| 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** | Triangle Company |
| --- | --- |
| **Contact Name** | Kiryl Lashley |
| **Contact Title** | Triangle Squad Pen Tester |

## 

## Document History

| **Version** | **Date** | **Author(s)** | **Comments** |
| --- | --- | --- | --- |
| 001 | December 1, 2022 | Kiryl Lashley |  |

# 

## 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.

* We weren’t able to easily ssh into any of Rekall’s computers
* Input validation prevented a large number of injection attacks
* Certain exploits were not possible due to certain updated software

### 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.

* Outdated software
* Poor Password policies
* Some systems allow anonymous ftp logins
* Sensitive information stored in easily accessible

There were a lot of weaknesses in this website. Some examples include old versions of software and another example would be on the very first vulnerability, I was able to use a very basic script on a text box to gain valuable information. As my report continues, I will continue to show other vulnerabilities my team and I were able to exploit to further the process of cracking TotalRekall.

## 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.]

## 

## Web Application CTF

## 

**Flag 1**

On the Welcome page text input box, use payload **<script>alert(“[text here]”)</script>** for XSS reflected attack

## 

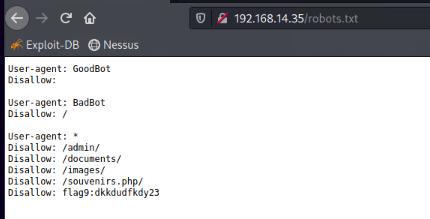
**Flag 8**

The second login is for Admins only. Due to sensitive data located in the HTML that is not encrypted, we obtained the user and password login for:

* Username: *dougquaid*
* Password: *kuato* 

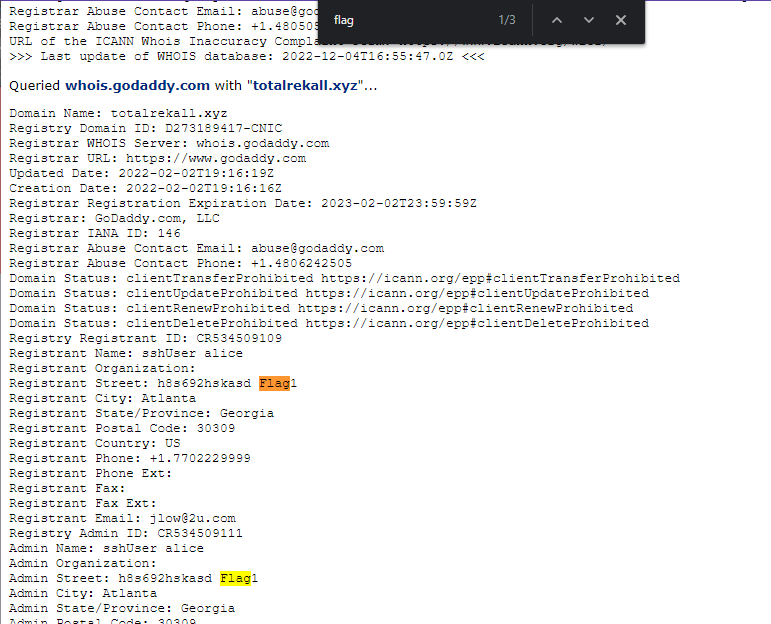
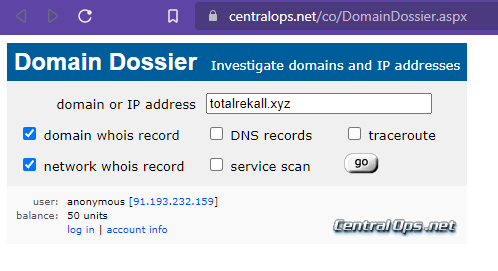
**Flag 9**

A common file on servers exposed to the public just by inputting robots.txt to the URL.



Linux Servers CTF

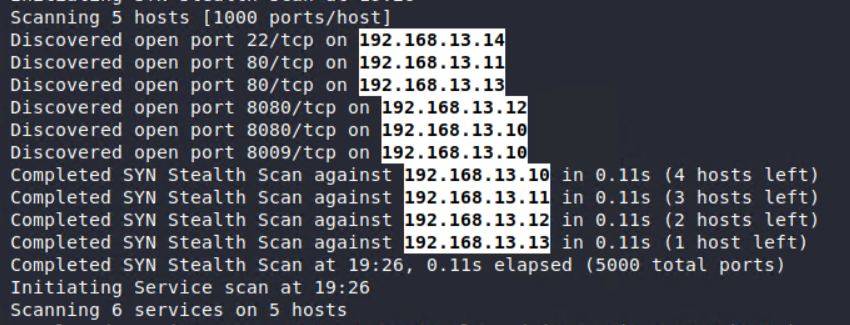
**Flag 1**

We identified this method through the MITRE ATT&CK framework and utilized Domain Dossier to do recon on totalrekall.xyz

**Flag 2**

This ping was already performed from the previous flags query, which indicates the IP the website is located.

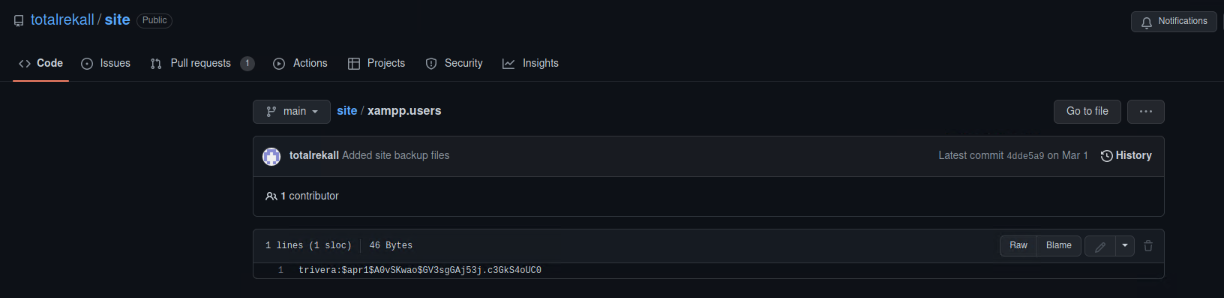
**Flag 4**

The nmap scan of 192.168.13.0/23 determined there are 5 hosts excluding the host we’re scanning from on the network subnet.

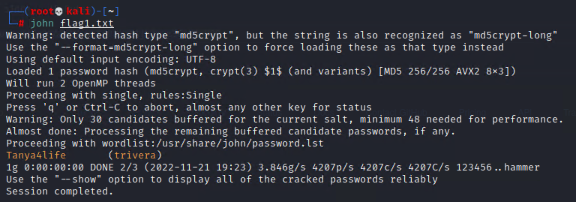
## 

## Windows CTF

**Flag 1**

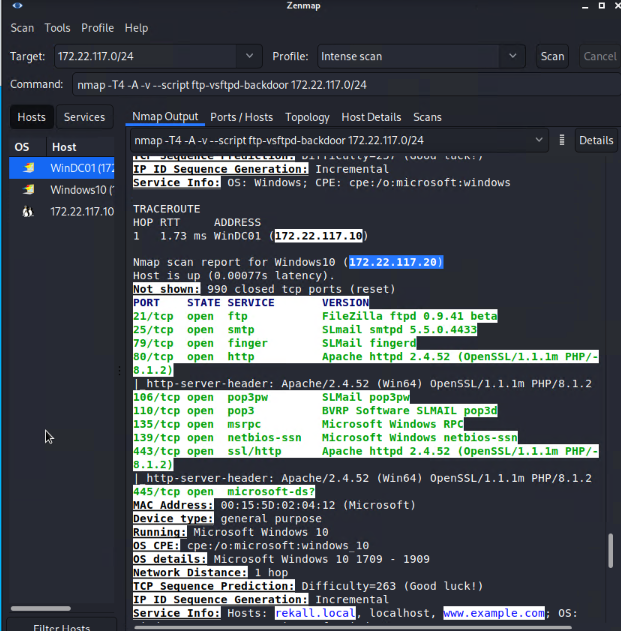
We searched GitHub for totalrekall and through the site repository, located the xampp.users page [https://github.com/totalrekall/site/blob/main/xampp.users] , which contained the below credentials.

After obtaining the hash, we used John the Ripper to decrypt the hashed password to get the login:

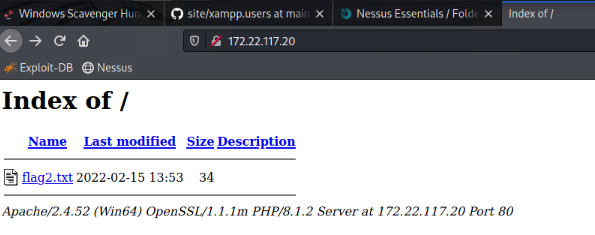
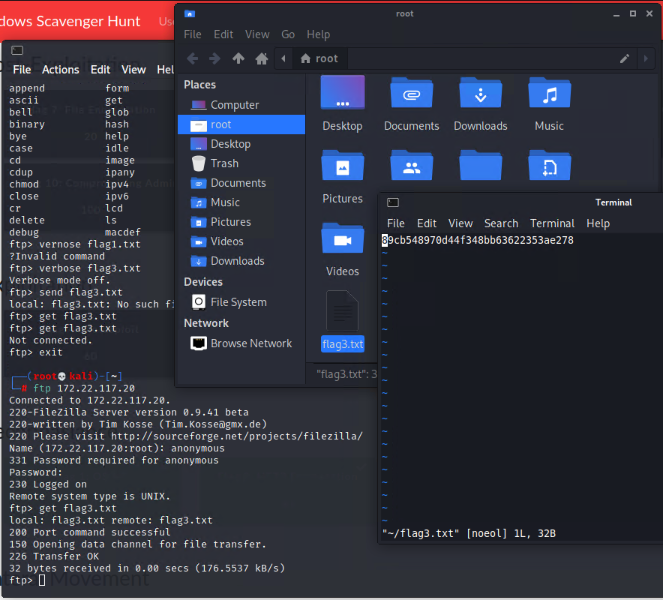
* User: *trivera /* Password: *Tanya4Life*

Flag 2

We performed a port scan of the subnet that our Kali machine is on *(172.22.117.0/24)*, which we got the following results below. We discovered there are 2 machines:

* Windows10 - 172.22.117.20
* WinDC01 - 172.22.117.10 
* This port scan revealed that port 80 is open on Windows10, which means there is a site we can access for this device.

Flag 3

* 

## Summary Vulnerability Overview

| **Vulnerability** | **Severity** |
| --- | --- |
| Web App - Reflected XSS on Welcome.php | **high** |
| Web App - Sensitive Information Exposure on Login.php | **critical** |
| Web App - Sensitive Information Exposure on robots.txt | **critical** |
| Linux Server - Recon with Domain Dossier | **low** |
| Linux Server - Recon with NMap | **low** |
| Windows - Github Repository Sensitive Information Exposure | **critical** |
| Windows - Recon with NMap to find Open Ports | **high** |
| Windows - Compromised Credentials to Access Unsecure File | **critical** |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

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

| **Scan Type** | **Total** |
| --- | --- |
| Hosts | 172.22.117.10  172.22.117.20 |
| Ports | 172.22.117.10: Port 53, 88, 135, 139, 389, 445, 464, 593, 636, 3268, 3269  172.22.117.20: Ports 21, 25, 79, 80, 106, 110, 135, 139, 443, 445 |

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

## Vulnerability Findings

| **Vulnerability 1** | **Findings** |
| --- | --- |
| **Title** | Reflected XSS on Welcome.php |
| **Type (Web app / Linux OS / WIndows OS)** | Web App |
| **Risk Rating** | High |
| **Description** | In the text box for your name input, inputs are not filtered and scripts will execute as proven with the alert we were able to create. |
| **Images** |  |
| **Affected Hosts** | 192.168.14.35 |
| **Remediation** |  |

| **Vulnerability 2** | **Findings** |
| --- | --- |
| **Title** | Sensitive Information Exposure on Login.php |
| **Type (Web app / Linux OS / WIndows OS)** | Web App |
| **Risk Rating** | Critical |
| **Description** | Admin credentials were visible in the HTML as plaintext. |
| **Images** |  |
| **Affected Hosts** | 192.168.14.35 |
| **Remediation** | Salt passwords and more secure storage on the server database than just being built into the HTML. |

| **Vulnerability 3** | **Findings** |
| --- | --- |
| **Title** | Sensitive Information Exposure on robots.txt |
| **Type (Web app / Linux OS / WIndows OS)** | Web App |
| **Risk Rating** | Critical |
| **Description** | Robots.txt is a common file known and in this case the public can easily access that information by changing the URL. |
| **Images** |  |
| **Affected Hosts** | 192.168.14.35 |
| **Remediation** | Limit user privileges based on zero trust, need-to-know basis. |

| **Vulnerability 4** | **Findings** |
| --- | --- |
| **Title** | Recon with Domain Dossier from MITRE ATT&CK |
| **Type (Web app / Linux OS / WIndows OS)** | Linux OS OSINT |
| **Risk Rating** | Low |
| **Description** | Domain |
| **Images** |  |
| **Affected Hosts** |  |
| **Remediation** |  |

| **Vulnerability 5** | **Findings** |
| --- | --- |
| **Title** | Recon with NMap |
| **Type (Web app / Linux OS / WIndows OS)** | Linux OS OSINT |
| **Risk Rating** | low |
| **Description** | Nmap scan of 192.168.13.0/24 |
| **Images** |  |
| **Affected Hosts** | 192.168.13.0/24 |
| **Remediation** | Make sure that any ports that are open are not being used to store any sensitive data and cannot be exploited. |

| **Vulnerability 6** | **Findings** |
| --- | --- |
| **Title** | Github Repository Sensitive Information Exposure |
| **Type (Web app / Linux OS / WIndows OS)** | Windows OS |
| **Risk Rating** | Critical |
| **Description** | Whole website was available to the public on GitHub repository. Sensitive information like the below hashed credential that was easily cracked with John the Ripper were displayed. |
| **Images** |  |
| **Affected Hosts** |  |
| **Remediation** | Do not post credentials to public repositories. |

| **Vulnerability 7** | **Findings** |
| --- | --- |
| **Title** | Recon with NMap to find Open Ports |
| **Type (Web app / Linux OS / WIndows OS)** | Windows OS |
| **Risk Rating** | medium |
| **Description** | Using NMap to discover which host have which open ports that could be exploited |
| **Images** |  |
| **Affected Hosts** | 172.22.117.0/24 |
| **Remediation** | Restrict open ports to public facing internet and/or disable ports not in use. |

Add any additional vulnerabilities below.

| **Vulnerability 8** | **Findings** |
| --- | --- |
| **Title** | Compromised Credentials to Access Unsecure File |
| **Type (Web app / Linux OS / WIndows OS)** | Windows OS |
| **Risk Rating** | Critical |
| **Description** | Using credentials found from another vulnerability and known open ports from a NMap scan, we were able to access and download a file. |
| **Images** |  |
| **Affected Hosts** | 172.22.117.20 |
| **Remediation** | Properly store credentials hashed in a secure database only, not on public repositories. |