# **Vulnerability Assessment and Penetration Testing (VAPT) Report**

## **1. Overview of the VAPT Setup**

* **Target System**: Metasploitable 2, which is intentionally designed to have vulnerabilities for learning and testing purposes.
* **Testing Platform**: Kali Linux, running in Oracle VirtualBox, used for performing the assessment with tools like Nmap.
* **Objective**: To find security weaknesses in the Metasploitable 2 system and suggest improvements based on the findings.

## **2. Summary of Nmap Scan Results**

|  |  |  |  |
| --- | --- | --- | --- |
| **Port** | **State** | **Service** | **Version** |
| 21/tcp | open | ftp | vsftpd 2.3.4 |
| 22/tcp | open | ssh | OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0) |
| 23/tcp | open | telnet | Linux telnetd |
| 25/tcp | open | smtp | Postfix smtpd |
| 53/tcp | open | domain | ISC BIND 9.4.2 |
| 80/tcp | open | http | Apache httpd 2.2.8 ((Ubuntu) DAV/2) |
| 111/tcp | open | rpcbind | 2 (RPC #100000) |
| 139/tcp | open | netbios-ssn | Samba smbd 3.X - 4.X (workgroup: WORKGROUP) |
| 445/tcp | open | netbios-ssn | Samba smbd 3.X - 4.X (workgroup: WORKGROUP) |
| 512/tcp | open | exec | netkit-rsh rexecd |
| 513/tcp | open | login | OpenBSD or Solaris rlogind |
| 514/tcp | open | tcpwrapped |  |
| 1099/tcp | open | java-rmi | GNU Classpath grmiregistry |
| 1524/tcp | open | bindshell | Metasploitable root shell |
| 2049/tcp | open | nfs | 2-4 (RPC #100003) |
| 2121/tcp | open | ftp | ProFTPD 1.3.1 |
| 3306/tcp | open | mysql | MySQL 5.0.51a-3ubuntu5 |
| 5432/tcp | open | postgresql | PostgreSQL DB 8.3.0 - 8.3.7 |
| 5900/tcp | open | vnc | VNC (protocol 3.3) |
| 6000/tcp | open | X11 | (access denied) |
| 6667/tcp | open | irc | UnrealIRCd |
| 8009/tcp | open | ajp13 | Apache Jserv (Protocol v1.3) |
| 8180/tcp | open | http | Apache Tomcat/Coyote JSP engine 1.1 |

During the scan, Nmap identified several open ports and their associated services:

* **Port 21 (FTP)**: vsFTPd version 2.3.4
  + **Risk**: This version has a known backdoor that could allow unauthorized access.
* **Port 22 (SSH)**: Open
  + **Note**: No vulnerabilities were detected in this service during the scan.
* **Port 23 (Telnet)**: Open
  + **Risk**: This service is not secure because it sends data in plain text.
* **Port 25 (SMTP)**: Open
  + **Risks**:
    - Vulnerable to man-in-the-middle attacks due to outdated security protocols.
* **Port 80 (HTTP)**: Open
  + **Risks**:
    - Potential for attacks like denial of service and SQL injection, which can compromise the web application.

## **3. Recommendations**

Based on the scan results, here are some basic recommendations:

* **FTP**:
  + Upgrade the vsFTPd version to a newer one or turn off the FTP service if it is not needed.
* **Telnet**:
  + Disable Telnet and use SSH instead for secure remote access.
* **SMTP**:
  + Update configurations to remove support for outdated security protocols.
* **HTTP**:
  + Implement input validation on web applications to prevent SQL injection.
  + Consider limiting access to the web server from untrusted sources to reduce the risk of denial-of-service attacks.
* **General Maintenance**:
  + Regularly update all software to the latest versions to patch known vulnerabilities.

## **4. Final Thoughts**

This VAPT assessment highlights the importance of finding and fixing vulnerabilities in systems. By following the recommendations, organizations can better protect their systems from unauthorized access and potential data breaches. Understanding and addressing these vulnerabilities is crucial in maintaining a secure environment.