# Network Vulnerability Assessment Report

## Final Project - DEPI

Prepared by:

Wael Ashraf, Mahmoud Ehab, Zeyad Assem, Haidy Karam, Nada Mohamed

Date: October 21st, 2024  
Version: 1.0

# Table of Contents

1. Executive Summary

2. Assessment Overview

3. Scope and Exclusions

4. Methodology

5. Technical Findings

6. Vulnerability Summary & Report Card

7. Tools Used

8. Final Recommendations

9. References

# Executive Summary

The purpose of this project was to assess the security posture of eight vulnerable machines from VulnHub. The penetration test revealed numerous vulnerabilities, including critical issues such as remote code execution, SQL injection, and misconfigurations that could lead to unauthorized access or complete system compromise. The report provides a comprehensive overview of the identified vulnerabilities, their risks, and suggested actions for remediation.

Key Findings:  
- Critical vulnerabilities: Remote Code Execution (RCE), SQL Injection, and misconfigured services.  
- Multiple services exposed with weak or no authentication, risking unauthorized access.  
- Numerous outdated software versions prone to known exploits.  
  
Recommendations:  
- Immediate patching and updates to mitigate discovered vulnerabilities.  
- Enforce stronger authentication mechanisms.  
- Regular monitoring and vulnerability scans to ensure a robust security posture.

# Assessment Overview

The objective of this security assessment was to identify, analyze, and report vulnerabilities in the following systems: Kioptrix, Metasploitable, and others as listed below. The assessment followed a structured approach to ensure comprehensive testing and accurate reporting of all security flaws.

Methodology:  
- \*\*Reconnaissance:\*\* Gathering information and identifying open ports/services.  
- \*\*Vulnerability Scanning:\*\* Automated tools to identify potential vulnerabilities.  
- \*\*Exploitation:\*\* Attempting to exploit vulnerabilities to confirm severity and impact.  
- \*\*Post-Exploitation:\*\* Evaluating impact after successful exploitation, including privilege escalation.  
- \*\*Reporting:\*\* Documenting findings with recommended mitigation steps.

# Scope and Exclusions

The following systems were tested as part of the assessment:

- Kioptrix Level 1  
- Kioptrix Level 2  
- Kioptrix Level 4  
- Lampiao  
- Metasploitable 1  
- Metasploitable 2  
- SkyTower 1  
- Stapler 1

Exclusions:

- Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks.

# Methodology

The assessment followed a structured penetration testing approach that involved both automated scanning and manual exploitation. The process included the following steps:  
- \*\*Information Gathering:\*\* Scanning for open ports and services, gathering metadata.  
- \*\*Vulnerability Scanning:\*\* Automated tools (e.g., Nmap, Burp Suite) were used to detect vulnerabilities.  
- \*\*Exploitation:\*\* Attempts were made to exploit weaknesses using Metasploit and other frameworks.  
- \*\*Post-Exploitation:\*\* Evaluating the impact of successful exploitation, privilege escalation, and data access.  
- \*\*Remediation and Reporting:\*\* Providing actionable recommendations to mitigate risks.

# Technical Findings

Detailed findings of the penetration test are as follows:

1. \*\*Apache 1.3 Vulnerabilities:\*\*  
- \*\*Impact:\*\* Remote Code Execution, Directory Traversal, Denial of Service.  
- \*\*Recommendation:\*\* Upgrade Apache to a supported version (2.x or later), configure security headers, and disable unnecessary modules.  
- \*\*Tools Used:\*\* Manual testing, Nmap.  
  
2. \*\*SQL Injection (Login Page):\*\*  
- \*\*Impact:\*\* Privilege Escalation, Unauthorized Administrative Access.  
- \*\*Recommendation:\*\* Use parameterized queries (prepared statements) and validate user input.  
- \*\*Tools Used:\*\* Burp Suite, Dirbuster.  
  
3. \*\*Samba Vulnerabilities (Trans2open Exploit):\*\*  
- \*\*Impact:\*\* Remote Code Execution leading to root access.  
- \*\*Recommendation:\*\* Upgrade Samba to a version not vulnerable to the exploit, implement network segmentation.  
- \*\*Tools Used:\*\* Metasploit, Manual exploitation.  
  
4. \*\*Backdoor in vsFTPd 2.3.4:\*\*  
- \*\*Impact:\*\* Remote Code Execution and root access.  
- \*\*Recommendation:\*\* Upgrade vsFTPd to the latest stable version.

# Vulnerability Summary & Report Card

The vulnerabilities discovered during this assessment were categorized by severity to prioritize remediation efforts:  
- \*\*Critical:\*\* 12 findings  
- \*\*High:\*\* 8 findings  
- \*\*Moderate:\*\* 4 findings  
- \*\*Low:\*\* 3 findings  
- \*\*Informational:\*\* 0 findings.

# Tools Used

Several tools were utilized to conduct the penetration test and gather data, including:  
- \*\*Metasploit Framework:\*\* Exploitation and post-exploitation.  
- \*\*Nmap:\*\* Network scanning and enumeration.  
- \*\*Burp Suite:\*\* Web application vulnerability scanning.  
- \*\*WPScan:\*\* WordPress security scanner.  
- \*\*Hydra:\*\* Brute-force attack testing.  
- \*\*Dirbuster:\*\* Directory brute-forcing.

# Final Recommendations

To mitigate the identified vulnerabilities and strengthen the security posture of the tested systems, we recommend the following actions:  
- \*\*Upgrade Outdated Software:\*\* Apply patches to outdated services like Apache, Samba, and WordPress.  
- \*\*Strengthen Authentication:\*\* Implement multi-factor authentication (MFA) and enforce strong password policies.  
- \*\*Harden System Configurations:\*\* Disable unused services, configure firewalls, and apply the principle of least privilege.  
- \*\*Regular Monitoring and Audits:\*\* Set up logging and monitoring systems (e.g., Splunk, ELK Stack) to detect malicious activity.

# References

1. OWASP Top 10 – https://owasp.org/www-project-top-ten/  
2. CVE Details – https://cve.mitre.org/  
3. NIST SP800-53 – https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final  
4. Exploit-DB – https://www.exploit-db.com/