| Cybersecurity |
| --- |
| Penetration Test Report |

Rekall Corporation

Penetration Test Report

# 

## 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** | CyberGrunt LLC |
| --- | --- |
| **Contact Name** | Charles Wallace |
| **Contact Title** | CyberSecurity Analyst |

## 

## Document History

| **Version** | **Date** | **Author(s)** | **Comments** |
| --- | --- | --- | --- |
| 001 | 4/26/2023 | Charles Wallace |  |
| 002 | 4/27/2023 | Charles Wallace |  |
| 003 | 5/1/2023 | Charles Wallace |  |

# 

## 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.

* Denial of DDOS Attacks to ensure network availability through a strong mitigation strategy.
* Mapping network architecture revealed no open source data penetration.
* Various tools such as Metasploit/Hashcat/Nmap are utilized to prevent unauthorized access.
* Intelligent strategies for defensive and offensive tasks.
* Continuous penetration testing to improve mitigation for identified vulnerabilities.

### 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 Application has vulnerabilities to SQL payload injection and XSS.
* HTML source code contains credentials.
* Outdated Apache Web Server is vulnerable to multiple exploits.
* SLMail server has vulnerabilities to exploits that allows shell access.
* Access to password hashes by unauthorized users was utilized for password cracking and privilege escalation.
* Rekall’s server physical address is publicly available.
* When conducting an IP lookup credentials were displayed.
* Potential vulnerabilities found in Rekall’s IP range when scanned (open ports, IP addresses, etc.).
* File enumeration and unauthorized access allowed through open ports.

## Executive Summary

CyberGrunt LLC conducted a penetration test of Rekall’s IT assets and found several vulnerabilities, including critical ones that could have potential catastrophic impacts on Rekall’s revenue or reputation. They were able to infiltrate Rekall’s various assets, extract sensitive data and escalate privileges within different systems.

CyberGrunt LLC initially tested Rekall’s Web Application and discovered several vulnerabilities. The Web App was found to be vulnerable to an XSS reflected attack, local file inclusion, and an XSS stored vulnerability on the comments page. SQL injection attacks were also identified on the login.php toolbar as well as the networking.php page that was vulnerable to a command injection attack.

During testing, CyberGrunt LLC was able to find that open source data was exposed and viewable using OSINT, and a stored certificate that was found by searching crt.sh. Surprisingly, user login credentials were found to be stored in plain view with the HTML source code of the login.php page, which could be seen by simply highlighting the page in a web browser. The file robots.txt was also exposed and readily accessible. CyberGrunt LLC then found user credentials in a Github repository that allowed unauthorized access to the web host’s files and directories. Additionally, the Apache server was found to have a Struts vulnerability due to being out of date.

CyberGrunt LLC then proceeded to test the Windows OS environment and found FTP Port 21 and Port 110, which is used for SLMail service, were open and vulnerable. Metasploit was used to discover this vulnerability, as well as gain access to a password hash file which was subsequently cracked and allowed the creation of a reverse shell. Scheduled tasks were readily visible with the Windows 10 Machine Task Scheduler, and Meterpreter could be used to display directories on public Windows directories.

In the Linux environment, CyberGrunt LLC was able to identify five IP addresses that were publicly exposed and vulnerable, and one of the hosts was found to be running Drupal. Stolen credentials were then used to access one of the hosts and escalate privileges to root. An additional commonly known shell RCE execution vulnerability was discovered using Meterpreter. The sudoers file was accessible using a Shellshock exploit in Metasploit.

In conclusion, the vulnerabilities that CyberGrunt LLC discovered could be exploited maliciously and cause massive damage to Rekall’s assets and the functionality of the business. CyberGrunt LLC has provided detailed recommendations to prevent harm and loss that could result from these vulnerabilities.

## 

## 

## 

## 

## Summary Vulnerability Overview

| **Vulnerability** | **Severity** |
| --- | --- |
| Local File Inclusion | **Critical** |
| SQL Injection | **Critical** |
| Sensitive Data Exposure | **Critical** |
| Sensitive Data Exposure | **Critical** |
| Command Injection | **Critical** |
| Shellshock on Web Server (Port 80) | **Critical** |
| Apache Struts (CVE-2017-5638) | **Critical** |
| Linux Privilege Escalation | **Critical** |
| SLMail Port 110 Exploited via Metasploit (SeattleMail) | **Critical** |
| Access System and Run lsa\_dump\_sam via Kiwi Shows Password Hashes | **Critical** |
| Admin Server Credentials Dumped via Kiwi | **Critical** |
| System Shell Executed with Dumped Admin Server Credentials | **Critical** |
| IPs visible with Nmap | **Critical** |
| Drupal (CVE-2019-6340) | **Critical** |
| Open Source Exposed Data | **High** |
| Apache Tomcat Remote Code Execution Vulnerability (CVE-207-12617) | **High** |
| Run as ALL Sudoer (CVE-2019-14287) | **High** |
| Open FTP Port 21 | **High** |
| Sensitive Information Stored in Public/Documents Folder | **High** |
| XSS Reflected | **Medium** |
| XSS Stored | **Medium** |
| Certificate Search via crt.sh | **Medium** |

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

| **Scan Type** | **Total** |
| --- | --- |
| Hosts | 172.22.117.20  172.22.117.10  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  106  110 |

| **Exploitation Risk** | **Total** |
| --- | --- |
| **Critical** | 14 |
| **High** | 5 |
| **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 reflected on host home page <script>alert(Document.cookie)</script> revealing flag 1. |
| **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 .php file from the tool bar located on the VR Planner page revealing flag 5. |
| **Images** |  |
| **Affected Hosts** | 192.168.14.35 |
| **Remediation** | Prevent file paths from being able to be appended directly; if possible, restrict API to allow inclusion only from a directory and the directories below it. |

| **Vulnerability 3** | **Findings** |
| --- | --- |
| **Title** | XSS Stored |
| **Type (Web app / Linux OS / WIndows OS)** | Web App |
| **Risk Rating** | Critical |
| **Description** | While accessing /Comments page, entered <script>alert(“Hi”)</script> to reveal Flag 3. |
| **Images** |  |
| **Affected Hosts** | 192.168.14.35 |
| **Remediation** | Implement XSS protection to disallow injection of script code |

| **Vulnerability 4** | **Findings** |
| --- | --- |
| **Title** | SQL Injection |
| **Type (Web app / Linux OS / WIndows OS)** | Web App |
| **Risk Rating** | Critical |
| **Description** | While access the /Login.php page, payload (Name or “1=1”) was entered in toolbar intended for password successfully resulting in exploit. Revealing flag 7. |
| **Images** |  |
| **Affected Hosts** | 192.168.14.35 |
| **Remediation** | Disallow web app to accept direct input and/ or implement character escaping. |

| **Vulnerability 5** | **Findings** |
| --- | --- |
| **Title** | Command Injection |
| **Type (Web app / Linux OS / WIndows OS)** | Web App |
| **Risk Rating** | Critical |
| **Description** | Navigation allowed from /Networking.php to 192.168.14.35/disclaimer.php?page=vendors.txt via 192.168.14.35/networking.php  Able to input “splunk” inside of toolbar intended for DNS check, revealing flag 10. |
| **Images** |  |
| **Affected Hosts** | 192.168.14.35 |
| **Remediation** | Implement input validation unintended access. |

| **Vulnerability 6** | **Findings** |
| --- | --- |
| **Title** | User Credentials Exposure |
| **Type (Web app / Linux OS / WIndows OS)** | Web App |
| **Risk Rating** | Critical |
| **Description** | User credentials are visible within the HTML of the Login.php page and when highlighting the page in a web browser. Revealing flag 8. |
| **Images** |  |
| **Affected Hosts** | 192.168.14.35 |
| **Remediation** | Delete this information from the HTML, also implement 2-factor authentication for additional enhanced security. |

| **Vulnerability 7** | **Findings** |
| --- | --- |
| **Title** | Sensitive Data Exposure |
| **Type (Web app / Linux OS / WIndows OS)** | Web App |
| **Risk Rating** | Medium |
| **Description** | Unrestricted access to robots.txt page. Revealing flag 9. |
| **Images** |  |
| **Affected Hosts** | 192.168.14.35 |
| **Remediation** | Restrict access to robots.txt to only authorized users. |

| **Vulnerability 8** | **Findings** |
| --- | --- |
| **Title** | Open source exposed data |
| **Type (Web app / Linux OS / WIndows OS)** | Linux OS |
| **Risk Rating** | Medium |
| **Description** | On the Domain Dossier webpage, viewed the WHOIS data with OSINT for totalrekall.xyz to access sensitive information. |
| **Images** |  |
| **Affected Hosts** | http://centralops.net/co/DomainDossier.aspx |
| **Remediation** | Ensure no sensitive data is being shared publicly, clean up WHOIS records. |

| **Vulnerability 9** | **Findings** |
| --- | --- |
| **Title** | Certificate search via crt.sh |
| **Type (Web app / Linux OS / WIndows OS)** | Linux OS |
| **Risk Rating** | Medium |
| **Description** | Searched for totalrekall.xyz on crt.sh, found stored certificate. |
| **Images** |  |
| **Affected Hosts** | 34.102.136.180 |
| **Remediation** | Protect information from being exposed by the crt.sh site. |

| **Vulnerability 10** | **Findings** |
| --- | --- |
| **Title** | Nmap Scan Results |
| **Type (Web app / Linux OS / WIndows OS)** | Linux OS |
| **Risk Rating** | Critical |
| **Description** | An Nmap scan on 192.168.13.0/28 revealed 5 hosts are visible with exposed IP’s. |
| **Images** |  |
| **Affected Hosts** | 192.168.13.10  192.168.13.11  192.168.13.12  192.168.13.13  192.168.13.14 |
| **Remediation** | Implement IP blocking for unauthorized users. |

| **Vulnerability 11** | **Findings** |
| --- | --- |
| **Title** | Aggressive Nmap Scan |
| **Type (Web app / Linux OS / WIndows OS)** | Linux OS |
| **Risk Rating** | Critical |
| **Description** | Ran aggressive Nmap scan (Nmap -A 192.168.13.0/28) to discover host running Drupal |
| **Images** |  |
| **Affected Hosts** | 192.178.13.12 |
| **Remediation** | Block probes, restrict information returned, slow down the aggressive Nmap scan, and/or return misleading information. |

| **Vulnerability 12** | **Findings** |
| --- | --- |
| **Title** | Nessus Scan |
| **Type (Web app / Linux OS / WIndows OS)** | Linux OS |
| **Risk Rating** | Medium |
| **Description** | Nessus scan revealed Apache Struts vulnerability |
| **Images** |  |
| **Affected Hosts** | 192.168.13.12 |
| **Remediation** | Perform regular updates of software such as Apache. |

| **Vulnerability 13** | **Findings** |
| --- | --- |
| **Title** | Privilege Escalation |
| **Type (Web app / Linux OS / WIndows OS)** | Linux OS |
| **Risk Rating** | Critical |
| **Description** | Able to escalate privileges via SSH from stolen credentials. |
| **Images** |  |
| **Affected Hosts** | 192.168.13.14 |
| **Remediation** | Close port 22, enforce stronger credentials, and/or implement 2-factor authentication. |

| **Vulnerability 14** | **Findings** |
| --- | --- |
| **Title** | Meterpreter shell RCE execution (CVE-2017-5638) |
| **Type (Web app / Linux OS / WIndows OS)** | Linux OS |
| **Risk Rating** | Critical |
| **Description** | Within Meterpreter, used multi/http/struts2\_content\_type\_ognl exploit with PAYLOAD= linux/x86/shell\_reverse\_tcp |
| **Images** |  |
| **Affected Hosts** | 192.168.13.12 |
| **Remediation** | Apply updates per vendor instructions. |

| **Vulnerability 15** | **Findings** |
| --- | --- |
| **Title** | Shellshock on Web Server (Port 80) |
| **Type (Web app / Linux OS / WIndows OS)** | Linux OS |
| **Risk Rating** | Critical |
| **Description** | Used exploit (multi/http/apache\_mod\_cgi\_bash\_env\_exec)  set TARGETURI /cgi-bin/shockme.cgi  shell  Navigate to /etc/sudoers for root privileges file |
| **Images** |  |
| **Affected Hosts** | 192.168.13.14 |
| **Remediation** | Edit the sudoers file to limit access for all sudo accounts, limit the orarom user from running commands (enabled for patching from Oracle platinum support), except for sudo su to root  orarom ALL = ALL, !/bin/su |

| **Vulnerability 16** | **Findings** |
| --- | --- |
| **Title** | Username and Password Hash in Github Repo |
| **Type (Web app / Linux OS / WIndows OS)** | Windows OS |
| **Risk Rating** | Critical |
| **Description** | Searching totalrekall’s Github page resulted in finding a site repository, which then lead to a page containing xampp.users that contained the credentials trivera:$apr1$A0vSKwao$GV3sgGAj53j.c3GkS4oUC0  These credentials were then cracked using john. Which displayed the password as Tanya4life |
| **Images** |  |
| **Affected Hosts** | Total Rekall web server |
| **Remediation** | Restrict access and remove credentials from Github |

| **Vulnerability 17** | **Findings** |
| --- | --- |
| **Title** | Port Scan of Subnet |
| **Type (Web app / Linux OS / WIndows OS)** | Windows OS |
| **Risk Rating** | Critical |
| **Description** | Using the credentials found in the Github repository to login, there was a single file there named flag2.txt  Method to Exploit:  Nmap 172.22.117.0/24  172.22.117.20 has port 80 open  Opened 172.22.117.20 in a web browser.  Provided credentials from Flag 1 (trivera Tanya4life) to login  File flag2.txt is located in the root directory |
| **Images** |  |
| **Affected Hosts** | 172.22.117.20 |
| **Remediation** | Require stronger credentials and/or a 2-factor authentication method. |

| **Vulnerability 18** | **Findings** |
| --- | --- |
| **Title** | FTP Enumeration |
| **Type (Web app / Linux OS / WIndows OS)** | Windows OS |
| **Risk Rating** | Critical |
| **Description** | Open Port 21 allows for FTP enumeration through FTP connection on the host IP which resulted in successful transfer and access/ download of vulnerable files. |
| **Images** |  |
| **Affected Hosts** | 172.22.117.20 |
| **Remediation** | Restrict access to Port 21 |

| **Vulnerability 19** | **Findings** |
| --- | --- |
| **Title** | SLMail Exploit |
| **Type (Web app / Linux OS / WIndows OS)** | Windows OS |
| **Risk Rating** | Critical |
| **Description** | Vulnerability in SLMail due to open port 110 was successfully exploited through use of windows/pop3/seattlelab\_pass exploit within Metasploit which resulted in a successful Meterpreter session. |
| **Images** |  |
| **Affected Hosts** | 172.22.117.20 |
| **Remediation** | Restrict access to Port 110, discontinue use of SLMail service and replace. |

| **Vulnerability 20** | **Findings** |
| --- | --- |
| **Title** | Windows 10 Machine Task Scheduler |
| **Type (Web app / Linux OS / WIndows OS)** | Windows OS |
| **Risk Rating** | Medium |
| **Description** | Within the Windows 10 machine, able to view details of scheduled tasks. |
| **Images** |  |
| **Affected Hosts** | 172.22.117.20 |
| **Remediation** | Change permissions of accounts to restrict unauthorized access. |

| **Vulnerability 21** | **Findings** |
| --- | --- |
| **Title** | Sensitive Data/ Credentials Dump |
| **Type (Web app / Linux OS / WIndows OS)** | Windows OS |
| **Risk Rating** | Critical |
| **Description** | Continued the use of the previous successful exploit via the Metasploit/Meterpreter session. Access to vulnerable passwords file was obtained, followed by the successful hash dump with post/windows/gather/hashdump. Passwords were then cracked using john, resulting in successful access to credentials and creation of a reverse shell. |
| **Images** |  |
| **Affected Hosts** | 172.22.117.20 |
| **Remediation** | Restrict access to vulnerable files by updating permissions on files and user permissions, move files to a non-public domain. |

| **Vulnerability 22** | **Findings** |
| --- | --- |
| **Title** | Public Directory Search |
| **Type (Web app / Linux OS / WIndows OS)** | Windows OS |
| **Risk Rating** | Medium |
| **Description** | Navigated to the Users\Public\Documents directory, used the ls command in Meterpreter to display files. |
| **Images** |  |
| **Affected Hosts** | 172.22.117.20 |
| **Remediation** | Move sensitive files to more secure areas and/or restrict unauthorized access. |