Bibliophile Library Penetration Testing Report

Prepared by:
Team 5
3 May 2025

CONFIDENTIAL

Table of Contents

Finding Classifications

Team 5 utilized a two-dimensional matrix, see below, consisting of the business impact and Common Vulnerability Scoring System v4.0 (CVSS)[1] score of each finding to categorize it within one of five overall security risk categories: informational, low, moderate, high, and critical. These categories were organized to prioritize the remediation of findings that would cause RAKMS financial loss, non-compliance with governance requirements, and reputational impact.

	Business Impact				
CVSS Score	**N/A (1)**	**Low (2)**	**Moderate (3)**	**High (4)**	**Critical (5)**
N/A – 0.0 (a)	🟦 1a	🟩 2a	🟧 3a	🟧 4a	🟥 5a
0.1 – 3.9 (b)	🟩 1b	🟧 2b	🟧 3b	🟥 4b	🟥 5b
4.0 – 6.9 (c)	🟧 1c	🟧 2c	🟥 3c	🟥 4c	🟪 5c
8.0 – 8.9 (d)	🟧 1d	🟥 2d	🟥 3d	🟪 4d	🟪 5d
9.0 – 10.0 (e)	🟥 1e	🟥 2e	🟪 3e	🟪 4e	🟪 5e

Overall Risk Key: 🟦 **Informational** 🟩 **Low** 🟧 **Moderate** 🟥 **High** 🟪 **Critical**

Business Impact

Team 5 incorporates business impact into the result for the categorization of a finding to help prioritize mitigation efforts and allocate resources effectively to address the most critical issues. We base our qualitative measurement on the ability of a finding to impact RAKMS's ability to conduct business, ensure public safety and security, protect customer information, or stay in compliance with government regulations and business standards. As Team 5 is operating under limited knowledge of the business operations of RAKMS, we would recommend RAKMS to review the business impact of these findings to provide a better understanding of the overall risk of said findings.

CVSS Score

The Common Vulnerability Scoring System (CVSS) is a widely recognized industry standard used to evaluate and communicate the severity of security vulnerabilities in computer systems and software. It provides a structured framework for assessing a vulnerability's potential impact, exploitability, complexity, and privileges required for exploitation, assigning it a numeric score from 0 to 10, with higher scores indicating greater risk. CVSS assists organizations in prioritizing and addressing security flaws by considering their impact on confidentiality, integrity, and availability. In our security assessments, we adhere to the CVSS framework, which allows us to accurately gauge the severity of vulnerabilities and effectively communicate their potential risks.

[1] https://www.first.org/cvss/v4.0/specification-document

Critical Risk Findings

⚠	Title of Finding		
Findings Categorization			
Business Impact		CVSS v4.0 Score	

Description

A vulnerability is a weakness in cybersecurity that can be exploited by attackers.

- What is the weakness or misconfiguration?
    - A weakness or misconfiguration is an issue with the system in which the is an issue the software code itself.
- Why is it a problem?
    - This is an issue because attackers could use these weaknesses to their advantage to leak data, change controls, and/or exploit company employees.

Business Impact

Vulnerabilities can have a major impact on business. If an attacker were to gain access, it could stop operations and hinder performance. Hackers can also leak or damage sensitive information. Overall, this could cost the business lots of money and damage their reputation- especially if user information got leaked.

Affected Systems

List of IPs, URLs, or specific systems that are vulnerable.

Format like:

192.168.102.4

192.168.102.5

192.168.102.6

192.168.102.7

192.168.102.50

192.168.102.60

Mitigations

These issues can be fixed by adding more security measures. The organization should add extra authentication and develop complex passwords.

References

https://debricked.com/blog/what-is-security-weakness/

Steps for Reproduction

1. 192.168.102.6
2. Enter credentials: admin:admin
3. Observe access to restricted dashboard

High Risk Findings

⊖	**Title: Eteneral Blue**		
Findings Categorization			
Business Impact		**CVSS v4.0 Score**	8.1-9.0

Description

A computer exploits software that was first developed by the NSA based on a zero-day vulnerability in Microsoft Windows that allowed users unauthorized access to computers connected to a network. Eternal Blue works on older Microsoft operating systems like Windows XP, Windows 8, Windows Server 2003, and Windows 7/8 and 10.

Business Impact

It can provide the highest level of system access and thus can be exploited remotely. You can expect for malicious payload delivery.

Affected Systems

Windows Vista,7,8.1,10, Server 2008,2012, and 2016

Mitigations

References

Steps for Reproduction

Moderate Risk Findings

◓	**Title: LDAP enumeration**		
Findings Categorization			
Business Impact		**CVSS v4.0 Score**	

Description

The LDAP protocol enables users the ability to locate data about an organization. Such as the users, files, and the device used on the network. This protocol is mainly run on the tcp port 389

Technical Impact

The technical impact would be the opportunity for attacks to gather information on usernames, addresses, and other data about the organization they are going after.

Affected Systems

Network protocols, and services using LDAP for authentication.

Mitigations

Regular security patched and monitoring of security advisors like the Microsoft Security Response Center.

References

https://windowsforum.com/threads/understanding-cve-2024-49127-a-critical-ldap-vulnerability-and-its-impact.347667/

https://www.hackercoolmagazine.com/ldap-enumeration-for-beginners/

Steps for Reproduction

Using a nmap script to check for weak passwords. Such as the command “nmap =n –sV –script “ldap* and not brute” -p 389 <target-ip-here>

Low Risk Findings

○	**Title: SMB Enumeration**		
Findings Categorization			
Business Impact		**CVSS v4.0 Score**	
CVSS Attack Vector			

Description

Low risk findings are vulnerabilities that do not affect the overall business very much. They should still be stopped, but at a lower priority.

Technical Impact

Low priority impacts still have a technical effect on a business. They could damage some of the data and hinder business performance.

Affected Systems

This was 192.168.102.5

Potential Compliance Violations

This means that the SMB servers are outdated which allow hackers to potentially exploit this.

Mitigations

To fix this, they should use nmap scripts to update smb script.

References

https://forum.hackthebox.com/t/having-smb-enum-issues-read-this/2369

Steps for Reproduction

Using netexec smb 192.168.102.5 then smbclient -L 192.168.102.5 -m NT1 -N.

Informational Findings

ⓘ	Privilege Escalation via Docker Contrainer Escape		
Findings Categorization			
Business Impact		CVSS v4.0 Score	

Description

Due to a misconfigured Docker Container, and an exposed console vulnerable to terminal command injection, the shadow file for the Vault server was exposed. Using John the Ripper and Rockyou, the admin password was trivial to obtain, and the Secret Book directory was accessible. The data was further stegonographically hidden in a pdf, though examination via cat was also trivial.

Affected Systems

Potential Compliance Violations

Mitigations

References

https://docketevents.com/pages/cd

Steps for Reproduction

Using the vulnerable terminal, inject the command " list & cat</etc/shadow' " to reveal the shadow file Decrypt offline using John, Hashcat, MD5sum, or any other tool. I used rockyou and was successful in minutes. SSH into the vault server using the admin account and password exposed from shadow Escape the Docker container using (check the ref document, my notes are missing the exact steps but it was one of those near the end) Navigate to the secret directory, then the secret directory disguised w a filename, then use any stefonographoc tool to discover the embedded message

Appendix B: Tools Used

Tool name	
Description	
Use Case	
Source	https://github.com/aws/aws-cli

Tool Name	
Description	
Use Case	
Source	https://portswigger.net/burp/communitydownload

Tool Name	
Description	
Use Case	
Source	https://github.com/jpillora/chisel