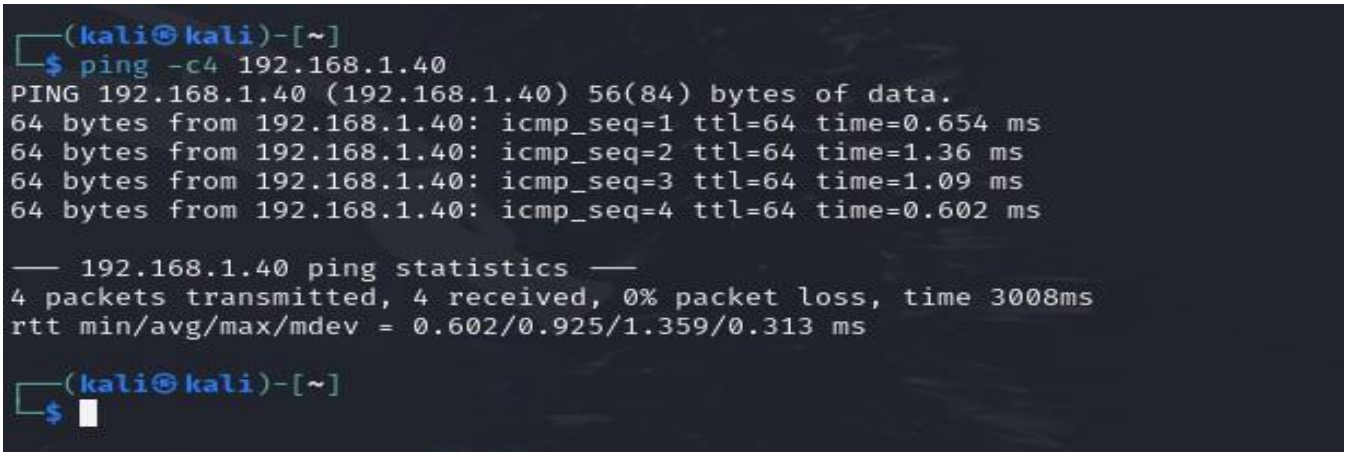
Controllo

Per verificare che le macchine fossero effettivamente sulla stessa rete ho usato il comando:

`ping`

da entrambe le macchine





```
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 08:00:27:4f:b1:59 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:fe4f:b159/64 scope link
       valid_lft forever preferred_lft forever
msfadmin@metasploitable:~$ ping -c4 192.168.1.25
PING 192.168.1.25 (192.168.1.25) 56(84) bytes of data.
64 bytes from 192.168.1.25: icmp_seq=1 ttl=64 time=11.2 ms
64 bytes from 192.168.1.25: icmp_seq=2 ttl=64 time=0.760 ms
64 bytes from 192.168.1.25: icmp_seq=3 ttl=64 time=0.667 ms
64 bytes from 192.168.1.25: icmp_seq=4 ttl=64 time=0.587 ms

--- 192.168.1.25 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3007ms
rtt min/avg/max/mdev = 0.587/3.320/11.268/4.589 ms
msfadmin@metasploitable:~$ _
```

Scan delle porte

Ho utilizzato nmap per vedere quali porte fossero aperte sulla Metasploit facendo:

`nmap -sV 192.168.1.25`

e ho potuto notare che la porta 23 era aperta

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.1.40
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-09 08:47 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify
valid servers with --dns-servers
Nmap scan report for 192.168.1.40
Host is up (0.011s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  shell       Netkit rshd
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux
_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 53.69 seconds
```

Avvio di Metasploit su Kali Linux

Lanciare msfconsole per accedere all'interfaccia di Metasploit:

```
msfconsole
```

Ricerca Modulo

Ho cercato il modulo con:

```
search auxiliary telnet_version
```

```
msf6 > search auxiliary telnet_version

Matching Modules
================

   #  Name                                                 Disclosure Date  Rank    Check  Descr
iption
   -  ----                                                 ---------------  ----    -----  -----
------
   0  auxiliary/scanner/telnet/lantronix_telnet_version                     normal  No     Lantr
onix Telnet Service Banner Detection
   1  auxiliary/scanner/telnet/telnet_version                               normal  No     Telne
t Service Banner Detection


Interact with a module by name or index. For example info 1, use 1 or use auxiliary/scanner/te
lnet/telnet_version
```

Caricamento del Modulo Telnet Version

Ho caricato il modulo auxiliary/scanner/telnet/telnet_version:

```
use auxiliary/scanner/telnet/telnet_version
```

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

Configurazione dei Parametri del Modulo

Impostare l'indirizzo IP del target (Metasploitable) e la porta Telnet (23):

```
set RHOSTS 192.168.1.40
```

Verificare che i parametri siano stati impostati correttamente:

```
show options
```

```
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                   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.
```

Esecuzione del Modulo

Eseguire il modulo per scansionare la versione del servizio Telnet in esecuzione sul target:

```
exploit
```

Verifica

Dopo l'esecuzione del modulo, ho quindi provato a collegarmi alla Meta tramite telnet con il comando:

```
telnet 192.168.1.40
```

E così mi sono ritrovato, finalmente, dentro Metasploitable