Kioptrix VM

Security Assessment Findings Report

Date: August 4th, 2023

Conducted by: Yujie Yamamoto

# Table of Contents

[Table of Contents 2](#_Toc142121901)

[Finding Severity Ratings 3](#_Toc142121902)

[Scope 3](#_Toc142121903)

[Executive Summary 4](#_Toc142121904)

[Attack Summary 4](#_Toc142121905)

[Enumeration 4](#_Toc142121906)

[Exploitation 5](#_Toc142121907)

[Vulnerabilities by Impact 7](#_Toc142121908)

[Penetration Test Findings 8](#_Toc142121909)

[Finding PT-001: trans2open – Samba 2.2.1.a (Critical) 8](#_Toc142121910)

[Finding PT-002: OpenFuck Remote Buffer Overflow – mod\_ssl < 2.8.7 9](#_Toc142121911)

[Finding PT-003: Default Webpage – Version Information Disclosure 10](#_Toc142121912)

# Finding Severity Ratings

The following table defines levels of severity and corresponding CVSS score range that are used throughout the document to assess vulnerability and risk impact.

| Severity | CVSS V3 Score Range | Definition |
| --- | --- | --- |
| Critical | 9.0-10.0 | Exploitation is straightforward and usually results in system-level compromise. It is advised to form a plan of action and patch immediately. |
| High | 7.0-8.9 | Exploitation is more difficult but could cause elevated privileges and potentially a loss of data or downtime. It is advised to form a plan of action and patch as soon as possible. |
| Moderate | 4.0-6.9 | Vulnerabilities exist but are not exploitable or require extra steps such as social engineering. It is advised to form a plan of action and patch after high-priority issues have been resolved. |
| Low | 0.1-3.9 | Vulnerabilities are non-exploitable but would reduce an organization’s attack surface. It is advised to form a plan of action and patch during the next maintenance window. |
| Informational | N/A | No vulnerability exists. Additional information is provided regarding items noticed during testing, strong controls, and additional documentation. |

# Scope

Since this is just a practice lab, the Kioptrix Machine was set into NAT network connection which shares with the host IP address.

|  |  |
| --- | --- |
| Assessment | Details |
| Network Penetration Test | 192.168.179.162 |

# Executive Summary

On August 4th, 2023, the Kioptrix Machine from TCM PEH Course was assessed through a network penetration test. All the activities conducted simulates a real penetration test event with the goal of:

* Identifying the vulnerabilities that can be exploited and potentially gain access to the machine.
* Determining the level of risk and impact of security weaknesses.
* Recommend possible mitigation to prevent such attacks.

The tester found critical level vulnerabilities that are easily found through basic reconnaissance that allowed remote code execution to gain high level access to the machine. The machine was found to be running an outdated version of operating system, software, and services.

## Attack Summary

The following table describes how the attacker gained machine access step by step:

### Enumeration

The attacker performed port scanning and service enumeration to gather information about the services running in Kioptrix Machine**.** The initial scan displays service version of the ports that are open using **Nmap**.

A screenshot of a computer

Description automatically generated

Figure 1. Nmap Scan Result

Nikto scan was run to gather more information about the services and open ports. Services running in http are outdated and can be exploited remotely.

A close-up of a document

Description automatically generated

Figure 2. Nikto Scan

During the initial reconnaissance, port 139 (smb) was open but didn’t give much information. Another scan is utilized using Metasploit to show the version of smb and to examine if there are potential vulnerabilities with the running version.

**A black text on a white background

Description automatically generated**

Figure 3. SMB scanner using Metasploit.

### Exploitation

**SMB Remote Code Execution**

After verifying that Samba 2.2.1a can be exploited using trans2open module, the attacker run Metasploit to automatically exploit the outdated service. This requires setting up the victim’s IP and the choosing correct payload.

A screenshot of a computer

Description automatically generated

Figure 4. smb exploit

**Apache mod\_ssl Remote Buffer Overflow**

The outdated version of mod\_ssl allows remote attackers to use a buffer overflow to execute arbitrary code. This attack utilizes an exploit called OpenFuck to gain interactive shell from the Kioptrix Machine to Attacker’s Machine.

A screenshot of a computer

Description automatically generated

Figure 5. Mod\_ssl buffer overflow exploit

One of the required parameters was to determine the target box. During the initial scan using Nmap, it was determined that the Kioptrix machine is running RedHat Linux OS and a web server of Apache version 1.3.20.



Figure 6. Target Box Parameter

# Vulnerabilities by Impact

The following chart illustrates the vulnerabilities found by impact:

## Penetration Test Findings

Finding PT-001: trans2open – Samba 2.2.1.a (Critical)

|  |  |
| --- | --- |
| Description: | Kioptrix Machine was running an old version of Samba server that is vulnerable to buffer overflow. This module is capable of exploiting samba versions from 2.2.0 to 2.2.8. The attacker gains high level access to the machine and also able to dump user credentials in a form of hashes. |
| Impact: | **CRITICAL** |
| Tools: | Metasploit |
| CVE Identifier: | CVE-2003-0201 |
| Vector String: | CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H |

**Exploitation Proof of Concept**

A screenshot of a computer

Description automatically generated

Figure 7. Buffer Overflow using Metasploit.

****

Figure 8. User hashes

**Remediation**

Update software and services to the latest version as well as ensuring that the password policy is strong for every user.

Finding PT-002: OpenFuck Remote Buffer Overflow – mod\_ssl < 2.8.7

|  |  |
| --- | --- |
| Description: | Kioptrix Machine was running an old version of Apache server that is vulnerable to buffer overflow. This module is capable of exploiting mod\_ssl versions that are below 2.8.7. The attacker gains high privilege access to the machine using this exploit. |
| Impact: | **CRITICAL** |
| Tools: | Manual Testing, OpenFuck |
| CVE Identifier: | CVE-2002-0082 |
| Vector String: | CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H |

**Exploitation Proof of Concept**

A screenshot of a computer

Description automatically generated

**Remediation**

Update Operating System to the latest version. It is highly recommended to upgrade to the latest version of RedHat Linux OS to have an updated security patch management to avoid remote code execution on outdated versions.

Finding PT-003: Default Webpage – Version Information Disclosure

|  |  |
| --- | --- |
| Description: | Kioptrix Machine was running default webpage which disclose server header version information. Having a default webpage corresponds to poor hygiene that leads to disclosing website architecture. |
| Impact: | **LOW** |

**Exploitation Proof of Concept**

**A screenshot of a computer

Description automatically generated**

**Not Found 
The requested URL Imanual/index.html was not found on this server. 
Apache/13.20 server at 127.0.0.1 port 80 **