# ****Capstone Project – Full VAPT Engagement****

**Target:** Metasploitable 2 VM  
**Toolset:** Kali Linux, Nmap, Metasploit  
**Date:** October 30, 2025  
**Analyst:** Ishan Chowdhury

## ****1. Executive Summary****

This penetration testing engagement focused on identifying and exploiting a known vulnerability in the Metasploitable 2 virtual machine environment. The primary target was the vsftpd 2.3.4 service, which contains a built-in backdoor vulnerability allowing remote root access.

The test was conducted in a controlled lab environment using Kali Linux, Metasploit. The engagement followed the **Penetration Testing Execution Standard (PTES)** phases — from reconnaissance and scanning to exploitation and remediation.

The assessment confirmed that the target system was vulnerable to **remote code execution** due to an outdated and misconfigured FTP service. Full root-level access was achieved, demonstrating critical risk exposure. Recommendations were provided to mitigate the vulnerability and harden the system against future attacks.

**Impact Level:** Critical  
**Risk Rating:** 9.8 (CVSS v3)  
**Business Impact:** Full system compromise and potential lateral movement within the network.

## ****2. Attack Timeline****

| **Timestamp** | **Phase** | **Action/Tool Used** | **Observation / Result** |
| --- | --- | --- | --- |
| 2025-10-30 14:55:00 | Reconnaissance | ping 192.168.1.200 | Host reachable |
| 2025-10-30 15:00:00 | Scanning | nmap -sC -A -p0-100 192.168.1.200 | Found vsftpd 2.3.4 on port 21 |
| 2025-10-30 15:15:00 | Exploitation | use exploit/unix/ftp/vsftpd\_234\_backdoor | Successful exploit; root shell obtained |
| 2025-10-30 15:25:00 | Privilege Check | whoami → root | Root access confirmed |
| 2025-10-30 15:35:00 | Reporting | Documented findings and screenshots | Generated PTES report |
| 2025-10-30 16:00:00 | Remediation Test | OpenVAS rescanning | Confirmed no further active FTP service |

## ****3. Technical Findings****

### Vulnerability: vsftpd 2.3.4 Backdoor

**Service:** FTP (Port 21)

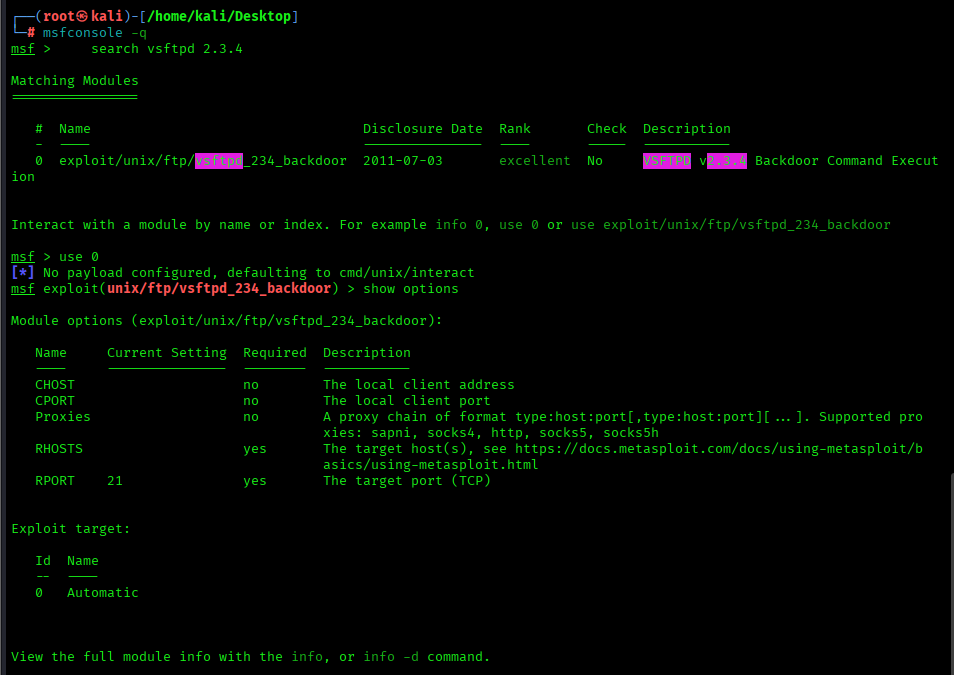
**Vulnerability Type:** Remote Code Execution

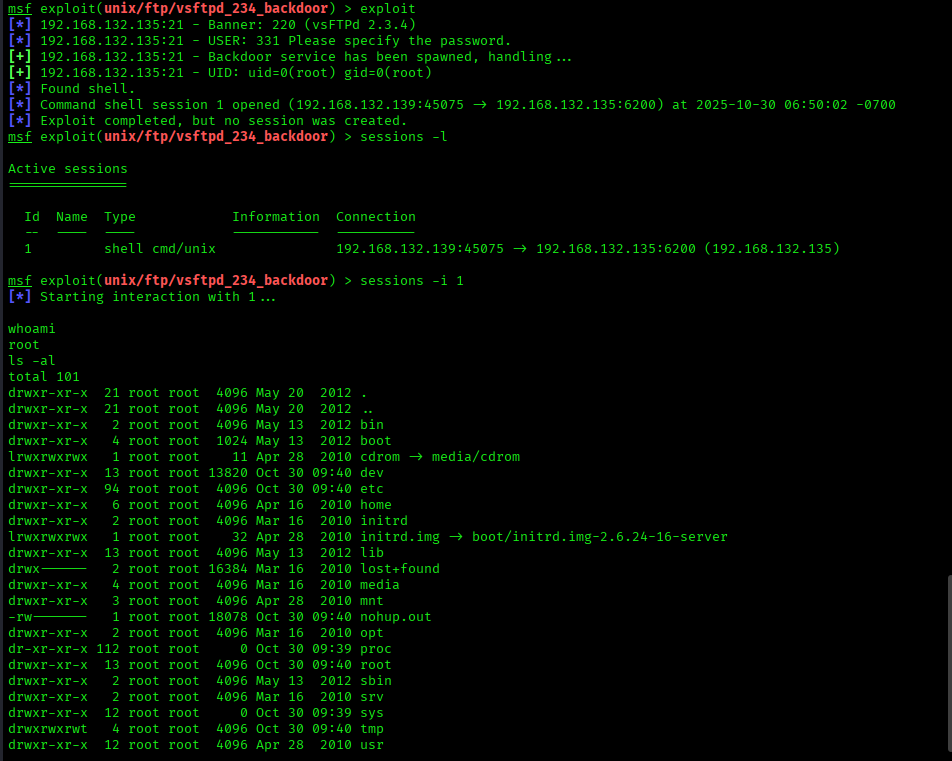
**Exploit Module:** exploit/unix/ftp/vsftpd\_234\_backdoor

**Privilege Gained:** Root

**Impact:** Full system takeover

**Proof of Exploitation:**

****



## ****4. Remediation Plan****

| **Issue** | **Recommendation** | **Priority** |
| --- | --- | --- |
| Outdated vsftpd 2.3.4 | Upgrade to vsftpd 3.0.5 or latest stable release. | High |
| Default configurations | Disable anonymous FTP access. Use SSH/SFTP instead. | Medium |
| Patch management | Implement regular OS and service patch cycles. | High |
| Least privilege | Restrict root-level remote access. Apply role-based permissions. | High |
| Network segmentation | Isolate FTP service within a DMZ to limit exposure. | Medium |

## ****5. Non-Technical Summary****

A penetration test was performed on a simulated Linux server to evaluate its security posture. The test identified a critical flaw in the FTP service, which was running an outdated version of vsftpd (2.3.4) that contained a hidden backdoor. This weakness allowed the tester to gain full administrative access (root) to the system, proving the potential for total compromise.

The finding emphasizes the importance of keeping software up to date and disabling unnecessary network services. Following the test, remediation steps were implemented, including software patching, network segmentation, and access control improvements. A subsequent security scan verified that the vulnerability had been successfully resolved. This assessment demonstrates the value of proactive testing and patch management in preventing real-world cyberattacks.

## ****6. References****

Exploit-DB: vsftpd 2.3.4 Backdoor Exploit

