| 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** | FastChips, LLC |
| --- | --- |
| **Contact Name** | Chirag Shah |
| **Contact Title** |  |

## 

## Document History

| **Version** | **Date** | **Author(s)** | **Comments** |
| --- | --- | --- | --- |
| 001 | 4/24/2023 | Chirag Shah |  |

# 

## 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.

* Data input verification on web application, some input fields properly verified data
* User: Administrator on Windows machine has a complex password that was unable to be compromised by using John the Ripper.

### 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.

Web App Vulnerabilities:

* Login credentials exposed on web application
* XSS Stored and Reflected vulnerabilities
* sensitive data (robots.txt) accessible on web application
* Local file inclusion vulnerability
* SQL injection vulnerability

Linux Vulnerabilities:

* SSH user information readily available on who.is
* nmap scan shows CVE-2019-6340 Drupal vulnerability
* HTTP port vulnerable to exploit
* weak user password
* privilege escalation vulnerability

Windows Vulnerabilities:

* Password hash posted on github
* confidential .txt file accessible from web browser
* Nmap scan reveals SLMail vulnerability
* Anonymous FTP login vulnerability
* Kiwi vulnerability to expose password ntlm hashes
* DCSync exploitable to view Administrator password hash
* Windows PSExec Vulnerability (SMB)

## Executive Summary

During the penetration test of Rekall Corp, multiple vulnerabilities were exposed and exploited to gain access to Rekall Corp’s network. Vulnerabilities were discovered on the web application, on the Linux server, as well as multiple Windows machines.

Testing of Rekall Corps’s web application revealed that it was vulnerable to Local File Inclusion, allowing a file to be uploaded to the webpage and run a script to reveal sensitive data. The web application was also vulnerable to XSS Reflected and Stored attacks, the Comments page allowed the stored xss attack, and the home page allowed for an xss reflected attack. SQL Injection attack was used on the login page to expose sensitive information. Administrator login credentials were easily viewable on the login page, and the files robots.txt and vendors.txt exposed DNS Check vulnerability.

Testing of Rekall Corp’s Linux server revealed that it was vulnerable to SSH due to weak password, and user information readily available online. Nmap scans also revealed multiple Drupal and HTTP vulnerabilities, which were exploited to gain access to the server and escalate privileges to root level.

The Windows machines were tested to reveal several open ports, including FTP on port 21 and SLMail on port 110. Login credentials were readily available on github, and these stolen credentials were used to gain access to the Windows machines. Sensitive data was viewable from a web browser, and Kiwi was utilized to expose multiple user password hashes, including Administrator. Compromised login credentials were used to gain access to the Domain Controller and escalate privileges to SYSTEM level.

## 

## 

## 

## 

## Summary Vulnerability Overview

| **Vulnerability** | **Severity** |
| --- | --- |
| Login Credentials exposed on Web Application | **Critical** |
| Web Application vulnerable to Stored and Reflected XSS Attacks | **High** |
| Sensitive Data accessible on Web Application | **Medium** |
| Web Application Vulnerable to Local File Inclusion Attacks | **Critical** |
| Web Application Vulnerable to SQL Injection Attacks | **Critical** |
| SSH User Information Exposed on Internet (who.is) | **Critical** |
| Nmap Scan Exposes Drupal Vulnerability | **Critical** |
| Struts - CVE-2017-5638 HTTP Port Vulnerability | **High** |
| Weak User Password | **Critical** |
| Sudoers Exploit Used to Escalate Privileges to Root | **Critical** |
| Windows Machine Username and Password Hash posted on Github | **Critical** |
| Sensitive Data (.txt) Accessible from Web Browser | **Medium** |
| Windows PSExec Vulnerability | **Critical** |
| Anonymous FTP Login Vulnerability (Port 21) | **Critical** |
| Kiwi Exploit To Expose Password Hashes | **High** |
| DCSync Exploitable to view Administrator Password Hash | **High** |
| SLMail Vulnerability (SMB) | **Critical** |

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

| **Scan Type** | **Total** |
| --- | --- |
| Hosts | 192.168.13.10  192.168.13.11  192.168.13.12  192.168.13.13  192.168.13.14  192.168.13.35  172.22.117.10  172.22.117.20 |
| Ports | 21, 22, 80, 8080, 110 |

| **Exploitation Risk** | **Total** |
| --- | --- |
| **Critical** | 11 |
| **High** | 4 |
| **Medium** | 2 |
| **Low** | 0 |

## Vulnerability Findings

| **Vulnerability 1** | **Findings** |
| --- | --- |
| **Title** | Login Credentials Exposed on Web Application |
| **Type (Web app / Linux OS / WIndows OS)** | Web Application |
| **Risk Rating** | Critical |
| **Description** | Login credentials for Admin were in plain view on the login page. Simply highlighting the page revealed the username as well as the password. |
| **Images** |  |
| **Affected Hosts** | 192.168.14.35 |
| **Remediation** | Remove login credential information from HTML file. |

| **Vulnerability 2** | **Findings** |
| --- | --- |
| **Title** | Web Application Vulnerable to Stored and Reflected XSS Attacks |
| **Type (Web app / Linux OS / WIndows OS)** | Web Application |
| **Risk Rating** | High |
| **Description** | XSS Reflected Vulnerability exploited by entering <script>alert</script> in the Name field on the home page. The XSS Stored Vulnerability can be exploited by entering the same command in the Comments section of the web application. |
| **Images** |  |
| **Affected Hosts** | 192.168.14.35 |
| **Remediation** | Input validation to prevent the running of a script in the data input field. |

| **Vulnerability 3** | **Findings** |
| --- | --- |
| **Title** | Sensitive Data (robots.txt) accessible on Web Application |
| **Type (Web app / Linux OS / WIndows OS)** | Web Application |
| **Risk Rating** | Medium |
| **Description** | Navigating to the Disclaimer page of the web application and editing the end of the address field to page=robots.txt reveals unintended information. |
| **Images** |  |
| **Affected Hosts** | 192.168.14.35 |
| **Remediation** | Move sensitive data files to different directory so they cannot be accessed from the web application. |

| **Vulnerability 4** | **Findings** |
| --- | --- |
| **Title** | Local File Inclusion Vulnerability |
| **Type (Web app / Linux OS / WIndows OS)** | Web Application |
| **Risk Rating** | Critical |
| **Description** | Vulnerability exploited by uploading a local .php file into the Planner page. |
| **Images** |  |
| **Affected Hosts** | 192.168.14.35 |
| **Remediation** | Restrict uploading of files to allow only requested file types and prevent uploaded files from being able to execute directly. |

| **Vulnerability 5** | **Findings** |
| --- | --- |
| **Title** | SQL Injection Vulnerability |
| **Type (Web app / Linux OS / WIndows OS)** | Web Application |
| **Risk Rating** | Critical |
| **Description** | Inputting OR ‘1=1 in the password field of the login page results in a successful SQL Injection Vulnerability Exploit. |
| **Images** |  |
| **Affected Hosts** | 192.168.14.35 |
| **Remediation** | Implement input validation to disallow direct input. |

| **Vulnerability 6** | **Findings** |
| --- | --- |
| **Title** | SSH User Information Readily Available online (Port 22) |
| **Type (Web app / Linux OS / WIndows OS)** | Linux OS |
| **Risk Rating** | Critical |
| **Description** | Online search for totalrekall.xyz reveals registrar data, including sshUser Information. |
| **Images** |  |
| **Affected Hosts** | totalrekall.xyz domain |
| **Remediation** | Remove or modify company information to hide specific user data, especially user ssh credentials. |

| **Vulnerability 7** | **Findings** |
| --- | --- |
| **Title** | Nmap Scan shows CVE-2019-6340 Drupal Vulnerability |
| **Type (Web app / Linux OS / WIndows OS)** | Linux OS |
| **Risk Rating** | Critical |
| **Description** | Aggressive NMAP scan reveals this machine to be running an exploitable Drupal vulnerability. Used Metasploit module exploit/unix/webapp/drupal\_restws\_unserialize to exploit vulnerability and gain access to machine. |
| **Images** |  |
| **Affected Hosts** | 192.168.13.13 |
| **Remediation** | Block scans of machines on the network, apply updates and security patches to minimize exploitable vulnerabilities. |

| **Vulnerability 8** | **Findings** |
| --- | --- |
| **Title** | Struts - CVE-2017-5638 TCP Reverse Shell Vulnerability (Port 80) |
| **Type (Web app / Linux OS / WIndows OS)** | Linux OS |
| **Risk Rating** | High |
| **Description** | Used msfconsole with module exploit/multi/http/struts2\_content\_type\_ognl to exploit struts vulnerability and gain access to the machine. |
| **Images** |  |
| **Affected Hosts** | 192.168.13.12 |
| **Remediation** | Apply updates and security patches to minimize exploitable vulnerabilities. |

| **Vulnerability 9** | **Findings** |
| --- | --- |
| **Title** | Weak User Password |
| **Type (Web app / Linux OS / WIndows OS)** | Linux OS |
| **Risk Rating** | Critical |
| **Description** | Using ssh login credentials obtained from online search and guessing passwords for user alice reveals the password to be the same as the username: alice |
| **Images** |  |
| **Affected Hosts** | 192.168.13.14 |
| **Remediation** | Enforce requirements for complex passwords from all users. |

| **Vulnerability 10** | **Findings** |
| --- | --- |
| **Title** | Sudoers Privilege Escalation Exploit (Port 22) |
| **Type (Web app / Linux OS / WIndows OS)** | Linux OS |
| **Risk Rating** | Critical |
| **Description** | Entering command sudo -u#-1 /bin/bash allows privilege escalation from user alice to user root. |
| **Images** |  |
| **Affected Hosts** | 192.168.13.14 |
| **Remediation** | Close SSH port 22. |

| **Vulnerability 11** | **Findings** |
| --- | --- |
| **Title** | Password Hash Posted on Github |
| **Type (Web app / Linux OS / WIndows OS)** | Windows OS |
| **Risk Rating** | Critical |
| **Description** | Online search for rekall on github reveals username and password hash. Using John the Ripper shows password to be Tanya4life for user: trivera. |
| **Images** |  |
| **Affected Hosts** | totalrekall domain |
| **Remediation** | Remove sensitive login credentials from github, implement stronger passwords. |

| **Vulnerability 12** | **Findings** |
| --- | --- |
| **Title** | Sensitive .txt File accessible from Web Browser |
| **Type (Web app / Linux OS / WIndows OS)** | Windows OS |
| **Risk Rating** | Medium |
| **Description** | Navigating to IP address of Windows machine 172.22.117.20/flag2.txt reveals unintended information. |
| **Images** |  |
| **Affected Hosts** | 172.22.117.20 |
| **Remediation** | Move sensitive data files to different directory, not accessible from web browser. |

| **Vulnerability 13** | **Findings** |
| --- | --- |
| **Title** | Windows Psexec (SMB) Vulnerability |
| **Type (Web app / Linux OS / WIndows OS)** | Windows OS |
| **Risk Rating** | Critical |
| **Description** | Used msfconsole exploit /windows/smb/psexec to gain access to the domain controller using compromised credentials of ADMBob password: Changeme! and was able to get SYSTEM level privileges. |
| **Images** |  |
| **Affected Hosts** | 172.22.117.10 |
| **Remediation** | Restrict access to sensitive files, apply security patches and updates to minimize vulnerabilities. |

| **Vulnerability 14** | **Findings** |
| --- | --- |
| **Title** | FTP Port Vulnerability (Port 21) |
| **Type (Web app / Linux OS / WIndows OS)** | Windows OS |
| **Risk Rating** | Critical |
| **Description** | Nmap scan revealed FTP Port 21 to be open. Attempted FTP with anonymous credentials and successfully exfiltrated sensitive data. |
| **Images** |  |
| **Affected Hosts** | 172.22.117.20 |
| **Remediation** | Close FTP Port 21 |

| **Vulnerability 15** | **Findings** |
| --- | --- |
| **Title** | NTLM Password Hashes Exposed with Kiwi |
| **Type (Web app / Linux OS / WIndows OS)** | Windows OS |
| **Risk Rating** | High |
| **Description** | Used Kiwi to dump password hashes, then used John the Ripper to crack password hashes. Obtained password for user:flag6 password: Computer! |
| **Images** |  |
| **Affected Hosts** | 172.22.117.20 |
| **Remediation** | Restrict access to sensitive data by modifying permissions. |

| **Vulnerability 16** | **Findings** |
| --- | --- |
| **Title** | DCSync Exploit to View Administrator Password Hash |
| **Type (Web app / Linux OS / WIndows OS)** | Windows OS |
| **Risk Rating** | High |
| **Description** | Loaded Kiwi and used meterpreter command dcsync\_ntlm Administrator to obtain NTLM password hash for user:Administrator. Attempted to use John the Ripper to crack password but was unsuccessful. |
| **Images** |  |
| **Affected Hosts** | 172.22.117.10 |
| **Remediation** | Apply updates and security patches as available, close unnecessary ports. User Administrator has complex password that was not compromised by John the Ripper. |

| **Vulnerability 17** | **Findings** |
| --- | --- |
| **Title** | SLMail Vulnerability |
| **Type (Web app / Linux OS / WIndows OS)** | Windows OS |
| **Risk Rating** | Critical |
| **Description** | Used msfconsole exploit/windows/pop3/seattlelab\_pass to exploit TCP reverse shell vulnerability and gained access to the machine. |
| **Images** |  |
| **Affected Hosts** | 172.22.117.20 |
| **Remediation** | Apply updates and security patches to minimize vulnerabilities. Close Unnecessary ports and exploitable services. |