| 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** | M&M Hackers |
| --- | --- |
| **Contact Name** | Mutasem Ayyoush |
| **Contact Title** | Penetration Tester |

## 

## Document History

| **Version** | **Date** | **Author(s)** | **Comments** |
| --- | --- | --- | --- |
| 001 | 09/28/2023 | Mutasem Ayyoush | critical vulnerabilities were found and to be remediated. |

# 

## 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
* M&M hackers did not succeed with the use of SQL injections against the web page.
* A few Web Application input fields are strongly secured against certain XSS attacks that require further research.
* The web application was easy to navigate through and user friendly.
* Inputting scripts did not work on certain pages of the website.

### 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.

* High-level summary of weaknesses here
* The Web application is vulnerable to multiple types of attacks, such as XSS scripting, Local File Inclusion, and Command Injections, which allow attackers to obtain confidential information and upload malicious scripts that are stored in Rekall’s host.
* Both Linux and Windows operating systems have been impacted by sensitive data exposure causing confidential information easily available to attackers who may have breached the system.
* Nmap scans detected multiple open ports, indicating vulnerabilities across the entire host.
* Kiwi and search operators were utilized to crack the passwords of multiple active users and get their login details.
* Critical vulnerabilities such as Shellshock, SLMail pop3d, and Apache Tomcat Remote Code Execution, were discovered on the Windows and Linux systems.
* Using the OSINT tools exposed information that can help attackers with their attacks and find weaknesses.

## Executive Summary

[Provide a narrative summary of your steps and findings, including screenshots. It’s fine to mention specifics (e.g., used Metasploit to exploit a vulnerable version of DistCC), but do not get too technical in these specifics. This should be an A–Z summary of your assessment.]

M&M hackers participated in a penetration testing for Rekall’s networking system during the last week of September and first week of October. The penetration testing was done by Mutasem Ayyoush and found multiple vulnerabilities within Rekal’sl cyber framework. Based on our findings,the company is lacking effective security measures which resulted in a large number of vulnerabilities being vulnerable to attack across the entire network. Important information such as active employees login credentials have been revealed to the public on the web application and network host. We used a popular tool called nmap and identified which ports were open that were not secured and the type of services behind those ports. These unprotected ports are a serious vulnerability that may allow hackers total access to the network and give them the opportunity to attack it. We found out a malicious script may be performed on the main page which is exposed to an XSS Reflected attack. Totalrekall’s website is at risk of local file inclusion which malicious php files can successfully be uploaded to the host. On the comments page, there is an XSS Stored vulnerability that allows a scripting code to be executed. An injection attack is also executable on the networking.php and login php pages by a command injection which is very critical. The admin login credentials were stored in the html code file which can also be revealed by highlighting the login.php page. We applied a searching operator to identify the robots.txt file which is accessible to the public and considered vulnerable resulting in confidential information to be exposed.

In the linux operating system, we identified several vulnerabilities. Sensitive data is exposed on the WHOIS and searching crt.sh. We were able to detect multiple ip addresses were vulnerable and not protected by exploiting different attack methods to the open ports. This resulted in obtaining access into the system and escalating our privileges to root and navigate through sensitive information. The Apache server came out to be out of date with a Struts vulnerability on another host, resulting in remote code execution. We used a shellshock exploit in metasploit which led to a meterpreter session and obtained access to the sudoers file. In the windows operating system,we also spotted multiple vulnerabilities in the system. We identified user login credentials that were stored in Rrekall’s github web application in hidden files that are accessible to the public as well and were successfully cracked. Additionally, Metasploit was utilized to execute several attack techniques against open ports including FTP port 21 and SLMail service port 110. It produced a reverse shell, which we were able to access the password hash file and use John to crack the hashes.After obtaining access in meterpreter we were able to navigate through directories and find the file we were looking for. Scheduled tasks were easily accessible in the meterpreter session by listing the windows directories.

## 

## Summary Vulnerability Overview

| **Vulnerability** | **Severity** |
| --- | --- |
| Day 1: Cross-Site Scripting XSS Reflected | **Medium** |
| Day 1:Cross-Site Scripting XSS Reflected | **Medium** |
| Day 1:Cross-Site Scripting XSS Stored | **Medium** |
| Day 1:Local File Inclusion | **High** |
| Day 1:Command Injection | **High** |
| Day 1:Sensitive Data Exposure | **Critical** |
| Day 1:Sensitive Data Exposure (searching for robots txt in the browser) | **High** |
| Day 2:Open Source Data Exposure | **Low** |
| Day 2: IP Address Host Exposed | **Low** |
| Day 2:SSL Certificate Research | **Low** |
| Day 2:NMap Scan 192.168.13.0/24 | **Medium** |
| Day 2: Nussus Scanning | **Critical** |
| Day 2:Remote Code Execution | **Critical** |
| Day 2: RCE/ShellShock Exploit | **Critical** |
| Day 3:Sensitive Data Exposure | **Critical** |
| Day 3:NMap Scanning 172.22.117.20/24 | **Medium** |
| Day 3:Obtained Access Through FTP | **High** |
| Day 3:SLMAIL Exploit Through Metasploit | **Critical** |
| Day 3:Performed Task Schedule | **Medium** |
| Day 3:Performed A Kiwi Session | **Critical** |
| Day 3:Applying the type command in meterpression in C:\Users\Public\Documents folder | **Critical** |

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

| **Scan Type** | **Total** |
| --- | --- |
| Hosts | 9 |
| Ports | 4 |

| **Exploitation Risk** | **Total** |
| --- | --- |
| **Critical** | 8 |
| **High** | 4 |
| **Medium** | 6 |
| **Low** | 3 |

## Vulnerability Findings

Day 1

| **Vulnerability 1** | **Findings** |
| --- | --- |
| **Title** | Cross-Site Scripting XSS Reflected |
| **Type (Web app / Linux OS / WIndows OS)** | web app |
| **Risk Rating** | medium |
| **Description** | A malicious script was reflected on the welcome page of totalrekall.xyz with the following <script>alert(‘mutasem is here’)</script> |
| **Images** |  |
| **Affected Hosts** | 192.168.14.35/welcome.php |
| **Remediation** | Input validation to prevent script being uploaded. |

| **Vulnerability 2** | **Findings** |
| --- | --- |
| **Title** | Cross-Site Scripting XSS reflected memory-planner |
| **Type (Web app / Linux OS / WIndows OS)** | Web app |
| **Risk Rating** | medium |
| **Description** | We typed “SCscriptRIPT” in the box in order to be separated in the payload for it to work. |
| **Images** |  |
| **Affected Hosts** | 192.168.14.35/Memory-Planner.php |
| **Remediation** | Input validation to prevent script being uploaded. |

| **Vulnerability 3** | **Findings** |
| --- | --- |
| **Title** | Stored Cross-Site Scripting XSS Stored |
| **Type (Web app / Linux OS / WIndows OS)** | web app |
| **Risk Rating** | medium |
| **Description** | After navigating to the comments, we entered a script <script>alert(“mutasem”)</script> in the comments box to reveal flag 3. |
| **Images** |  |
| **Affected Hosts** | 192.168.14.35/comments.php |
| **Remediation** | input validation and limiting user input |

| **Vulnerability 4** | **Findings** |
| --- | --- |
| **Title** | Local file inclusion |
| **Type (Web app / Linux OS / WIndows OS)** | web app |
| **Risk Rating** | high |
| **Description** | uploading a malicious php file into the server that contains commands. |
| **Images** |  |
| **Affected Hosts** | 192.168.14.35/Memory-Planner.php |
| **Remediation** | restrict users from the ability to upload files into the local file system. |

| **Vulnerability 5** | **Findings** |
| --- | --- |
| **Title** | Sensitive Data Exposure |
| **Type (Web app / Linux OS / WIndows OS)** | web app |
| **Risk Rating** | critical |
| **Description** | The login credentials are stored in the html and we can reveal these credentials by highlighting the webpage. We can see the networking tools that are provided for the admin. |
| **Images** |  |
| **Affected Hosts** | 192.168.14.35/login.php and 192.168.14.35/networking.php |
| **Remediation** | remove credential data from html code or header. |

| **Vulnerability 6** | **Findings** |
| --- | --- |
| **Title** | Sensitive Data Exposure by inputting robots.txt in the browser after the ip address. |
| **Type (Web app / Linux OS / WIndows OS)** | web app |
| **Risk Rating** | high |
| **Description** | Unrestricted access to robots.txt page and hidden files/pages exposed. |
| **Images** |  |
| **Affected Hosts** | 192.168.14.35/robots.txt |
| **Remediation** | Limit access to authorized users |

| **Vulnerability 7** | **Findings** |
| --- | --- |
| **Title** | Command Injection |
| **Type (Web app / Linux OS / WIndows OS)** | web app |
| **Risk Rating** | high |
| **Description** | An advance payload command was uploaded in the MX record checker field, www.welcometorecall.com | cat vendors.txt |
| **Images** |  |
| **Affected Hosts** | 192.168.14.35/networking.php |
| **Remediation** | input validation and applying a scripting injection prevention system. |

Add any additional vulnerabilities below.

Day 2

| **Vulnerability 1** | **Findings** |
| --- | --- |
| **Title** | Open Source Data Exposure |
| **Type (Web app / Linux OS / WIndows OS)** | Linux |
| **Risk Rating** | low |
| **Description** | sensitive data is exposed on the WHOIS for totalrekall.xyz on the domain dossier webpage. |
| **Images** |  |
| **Affected Hosts** | 192.168.14.35 |
| **Remediation** | Ensure no sensitive data is uploaded to the public. |

| **Vulnerability 2** | **Findings** |
| --- | --- |
| **Title** | IP Address Host Exposed |
| **Type (Web app / Linux OS / WIndows OS)** | Linux |
| **Risk Rating** | Low |
| **Description** | After typing the domain it revealed the ip address as shown below. |
| **Images** |  |
| **Affected Hosts** | 34.102.136.180 |
| **Remediation** | Configuring a firewall to block certain ip addresses establishing a connection into the network. |

| **Vulnerability 3** | **Findings** |
| --- | --- |
| **Title** | SSL Certificate Research |
| **Type (Web app / Linux OS / WIndows OS)** | Linux |
| **Risk Rating** | Low |
| **Description** | sensitive information is revealed by searching, ssl certificate research about totalrekall.xyz |
| **Images** |  |
| **Affected Hosts** | https://crt.sh/?q=totalrekall.xyz |
| **Remediation** | prevent no data from being exposed. |

| **Vulnerability 4** | **Findings** |
| --- | --- |
| **Title** | Nmap scan on the entire network of totalrekall 192.168.13.0/24 |
| **Type (Web app / Linux OS / WIndows OS)** | Linux |
| **Risk Rating** | Medium |
| **Description** | We used nmap to conduct a scan identifying which ports are open, the services behind those ports, and their versions. |
| **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** | close unnecessary open ports |

| **Vulnerability 5** | **Findings** |
| --- | --- |
| **Title** | Apache struts vulnerability found through Nussus Scanning |
| **Type (Web app / Linux OS / WIndows OS)** | Linux |
| **Risk Rating** | critical |
| **Description** | An Apache Struts 2.3.5 - 2.3.31 vulnerability is found through Nussus scanning  against the host 192.168.13.12 which allows for remote code execution. |
| **Images** |  |
| **Affected Hosts** | 192.168.13.12 |
| **Remediation** | Update to the most recent version of Apache Struts after performing a test and ensure no unauthorized system changes have been made on the system before employing the patch. |

| **Vulnerability 6** | **Findings** |
| --- | --- |
| **Title** | Apache Tomcat Remote Code Execution Vulnerability (CVE-2017-12617) |
| **Type (Web app / Linux OS / WIndows OS)** | Linux |
| **Risk Rating** | critical |
| **Description** | We performed a metasploit exploit on the host 192.168.13.10 which allowed for a Remote Code Execution and retrieved a reverse shell session. |
| **Images** |  |
| **Affected Hosts** | 192.168.13.10 |
| **Remediation** | Update Tomcat to the latest version, which resolves the vulnerability. |

| **Vulnerability 7** | **Findings** |
| --- | --- |
| **Title** | RCE and shellshock exploit in Metasploit on host 192.168.13.11 |
| **Type (Web app / Linux OS / WIndows OS)** | Linux |
| **Risk Rating** | critical |
| **Description** | We used shellshock on host 192.168.13.11 to gain access and compromise the system. |
| **Images** |  |
| **Affected Hosts** | 192.168.13.11 |
| **Remediation** | applying a patch and limiting access for certain users |

Day 3

| **Vulnerability 1** | **Findings** |
| --- | --- |
| **Title** | Found the username and password hash for one of the users of totalrekall on the github page (Sensitive Data exposure) |
| **Type (Web app / Linux OS / WIndows OS)** | windows |
| **Risk Rating** | critical |
| **Description** | A certain search operator was used to identify where the credentials of the user are stored in and any additional information. We used john to crack the password of the user that was in a txt file and revealed the password. |
| **Images** |  |
| **Affected Hosts** | https://github.com/totalrekall/site |
| **Remediation** | Delete the sensitive information on the website and get rid of the specific searching operators to ensure that no important information is available to the public. |

| **Vulnerability 2** | **Findings** |
| --- | --- |
| **Title** | Nmap scanning on the host 172.22.117.20/24 |
| **Type (Web app / Linux OS / WIndows OS)** | windows |
| **Risk Rating** | medium |
| **Description** | Performed an nmap scan on the following host 172.22.117.20/24 and found 172.22.117.20 has an http port 80 open. We entered the ip address into the browser and prompted us for a login and used the username and password from flag1. |
| **Images** |  |
| **Affected Hosts** | 172.22.117.20 |
| **Remediation** | Apply a 2 factor authentication. |

| **Vulnerability 3** | **Findings** |
| --- | --- |
| **Title** | Obtained access into host 172.22.117.20 through ftp |
| **Type (Web app / Linux OS / WIndows OS)** | windows |
| **Risk Rating** | high |
| **Description** | Performed an aggressive nmap scan on the host 172.22.117.20 and found port 21 ftp server was open. We successfully obtained access and were able to identify the location of the file. |
| **Images** |  |
| **Affected Hosts** | 172.22.117.20 |
| **Remediation** | Limit access to port 21 or close it. |

| **Vulnerability 4** | **Findings** |
| --- | --- |
| **Title** | Applied SLMAIL exploit to obtain access to the host 172.22.117.20 |
| **Type (Web app / Linux OS / WIndows OS)** | Windows |
| **Risk Rating** | critical |
| **Description** | The attack was successfully exploited within metasploit due to port 110 open which led to an access in the meterpreter session and identified the location of the file. |
| **Images** |  |
| **Affected Hosts** | 172.22.117.20 |
| **Remediation** | Limit access to port 110 and stop SLMail service. |

| **Vulnerability 5** | **Findings** |
| --- | --- |
| **Title** | Task Schedule |
| **Type (Web app / Linux OS / WIndows OS)** | windows |
| **Risk Rating** | medium |
| **Description** | Accessing the windows 10 machine and viewing the scheduled tasks. |
| **Images** |  |
| **Affected Hosts** | 172.22.117.20 |
| **Remediation** | Limit access to certain users by changing the permissions of the file. |

| **Vulnerability 6** | **Findings** |
| --- | --- |
| **Title** | Performed a kiwi session to crack the hash |
| **Type (Web app / Linux OS / WIndows OS)** | windows |
| **Risk Rating** | critical |
| **Description** | We used kiwi in the meterpreter session to access the password hashes in a file and copied it in a txt file. We used john which successfully cracked the password hashes which results in a reverse shell. |
| **Images** |  |
| **Affected Hosts** | 172.22.117.20 |
| **Remediation** | Limit access to certain files by changing the permissions and changing user permissions. |

| **Vulnerability 7** | **Findings** |
| --- | --- |
| **Title** | Applying the type command in meterpression in C:\Users\Public\Documents folder |
| **Type (Web app / Linux OS / WIndows OS)** | windows |
| **Risk Rating** | critical |
| **Description** | We identified where the file is located in the meterpreter session and used the type command to read the file. |
| **Images** |  |
| **Affected Hosts** | 172.22.117.20 |
| **Remediation** | Limit access to certain files by changing the permissions and changing user permissions |