Compito S7-L2

Exploit Telnet con Metasploit

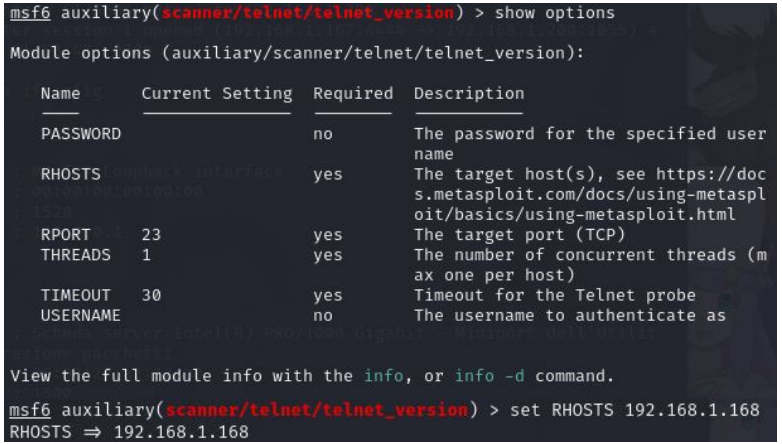
Apriamo un terminale di Kali e inseriamo il comando msfconsole. Poi, in un altro terminale, effettuiamo la scansione delle porte con nmap -Pn -sV ip. Ora torniamo su msfconsole e eseguiamo search auxiliary telnet_version.

```
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
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)
```

```
msf6 > search auxiliary telnet_version

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

   #  Name                                                  Disclosure Date  Rank
k    Check  Description
   -  ----   -----------
   0  auxiliary/scanner/telnet/lantronix_telnet_version                      nor
mal  No     Lantronix Telnet Service Banner Detection
   1  auxiliary/scanner/telnet/telnet_version                                nor
mal  No     Telnet Service Banner Detection


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

msf6 > use 1
```

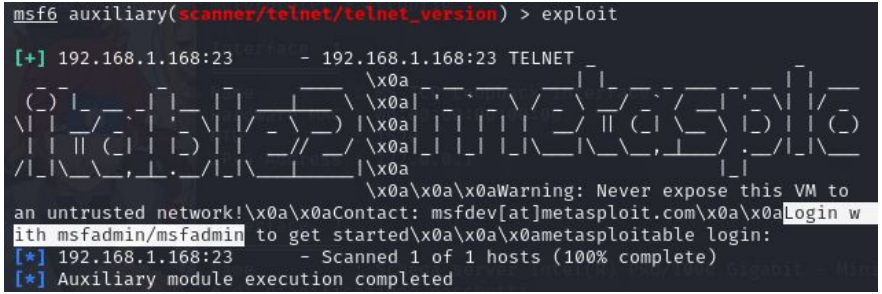
Exploit Telnet con Metasploit

Andiamo a vedere le opzioni e, per tutte le informazioni necessarie, le compiliamo.



Exploit Telnet con Metasploit

Ora andiamo a far partire l'exploit. Possiamo notare di aver ricevuto la scansione con successo e di conseguenza ottenuto le credenziali. Ora possiamo accedere a Telnet normalmente con le credenziali ottenute.



Exploit Telnet con Metasploit

Come puoi vedere, ho inserito con successo le credenziali ottenute e sono entrato nel servizio normalmente.