

Metasploit: auxiliary modules

L'obiettivo dell'esercizio è utilizzare un modulo ausiliario di Metasploit per scoprire le credenziali di accesso al protocollo Telnet su Metasploitable. Successivamente, con le credenziali ottenute, si procede ad accedere alla macchina target tramite il client Telnet.

Avvio di Metasploit con il comando
msfconsole.

Utilizzo del modulo ausiliario
use auxiliary/scanner/telnet/telnet_version

Configurato i parametri per il modulo
set RHOSTS 192.168.1.149

lancio l'exploit

```
Name      Current Setting  Required  Description
-----
PASSWORD  192.168.1.149    no        The password for the specified username
RHOSTS    192.168.1.149    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  none             no        The username to authenticate as

View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/telnet/telnet_version) > exploit

[*] 192.168.1.149:23 - 192.168.1.149:23 TELNET
[*] 192.168.1.149:23 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

In foto sono evidenziate le credenziali di accesso al servizio telnet in esecuzione sulla macchina target.

Per verificare le credenziali ho aperto un nuovo terminale su kali linux e digitato
telnet 192.168.1.149

Inserite le credenziali di accesso al servizio telnet, confermando l'esito positivo dell'esercizio.

```

(kali@kali)-[~]
$ telnet 192.168.1.149
Trying 192.168.1.149 ...
Connected to 192.168.1.149.
Escape character is '^]'.
msf5 auxiliary( ) > set RHOST 192.168.1.149
RHOST => 192.168.1.149
msf5 auxiliary( ) >

Name      Current Setting  Required  Description
-----
Warning: Never expose this VM to an untrusted network!
RHOST     192.168.1.149   yes       The target host(s), see https://docs.metasploit.com/docs
Contact: msfdev[at]metasploit.com           The target port (TCP)
THREADS   1                yes       The number of concurrent threads (max one per host)
Login with msfadmin/msfadmin to get started out for the Telnet probe
USERNAME   no               The username to authenticate as

msf5auxiliary login: msfadmin
Password:
Last login: Tue Nov 12 08:43:48 EST 2024 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.

```

Conclusione

L'esercizio ha evidenziato come i moduli ausiliari di Metasploit possano essere utilizzati per raccogliere informazioni dettagliate sui servizi attivi, in questo caso Telnet, migliorando la comprensione del sistema target prima di eseguire ulteriori attacchi.