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

Contact Information

Company Name	All-American Pentesting
Contact Name	Tyler Keaton
Contact Title	Penetration Tester

Document History

Version	Date	Author(s)	Comments
001	Monday, April 24, 2023	Keaton, Tyler A.	

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.

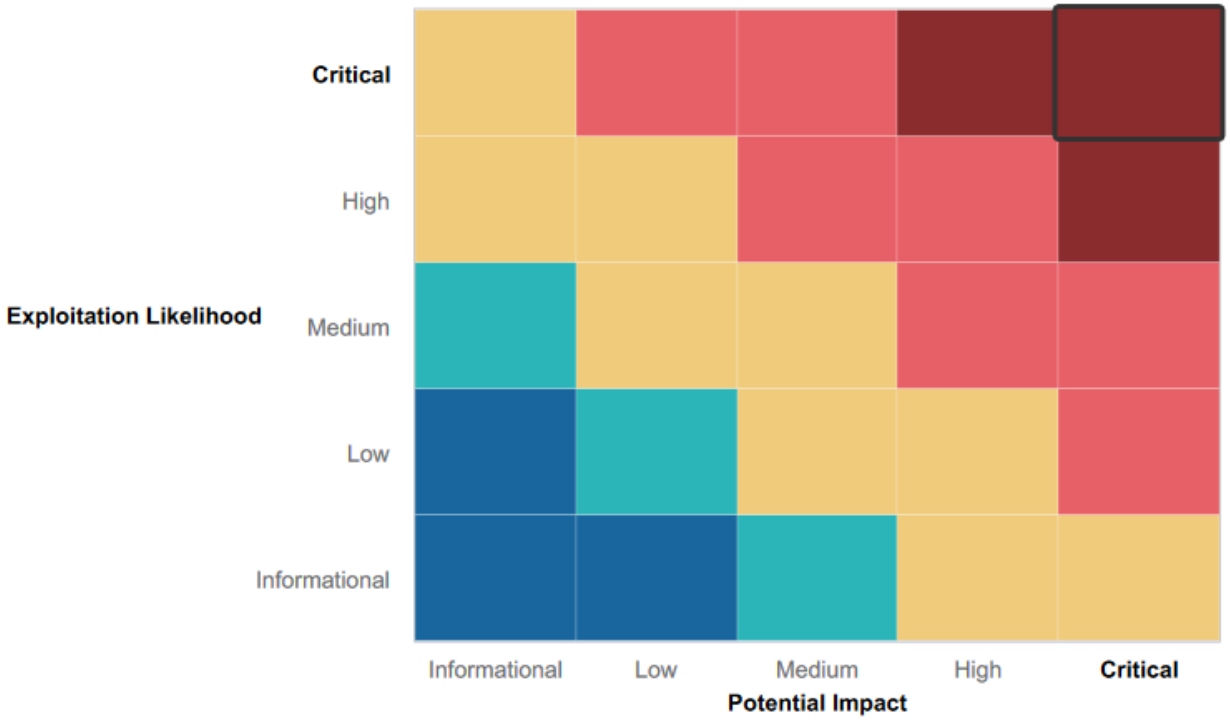
Executive Summary of Findings

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:



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.

-
-
-

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.

- XSS and SQl Injection vulnerability
- Log-In credentials exposed within HTML source code
- Web app susceptible to PHP local file injection exploits
- Credentials easily found on Rekall GitHub repositories
- Users with simple password are easily susceptible to brute force attack
- Apache is vulnerable to numerous attacks due to being outdated
- SLMail server vulnerable to attacks through access to shell
- Rekall server IP Addresses and open ports are easily available when scanned for

Executive Summary

Throughout the course of All-American Pentesting's penetration test of TotalRekall's system and web application, All_American Pentesting was able to identify numerous vulnerabilities to the security of both the web app and Total Rekall's system. While some of these vulnerabilities are rather small and pose minimal threat to Total Rekall and their assets, others are critical and could pose a very significant threat to Total Rekall's assets. The discovered vulnerabilities allowed All-American Pentesting to use a variety of payloads to gain access to Total Rekall's web app as well as their system, remove sensitive data regarding the company, and escalate privileges within Total Rekall's system. These steps are shown below.

The first order of business for All-American Pentesting, was to test the security of the web application. The web application in question displayed a vulnerability to malicious script being run on the applications home page through multiple XSS (Cross Site Scripting) attacks. These attacks were successful in numerous areas of the web application. These areas include the home page as well as the comments page. The application also displayed a vulnerability to Local File Inclusion which allowed for files to be uploaded to the web applications VR Planner area of the web page. A vulnerability was also discovered on the web application's Login.php page through SQL injection which involves the injection of malicious code into the web application.

Open source data was also discovered through use of the OSINT frameworks. More specifically, through the use of Domain Dossier, you are able to view the WHOIS data for Total Rekall including information such as the physical location of the company that owns the domain name, IP addresses, date of creation, admin, etc. Information regarding the domain certification was also discovered to be viewable by searching crt.sh for "totalrekall.xyz". Admin login credentials were also discovered to be viewable in the HTML file of the login.php page of the web application. Login credentials were also discovered in Total Rekall's GitHub repository which allowed for the pentester to access host files and directories.

The next area tested was the Linux OS environment. Through the use of nmap scans on the network and subnet, All-American Pentesting was able to discover numerous hosts with IP addresses public on the subnet as well as one host was discovered to be running Drupal.

There were many vulnerabilities found within the Windows OS environment. FTP Enumeration was successful due to port 21 being open. A Meterpreter session was successfully created due to port 110 being open. A list of scheduled tasks was available and public using a Meterpreter shell. Also through the use of a Meterpreter shell, password files were accessible and password hashes were easily cracked. Many other sensitive files were public through Meterpreter as well. Using Kiwi, cached credentials were easily discovered and cracked.

In summary, Total Rekall's systems have numerous vulnerabilities that could be exploited by malicious actors in order to gain access to files, damage assets, and affect the overall functionality and business of Total Rekall. The purpose of this report is to reflect those vulnerabilities and for All-American Pentesting to provide consultation regarding these vulnerabilities and their remediation.

Summary Vulnerability Overview

Vulnerability	Severity
XSS reflected	Medium
XSS reflected (Advanced)	Medium
XSS stored	Critical
Sensitive Data Exposure	Critical
Local File Inclusion	Critical
Local File Inclusion (Advanced)	Critical
Sensitive Data Exposure	Critical
Open Source Data Exposure	Medium
Open Source Data Exposure	Medium
Nmap Scan Results	Critical
Nmap Scan Results (Aggressive)	Critical
User Credential Exposure (Hashed)	Critical
Subnet Nmap Scan Results	Critical
FTP Enumeration	Critical
SLMail Exploit	Critical
Windows Task Schedule Vulnerability	Critical
Sensitive Data Exposure/ Credential Dump	Critical
Public Directory Search	Medium
User Credential Exposure/ Credential Dump	Critical

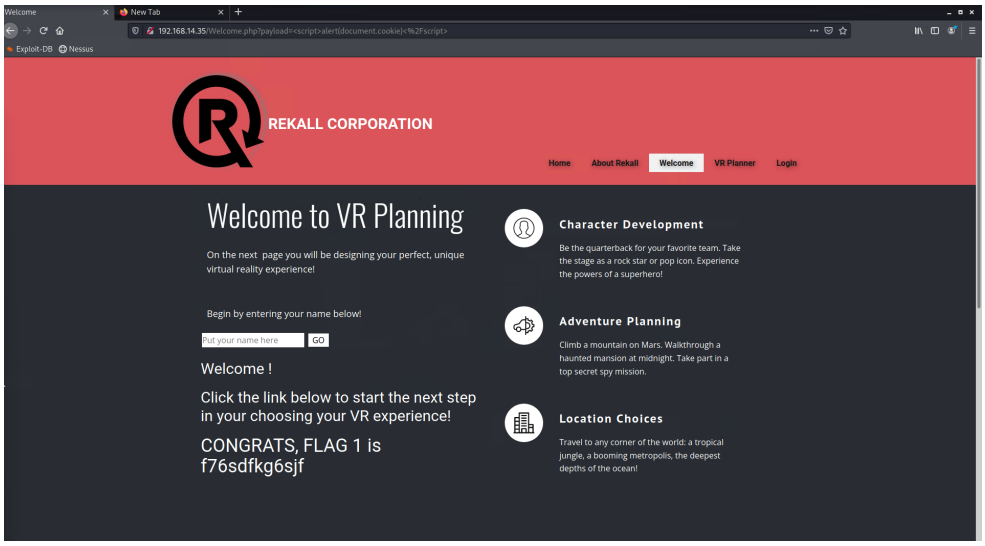
The following summary tables represent an overview of the assessment findings for this penetration test:

Scan Type	Total
Hosts	172.22.117.20 172.22.117.10 192.168.13.10 192.168.13.11 192.168.13.12 192.168.13.13 192.168.13.14 192.168.13.35
Ports	21 22 80 110

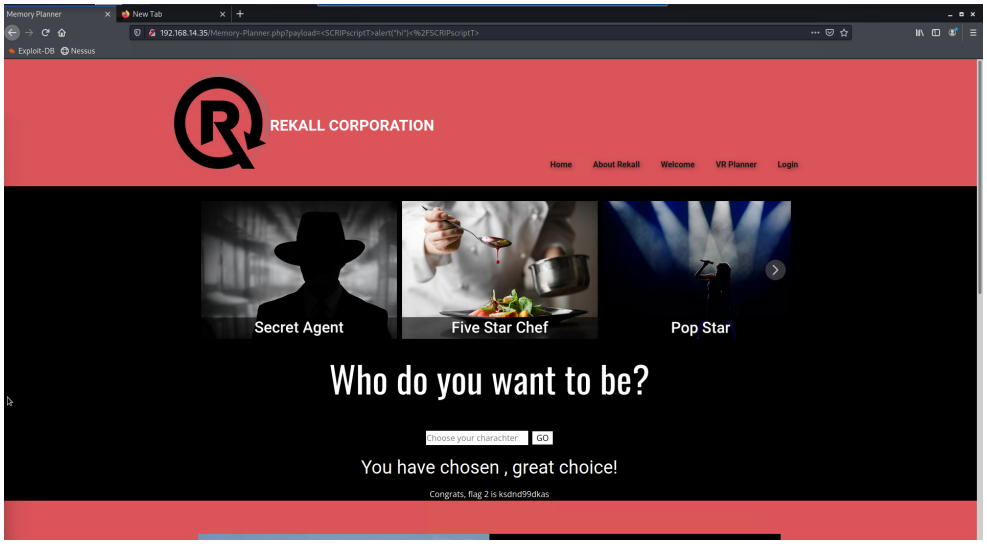
Exploitation Risk	Total
Critical	14

High	0
Medium	5
Low	0

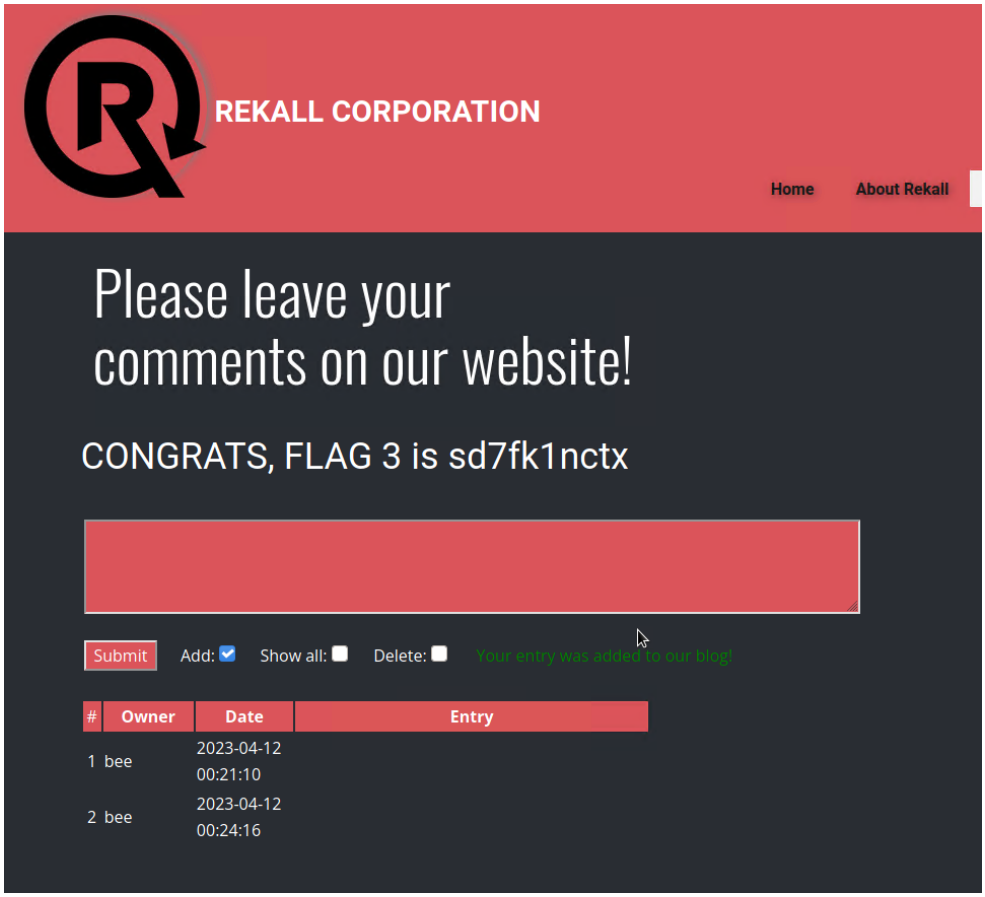
Vulnerability Findings

Vulnerability 1	Findings
Title	XSS Reflected
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	Medium
Description	Malicious script was reflected successfully on the web applications home page using <script>alert(“Hi Robert”)</script>
Images	
Affected Hosts	192.168.14.35
Remediation	input validation

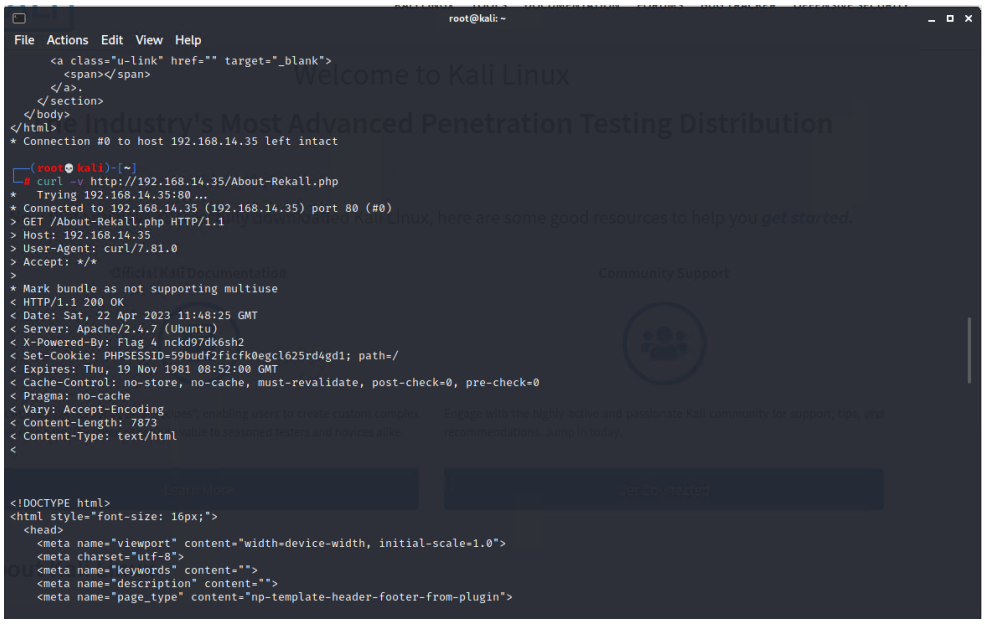
Vulnerability 2	Findings
Title	XSS Reflected (Advanced)
Type (Web app / Linux OS / WIndows OS)	Web Application

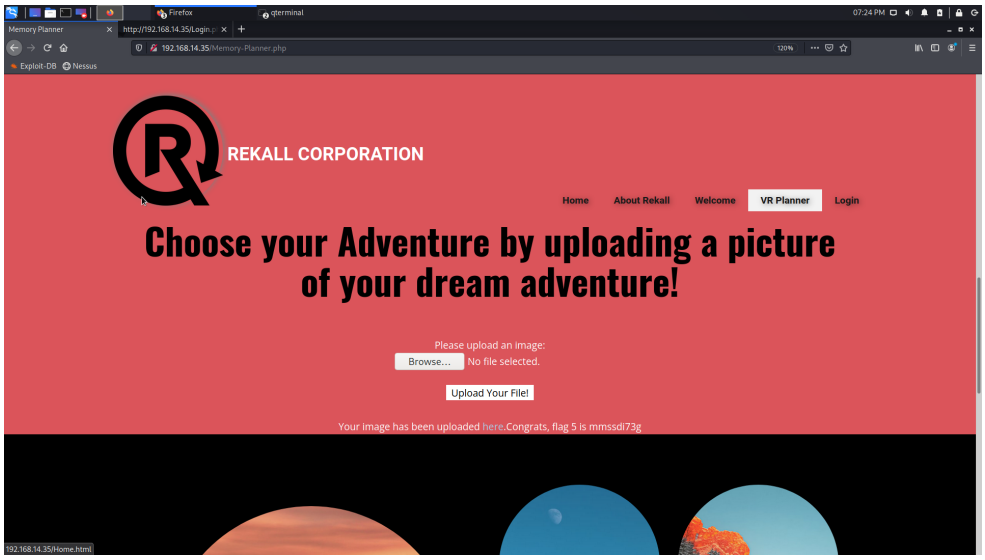
Risk Rating	Medium
Description	Use of malicious script to bypass input validation using code such as <SCRIPscriptT>alert("hi")</SCRIPscripTt>
Images	
Affected Hosts	192.168.14.35
Remediation	use XSS protection that protects against the use of script code

Vulnerability 3	Findings
Title	XSS Stored
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	Critical
Description	Entering <script>alert(“Hi”)</script> into the comment box revealed the third flag

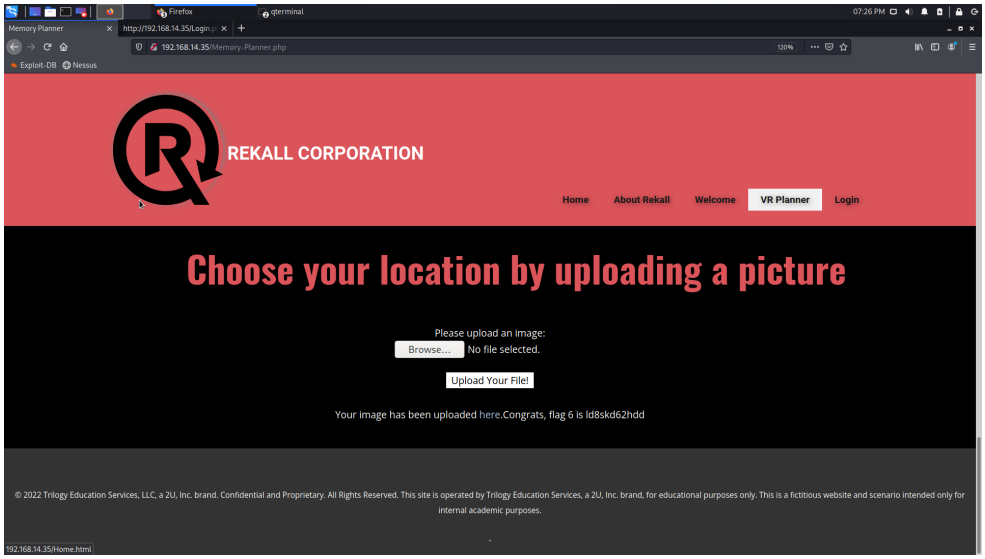
Images	
Affected Hosts	192.168.14.35
Remediation	Use XSS protection that protects against the use of script code

Vulnerability 4	Findings
Title	Sensitive Data Exposure
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	Critical
Description	The Curl command is used to

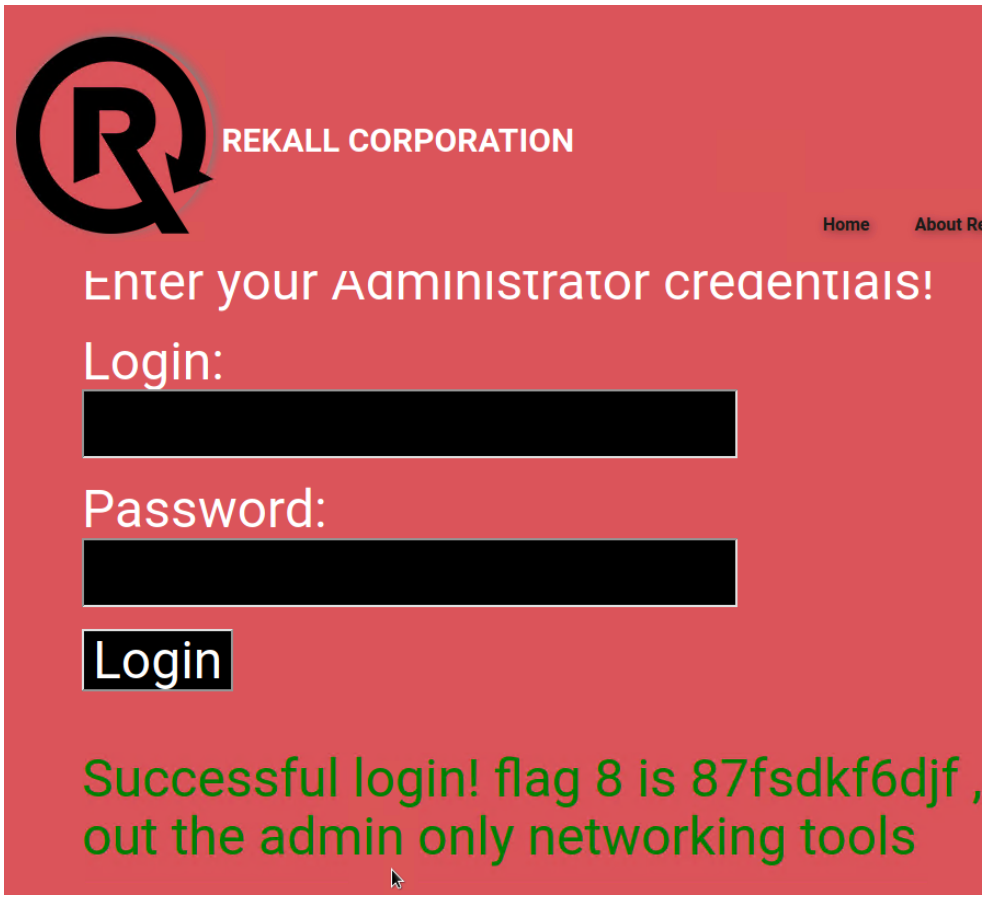
Images	
Affected Hosts	192.168.14.35
Remediation	apply stronger data encryption

Vulnerability 5	Findings
Title	Local File Inclusion
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	Critical
Description	PHP> file was uploaded to the VR Planner page
Images	
Affected Hosts	192.168.14.35

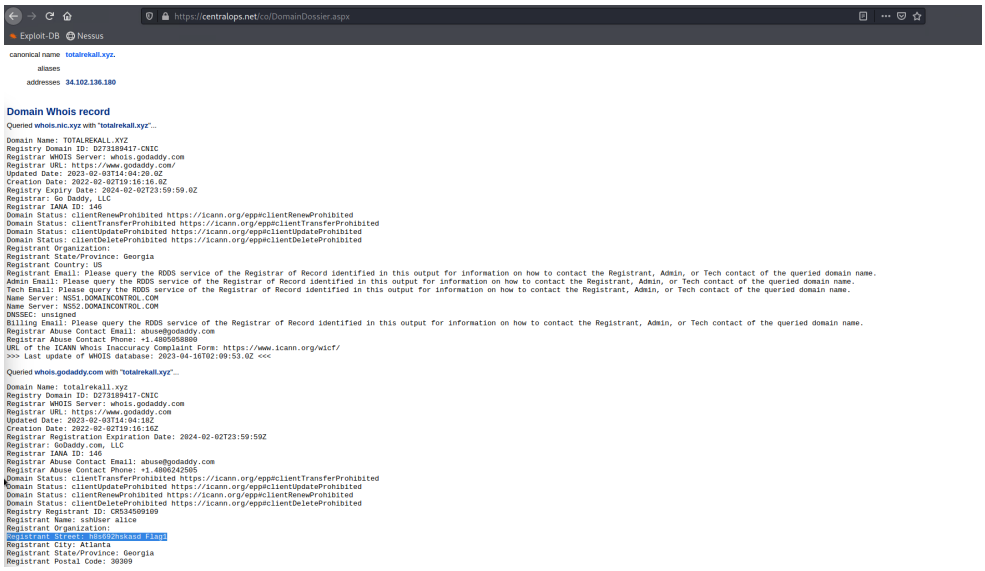
Remediation	Use whitelisted files and ignore all other files submitted to the web app

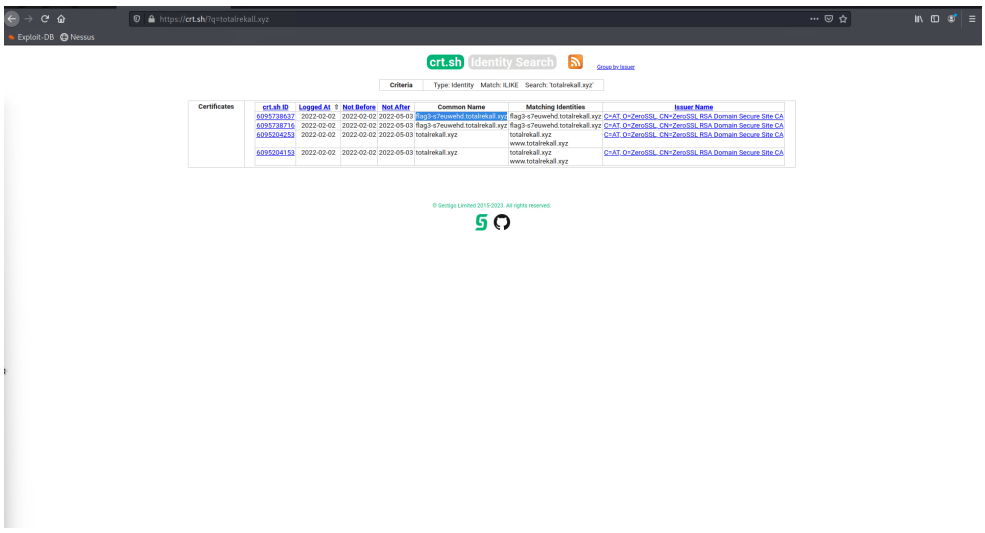
Vulnerability 6	Findings
Title	Local File Inclusion (Advanced)
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	Critical
Description	Input Validation checks for .jpg. Easily bypassed with the inclusion of .php
Images	
Affected Hosts	192.168.14.35
Remediation	Use whitelisted files and ignore all others

Vulnerability 7	Findings
Title	Sensitive Data Exposure
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	Critical
Description	Username and password are visible in HTML source code

Images	
Affected Hosts	192.168.14.35
Remediation	Delete Information from HTML source code and implement 2-factor authentication

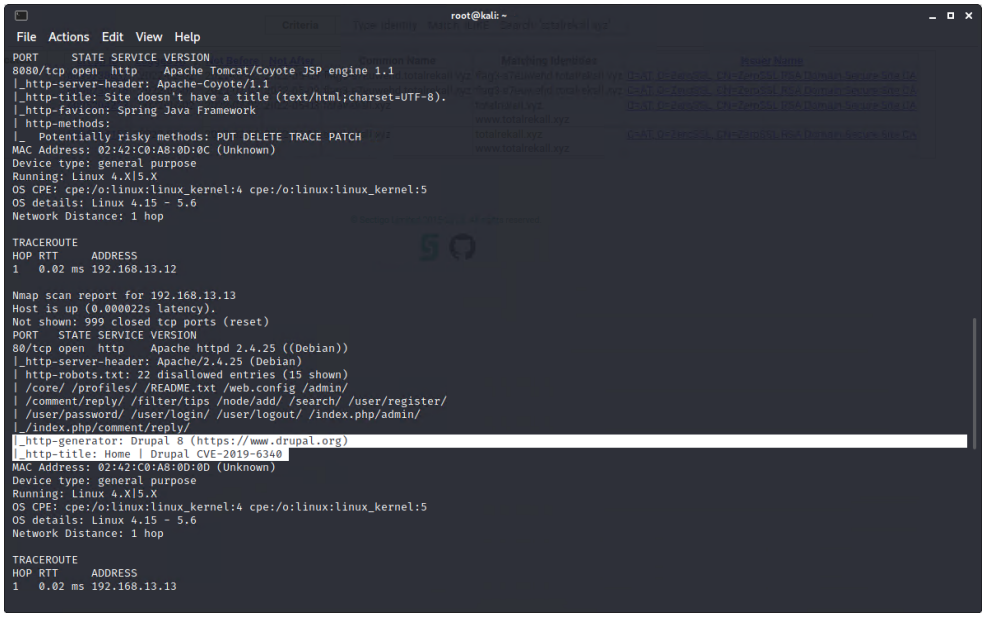
Vulnerability 8	Findings
Title	Open Source Data Exposure
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	Medium
Description	Sensitive information is visible on the Domain Dossier website under WHOIS data through OSINT for totalrekall.xyz

Images	
Affected Hosts	https://centralops.net/co/DomainDossier.aspx
Remediation	Make sure none of your sensitive data is public

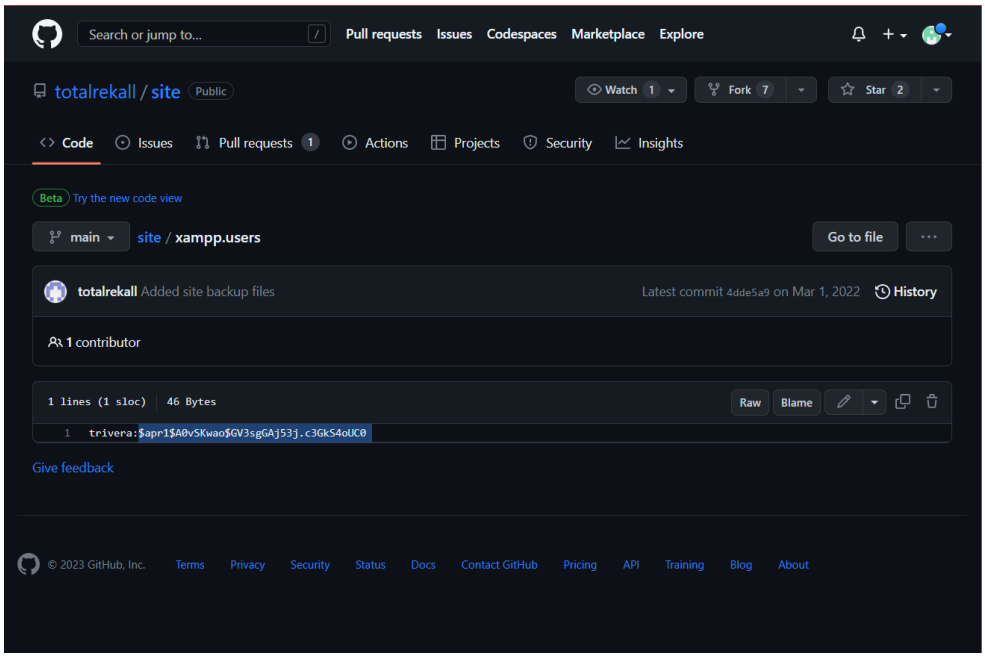
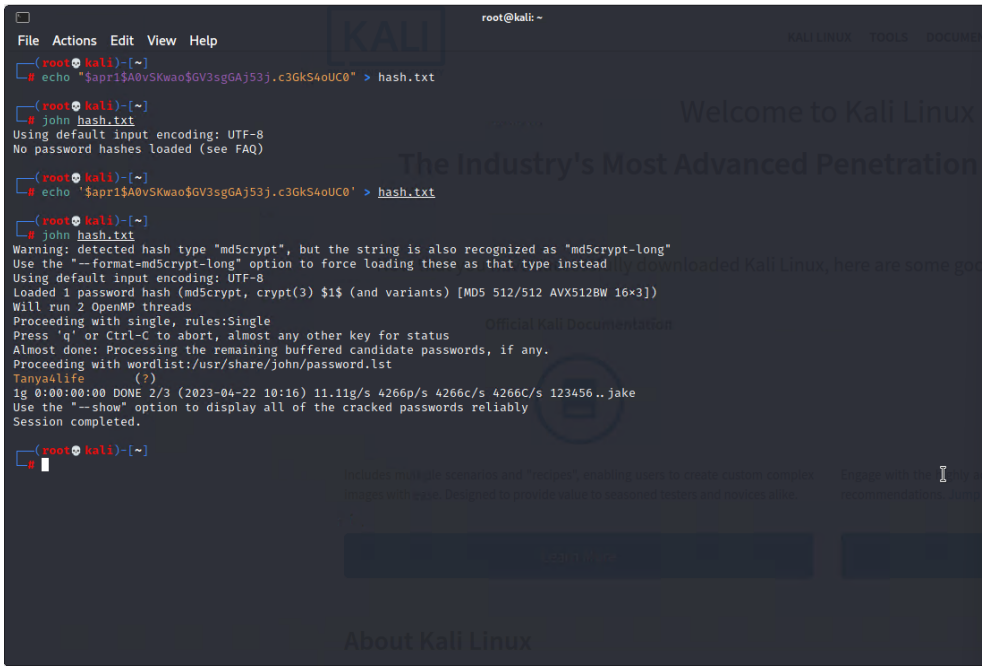
Vulnerability 9	Findings
Title	Open Source Data Exposure
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	Medium
Description	totalrekall.xyz was search on crt.sh and certificate information was found
Images	
Affected Hosts	34.102.136.180
Remediation	encrypt information so it won't be exposed on the crt.sh site

Vulnerability 10	Findings
Title	Nmap Scan Results
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	Nmap scan of the network revealed 5 hosts with IP addresses
Images	
Affected Hosts	192.168.13.10 192.168.13.11 192.168.13.12 192.168.13.13 192.168.13.14
Remediation	Block IP addresses for unauthorized users

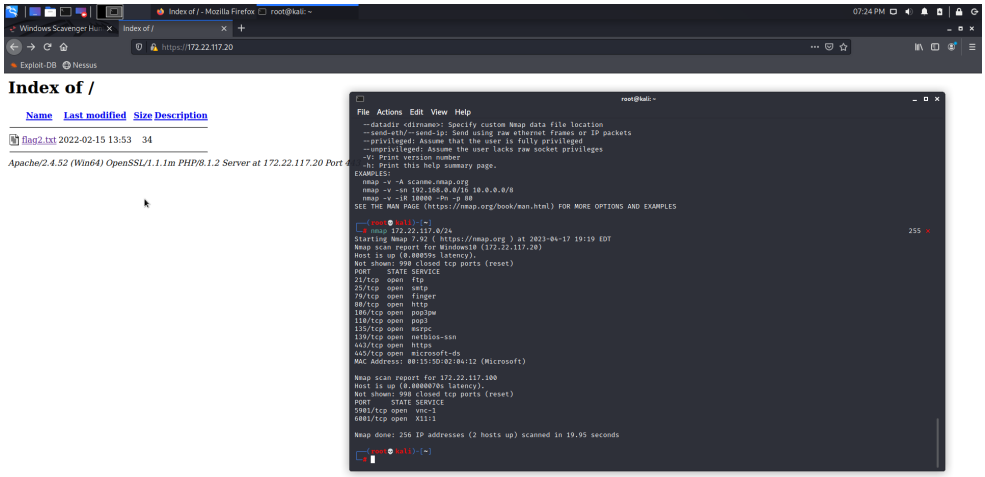
Vulnerability 11	Findings
Title	Nmap Scan Results (Aggressive)
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	Aggressive nmap scan reveals host is running Drupal

Images	
Affected Hosts	192.178.13.12
Remediation	Block scans and restrict returned information

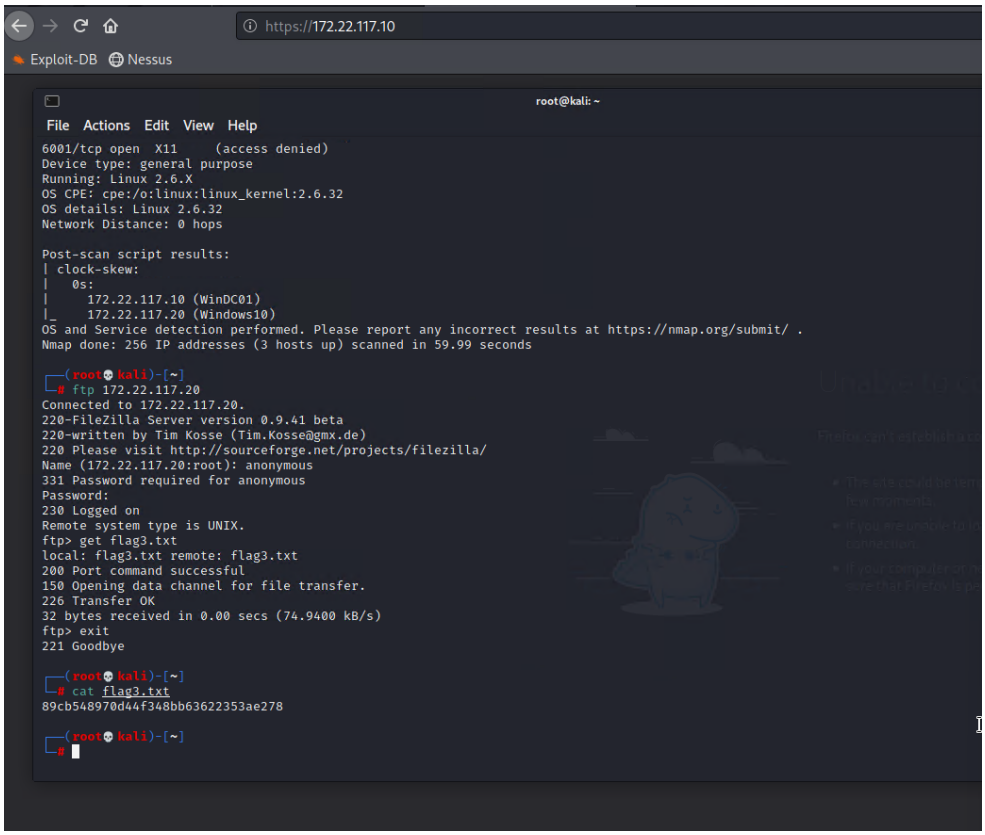
Vulnerability 12	Findings
Title	User Credential Exposure
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	Critical
Description	User credential hash is easily found on total rekall GitHub repository

Images	 
Affected Hosts	https://github.com/totalrekall/site/blob/main/xampp.users
Remediation	Remove sensitive information from public view

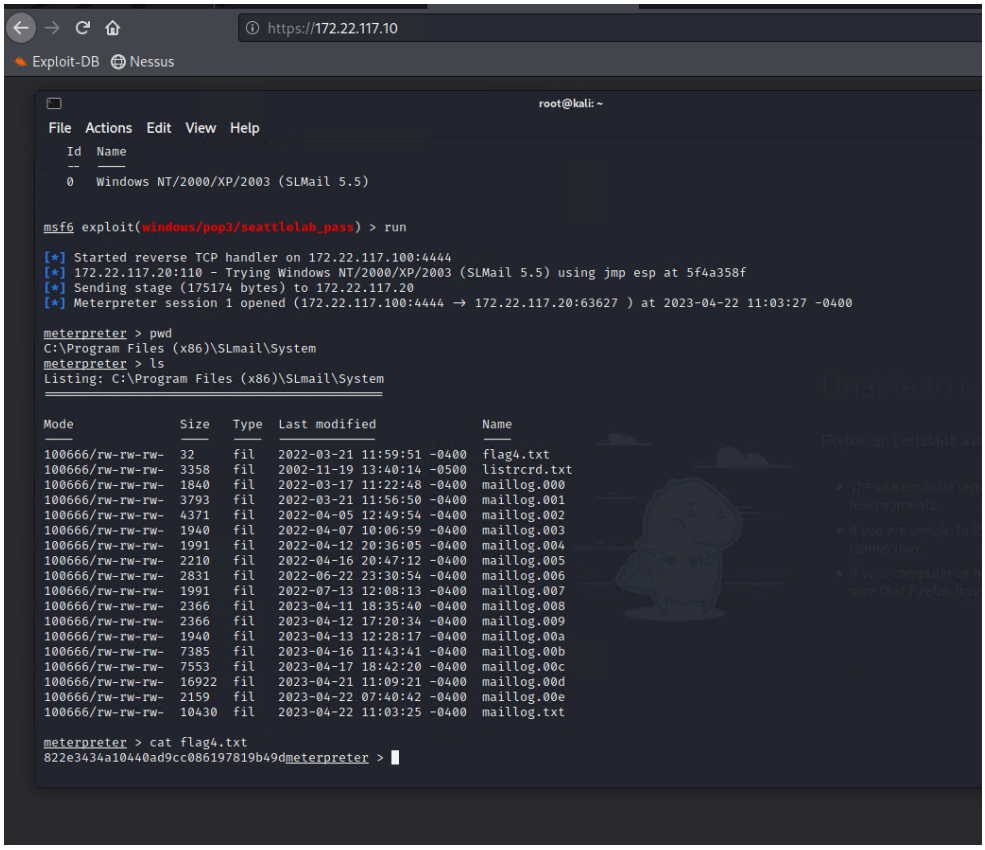
Vulnerability 13	Findings
Title	Subnet Port Scan
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	Critical

Description	An Nmap scan of the subnet revealed port 80 to be open and using credentials from repository, pentesters were able to gain access to the root directory
Images	
Affected Hosts	1172.22.117.20
Remediation	Require stronger credentials or use 2-factor authentication

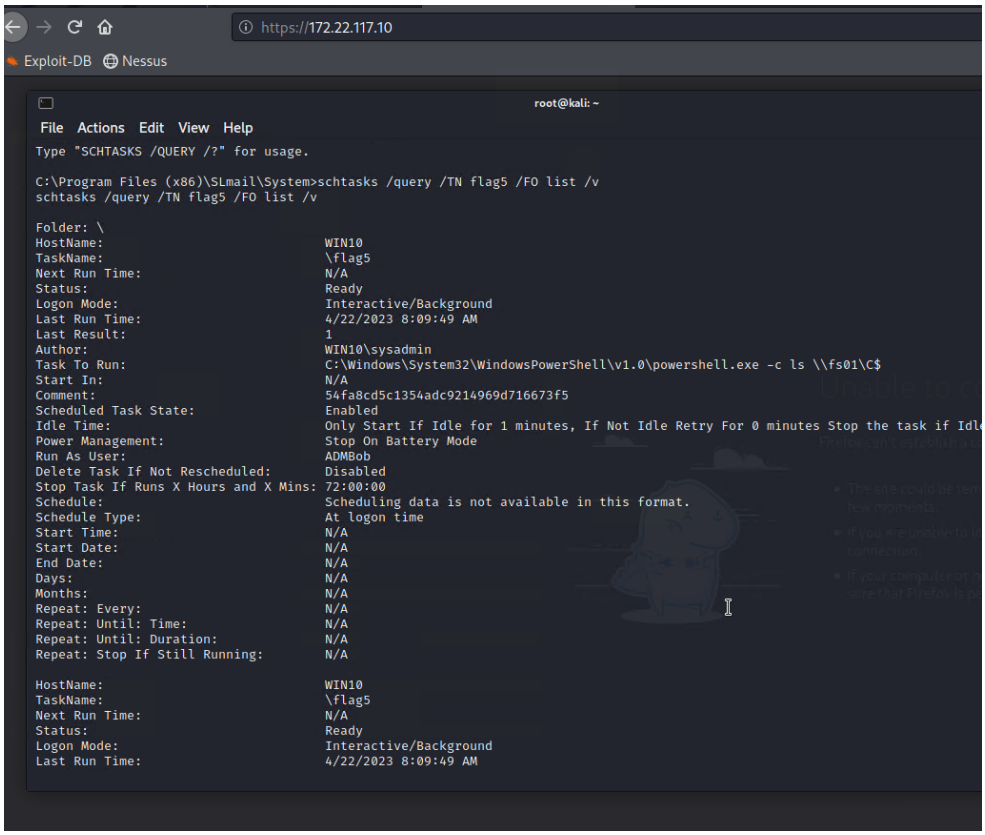
Vulnerability 14	Findings
Title	FTP Enumeration
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Critical
Description	Open port 21 allows for FTP connection to host IP resulting in successful access and download of files

Images	
Affected Hosts	172.22.117.20
Remediation	close or restrict access to port 21

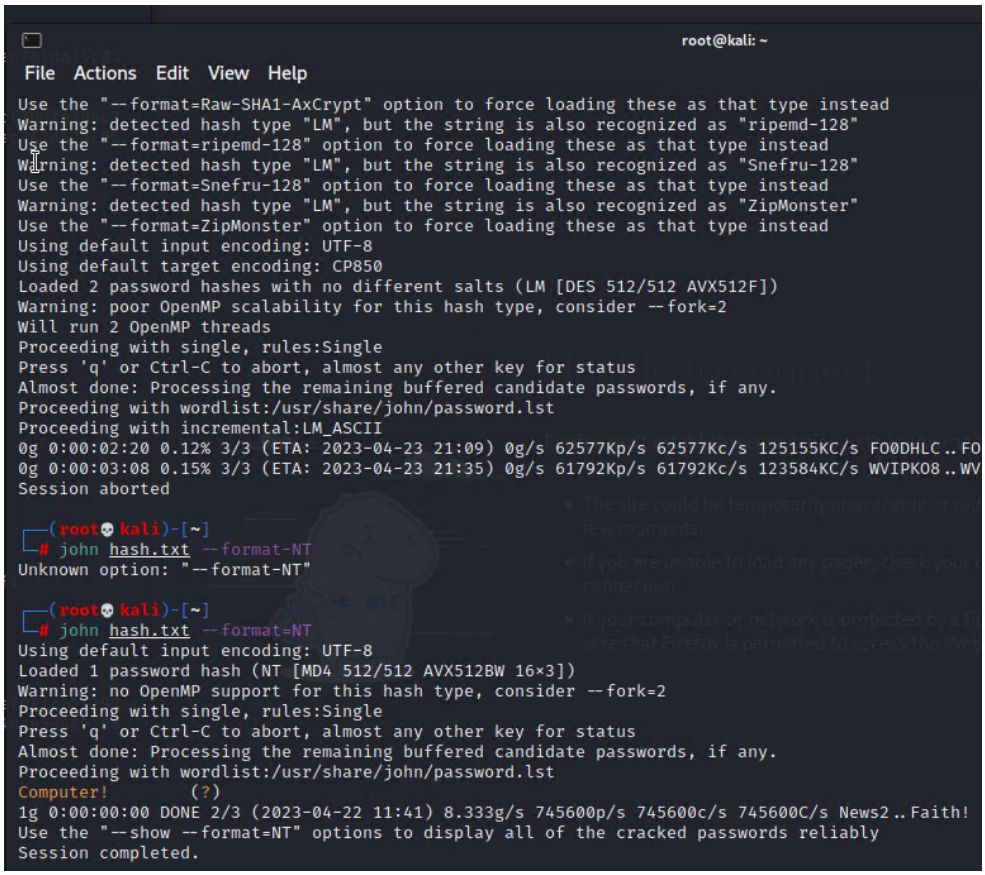
Vulnerability 15	Findings
Title	SLMail Exploit
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Critical
Description	Open port 110 with the use of windows.pop3.seatlelab_pass exploit in Metasploit allowed for the successful creation of a Meterpreter session

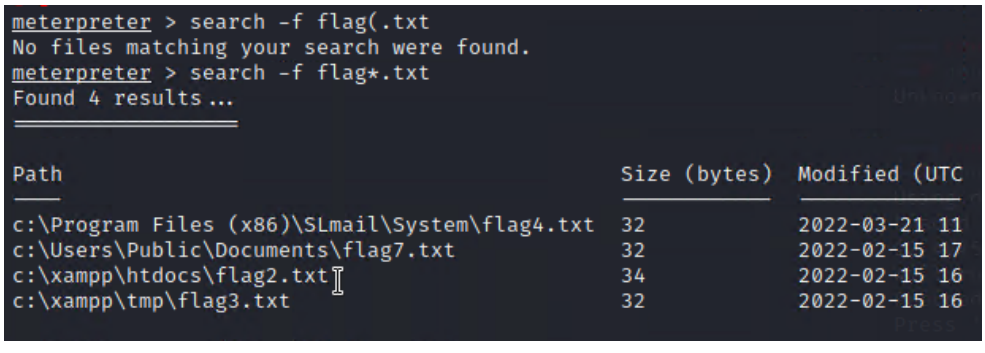
Images	
Affected Hosts	172.22.117.20
Remediation	Close or restrict access to port 110 and/or remove SLMail service

Vulnerability 16	Findings
Title	Windows Task Schedule vulnerability
Type (Web app / Linux OS / WIndows OS)	WIndows OS
Risk Rating	Critical
Description	Scheduled tasks can be seen through the use of a Meterpreter shell and using the command schtasks /query

Images	
Affected Hosts	172.22.117.10
Remediation	Update user file restrictions

Vulnerability 17	Findings
Title	Sensitive Data Exposure/ Credential Dump
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Critical
Description	Continuing to use Metasploit and the Meterpreter session, password files were easily accessible. passwords were easily cracked using John.

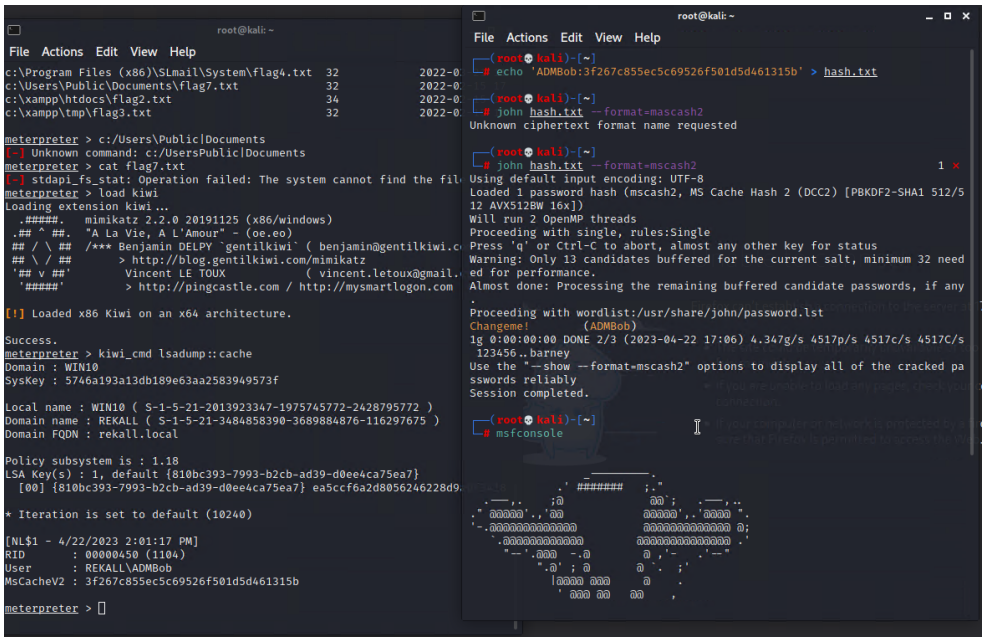
Images	
Affected Hosts	172.22.117.20
Remediation	Update user permissions on files

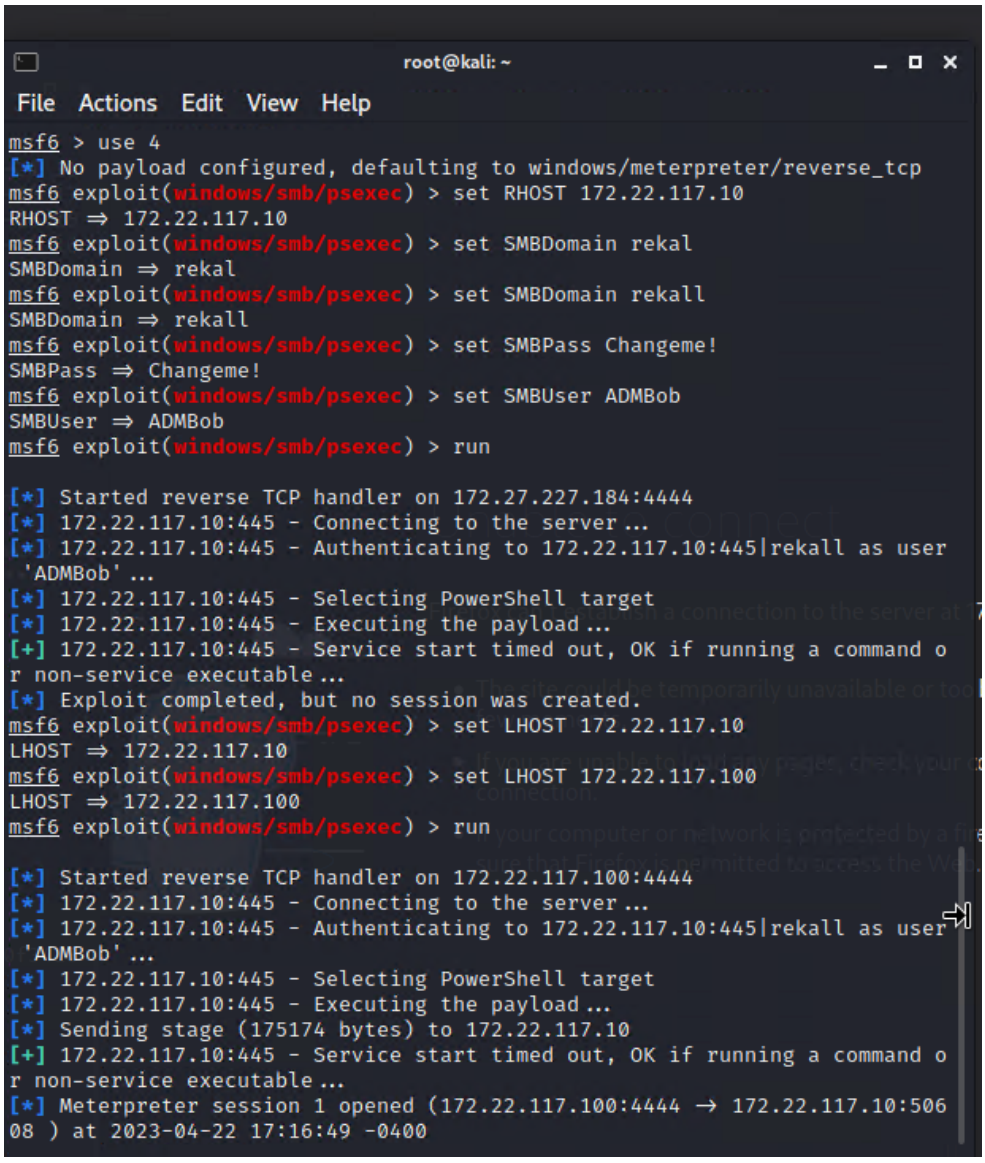
Vulnerability 18	Findings
Title	Public Directory Search
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Medium
Description	Using the search command in Meterpreter revealed the flag7.txt file
Images	

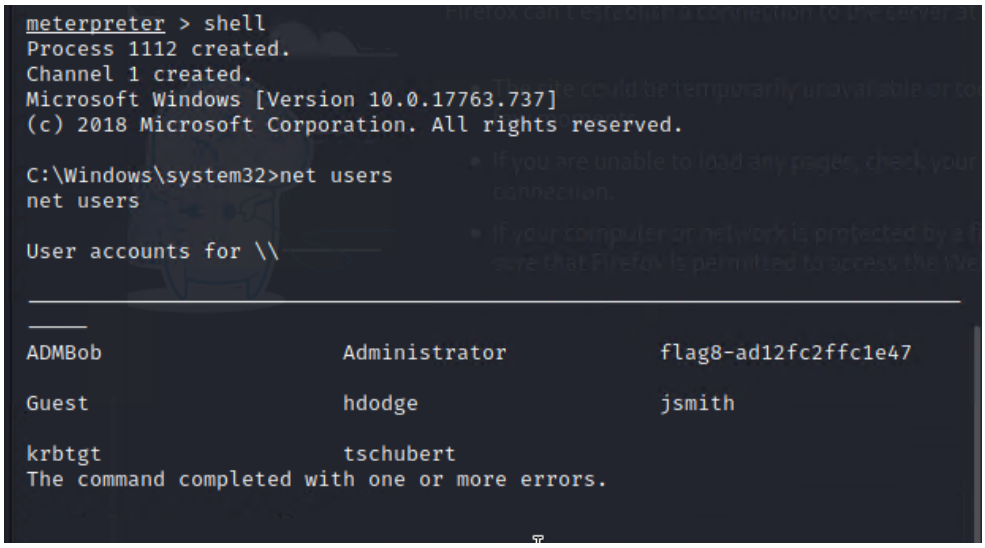
Affected Hosts	172.22.117.20
Remediation	restrict unauthorized access to sensitive files

Vulnerability 19	Findings
Title	User Credential Exposure/ Credential Dump
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Critical
Description	Using Kiwi to dump cached credentials reveals ADMBob as administrator. Using John, the hashed password can be cracked

Images





	
Affected Hosts	172.22.117.10
Remediation	Clear cache regularly, Better secure sensitive information