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	The NC1 Group
Contact Name	Allison Ray, Rob Kupper, Brianna Green, Jolyne Ndombe, Richard Gray
Contact Title	

Document History

Version	Date	Author(s)	Comments
001	3/5/2024	Brianna Green, Richard Gray, Allison Ray, Jolyne Ndombe, Robert Kupper	First and Final

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 network and system 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.

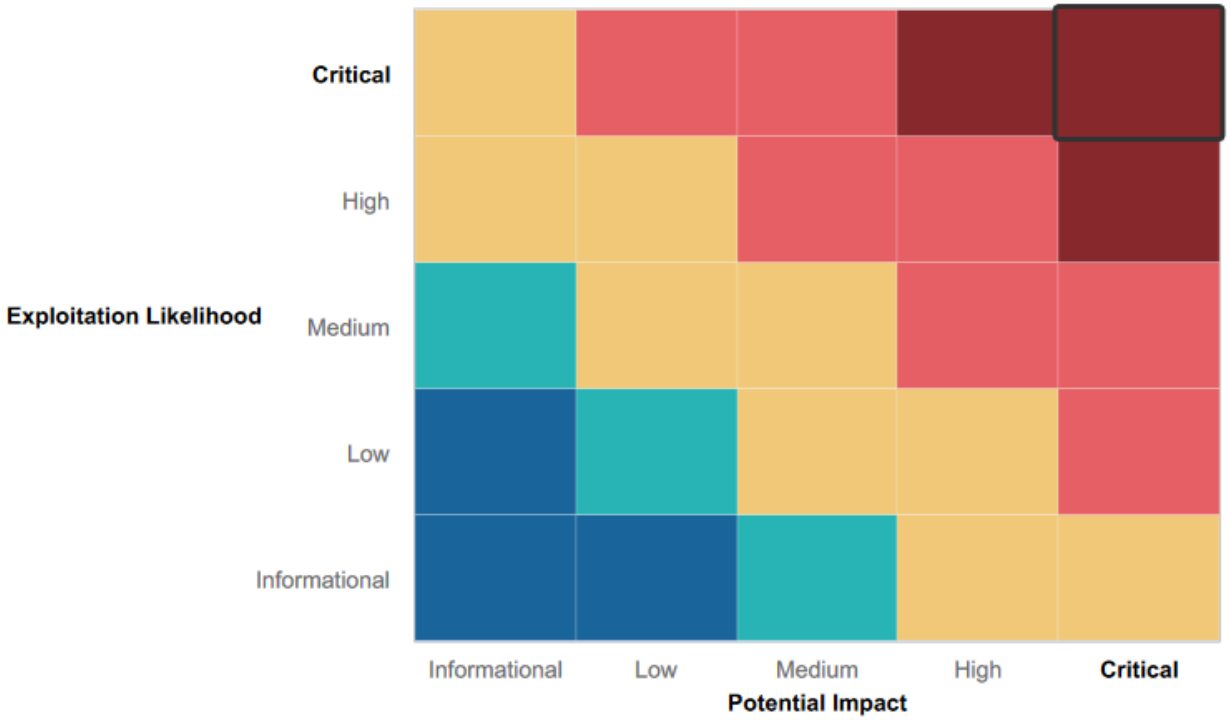
Executive Summary of Findings

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.

- Certain web application input fields were protected against XSS exploits and required further probing
- Some input fields had proper input validation

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 App is vulnerable to several attacks, including XSS scripting, Local File Inclusion (LFI), and command injections, leaving vulnerable data to be easily accessed and the potential to upload malicious scripts to be stored on Rekall's servers.
- Credentials were being stored in HTML source code
- Rekall's server physical address is publicly available
- Linux and Windows machines were both found to have several cases of sensitive data exposure, which left important information easily accessible and could compromise the system.
- Several open ports were discovered with basic Nmap scans, revealing potential vulnerabilities throughout Rekall's network.

Executive Summary

During our penetration testing of Rekall's IT assets, The NC1 group identified several vulnerabilities. These vulnerabilities include several critical ones that could have a devastating impact on Rekall's revenue and reputation. The NC1 group was able to infiltrate Rekall's assets, gain access to sensitive data, and escalate privileges within systems. We began by testing Rekall's Web Application, which was found to be vulnerable to multiple attacks. Specifically, we discovered that the web app was vulnerable to an XSS Reflected attack that allowed malicious scripts to be run on the home page. Local File Inclusion (LFI) was also possible, as files could be uploaded from the VR Planner page. For example, a Local File Inclusion was successfully executed by uploading a sample .php file from the toolbar to find flag 5. Furthermore, an XSS-stored vulnerability was identified on the comments page that allowed for scripting code to be run. Additionally, SQL injection attacks could be run on the login.php toolbar, and the networking.php page was vulnerable to a command injection attack. We were shocked to find that user credentials were stored in plain view within the HTML source code of the login.php page, making them easily accessible to anyone who highlighted the page in a web browser. The file robots.txt was also exposed and easily accessible. Research uncovered user credentials in a GitHub repository, which led to unauthorized access to the web host's files and directories. Within the Linux environment, The NC1 group discovered that 5 IP addresses were publicly exposed and vulnerable. We found that FTP port 21 was open and vulnerable for the Windows environment, as was Port 110, which is used for the SLMail service. A password hash file was accessed through Metasploit, which could be cracked. Meterpreter could also be used to display directories on public Windows directories. In conclusion, the vulnerabilities identified by The NC1 group could be exploited maliciously to cause massive damage to the assets and functionality of the business. Therefore, The NC1 group has provided recommendations for mitigating each of these vulnerabilities to prevent any harm or loss that could result.

Summary Vulnerability Overview

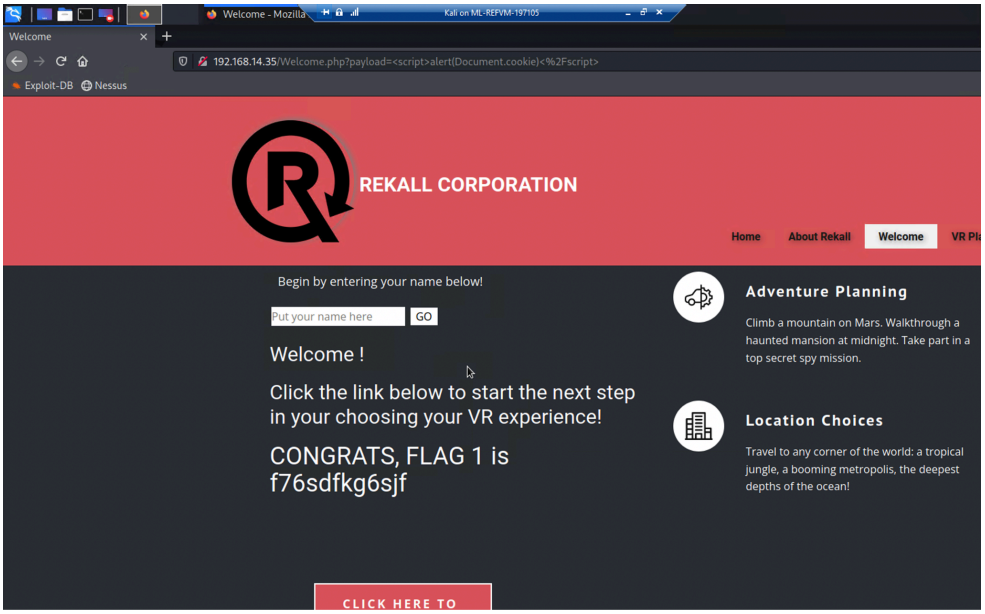
Vulnerability	Severity
Cross Site Scripting Vulnerability (XSS) in the “Put your name in Here”.	**High**
Reflected Cross Site Scripting Vulnerability (XSS) Memory-Planner.php webpage	**Medium**
XSS Vulnerability On the comments page	**Medium**
Sensitive Data Exposure - In HTTP header	**Low**
Local File Inclusion (LFI)	**Critical**
Local file Extraction	**Medium**
Sensitive data exposure (login credentials stored in HTML comments)	**Critical**
Sensitive data exposure (login credentials in an accessible file (robots.txt).	**Medium**
Whois Domain/ totalrekall website- User name alice in records	**Medium**
Sensitive data stored in TXT of DNS Record	**Low**
Data from the CRT record was used in enumerating the network	**Low**
Nmap Scan/Network Host	**Medium**
FTP	**Medium**
GitHub Page Totalrekall	**Low**

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

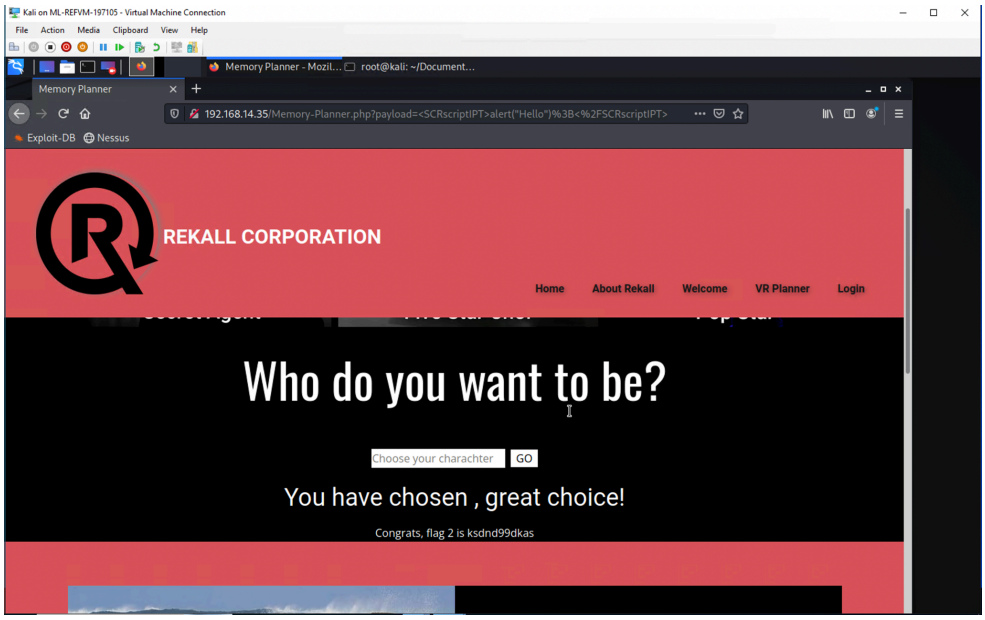
Scan Type	Total
Hosts	172.22.117.20 172.22.117.100 34.102.136.180 192.168.13.10 192.168.13.12 192.168.14.35 192.168.13.14 192.168.13.13
Ports	21, 22, 80, 110,106

Exploitation Risk	Total
Critical	4
High	1
Medium	2
Low	2

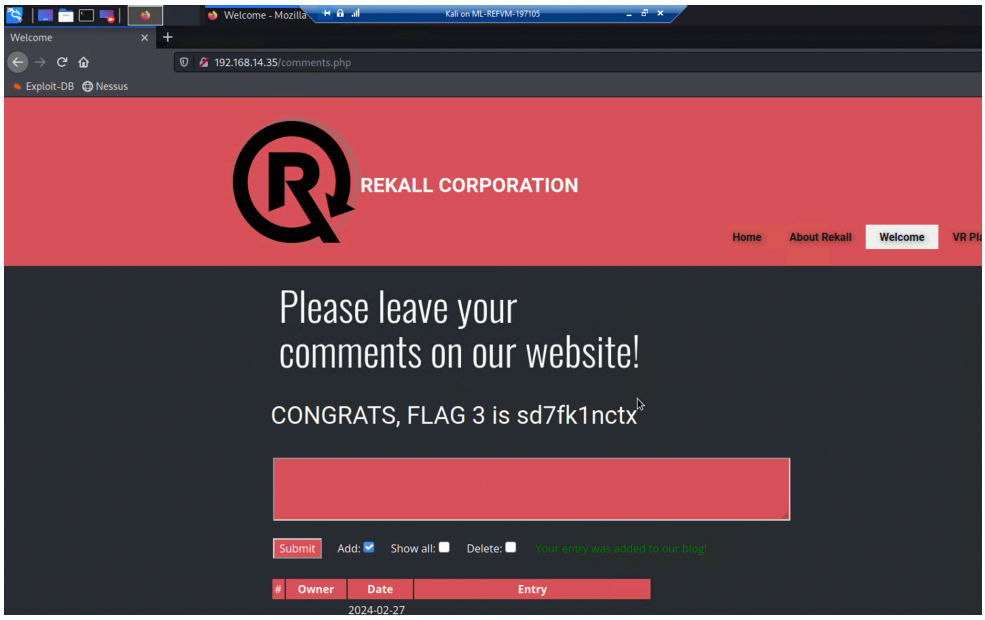
Vulnerability Findings

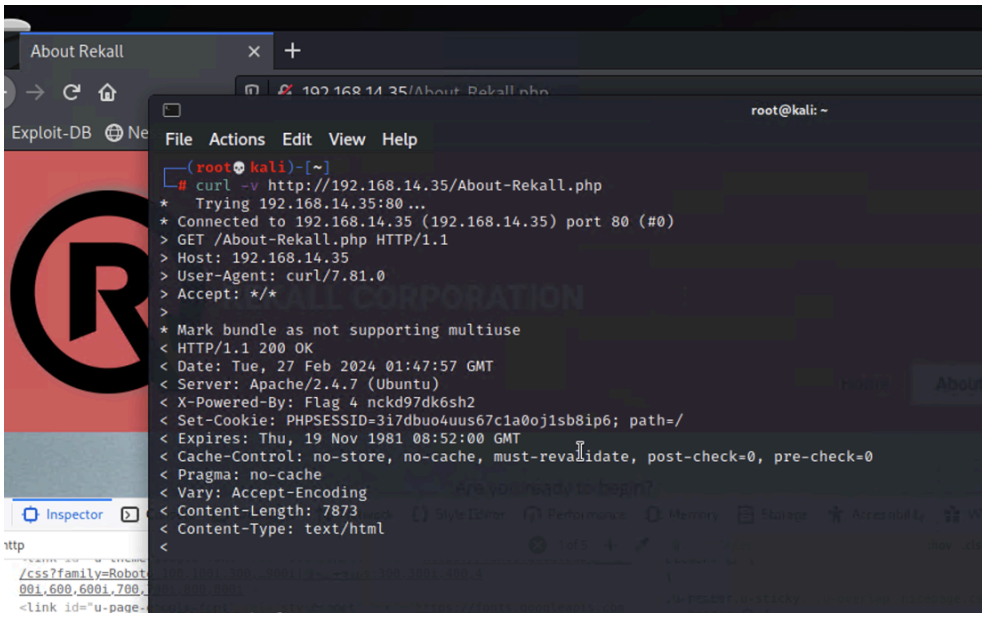
Vulnerability 1	Findings
Title	XSS Vulnerability
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	High
Description	Enter Playload in “ Put your name in Here” <script>alert(Document.cookie)</script>
Images	
Affected Hosts	192.168.14.35
Remediation	Input Validation

Vulnerability 2	Findings
Title	XSS Reflected
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Medium
Description	Used the payload below on the Memory-Planner.php webpage <SCRscriptIPT>alert(“Hello”);</SCRscriptIPT>

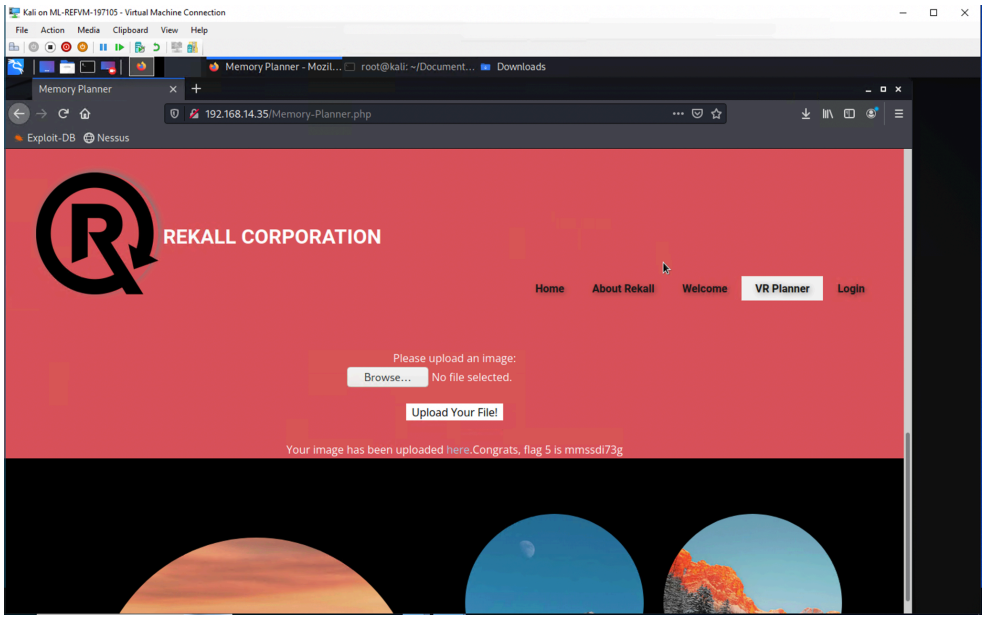
Images	
Affected Hosts	192.268.14.35
Remediation	input validation

Vulnerability 3	Findings
Title	XSS Vulnerabilities
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Critical
Description	On the comments page, we entered <script>alert(“cheers”);</script> to reveal flag 3

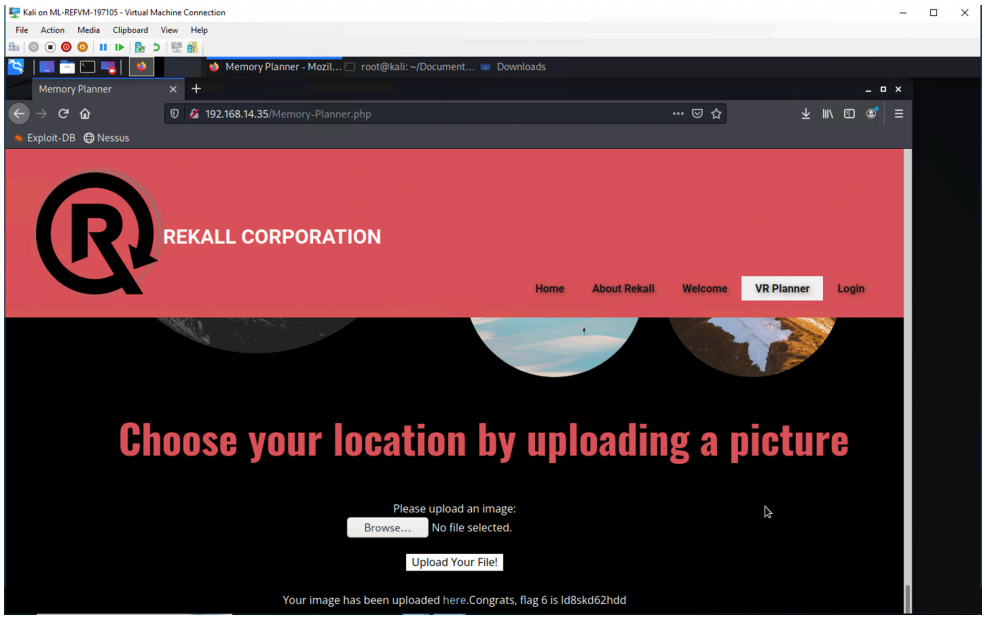
Images	
Affected Hosts	192.168.14.35
Remediation	Implement XSS protection to disallow the injection of script code

Vulnerability 4	Findings
Title	Sensitive Data Exposure
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Low
Description	Found flag in HTTP header by using curl -v http//192.168.14.35/About-Rekall.php
Images	

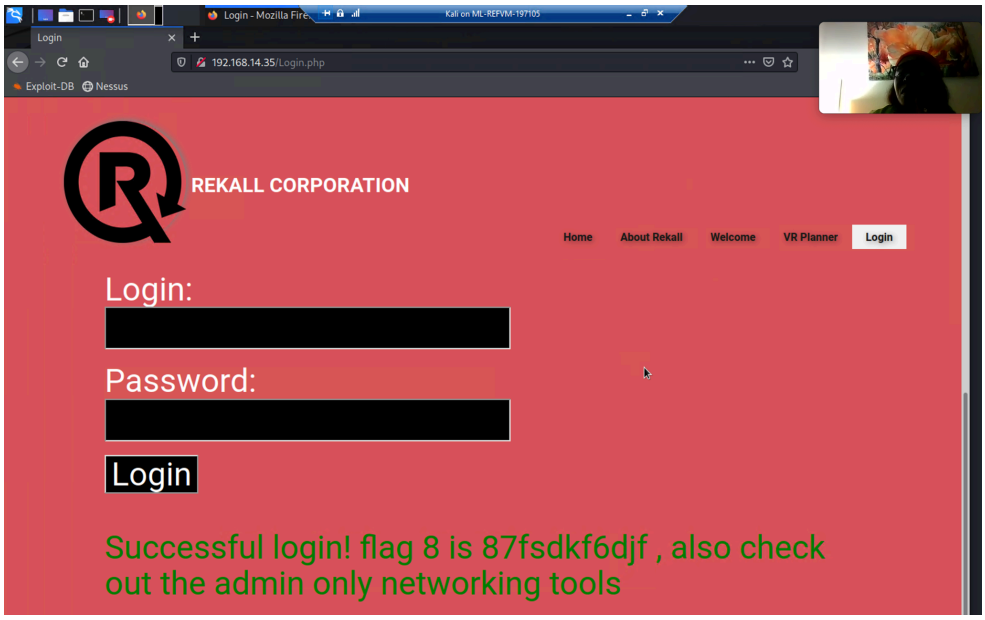
Affected Hosts	AboutRekall.php

Vulnerability 5	Findings
Title	Local File Inclusion (LFI)
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Critical
Description	LFI successfully executed by uploading a sample .php file from the toolbar that was located on the VR Planner page
Images	
Affected Hosts	192.168.14.35
Remediation	Limit the API to allow inclusion only from a directory and directories below it. This ensures that any potential attack cannot perform a directory traversal attack.

Vulnerability 6	Findings
Title	Local file
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Medium
Description	Changed the test.jpg file name to test.jpg.php and uploaded the file to get the flag

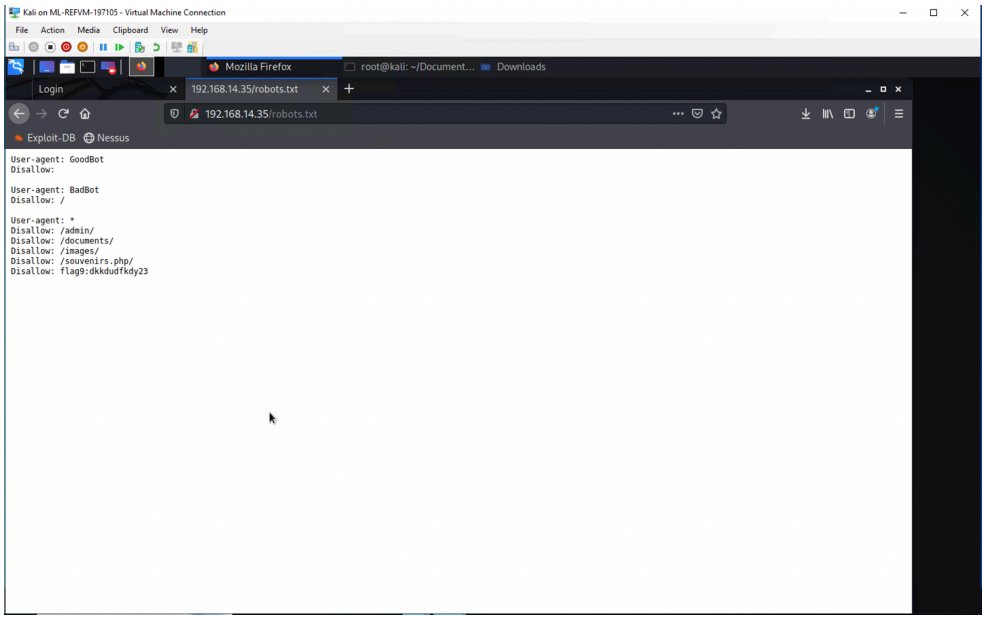
Images	
Affected Hosts	192.168.14.35
Remediation	Strong input validation, limiting file types for uploads, and restricting file paths to prevent the execution of unintended files

Vulnerability 7	Findings
Title	Sensitive data exposure
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Critical
Description	Found the credentials in the HTML source code, entered login and password on the login.php page

Images	
Affected Hosts	login.php
Remediation	Sensitive information shouldn't be stored in HTML comments or publicly accessible code, implement proper access controls, and encrypt sensitive data whenever possible

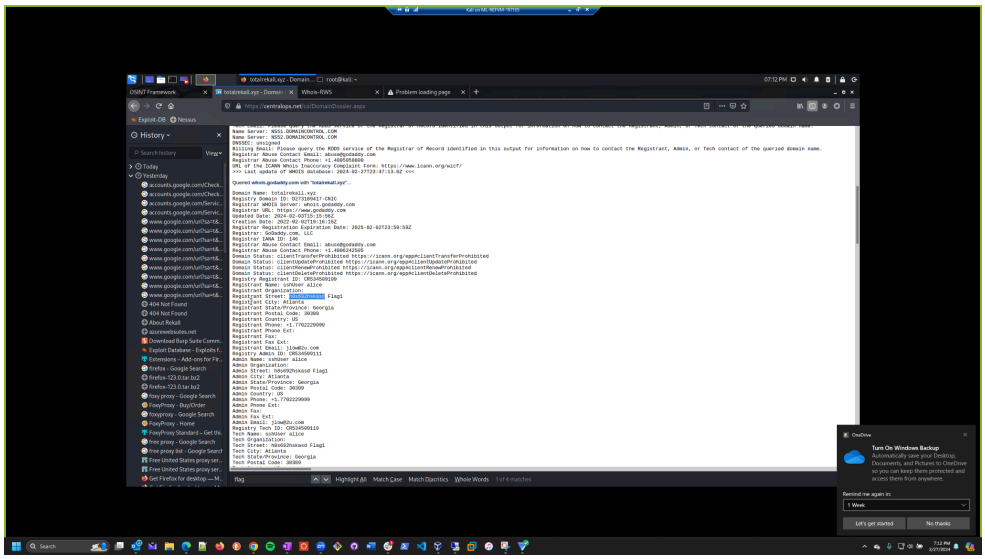
Add any additional vulnerabilities below.

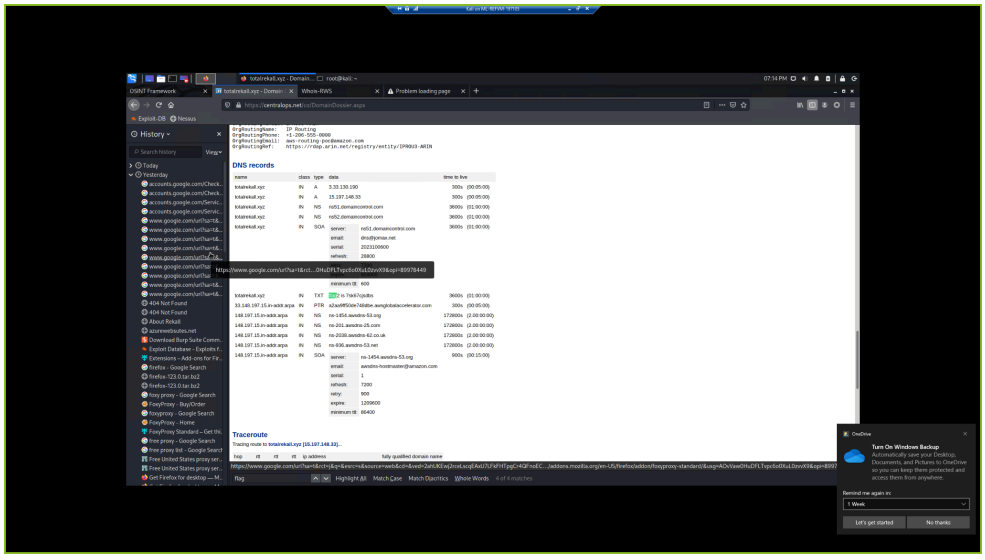
Vulnerability 8	Findings
Title	Sensitive data exposure
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	medium
Description	Checked robots.txt with IP and found flag 9

Images	
Affected Hosts	192.186.14.35
Remediation	Don’t store sensitive information in robots.txt or other publicly accessible files. Use appropriate access controls and authentication mechanisms.

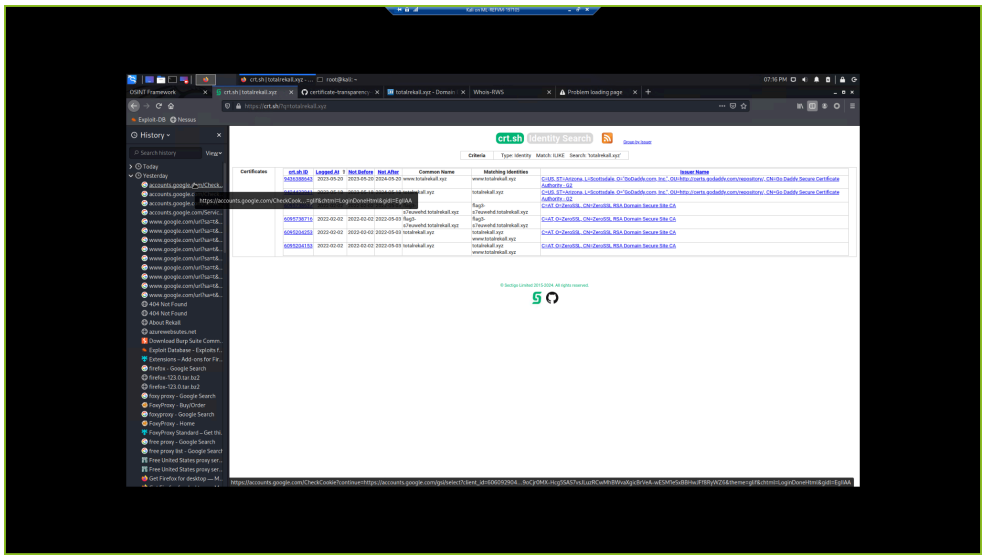
DAY 2

Vulnerability 1	Findings
Title	Whois Domain/ total recall website
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	low
Description	Use Dossier source tool within domain dossier to find information about whois domain for totalrekall.xyz

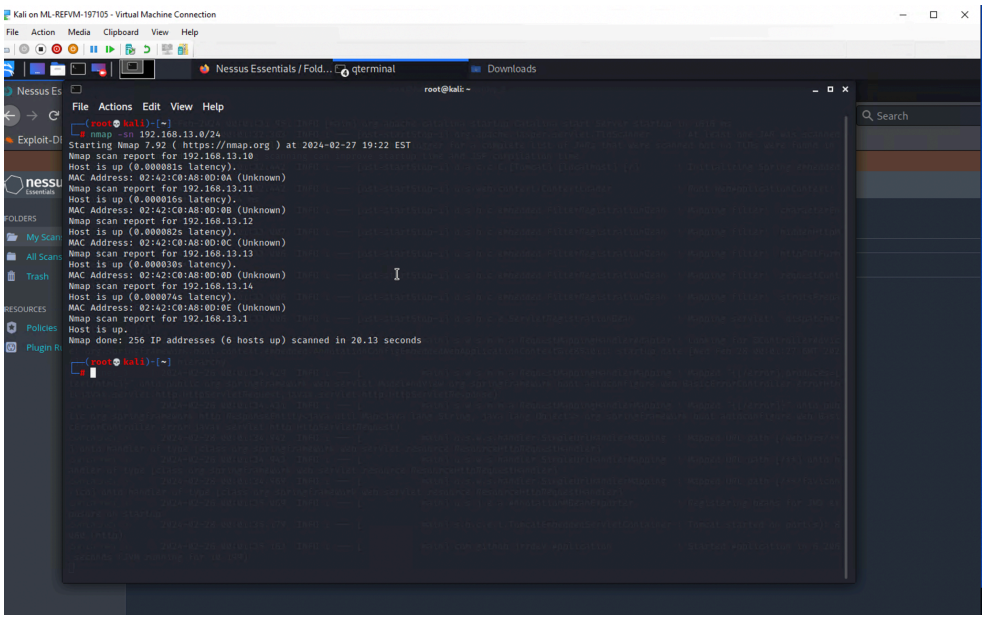
Images	

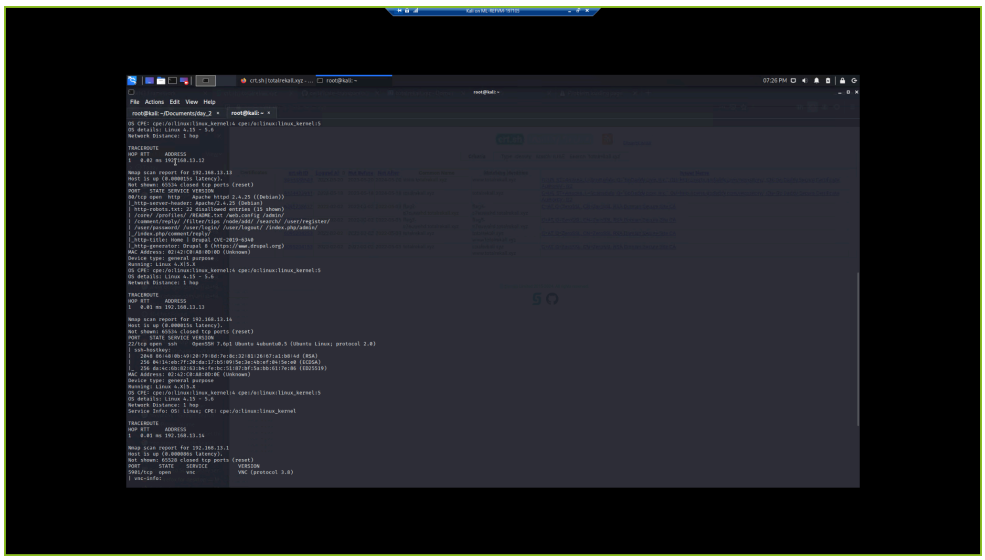
Vulnerability 2	Findings
Title	Whois Lookup IP
Type (Web app / Linux OS / WIndows OS)	Linux
Risk Rating	low
Description	looked up DNS records
Images	

Vulnerability 3	Findings
Title	Open source data

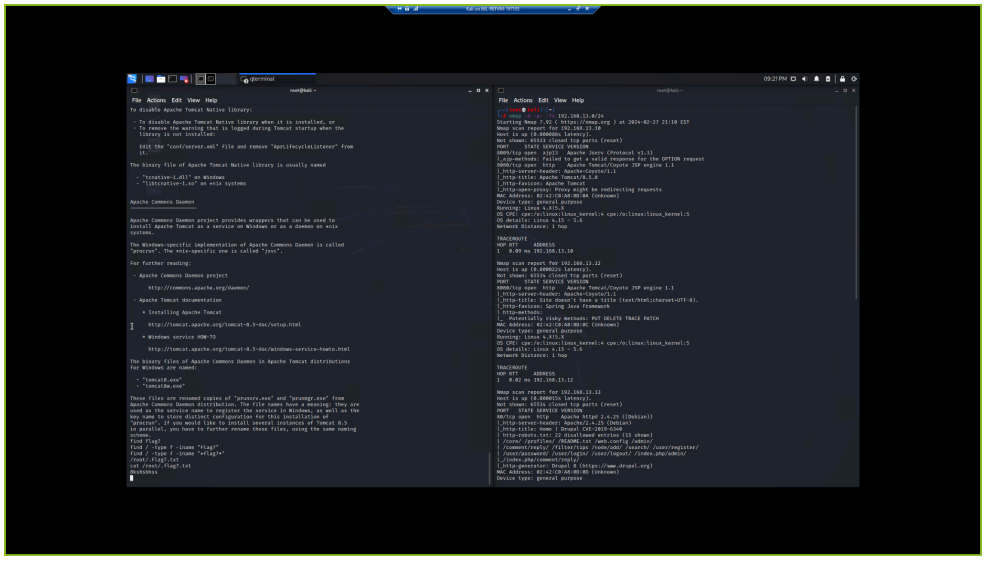
Type (Web app / Linux OS / WIndows OS)	web app
Risk Rating	Low
Description	searched for total recall xyz on crt.sh
Images	

Vulnerability 4	Findings
Title	NMap Scan Results
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	critical
Description	NMap scan on 192.168.13.0/24 showed 5 hosts are visible with exposed IP's

Images	

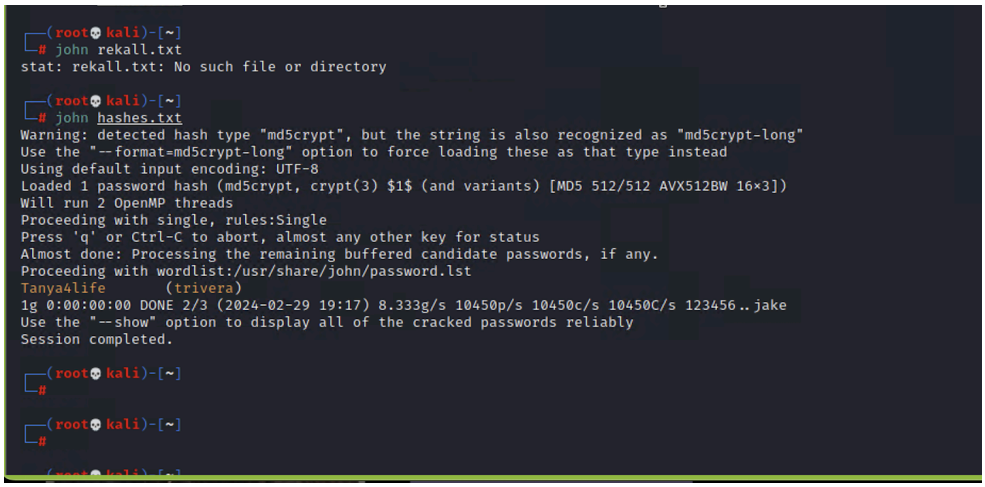
Vulnerability 5 (Flag 5)	Findings
Title	Open VNC port using an unpatched version (3.8)
Type (Web app / Linux OS / WIndows OS)	Linux
Risk Rating	Critical
Description	An outdated version of VNC is running that will allow access to a command shell
Images	

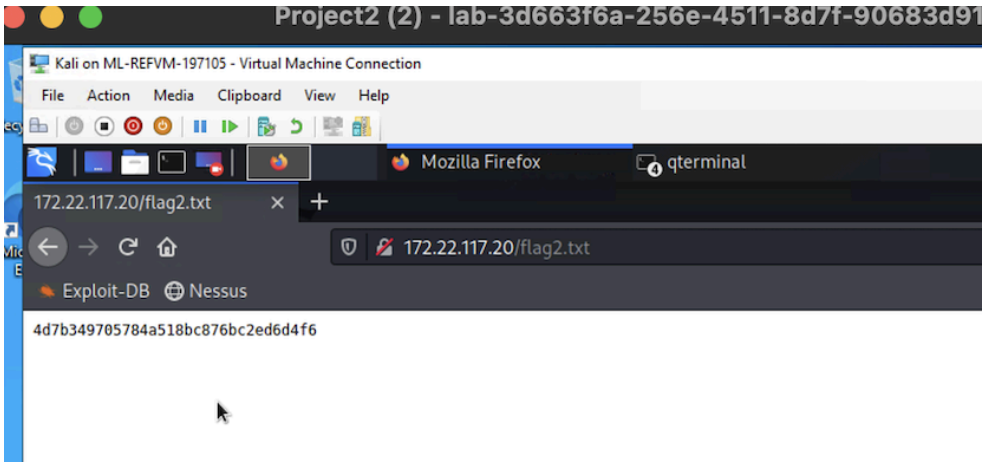
Vulnerability 6 (Flag 6)	Findings

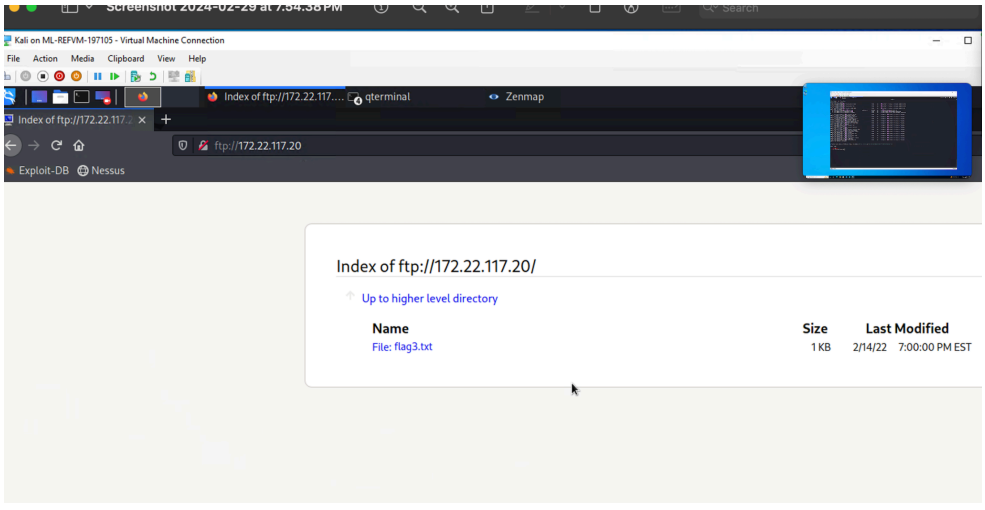
Title	Command Shell
Type (Web app / Linux OS / WIndows OS)	Linux
Risk Rating	High
Description	Using Vulnerability 5 we were able to create a command shell and view files on the compromised machine.
Images	

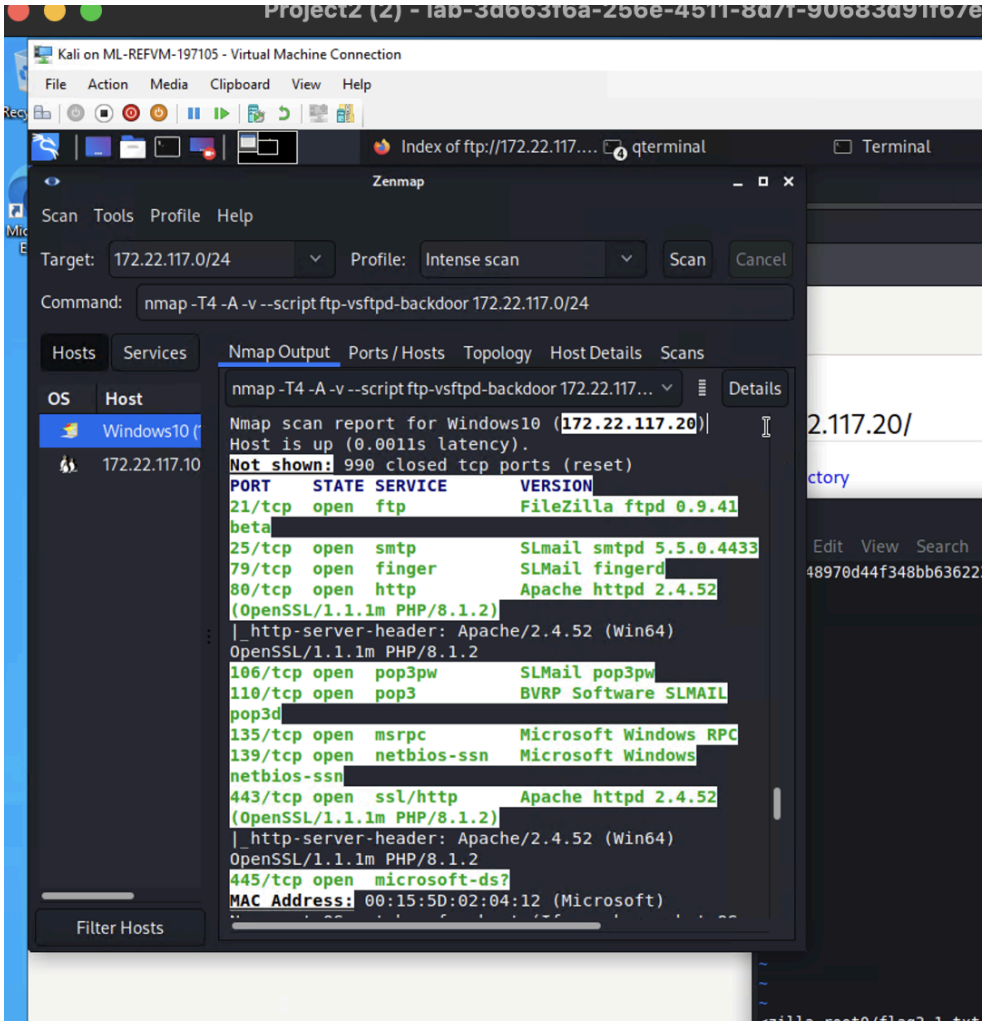
DAY 3

Vulnerability 1 (Flag 1)	Findings
Title	GitHub Page Totalrekall
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Low
Description	Searched GitHub repositories to totalrekall and found the credentials with the hashes password and cracked it with john.

Images	

Vulnerability 2 (Flag 2)	Findings
Title	Nmap Scan/ Network Host
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Medium
Description	Nmap scan on 172.22.117.0/24 for two servers revealed and 172.22.117.20 and 172.22.117.10. I went to the browser seen below and entered the server ending in 20 and found a flag and credentials.
Images	

Vulnerability 3 (Flag 3)	Findings
Title	FTP
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Medium
Description	Scanned in Zenmap and FTP port 21 was open and vulnerable to access. I ftp://172.22.117.20 from the browser which led to finding flag 3.
Images	



Vulnerability 4 (Flag 4)	Findings
Title	SLMAIL
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	critical
Description	open port 110 was exploited that made SLMail vulnerable

Images