| Cybersecurity |
| --- |
| Penetration Test Report |

Rekall Corporation

Penetration Test Report

**Student Note: Complete all sections highlighted in yellow.**

# 

## Confidentiality Statement

This document contains confidential and privileged information from Rekall Inc. (henceforth known as Rekall). The information contained in this document is confidential and may constitute inside or non-public information under international, federal, or state laws. Unauthorized forwarding, printing, copying, distribution, or use of such information is strictly prohibited and may be unlawful. If you are not the intended recipient, be aware that any disclosure, copying, or distribution of this document or its parts is prohibited.

Table of Contents

[Confidentiality Statement 2](#_30j0zll)

[Contact Information 4](#_1fob9te)

[Document History 4](#_3znysh7)

[Introduction 5](#_2et92p0)

[Assessment Objective 5](#_3dy6vkm)

[Penetration Testing Methodology 6](#_2s8eyo1)

[Reconnaissance 6](#_17dp8vu)

[Identification of Vulnerabilities and Services 6](#_3rdcrjn)

[Vulnerability Exploitation 6](#_26in1rg)

[Reporting 6](#_lnxbz9)

[Scope 7](#_35nkun2)

[Executive Summary of Findings 8](#_44sinio)

[Grading Methodology 8](#_z337ya)

[Summary of Strengths 9](#_3j2qqm3)

[Summary of Weaknesses 9](#_1y810tw)

[Executive Summary Narrative](#_4i7ojhp) 10

[Summary Vulnerability Overview 1](#_2xcytpi)3

Vulnerability Findings [1](#_1ci93xb)4

# 

## Contact Information

| **Company Name** | HolmesCyber Shield |
| --- | --- |
| **Contact Name** | Jordan Holmes |
| **Contact Title** | Penetration Tester |

## 

## Document History

| **Version** | **Date** | **Author(s)** | **Comments** |
| --- | --- | --- | --- |
| 001 | 10/29/2023 | Jordan Holmes |  |

# 

## Introduction

In accordance with Rekall policies, our organization conducts external and internal penetration tests of its networks and systems throughout the year. The purpose of this engagement was to assess the networks’ and systems’ security and identify potential security flaws by utilizing industry-accepted testing methodology and best practices.

For the testing, we focused on the following:

* Attempting to determine what system-level vulnerabilities could be discovered and exploited with no prior knowledge of the environment or notification to administrators.
* Attempting to exploit vulnerabilities found and access confidential information that may be stored on systems.
* Documenting and reporting on all findings.

All tests took into consideration the actual business processes implemented by the systems and their potential threats; therefore, the results of this assessment reflect a realistic picture of the actual exposure levels to online hackers. This document contains the results of that assessment.

### Assessment Objective

The primary goal of this assessment was to provide an analysis of security flaws present in Rekall’s web applications, networks, and systems. This assessment was conducted to identify exploitable vulnerabilities and provide actionable recommendations on how to remediate the vulnerabilities to provide a greater level of security for the environment.

We used our proven vulnerability testing methodology to assess all relevant web applications, networks, and systems in scope.

Rekall has outlined the following objectives:

Table 1: Defined Objectives

| **Objective** |
| --- |
| Find and exfiltrate any sensitive information within the domain. |
| Escalate privileges. |
| Compromise several machines. |

# 

## Penetration Testing Methodology

### Reconnaissance

### 

We begin assessments by checking for any passive (open source) data that may assist the assessors with their tasks. If internal, the assessment team will perform active recon using tools such as Nmap and Bloodhound.

### Identification of Vulnerabilities and Services

We use custom, private, and public tools such as Metasploit, hashcat, and Nmap to gain perspective of the network security from a hacker’s point of view. These methods provide Rekall with an understanding of the risks that threaten its information, and also the strengths and weaknesses of the current controls protecting those systems. The results were achieved by mapping the network architecture, identifying hosts and services, enumerating network and system-level vulnerabilities, attempting to discover unexpected hosts within the environment, and eliminating false positives that might have arisen from scanning.

### Vulnerability Exploitation

Our normal process is to both manually test each identified vulnerability and use automated tools to exploit these issues. Exploitation of a vulnerability is defined as any action we perform that gives us unauthorized access to the system or the sensitive data.

### Reporting

Once exploitation is completed and the assessors have completed their objectives, or have done everything possible within the allotted time, the assessment team writes the report, which is the final deliverable to the customer.

# 

## Scope

Prior to any assessment activities, Rekall and the assessment team will identify targeted systems with a defined range or list of network IP addresses. The assessment team will work directly with the Rekall POC to determine which network ranges are in-scope for the scheduled assessment.

It is Rekall’s responsibility to ensure that IP addresses identified as in-scope are actually controlled by Rekall and are hosted in Rekall-owned facilities (i.e., are not hosted by an external organization). In-scope and excluded IP addresses and ranges are listed below.

# 

# 

## Executive Summary of Findings

## 

### Grading Methodology

Each finding was classified according to its severity, reflecting the risk each such vulnerability may pose to the business processes implemented by the application, based on the following criteria:

**Critical**: Immediate threat to key business processes.

**High**: Indirect threat to key business processes/threat to secondary business processes.

**Medium**: Indirect or partial threat to business processes.

**Low**: No direct threat exists; vulnerability may be leveraged with other vulnerabilities.

Informational: No threat; however, it is data that may be used in a future attack.

As the following grid shows, each threat is assessed in terms of both its potential impact on the business and the likelihood of exploitation:

Chart

Description automatically generated with medium confidence

### 

### Summary of Strengths

While the assessment team was successful in finding several vulnerabilities, the team also recognized several strengths within Rekall’s environment. These positives highlight the effective countermeasures and defenses that successfully prevented, detected, or denied an attack technique or tactic from occurring.

* Input Validation

### Summary of Weaknesses

We successfully found several critical vulnerabilities that should be immediately addressed in order to prevent an adversary from compromising the network. These findings are not specific to a software version but are more general and systemic vulnerabilities.

* Credentials are not safeguarded
* IPs are easily accessible
* Website open to various web attacks
* Open ports
* Access to credentials are in HTML code

## Executive Summary

This executive summary provides an overview of the penetration testing done on a Windows OS environment and the Rekall website. The primary objective of the assessment was to identify vulnerabilities and assess the security posture of both these systems.

## 

## In the evaluation of the Windows OS environment, our penetration testing team employed Metasploit, a very popular penetration testing tool. The primary focus was on port 21, used for FTP services. Multiple vulnerabilities were identified, leading to successful exploitation. Through these exploits, unauthorized access was gained, allowing us to utilize Meterpreter to access files and directories on the Windows machine. This showed that there are potential security weaknesses in the environment that need immediate attention.

## 

## The evaluation of the Rekall website revealed multiple vulnerabilities, including but not limited to XSS (Cross-Site Scripting) reflected attacks, local file inclusion, command injection, and SQL injection. These findings indicate a range of critical security issues that expose the website to various forms of compromise, data theft, and unauthorized access.

In conclusion, the penetration testing exercise exposed multiple vulnerabilities in both the Windows OS environment and the Rekall website, which could result in serious security incidents if not handled correctly and in a timely manner. Scheduled pentest’s on the company's Windows OS environment and the Rekall website should be at least once or twice a year.

## 

## 

## Summary Vulnerability Overview

| **Vulnerability** | **Severity** |
| --- | --- |
| Command Injection | **Critical** |
| SQL Injection | **Critical** |
| FTP Port 21 Open | **High** |
| Nmap being used to see IPs | **High** |
| XSS Reflected | **Medium** |
| XSS Stored | **Medium** |
| Local File Inclusion | **Critical** |
| crt.sh was easily obtained (Searched the certificate) | **Medium** |

The following summary tables represent an overview of the assessment findings for this penetration test:

| **Scan Type** | **Total** |
| --- | --- |
| Hosts | 192.168.14.35, 192.168.13.0/24,  192.168.13.10, 192.168.13.11,  192.168.13.12, 192.168.13.14 |
| Ports | 21, 22, |

| **Exploitation Risk** | **Total** |
| --- | --- |
| **Critical** | 3 |
| **High** | 2 |
| **Medium** | 3 |
| **Low** | 0 |

## Vulnerability Findings

| **Vulnerability 1** | **Findings** |
| --- | --- |
| **Title** | Reflected XSS |
| **Type (Web app / Linux OS / WIndows OS)** | Web App |
| **Risk Rating** | Critical |
| **Description** | Malicious Script |
| **Images** |  |
| **Affected Hosts** | 192.168.14.35 |
| **Remediation** | XSS Protection |

| **Vulnerability 2** | **Findings** |
| --- | --- |
| **Title** |  |
| **Type (Web app / Linux OS / WIndows OS)** | Web App |
| **Risk Rating** | Critical |
| **Description** | Malicious Script |
| **Images** |  |
| **Affected Hosts** | 192.168.14.35 |
| **Remediation** | Stronger input validation |

| **Vulnerability 3** | **Findings** |
| --- | --- |
| **Title** | XSS Stored |
| **Type (Web app / Linux OS / WIndows OS)** | Web App |
| **Risk Rating** | Critical |
| **Description** | Entered another script in the comments section. |
| **Images** |  |
| **Affected Hosts** | 192.168.14.35 |
| **Remediation** | XSS Protection |

| **Vulnerability 4** | **Findings** |
| --- | --- |
| **Title** |  |
| **Type (Web app / Linux OS / WIndows OS)** | Web App |
| **Risk Rating** | High |
| **Description** | Captured traffic using FoxyProxy and BurpSuite |
| **Images** |  |
| **Affected Hosts** | 192.168.14.35 |
| **Remediation** | Use HTTPS for more security |

| **Vulnerability 5** | **Findings** |
| --- | --- |
| **Title** |  |
| **Type (Web app / Linux OS / WIndows OS)** | Web App |
| **Risk Rating** | Critical |
| **Description** | Able to highlight web page to get flag 12. |
| **Imag**  **es** |  |
| **Affected Hosts** | 192.168.14.35 |
| **Remediation** | Fix HTML or PHP code |

| **Vulnerability 6** | **Findings** |
| --- | --- |
| **Title** |  |
| **Type (Web app / Linux OS / Windows OS)** | Web App |
| **Risk Rating** | Medium |
| **Description** | Found certificate information on crt.sh |
| **Images** |  |
| **Affected Hosts** |  |
| **Remediation** | Better security over totalrekall.xyz information |

| **Vulnerability 7** | **Findings** |
| --- | --- |
| **Title** | nmap |
| **Type (Web app / Linux OS / Windows OS)** | Linux OS |
| **Risk Rating** | Medium |
| **Description** | Scanned all available IP addresses within subnet |
| **Images** |  |
| **Affected Hosts** | 192.168.13.10  192.168.13.11  192.168.13.12  192.168.13.13  192.168.13.14 |
| **Remediation** | Block IPs from unauthorized parties |

| **Vulnerability 8** | **Findings** |
| --- | --- |
| **Title** |  |
| **Type (Web app / Linux OS / Windows OS)** | Windows OS |
| **Risk Rating** | Critical |
| **Description** | Able to access port 21 |
| **Images** |  |
| **Affected Hosts** |  |
| **Remediation** | Close port 21 |