Vulnerability Assessment and Penetration Testing (VAPT) on Kioptrix Level 1

Prepared by: Cinchana S
Role: VAPT Intern
Environment: Controlled Lab
Date: 16-01-2026

Executive Summary

A full penetration test was conducted on the Kioptrix Level 1 virtual machine to simulate a real-world attack scenario. The assessment followed PTES phases including reconnaissance, exploitation, post-exploitation, and reporting. Multiple critical vulnerabilities were identified and successfully exploited, leading to full root compromise of the target system.

Assessment Scope and Setup

- **Target:** Kioptrix Level 1 VM
- **Network Mode:** NAT Network
- **Attacker System:** Kali Linux
- **Assessment Type:** Internal Penetration Test

Reconnaissance and Enumeration

The reconnaissance phase began by identifying live hosts on the local network.

Commands Used

- nmap -sn 192.168.0.0/24
- nmap -p- -A 192.168.0.11

Additional enumeration was performed using:

- Nikto (web server vulnerabilities)
- Gobuster (directory enumeration)
- Enum4linux and smbclient (SMB enumeration)
- Manual web analysis and Wappalyzer

This phase revealed outdated services including **Apache with mod_ssl**, and a vulnerable **Samba service**.

Exploitation Phase

Exploit Method 1: Samba trans2open

- **Exploit Used:** exploit/linux/samba/trans2open
- **Payload:** payload/generic/shell_reverse_tcp

This exploit resulted in immediate **root-level access**, confirming a critical vulnerability.

Exploit Method 2: Apache mod_ssl Remote Buffer Overflow

- Identified vulnerable mod_ssl version using reconnaissance
- Located exploit via:
    1. searchsploit mod_ssl 2.8
    2. searchsploit -m unix/remote/47080.c

The exploit code was modified and compiled successfully. The exploit was executed against the target, resulting in **root access**. Post-exploitation activities included reviewing system files and reading confirmation messages, including a congratulatory mail indicating successful compromise.

Vulnerability Scanning and Detection (OpenVAS)

After exploitation, an OpenVAS scan was conducted against the Kioptrix VM to validate discovered vulnerabilities.

OpenVAS Findings Log

Timestamp	TargetIP	Vulnerability	PTES Phase
2026-01-13 19:00	192.168.0.11	Samba RCE	Exploitation
2026-01-13 19:05	192.168.0.11	Apache mod_ssl RCE	Exploitation

Remediation Recommendations

- Upgrade Apache and OpenSSL to supported versions
- Disable or restrict SMB services
- Apply vendor security patches
- Implement network segmentation
- Perform routine vulnerability scanning and patch management

Non-Technical Summary for Management

The security assessment of the Kioptrix system revealed multiple critical weaknesses that allowed full system compromise. Outdated services exposed the server to remote attacks, enabling attackers to gain administrator-level control. Such vulnerabilities could lead to data breaches, service disruption, or complete infrastructure takeover. Regular patching, service hardening, and continuous security testing are essential to reduce these risks. Addressing these issues proactively will significantly improve the organization's security posture and resilience against real-world cyber threats.

Conclusion

This capstone project successfully demonstrated a complete VAPT lifecycle, from reconnaissance to exploitation and reporting. The exercise reinforced the importance of layered security controls, timely patching, and clear communication of risks to both technical and non-technical stakeholders.