| 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** | Evans Pentesting LLC |
| --- | --- |
| **Contact Name** | Hassan Evans |
| **Contact Title** | CEO |

## 

## Document History

| **Version** | **Date** | **Author(s)** | **Comments** |
| --- | --- | --- | --- |
| 001 | 04/20/2025 | Hassan Evans | DAY 1 |
| 002 | 04/22/2025 | Hassan Evans | DAY 2 |
| 003 | 04/26/2025 | Hassan Evans | DAY 3 |
| 004 | 04/28/2025 | Hassan Evans | SUMMARY |

# 

## 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 a 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 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.

* Antimalware is up to date

### Summary of Weaknesses

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

* Local File Inclusion
* Sensitive Data Exposure
* XXS Vulnerabilities
* Data Exposure
* User permissions
* Safeguard password hashes
* Remove usernames from open-source websites
* Update and patch the software

## Executive Summary

Evans Pentesting LLC conducted a comprehensive security assessment of Rekall to identify vulnerabilities and provide remediation recommendations to strengthen the organization's overall security.

The assessment began with reconnaissance of the Rekall web application hosted at 192.168.14.35. Various scanning scripts were executed to detect potential security weaknesses, including local file inclusion (LFI) vulnerabilities that allowed unauthorized access to sensitive areas of the website.

On Day 2, the assessment expanded to include external sources. Using Domain Dossier, we performed a WHOIS lookup on totalrekall.xyz, uncovering additional information that revealed vulnerabilities. An nslookup was also conducted to identify exposed network configurations. Further analysis was carried out through SSL, where additional weaknesses were found. We executed multiple Nmap scans, including aggressive scanning techniques, and ran a Nessus vulnerability scan against the IP address 192.168.13.12. Exploitation efforts targeted a misconfigured Tomcat server, leading to the discovery of critical vulnerabilities.

On Day 3, a GitHub website was found containing a username and a hashed password. Using these credentials, we were able to uncover further vulnerabilities. Additional Nmap scans revealed open ports. We also performed an FTP scan on the IP address 172.22.117.20, which exposed more weaknesses. Exploits such as SLMail and load Kiwi were utilized to successfully identify further vulnerabilities. Finally, sensitive data in the files was located within /Users/Public/Documents, leading to additional findings.

Throughout the engagement, tools such as Metasploit, Nessus, Nmap, and various scripts were instrumental in identifying security issues. Based on these results, we are providing actionable recommendations to Rekall to mitigate the identified vulnerabilities and enhance the security of their systems and data against potential cyber threats.

## 

## 

## 

## 

## Summary Vulnerability Overview

| **Vulnerability** | **Severity** |
| --- | --- |
| Day 1  Flag1 Welcome XSS Script | **HIGH** |
| XSS memory-planner | **HIGH** |
| XSS Stored Vulnerabilites | **HIGH** |
| Sensitive Data | **LOW** |
| Local File Inclusion memory-planner | **HIGH** |
| local file inclusion Vulnerability | **HIGH** |
|  |  |
|  |  |
| Day 2  flag1 Open source exposed data | **LOW** |
| nslookup totalrekall.xyz | **LOW** |
| SSL and CRT | **LOW** |
| nmap scan | **MEDIUM** |
| aggressive nmap scan | **HIGH** |
| nessus scan | **CRITICAL** |
| APACHE Struts | **CRITICAL** |
| Day 3  Flag 1 Unprotected user information | **LOW** |
| nmap scan 172.22.117.0/24 | **MEDIUM** |
| FTP 172.22.117.20 | **MEDIUM** |
| SLMAIL | **MEDIUM** |
| SCHEDULE TASK VULNERABILITY | **MEDIUM** |
| LOAD KIWI | **CRITICAL** |
| DATA EXPOSURE | **CRITICAL** |

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

| **Scan Type** | **Total** |
| --- | --- |
| Hosts | Totalrekall.xyz  192.168.13.10  192.168.13.11  192.168.13.12  192.168.13.13  192.168.13.14  192.168.13.1  172.22.117.20 |
| Ports | linux  110  4444  Windows  21  25  53  80  110 |

| **Exploitation Risk** | **Total** |
| --- | --- |
| **Critical** | 3 |
| **High** | 6 |
| **Medium** | 5 |
| **Low** | 5 |

## Vulnerability Findings

| **Day 1 Flag 1** | **Findings** |
| --- | --- |
| **Title** | Welcome page XSS SCRIPT |
| **Type (Web app / Linux OS / WIndows OS)** | web app |
| **Risk Rating** | critical |
| **Description** | First, make sure you have Docker running in your terminal. Then head over to the http://192.168.14.35. Click on the welcome tab on the website. You will then need to enter the XSS script where it says put your name here. You then click on go and the flag 1 will then appear. |
| **Images** |  |
| **Affected Hosts** | 192.168.14.35/Welcome.php |
| **Remediation** | Implement validation. |

| **Day1 Flag 2** | **Findings** |
| --- | --- |
| **Title** | XSS memory-planner |
| **Type (Web app / Linux OS / WIndows OS)** | Web app |
| **Risk Rating** | critical |
| **Description** | At the bottom of the 192.168.14.35/welcome.php page is a box that says “click here to start planning.” Once you click that box, you will end up at the 192.168.14.35/Memory-planner.php. You will then enter the second script which is <SCRIPTscripT>alert(“hi”)</SCRIPTscripTt> in the choose your character field which leads to flag number 2. |
| **Images** |  |
| **Affected Hosts** | 192.168.14.35/Memory-planner.php |
| **Remediation** |  |

| **Day 1 Flag 3** | **Findings** |
| --- | --- |
| **Title** | comments page |
| **Type (Web app / Linux OS / WIndows OS)** | Web OS |
| **Risk Rating** | HIGH |
| **Description** | While on the rekall website we went over to the comments page and entered in the XXS script which gave us flag 3 |
| **Images** |  |
| **Affected Hosts** | 192.168.14.35 |
| **Remediation** | XXS vulnerability. |

| **Day 1 Flag 4** | **Findings** |
| --- | --- |
| **Title** | Sensitive data |
| **Type (Web app / Linux OS / WIndows OS)** | Web App |
| **Risk Rating** | low |
| **Description** | I ran the command curl -v <http://192.168.14.35/about>-rekall.php. curl -v means very verbose mode, which shows the entire request and response. It showed detailed information about the connection of the website. It also showed flag 4 which was listed. |
| **Images** |  |
| **Affected Hosts** | 192.168.14.35/About-Rekall.php |
| **Remediation** | Comments in the curl |

| **Day 1 Flag 5** | **Findings** |
| --- | --- |
| **Title** | Local File Inclusion- Memory Planner |
| **Type (Web app / Linux OS / WIndows OS)** | Web OS |
| **Risk Rating** | High |
| **Description** | Creating a test file as a .php and uploading the file into the “Browse” field. |
| **Images** |  |
| **Affected Hosts** | 192.168.14.35/Memory-Planner.php |
| **Remediation** | Don't include files on the web server. That can lead to the website being compromised. |

| **Day 1 Flag 6** | **Findings** |
| --- | --- |
| **Title** | Local File Inclusion vulnerability |
| **Type (Web app / Linux OS / WIndows OS)** | Web OS |
| **Risk Rating** | Medium |
| **Description** | Create a file with the .jpg or .php extension and upload it into the location field. |
| **Images** |  |
| **Affected Hosts** | memory planner.php |
| **Remediation** | Don't allow files on the web server that can be compromised. |

| **Day 2 Flag 1** | **Findings** |
| --- | --- |
| **Title** | Domain Dossier |
| **Type (Web app / Linux OS / WIndows OS)** | Web app |
| **Risk Rating** | High |
| **Description** | I navigated through osnitframework.com. Domain name was my first click, next was WhoisRecords, and Domain Dossier was the last click. which then lead me to the website [Domain Dossier - Investigate domains and IP addresses, get owner and registrar information, see whois and DNS records](https://centralops.net/co/DomainDossier.aspx). I then looked up totalrekall.xyz by checking the domain whois record box on that page. Flag 1 was located on this page. |
| **Images** |  |
| **Affected Hosts** | totalrekall.xyz |
| **Remediation** | Remove sensitive data from this website. |

| **Day 2 Flag 2** | **Findings** |
| --- | --- |
| **Title** | DNS records for totalrekall.xyz |
| **Type (Web app / Linux OS / WIndows OS)** | linux OS |
| **Risk Rating** | low |
| **Description** | First, I ran the nslookup for totalrekall.xyz. Nslookup asks for information like IP address and other records. I wanted a more specific search, so I searched nslookup -type=TXT totalrekall.xyz. This search gives me all the records with txt in them, which led to me finding the flag, which is (7sk67cjsdbs). |
| **Images** |  |
| **Affected Hosts** | totalrekall.xyz |
| **Remediation** | Delete any records of any TXT in the TXT records. Also, do regular checks to make sure no data is in there. |

| **Day 2 Flag 3** | **Findings** |
| --- | --- |
| **Title** | SSL AND CRT |
| **Type (Web app / Linux OS / WIndows OS)** | Web App |
| **Risk Rating** | low |
| **Description** | crt.sh is an open-source website. I typed in totalrekall.xyz in the search bar. which led to me finding flag 3. |
| **Images** |  |
| **Affected Hosts** | totalrekall.xyz |
| **Remediation** | Limit DNS records |

| **Day 2 Flag 4** | **Findings** |
| --- | --- |
| **Title** | Nmap scan |
| **Type (Web app / Linux OS / WIndows OS)** | Linux |
| **Risk Rating** | Critical |
| **Description** | Inside Kali, I ran an nmap scan. The command I used was nmap -sn 192.168.13.0/24. I got back 6 scanned hosts. host 5 which lead me to finding flag 4. |
| **Images** |  |
| **Affected Hosts** | 192.168.13.10 192.168.13.11 192.168.13.12 192.168.13.13 192.168.13.14 192.168.13.1 |
| **Remediation** | Block unauthorized users. |

| **Day 2 Flag 5** | **Findings** |
| --- | --- |
| **Title** | Aggressive Nmap scan |
| **Type (Web app / Linux OS / WIndows OS)** | Linux OS |
| **Risk Rating** | Critical |
| **Description** | I ran an aggressive nmap -A 192.168.13.0/24. The results show the Drupal host, which was 192.168.13.13. |
| **Images** |  |
| **Affected Hosts** | 192.168.13.13 |
| **Remediation** | prevent probes |

| **Day 2 Flag 6** | **Findings** |
| --- | --- |
| **Title** | Nessus scan |
| **Type (Web app / Linux OS / WIndows OS)** | Web OS |
| **Risk Rating** | Medium |
| **Description** | Went to the Nessus website to run a basic network scan for 192.168.13.12. After running the search, I got about 15 vulnerabilities, one of which was critical. The critical vulnerability gave me all the details, plus the ID, which was the flag 97610. |
| **Images** |  |
| **Affected Hosts** | 192.168.13.12 |
| **Remediation** | Patch software, and do weekly checkups to make sure no new vulnerabilities. |

| **Day 2 Flag 7** | **Findings** |
| --- | --- |
| **Title** | Apache |
| **Type (Web app / Linux OS / WIndows OS)** | Linux OS |
| **Risk Rating** | Critical |
| **Description** | I ran msfconsole inside of Kali to search for the Metasploit Apache Tomcat RCE. Used the 6 exploit for all the exploits that popped up. Set the RHOST to 192.168.13.10, then ran the exploit. First, I typed ls -l to list all files and directories. I needed a more specific search, so I searched for find-type f -iname “\**flag*\*”, which searches for any file with the term flag. I see root/.flag7.txt. I then changed my directory back to root, then ran the cat .flag7.txt to see what was inside the file. Which led to me finding flag 7. |
| **Images** |  |
| **Affected Hosts** | 192.168.13.10 |
| **Remediation** | patch apache. |

| **Day 3 flag 1** | **Findings** |
| --- | --- |
| **Title** | totalrekall github page discovery |
| **Type (Web app / Linux OS / WIndows OS)** | web app |
| **Risk Rating** | critical |
| **Description** | Researching the website, we came across the findings of a user and a password hash. The user name was trivera. |
| **Images** |  |
| **Affected Hosts** | totalrekall github website. |
| **Remediation** | Remove the user name and password hash from GitHub. |

| **Day 3 Flag 2** | **Findings** |
| --- | --- |
| **Title** | Nmap 172.22.117.0/24 scan |
| **Type (Web app / Linux OS / WIndows OS)** | linux OS |
| **Risk Rating** | critical |
| **Description** | ran nmap for IP address 172.22.117.0/24. The scan gave me the IP address 172.22.117.20 with the open ports of 80 and 443, which are http and https. In the URL I typed 172.22.117.20, and I got the prompt to enter the username and password I got from flag one which was, which led to me getting flag2 |
| **Images** |  |
| **Affected Hosts** | 172.22,117.20 |
| **Remediation** | Enforce 2FA (two factor authentication) |

| **DAY 3 FLAG 3** | **Findings** |
| --- | --- |
| **Title** | FTP 172.22.117.20 |
| **Type (Web app / Linux OS / WIndows OS)** | LINUX OS |
| **Risk Rating** | MEDIUM |
| **Description** | I first ran an nmap of 172.22.117.20. The results from the nmap show that port 21 FTP is open. I then ran FTP 172.22.117.20. I got access and used the anonymous name, leaving the password empty. The next command I ran was get flag3.txt. I ran exit to get back to Kali, and then I ran the command cat flag3.txt, and that displayed the flag |
| **Images** |  |
| **Affected Hosts** | 172.22.117.20 |
| **Remediation** | Use SFTP over FTP. SFTP has a more secure encryption and is more firewall-friendly. |

| **DAY 3 FLAG 4** | **Findings** |
| --- | --- |
| **Title** | SLMAIL SERVICE |
| **Type (Web app / Linux OS / WIndows OS)** | linux OS |
| **Risk Rating** | MEDIUM |
| **Description** | I ran nmap -A 172.22.117.20 gives all the open ports, OS detection, and version detection. The results show port 110 and the SLMail exploit. I then ran msfconsole and searched slmail. I used the exploit and went to the options to make the changes. I set the LHOST to 172.22.117.100 and RHOST to 172.22.117.20. Lhost is the local host (me), and Rhost is the remote host (them). Once that was complete, i ran the run command to run the exploit. Once I get access, I ran the ls command and the flag4.txt is the first file. |
| **Images** |  |
| **Affected Hosts** | 172.22.117.20 |
| **Remediation** | close port 110 |

| **DAY 3 FLAG 5** | **Findings** |
| --- | --- |
| **Title** | TASK SCHEDULER |
| **Type (Web app / Linux OS / WIndows OS)** | WINDOWS OS |
| **Risk Rating** | MEDIUM |
| **Description** | While using the previous metasploit I ran schtasks/ query to get a list of scheduled tasks. while seeing the schedule tasks i found flag5 |
| **Images** |  |
| **Affected Hosts** | 172.22.117.20 |
| **Remediation** | Patch system to make sure patches are up to date. |

| **DAY 3 FLAG 6** | **Findings** |
| --- | --- |
| **Title** | LOAD KIWI |
| **Type (Web app / Linux OS / WIndows OS)** | LINUX OS |
| **Risk Rating** | CRITICAL |
| **Description** | While still in the exploit of SLmail, I ran the command load kiwi, which is an extension. I then ran the command lsa\_dump\_sam, and it revealed flag6. |
| **Images** |  |
| **Affected Hosts** | 172.22.117.20 |
| **Remediation** | Store password hashes more securely. |

| **Day 3 Flag 7** | **Findings** |
| --- | --- |
| **Title** | Sensitive data exposure |
| **Type (Web app / Linux OS / WIndows OS)** | WINDOWS OS |
| **Risk Rating** | MEDIUM |
| **Description** | While inside meterpreter i ran the command cd /Users/Public?Documents. I then ran the ls command to get a list of all files and directories. flag7.txt was listed at the bottom. Ran cat flag7.txt to get the flag. |
| **Images** |  |
| **Affected Hosts** | 172.22.117.20 |
| **Remediation** | Search and find all sensitive or confidential data. Delete information if necessary. Then, change the permissions to ensure no one can have access to these files. |