| 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** | CyberDenfense |
| --- | --- |
| **Contact Name** | Stuart Koch |
| **Contact Title** | Penetration Tester |

## 

## Document History

| **Version** | **Date** | **Author(s)** | **Comments** |
| --- | --- | --- | --- |
| 001 | 10/26/2022 | Stuart Koch | Initial Report |

# 

## 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.

* High-level summary of strengths here
* NOTE: There were no notable security controls present to interfere with the penetration test.
* We expected to see some sort of firewall and antivirus set up. This was not found presently.

### 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.

* We first discovered a vulnerability that was a scripting vulnerability on the Rekall Corporation Website. This can be used by an attacker to inject malicious code.
* We also used the same vulnerability above to do command injection on the input method.
* We were able to use directory traversal to gain access to the root directory and access text files in it.
* We were able to use directory traversal to gain access to an admin account as the login credentials were saved in a text file.
* We also used directory traversal which gave us information about the SIEM used, the firewalls, cloud, and load balancer vendors. This could easily be used for further attacks.
* The upload function on the Rekall website to upload a .php file into the choose your adventure function.
* We also discovered that you can use the scripting vulnerability in the VR Planner sections under the who do you want to be search bar.
* We found this vulnerability using a domain name who is record and domain dossiers. We are able to see the SSH username for the admin using the OSINT framework. It also exposed the location of the server and the admin email too.
* We were able to run and address lookup on totalrekall.xyz to find the ip address. This could be used to further exploit the website.
* We ran an nmap scan against ip addresses to determine what hosts were up and accessible that we could possibly exploit.
* We found the language used for the apache server was Drupal using nmap this information can help narrow down more attack vectors.
* Next we ran a Network Discovery scan to view the machine's vulnerabilities.
* Then we used metasploit to start a session into the vulnerable machine using one of the vulnerabilities we found earlier.
* Then we used metasploit again to start a shell session so we could have access to machine files. We then viewed the /etc/passwd file.
* Then we used metasploit to download a file from the guest machine to the attacker machine.
* We used google dorking and googling to find the github of Totalrekall and discovered a username and hashed passwords in the repositories section.
* After finding the user trivera’s hashed password and username, we put them in a text file and hashed the file using John the Ripper.
* We then found the IP Address and found out port 80 was open.
* We then used metasploit to launch a meterpreter session and gain control of the machine as the system user.
* We used lsa\_dump\_sam in meterpreter we ended up finding a username and a a hashed password which we then cracked using John the Ripper.
* We then used the credentials we found earlier to run a payload using meterpreter as AUTHORITY/SYSTEM. Then within meterpreter we were able to obtain a hashed password and unhashed it using John the Ripper.

## Executive Summary

## 

## 

* CyberDefense began penetration testing activities on 22 October, 2022.
* Limitations were established based on agreements reached between CyberDefense and Rekall.
* Many of our attacks and exploits were successful in getting into Rekall’s environment.
* Initial reconnaissance was done using cross-site scripting and web injection vulnerability exploits.
* We were able to use command injection to inject scripts into multiple parts of Rekalls website.
* We were able to gain access to the root directory and other files using directory traversal to access sensitive text files.
* We were able to use directory traversal to gain access to an administrator account as the login was saved in a text file.
* We were able to gain access to a text file containing the vendors of networking and cloud equipment that could be valuable information to an attacker.
* We were able to upload potentially malicious files into the file uploader on the Choose your destination part of the website.
* We ran a scan against machines and found vulnerabilities that could be exploited.
* We were able to use these exploits to get into machines and view and make changes to sensitive information.
* Pentesters were able to penetrate the environment using credentials from text files saved on various machines.

CyberDefense ended pentesting on 26 October 2022.

## 

## 

## Summary Vulnerability Overview

| **Vulnerability** | **Severity** |
| --- | --- |
| Cross-Site Scripting vulnerabilities on website | **Medium** |
| Administrator Credentials saved in text files | **Critical** |
| User Credentials saved in a text files | **Low** |
| URL editing to gain access to root files | **High** |
| Employee contact information visible using who is | **Low** |
| Vulnerable ports and service open to the internet | **Critical** |
| Weak user passwords | **Medium** |
| Ability to upload script files to portions of the website | **Medium** |
| Used apache vulnerability to open up a shell on remote | **High** |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

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

| **Scan Type** | **Total** |
| --- | --- |
| Hosts | 192.168.13.13, |
| Ports | 80, 22, 21 |

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

## Vulnerability Findings

| **Vulnerability 1** | **Findings** |
| --- | --- |
| **Title** | Cross Site Scripting Vulnerabilities |
| **Type (Web app / Linux OS / WIndows OS)** | Web app |
| **Risk Rating** | Medium |
| **Description** | There was quite a few Cross-site scripting vulnerabilities on the Rekall website webapp. |
| **Images** |  |
| **Affected Hosts** |  |
| **Remediation** | Use input verification to verify the input so that scripts cannot be run in the input text boxes. |

| **Vulnerability 2** | **Findings** |
| --- | --- |
| **Title** | Administrator Credentials Saved in Text files |
| **Type (Web app / Linux OS / WIndows OS)** |  |
| **Risk Rating** | Critical |
| **Description** | Administrator login credentials saved in text files is insecure. |
| **Images** |  |
| **Affected Hosts** |  |
| **Remediation** | Have better user training on proper password practices. This will help prevent admin credentials from being stored in the future. |

| **Vulnerability 3** | **Findings** |
| --- | --- |
| **Title** | URL editing to gain access to root files |
| **Type (Web app / Linux OS / WIndows OS)** | web app |
| **Risk Rating** | High |
| **Description** | We used url modification to access the root file on webapp. |
| **Images** |  |
| **Affected Hosts** |  |
| **Remediation** | First you can put security controls in place so only non sensitive files are stored on the location that are facing the internet. |

| **Vulnerability 4** | **Findings** |
| --- | --- |
| **Title** | WHOIS registrar employee information open to public |
| **Type (Web app / Linux OS / WIndows OS)** | web app |
| **Risk Rating** | low |
| **Description** | WHOIS lookup gave us an admin username and the location of the server this can be used by an attacker. |
| **Images** |  |
| **Affected Hosts** |  |
| **Remediation** | You should try to avoid having at least the username and location out on the internet and try to keep the information as generic as possible. |

| **Vulnerability 5** | **Findings** |
| --- | --- |
| **Title** | No a |
| **Type (Web app / Linux OS / WIndows OS)** | Linux OS and Windows OS |
| **Risk Rating** | Vulnerable |
| **Description** | This could allow an attacker easy access to your company network and systems. |
| **Images** |  |
| **Affected Hosts** |  |
| **Remediation** | I also recommend a firewall with rules too as this will help prevent attacks like this in the future. |

| **Vulnerability 6** | **Findings** |
| --- | --- |
| **Title** | Allow scripts to be uploaded to upload functions of webapp |
| **Type (Web app / Linux OS / WIndows OS)** | web app |
| **Risk Rating** | medium |
| **Description** | We were successfully able to upload a php script by tricking the system into thinking it was a jpg file that could be used by a malicious actor to upload a malicious script into your system. |
| **Images** |  |
| **Affected Hosts** |  |
| **Remediation** | To set stricter limitations and parameters on what can be uploaded and what it will accept so that scripts cannot be uploaded. |

| **Vulnerability 7** | **Findings** |
| --- | --- |
| **Title** | Use apache vulnerability to open up a remote shell |
| **Type (Web app / Linux OS / WIndows OS)** | Linux OS |
| **Risk Rating** | High |
| **Description** | This in turn gave us control and access to the target machine. |
| **Images** |  |
| **Affected Hosts** |  |
| **Remediation** | The resolution for this would be to update and patch apache so that this vulnerability would be less likely to occur in the future. |

Add any additional vulnerabilities below.