Kioptrix Level 1 - Vulnerability Assessment Report

This document summarizes the key vulnerabilities identified during the reconnaissance and scanning phase of the Kioptrix Level 1 penetration test.

1. Apache/2.0.52 (CentOS)

- Outdated version with multiple known vulnerabilities including remote code execution (RCE).
- CVEs include: CVE-2004-0940, CVE-2005-2700, CVE-2005-3352.
- Recommendation: Upgrade to a supported Apache version.

2. Samba smbd 2.2.1a (Ports 139, 445)

- Vulnerable to multiple remote exploits including trans2open.
- Confirmed remote code execution using Metasploit module: exploit/linux/samba/trans2open.
- Recommendation: Patch or disable outdated SMB protocol.

3. OpenSSH 2.9p2 (Protocol 1.99)

- Supports outdated protocol with known downgrade attacks.
- May be vulnerable to traffic sniffing or weak encryption.
- Recommendation: Upgrade to OpenSSH 8+ and disable Protocol 1.

4. Directory Listing Enabled (/icons)

- Nikto scanner revealed accessible /icons directory with listing enabled.
- Allows enumeration of files and potential leakage of sensitive information.
- Recommendation: Disable directory listing in Apache config.

5. Service Banner Disclosure

- Services disclose version info in banner responses.
- Enables fingerprinting and targeted attacks.
- Recommendation: Suppress version banners and use a firewall.

6. General System Hardening

- Lack of firewall or service isolation.
- All services fully accessible from attacker IP.
- Recommendation: Enforce access controls and minimize exposed services.

Conclusion:

The Kioptrix Level 1 machine is intentionally vulnerable and contains multiple weak points ideal for training in penetration testing techniques.