🛡️ Professional Penetration Testing Final Report

Executive Summary

This report consolidates the results of a comprehensive penetration testing project based on the **PTES (Penetration Testing Execution Standard)**. The test was conducted in a controlled lab environment using **Parrot OS** as the attacking system and **Metasploitable 2** as the target. The project followed all phases of professional penetration testing, including reconnaissance, vulnerability analysis, network testing, exploitation, and reporting. Critical vulnerabilities such as anonymous FTP access, outdated Apache, and SSL misconfigurations were identified and successfully exploited, leading to a root shell on the target. The report includes all technical findings, screenshots, and remediation recommendations.

Scope & Methodology

🔹 PTES Phases Followed:

1. Pre-Engagement
2. Intelligence Gathering
3. Threat Modeling
4. Vulnerability Analysis
5. Exploitation
6. Post-Exploitation
7. Reporting

🔹 Environment:

- **Attacker Machine**: Parrot OS (Host-Only Network, VirtualBox)
- **Target Machine**: Metasploitable 2 (10.138.16.109)

🔹 Tools Used:

- **Recon & Scanning**: Nmap, Enum4Linux, Whois, dig
- **Web Testing**: Nikto
- **Password Attacks**: Hydra

- **Exploitation**: Metasploit
- **Traffic Analysis**: Wireshark
- **Reporting**: LibreOffice Writer / Word

Reconnaissance

🔸 Passive Recon:

- WHOIS and dig revealed limited public info due to Heroku's DNS structure.
- Email/subdomain enumeration failed due to tool/API issues (theHarvester, sublist3r).
- Manual web browsing attempted (GUI restricted under root).

🔸 Active Recon:

- Nmap ping scan on `10.138.16.0/24`: 2 live hosts discovered.
- Full port scan against Metasploitable 2 revealed open ports:
    - FTP (21), SSH (22), Telnet (23), HTTP (80), SMB (139, 445), RMI (1099)

Vulnerability Assessment Findings

Service	Vulnerability	Risk	Fix Recommendation
FTP	Anonymous login allowed	High	Disable anonymous login
Apache 2.2.8	Severely outdated, directory indexing enabled	High	Upgrade Apache and disable indexing
SSL	POODLE (CVE-2014-3566), CCS Injection (CVE-2014-0224)	High	Disable SSLv3, patch OpenSSL
RMI	Remote Code Execution risk	High	Secure RMI configuration and access control
Web Server	phpinfo.php exposed	Medium	Remove phpinfo files from public access
HTTP	Vulnerable to Slowloris (CVE-2007-6750)	Medium	Implement rate limiting, use reverse proxy

Scans were performed with:

- `nmap -sS -sV -T4 -p- 10.138.16.109`
- `nmap --script vuln 10.138.16.109`
- `nikto -h http://10.138.16.109`

Network Testing Results

🔸 Protocols Tested:

- FTP, SSH, HTTP, Telnet

🔸 Enum4Linux Output:

- Revealed NetBIOS hostname and WORKGROUP
- Shared folders and usernames listed

🔸 Network Mapping:

- Attacker → Parrot OS
- Target → Metasploitable 2
- Services → FTP, SSH, HTTP, Telnet, RMI

(Network map created in Draw.io — Screenshot included)

🔸 Wireshark Traffic Analysis:

- Filter: `ip.addr == 10.138.16.109`
- Captured ICMP packets confirming host was live
- No encryption seen in telnet/ftp traffic
- Traffic behavior matched expectations

Exploitation Proofs

✅ Metasploit Exploitation

- **Exploit Used**: `exploit/unix/ftp/vsftpd_234_backdoor`
- **Target**: FTP (Port 21)
- **Result**: Shell opened as root (`uid=0`)
- **Command Output**: Verified with `ls`, shell prompt, and root directory access

❌ Hydra Password Attack

Command Attempted:

bash

CopyEdit

```
hydra -l root -P /usr/share/wordlists/rockyou.txt ssh://10.138.16.109
```

-
- **Result**: Failed — missing wordlist file
- **Recommendation**: Decompress rockyou.txt.gz and retry

Post-Exploitation

- After gaining root access, full control over the system was confirmed.
- Explored directories and accessed `/etc/passwd`, `config/`, and web app files.
- Demonstrated ability to tamper with or exfiltrate system data.
- In a real scenario, this level of access would lead to severe data compromise.

Remediation Recommendations

Issue	Recommendation
Anonymous FTP	Disable or restrict login
Outdated Apache	Upgrade and disable indexing
SSL Vulnerabilities	Disable SSLv3, update to TLS 1.2+, patch OpenSSL
RMI Open Access	Harden service, restrict port via firewall
Telnet Access	Replace with SSH or disable
Exposed phpinfo	Delete sensitive development/testing files
General Hardening	Use host firewall, apply least privilege

Appendix

📎 Included artifacts:

- Full Nmap service & vulnerability scans
- Nikto scan results (Apache 2.2.8)
- Enum4Linux output
- Metasploit shell screenshots
- Hydra password attack attempt
- Wireshark packet capture
- Metasploitable2 web UI
- Hand-drawn network map diagram