|  |
| --- |
| DC CyberSecurity Group |
| 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](#_heading=h.1fob9te)

[Contact Information 4](#_heading=h.2et92p0)

[Document History 4](#_heading=h.3dy6vkm)

[Introduction 5](#_heading=h.4d34og8)

[Assessment Objective 5](#_heading=h.3rdcrjn)

[Penetration Testing Methodology 6](#_heading=h.lnxbz9)

[Reconnaissance 6](#_heading=h.1ksv4uv)

[Identification of Vulnerabilities and Services 6](#_heading=h.2jxsxqh)

[Vulnerability Exploitation 6](#_heading=h.z337ya)

[Reporting 6](#_heading=h.3j2qqm3)

[Scope 7](#_heading=h.1y810tw)

[Executive Summary of Findings 8](#_heading=h.2xcytpi)

[Grading Methodology 8](#_heading=h.qsh70q)

[Summary of Strengths 9](#_heading=h.41mghml)

[Summary of Weaknesses 9](#_heading=h.49x2ik5)

[Executive Summary Narrative 10](#_heading=h.2grqrue)

[Summary Vulnerability Overview 1](#_heading=h.vx1227)3

Vulnerability Findings [1](#_heading=h.3fwokq0)4

# 

## Contact Information

|  |  |
| --- | --- |
| **Company Name** | DC CyberSecurity Group |
| **Contact Name** | Brian Massett,Matthew Davis, Joshua Schauert, Evan Hoey, Michael Valdivia |
| **Contact Title** | Chief Coordination Officer |

## 

## Document History

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Author(s)** | **Comments** |
| 001 | 8/8/2022 | Yancey Norris |  |
| 002 | 8/8/2022 | Matthew Davis |  |
| 003 | 8/6/2022 | Joshua Schauert | 3 revisions, completed on 8/9 |
| 004 | 8/9/2022 | Evan Hoey |  |
| 005 | 8/9/2022 | Brian Massett |  |
| 006 | 8/8/2022 | Michael Valdivia |  |

# 

## 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.

* Mitigation strategy in place for denial of DDOS Attacks to ensure network availability
* No vulnerable open source data penetration due to mapping network architecture
* Tools like Metasploit/Hashcat/Nmap are utilized to prevent unauthorized access
* Forward-thinking defensive and offensive strategy
* Current and continuing penetration testing to identify vulnerabilities for mitigation

### 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 is vulnerable to XSS and SQL payload injection
* Credentials are being stored in HTML source code
* Apache web server is outdated and vulnerable to multiple exploits
* SLMail server is vulnerable to exploits which allow access to shell
* Unauthorized access to password hashes allow for password cracking and privilege escalation
* Rekall’s server physical address is publicly available
* Credentials are displayed when doing a IP lookup
* IP addresses within Rekall’s IP range display potential vulnerabilities (open ports, IP addresses, etc.) when scanned
* Open ports allow for file enumeration and unauthorized access

## Executive Summary

## During the Penetration Testing of Rekall’s IT assets, DC CyberSecurity Group was able to identify multiple vulnerabilities, including a number of Critical vulnerabilities that could have a potentially catastrophic impact on the revenue or reputation of Rekall. DC CyberSecurity Group was able to infiltrate Rekall’s assets, exfiltrate sensitive data, and escalate privileges within systems, as below.

DC CyberSecurity Group tested Rekall’s Web Application first. We determined it to be vulnerable to an XSS Reflected attack as malicious script can be run on the home page. The Web App is also vulnerable to Local File Inclusion as files can be uploaded from the VR Planner web page. An XSS Stored vulnerability was identified on the Comments page as it allows scripting code to be run. SQL Injection attacks can also be run on the Login.php toolbar, and the Networking.php page is vulnerable to a Command Injection attack.

Open source data was determined to be exposed and viewable using OSINT, and searching crt.sh showed a stored certificate. Furthermore, somewhat shockingly, user login credentials were actually stored in plain view within the HTML source code of the Login.php page and could even be seen while simply highlighting the page in a web browser. The file robots.txt was also determined to be exposed and readily accessible. Research uncovered user credentials in a Github repository that resulted in unauthorized access to the web hosts files and directories. The Apache server was found to be out-of-date with a Struts vulnerability.

The Windows OS environment was tested next, and DC CyberSecurity Group discovered that FTP Port 21 was open and vulnerable, as was Port 110, which is used for SLMail service. Metasploit was used to discover this vulnerability, as well as to gain access to a password hash file which was subsequently cracked and enabled the creation of a reverse shell. Additionally, scheduled tasks were readily visible within the Windows 10 Machine Task Scheduler, and Metepreter could be used to display directories on public Windows directories.

Within the Linux environment, DC CyberSecurity Group was able to reveal 5 IP addresses that were publicly exposed and vulnerable, and one of the hosts was found to be running Drupal. Stolen credentials were used to access one host and escalate privileges to root. An additional common known shell RCE execution vulnerability was discovered using Meterpreter. The sudoers file was accessible using a Shellshock exploit in Metasploit as well.

## 

## In summary, these vulnerabilities could be exploited maliciously to cause massive damage within the assets and to the functionality of the business in general. DC CyberSecurity Group has provided detailed recommendations for mitigating each of these vulnerabilities to prevent harm and loss that could result.

## 

## 

## 

## Summary Vulnerability Overview

| **Vulnerability** | **Severity** |
| --- | --- |
| Local File Inclusion | **Critical** |
| SQL Injection | **Critical** |
| Sensitive Data Exposure | **Critical** |
| User Credentials 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-2017-12617) | **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 |
| Informational | 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> |
| **Image** |  |
| **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 |
| **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 |
| **Image** |  |
| **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 accessing /Login.php page, payload (Name or “1=1”) was entered in toolbar intended for password successfully resulting in exploit |
| **Image** |  |
| **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 |
| **Images** |  |
| **Affected Hosts** | 192.168.14.35 |
| **Remediation** | Implement input validation unintended access |

|  |  |
| --- | --- |
| **Vulnerability 6** | **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 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 7** | **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 successful Meterpreter session |
| **Images** |  |
| **Affected Hosts** | 172.22.117.20 |
| **Remediation** | Restrict access to Port 110, disuse SLMail service and replace |

|  |  |
| --- | --- |
| **Vulnerability 8** | **Findings** |
| **Title** | Sensitive Data/Credentials Dump |
| **Type (Web App / Linux OS / WIndows OS)** | Windows OS |
| **Risk Rating** | Critical |
| **Description** | Continued use of previous successful exploit via Metasploit/Meterpreter session; access to vulnerable passwords file obtained, followed by successful hash dump within post/windows/gather/hashdump. Passwords 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 an non-public domain |

|  |  |
| --- | --- |
| **Vulnerability 9** | **Findings** |
| **Title** | Open source exposed data |
| **Type (Web App / Linux OS / WIndows OS)** | Web App |
| **Risk Rating** | Medium |
| **Description** | On the Domain Dossier webpage, viewed the WHOIS data with OSINT for Total rekall.xyz to access sensitive information |
| **Images** |  |
| **Affected Hosts** | https://centralops.net/co/DomainDossier.aspx |
| **Remediation** | Ensure no sensitive data is being shared publicly, clean up WHOIS records |

|  |  |
| --- | --- |
| **Vulnerability 10** | **Findings** |
| **Title** | Certificate Search via crt.sh |
| **Type (Web App / Linux OS / WIndows OS)** | Web App |
| **Risk Rating** | Medium |
| **Description** | Searched for totalrekall.xyz on crt.sh, found stored certificate |
| **Image** |  |
| **Affected Hosts** | 34.102.136.180 |
| **Remediation** | Protect information from being exposed by the crt.sh site |

|  |  |
| --- | --- |
| **Vulnerability 11** | **Findings** |
| **Title** | Nmap Scan Results |
| **Type (Web App / Linux OS / WIndows OS)** | Linux OS |
| **Risk Rating** | Critical |
| **Description** | An Nmap scan on 192.168.13.0/24 revealed 5 hosts are visible with exposed IP’s |
| **Image** |  |
| **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 12** | **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 13** | **Findings** |
| **Title** | User Credentials Exposure |
| **Type (Web App / Linux OS / WIndows OS)** | Web App |
| **Risk Rating** | Critical |
| **Description** | User credentials are visible within HTML of the Login.php and when highlighting page in a web browser |
| **Images** |  |
| **Affected Hosts** | 192.168.14.35 |
| **Remediation** | Delete this information from the HTML, implement 2-factor authentication for enhanced security- |

|  |  |
| --- | --- |
| **Vulnerability 14** | **Findings** |
| **Title** | Sensitive Data Exposure |
| **Type (Web App / Linux OS / WIndows OS)** | Web App |
| **Risk Rating** | Medium |
| **Description** | Unrestricted access to robots.txt page |
| **Image** |  |
| **Affected Hosts** | 192.168.14.35 |
| **Remediation** | Restrict access to robots.txt to authorized users |

|  |  |
| --- | --- |
| **Vulnerability 15** | **Findings** |
| **Title** | Nessus scan |
| **Type (Web App / Linux OS / WIndows OS)** | Web App |
| **Risk Rating** | Medium |
| **Description** | Nessus scan revealed Apache Struts vulnerability |
| **Image** |  |
| **Affected Hosts** | 192.168.13.12 |
| **Remediation** | Perform regular updates on Apache |

|  |  |
| --- | --- |
| **Vulnerability 16** | **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 17** | **Findings** |
| **Title** | Meterpreter shell RCE execution (CVE 2017-5638) |
| **Type (Web App / Linux OS / WIndows OS)** | Linux OS |
| **Risk Rating** | Critical |
| **Description** | With 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 18** | **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 |
| **Image** |  |
| **Affected Hosts** | 192.168.13.14 |
| **sdRemediation** | 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 19** | **Findings** |
| **Title** | Username and Password Hash in Repo |
| **Type (Web App / Linux OS / WIndows OS)** | Web App |
| **Risk Rating** | Critical |
| **Description** | Using credentials found in Github repo, was able to crack password and gain access |
| **Images** |  |
| **Affected Hosts** | Total Rekall web server |
| **Remediation** | Restrict access and remove credentials from Github |

|  |  |
| --- | --- |
| **Vulnerability 20** | **Findings** |
| **Title** | Port Scan of Subnet |
| **Type (Web App / Linux OS / WIndows OS)** | Web App |
| **Risk Rating** | Critical |
| **Description** | Using credentials gained from Github repo to login, there was a single file there named flag2.txt containing the flag  Method/Payload 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 * Provide credentials from Flag 1 (trivera Tanya4life) to log in * File flag2.txt is located in root directory |
| **Image** |  |
| **Affected Hosts** | 172.22.117.20 |
| **Remediation** | Require stronger credentials and or 2-factor authentication |

|  |  |
| --- | --- |
| **Vulnerability 21** | **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 |
| **Image** |  |
| **Affected Hosts** | 172.22.117.20 |
| **Remediation** | Change permissions of accounts to restrict unauthorized access |

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