Penetration Testing Execution Standard (PTES) Report

Target Information

- **Target System:** Metasploitable2
- **IP Address:** 192.168.227.129
- **Operating System:** Ubuntu 8.04 (Hardy Heron)
- **Testing Environment:** Internal Lab
- **Tester:** Atharva Dave
- **Date:** December 2025

---

1. Introduction

This penetration test was performed to evaluate the security posture of the target system by identifying vulnerabilities, validating exploitability, and assessing potential business impact. The assessment followed the **Penetration Testing Execution Standard (PTES)** to ensure a structured and professional approach.

---

2. Scope and Rules of Engagement (PTES Phase 0)

In-Scope

- Target IP: `192.168.227.129`
- All network services and web applications hosted on the target
- Authenticated and unauthenticated testing

Out-of-Scope

- Denial-of-Service attacks
- Attacks outside the lab environment

---

3. Methodology

The engagement followed the PTES framework:

Phase	Description
Phase 0	Pre-engagement interactions
Phase 1	Intelligence Gathering
Phase 2	Threat Modeling
Phase 3	Vulnerability Analysis
Phase 4	Exploitation
Phase 5	Post-Exploitation
Phase 6	Reporting
Phase 7	Remediation

---

4. Intelligence Gathering (PTES Phase 1)

Tools Used

- Nmap

Command Executed

```
nmap -sV -O 192.168.227.129
```

Key Findings

- Apache Web Server
- Apache Tomcat
- distcc service
- MySQL Database Server
- DVWA Web Application

---

5. Vulnerability Analysis (PTES Phase 3)

Tool Used

- OpenVAS

The vulnerability scan identified multiple **High and Critical severity** issues, including outdated services, weak authentication mechanisms, and remote code execution vulnerabilities.

📎 Detailed findings are documented in the attached OpenVAS report.

---

6. Exploitation (PTES Phase 4)

6.1 SQL Injection – DVWA (Critical)

- **Vulnerable Parameter:** `id`
- **Tool Used:** sqlmap
- **Database Identified:** MySQL

Results:

- Extracted databases including `dvwa` and `mysql`
- Dumped `users` table
- Cracked MD5 password hashes using dictionary attack

Impact: Complete compromise of application authentication.

6.2 Remote Code Execution – distcc (Critical)

- **Exploit Used:** `exploit/unix/misc/distcc_exec`
- **Result:** Reverse shell obtained as `daemon` user

This vulnerability allows attackers to execute arbitrary commands remotely.

---

7. Post-Exploitation (PTES Phase 5)

Privilege Escalation

A misconfigured SUID binary (`nmap`) was identified and exploited.

```
nmap --interactive
!sh
```

Result

```
whoami
root
```

✔️ Full root access achieved

---

8. Risk Summary

Vulnerability	Severity
SQL Injection	Critical
Weak Password Hashing (MD5)	High
Remote Code Execution	Critical
Privilege Escalation	Critical

---

9. Remediation Recommendations (PTES Phase 7)

- Implement prepared statements to prevent SQL Injection
- Use strong hashing algorithms such as bcrypt or Argon2
- Disable unnecessary services like distcc
- Remove or restrict SUID binaries
- Regularly patch OS and applications
- Enforce strong password policies

---

10. Conclusion

The penetration test demonstrated that the target system is critically vulnerable and can be fully compromised by an attacker. Immediate remediation is required before deployment in any production environment.