| 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** | Ryan’s LLC |
| --- | --- |
| **Contact Name** | Ryan Whittaker |
| **Contact Title** | PenTester |

## 

## Document History

| **Version** | **Date** | **Author(s)** | **Comments** |
| --- | --- | --- | --- |
| 001 | 06/21/23 | Ryan | N/A |
| 002 | 06/22/23 | Ryan | N/A |
| 003 | 06/26/23 | Ryan | N/A |
| 004 | 06/29/23 | Ryan | N/A |

# 

## 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.

* Hired a team for current and continuing penetration testing to find and provide mitigation strategies for vulnerabilities
* Strategies in place for denying DDoS attacks to make sure the networks stays available
* Tools like Metasploit, Nmap utilized to prevent unauthorized access

### 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 being stored in HTML code on the web application
* The web application is vulnerable to SQL and XSS payload injections
* The apache web server is vulnerable due to being outdated
* There is unauthorized access to password hashes which allows the cracking of credentials and allows privilege escalation.
* SLMail server is vulnerable allowing for exploits resulting in gaining a shell
* There are credentials that can be located when doing IP lookups
* The physical server address for Rekall is available publicly
* Numerous open ports allow for file enumeration and unauthorized access
* When scanning Rekall’s IP range, it shows various potential vulnerabilities including IP addresses and open Ports.

## Executive Summary

**During the penetration testing of Rekall's IT assets, Ryan’s LLC successfully identified multiple vulnerabilities, including several critical ones that have the potential to cause severe harm to Rekall's revenue and reputation. Ryan’s LLC was able to infiltrate Rekall's assets, exfiltrate sensitive data, and escalate privileges within various systems.**

**The initial focus of the penetration testing was Rekall's web application. Ryan’s LLC discovered that the web application was susceptible to an XSS Reflected attack, allowing malicious scripts to be executed on the home page. Additionally, the web app was found to be vulnerable to Local File Inclusion, allowing file uploads through the VR Planner web page. Another vulnerability, an XSS Stored vulnerability, was identified on the Comments page, allowing the execution of scripting code. The Login.php toolbar was found to be susceptible to SQL Injection attacks, and the Networking.php page was vulnerable to Command Injection attacks.**

**Further investigation revealed that open source data was exposed and accessible through OSINT techniques, and a search on crt.sh unveiled a stored certificate. Shockingly, user login credentials were discovered to be stored in plain view within the HTML source code of the Login.php page, visible simply by highlighting the page in a web browser. The exposure of the file robots.txt was also detected, providing readily accessible information. Research uncovered user credentials in a Github repository, leading to unauthorized access to the web host's files and directories. Furthermore, it was determined that the Apache server was running an outdated version with a known Struts vulnerability.**

**Carrying on to the Windows OS environment, Ryan’s LLC found that FTP Port 21 and Port 110 (used for SLMail service) were both open and vulnerable. These vulnerabilities were discovered using Metasploit, which also enabled access to a password hash file that was subsequently cracked, allowing the creation of a reverse shell. Additionally, scheduled tasks were easily visible within the Windows 10 Machine Task Scheduler, and Metepreter was employed to display directories on public Windows directories.**

**Within the Linux environment, Ryan’s LLC identified five publicly exposed and vulnerable IP addresses, with one of the hosts running Drupal. Stolen credentials were utilized to gain access to one host and escalate privileges to root. Another vulnerability, a common known shell RCE execution vulnerability, was discovered using Meterpreter. The sudoers file was found to be accessible using a Shellshock exploit in Metasploit.**

**In summary, these vulnerabilities pose significant risks that could be exploited maliciously, resulting in substantial damage to Rekall's assets and overall business operations. Ryan’s LLC has provided detailed recommendations for mitigating each of these vulnerabilities to prevent potential harm and loss.**

## 

## 

## 

## Summary Vulnerability Overview

| **Vulnerability** | **Severity** |
| --- | --- |
| Local File Inclusion | **Critical** |
| Sensitive Data exposure | **Critical** |
| SQL Injection | **Critical** |
| Command Injection | **Critical** |
| User Credentials exposure | **Critical** |
| Apache Struts (CVE-2017-5638) | **Critical** |
| Linux Privilege escalation | **Critical** |
| IPs visible using Nmap | **Critical** |
| Drupal (CVE-2019-6340) | **Critical** |
| SLMail Port 110 exploited with Metasploit (SeattleMail) | **Critical** |
| Accessed system and used Kiwi to show password hashes | **Critical** |
| Shellshock (Port 80) on web server | **Critical** |
| Unauthorized Port 22 access | **Critical** |
| Exposed Data through Open Source means | **High** |
| Apache tomcat (CVE-2017-12617) | **High** |
| Port 21 FTP open | **High** |
| Sensitive information stored in a public documents folder | **High** |
| XSS Stored | **Medium** |
| XSS Reflected | **Medium** |
| Certificate search on Crt.sh | **Medium** |

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

| **Scan Type** | **Total** |
| --- | --- |
| Hosts | 172.22.117.10  172.22.117.20  192.168.13.10  192.168.13.11  192.168.13.12  192.168.13.13  192.168.13.14  192.168.14.35 |
| Ports | 21  22  80  110  8009  8080 |

| **Exploitation Risk** | **Total** |
| --- | --- |
| **Critical** | 13 |
| **High** | 4 |
| **Medium** | 3 |
| **Low** | 0 |

## Vulnerability Findings

| **Vulnerability 1** | **Findings** |
| --- | --- |
| **Title** | XSS Reflected |
| **Type (Web app / Linux OS / WIndows OS)** | Web App |
| **Risk Rating** | Medium |
| **Description** | Malicious Script successfully used on the home page on the Rekall site. Script used ( <script>alert(Hello There)</script> |
| **Images** |  |
| **Affected Hosts** | 192.168.14.35 |
| **Remediation** | Input validation |

| **Vulnerability 2** | **Findings** |
| --- | --- |
| **Title** | Local File Inclusion |
| **Type (Web app / Linux OS / WIndows OS)** | Web App |
| **Risk Rating** | Critical |
| **Description** | LFI successfully executed, uploaded a .php file on the VR planner page |
| **Images** |  |
| **Affected Hosts** | 192.168.14.35 |
| **Remediation** | Prevent file paths from being appended to directly |

| **Vulnerability 3** | **Findings** |
| --- | --- |
| **Title** | XSS Stored |
| **Type (Web app / Linux OS / WIndows OS)** | Web App |
| **Risk Rating** | Critical |
| **Description** | While accessing the comments page, used a script (<script>alert(“Hello”)</script> |
| **Images** |  |
| **Affected Hosts** | 192.168.14.35 |
| **Remediation** | Use XSS protection to stop script code from being injected |

| **Vulnerability 4** | **Findings** |
| --- | --- |
| **Title** | SQL Injection |
| **Type (Web app / Linux OS / WIndows OS)** | Web App |
| **Risk Rating** | Critical |
| **Description** | On the login.php page, used the payload of (Name or “1=1”) in the password field resulting in the exploit |
| **Images** |  |
| **Affected Hosts** | 192.168.14.35 |
| **Remediation** | Use character escaping or stop direct input on the web app |

| **Vulnerability 5** | **Findings** |
| --- | --- |
| **Title** | Command Injection |
| **Type (Web app / Linux OS / WIndows OS)** | Web App |
| **Risk Rating** | Critical |
| **Description** | Went to Networking.php and in the DNS check box, inserted [www.example.com](http://www.example.com) && cat vendors.txt which showed the exploiit |
| **Images** |  |
| **Affected Hosts** | 192.168.14.35 |
| **Remediation** | Use input validation |

| **Vulnerability 6** | **Findings** |
| --- | --- |
| **Title** | FTP enumeration |
| **Type (Web app / Linux OS / WIndows OS)** | Windows OS |
| **Risk Rating** | Critical |
| **Description** | Port 21 was open which allowed FTP enumeration. Connected on Host IP and was able to access and transfer out vulnerable files |
| **Images** |  |
| **Affected Hosts** | 172.22.117.20 |
| **Remediation** | Restrict Port 21 access |

| **Vulnerability 7** | **Findings** |
| --- | --- |
| **Title** | SLMail Exploit |
| **Type (Web app / Linux OS / WIndows OS)** | Windows OS |
| **Risk Rating** | Critical |
| **Description** | An open Port 110 allowed for an exploit through metasploit (windows/pop3/seattlelab\_pass) which resulted in a meterpreter session |
| **Images** |  |
| **Affected Hosts** | 172.22.117.20 |
| **Remediation** | Close Port 110 and replace the SLMail service |

| **Vulnerability 8** | **Findings** |
| --- | --- |
| **Title** | Sensitive Data/Credentials Dump |
| **Type (Web app / Linux OS / WIndows OS)** | Windows OS |
| **Risk Rating** | Critical |
| **Description** | Using the previous meterpreter session, gained access to vulnerable password files and a successful hash dump with the post/windows/gather/hashdump exploit. Then used John to crack the hashes and then used cracked credentials to gain a reverse shell |
| **Images** |  |
| **Affected Hosts** | 172.22.117.20 |
| **Remediation** | Update permissions on files to restrict access, and also move files to a less public domain |

| **Vulnerability 9** | **Findings** |
| --- | --- |
| **Title** | Public Directory search |
| **Type (Web app / Linux OS / WIndows OS)** | Windows OS |
| **Risk Rating** | Medium |
| **Description** | Inside of the Users\Public\Documents Directory there is a sensitive file viewed with the ls command. |
| **Images** |  |
| **Affected Hosts** | 172.22.117.20 |
| **Remediation** | Move sensitive files into more restricted areas instead of more publicly accessible directories |

| **Vulnerability 10** | **Findings** |
| --- | --- |
| **Title** | Windows 10 Machine Task Scheduler |
| **Type (Web app / Linux OS / WIndows OS)** | Windows OS |
| **Risk Rating** | Medium |
| **Description** | On the windows 10 machine, could view details on the scheduled tasks. |
| **Images** |  |
| **Affected Hosts** | 172.22.117.20 |
| **Remediation** | Change account permissions to deny access to unauthorized users |

| **Vulnerability 11** | **Findings** |
| --- | --- |
| **Title** | Open Source exposed Data |
| **Type (Web app / Linux OS / WIndows OS)** | Web App |
| **Risk Rating** | Medium |
| **Description** | You can view WHOIS info with OSINT for total rekall.xyz and see sensitive information |
| **Images** |  |
| **Affected Hosts** | https://centralops.net/co/DomainDossier.aspx |
| **Remediation** | Stop sensitive data from being shared publicly, make sure WHOIS records are cleaned up |

| **Vulnerability 12** | **Findings** |
| --- | --- |
| **Title** | Certificate Search via crt.sh |
| **Type (Web app / Linux OS / WIndows OS)** | Web app |
| **Risk Rating** | Medium |
| **Description** | Found stored certificate info for totalrekall.xyz on crt.sh site. |
| **Images** |  |
| **Affected Hosts** | 34.102.136.180 |
| **Remediation** | Protect Info from being exposed on sites like crt.sh |

| **Vulnerability 13** | **Findings** |
| --- | --- |
| **Title** | NMAP scan |
| **Type (Web app / Linux OS / WIndows OS)** | Linux OS |
| **Risk Rating** | Critical |
| **Description** | Running an Nmap scan on the 192.168.13.0/24 range returned 5 visible hosts with exposed IPs |
| **Images** |  |
| **Affected Hosts** | 192.168.13.10  192.168.13.11  192.168.13.12  192.168.13.13  192.168.13.14 |
| **Remediation** | Use IP blocking for unauthorized users |

| **Vulnerability 14** | **Findings** |
| --- | --- |
| **Title** | Aggressive Zenmap scan |
| **Type (Web app / Linux OS / WIndows OS)** | Linux OS |
| **Risk Rating** | Critical |
| **Description** | Ran an aggressive scan against 192.168.13.0.28 to discover a host running Drupal. |
| **Images** |  |
| **Affected Hosts** | 192.168.13.12 |
| **Remediation** | Block probes to the host, return restricted info or return incorrect info. |

| **Vulnerability 15** | **Findings** |
| --- | --- |
| **Title** | Users Credentials Exposed |
| **Type (Web app / Linux OS / WIndows OS)** | Web App |
| **Risk Rating** | Critical |
| **Description** | You can view users' credentials near the login boxes by highlighting the page or in the HTML. |
| **Images** |  |
| **Affected Hosts** | 192.168.14.35 |
| **Remediation** | Delete that info from the HTML and use two factor authentication |

| **Vulnerability 16** | **Findings** |
| --- | --- |
| **Title** | Sensitive data exposure |
| **Type (Web app / Linux OS / WIndows OS)** | Web App |
| **Risk Rating** | Medium |
| **Description** | Unrestricted access to the robots.txt page that sensitive |
| **Images** |  |
| **Affected Hosts** | 192.168.14.35 |
| **Remediation** | Deny access to robots.txt from unauthorized users. |

| **Vulnerability 17** | **Findings** |
| --- | --- |
| **Title** | Nessus Scan |
| **Type (Web app / Linux OS / WIndows OS)** | Web App |
| **Risk Rating** | Medium |
| **Description** | There was an Apache struts vulnerability found in the nessus scan |
| **Images** |  |
| **Affected Hosts** | 192.168.13.12 |
| **Remediation** | Update Apache |

| **Vulnerability 18** | **Findings** |
| --- | --- |
| **Title** | Username and Password hash in Github Repo |
| **Type (Web app / Linux OS / WIndows OS)** | Web App |
| **Risk Rating** | Critical |
| **Description** | With credentials found in Github, I cracked the password hash and could login successfully. |
| **Images** |  |
| **Affected Hosts** | Rekall web server |
| **Remediation** | Make sure credentials aren’t stored in github and Restrict access |

| **Vulnerability 19** | **Findings** |
| --- | --- |
| **Title** | Meterpreter Shell RCE (CVE 2017-5638) |
| **Type (Web app / Linux OS / WIndows OS)** | Linux OS |
| **Risk Rating** | Critical |
| **Description** | Using Meterpreter, the multi/http/struts2\_content\_type\_ongl exploit was used with the Payload= linux/x86/shell\_reverse\_tcp |
| **Images** |  |
| **Affected Hosts** | 192.168.13.12 |
| **Remediation** | Apply updates based on vendor |

| **Vulnerability 20** | **Findings** |
| --- | --- |
| **Title** | Escalated Privileges |
| **Type (Web app / Linux OS / WIndows OS)** | Linux OS |
| **Risk Rating** | Critical |
| **Description** | Able to use SSH to gain escalated privileges using stolen user info. |
| **Images** |  |
| **Affected Hosts** | 192.168.13.14 |
| **Remediation** | Require stronger login info, Restrict use of port 22. |