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

Contact Information

Company Name	Tesfay Solutions
Contact Name	Alula Tesfay
Contact Title	Jr. Penetration Tester

Document History

Version	Date	Author(s)	Comments
001	February 03, 2025	Alula Tesfay	Day 1
002	February 04, 2025	Alula Tesfay	Day 2
003	February 06, 2025	Alula Tesfay	Day 3

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.

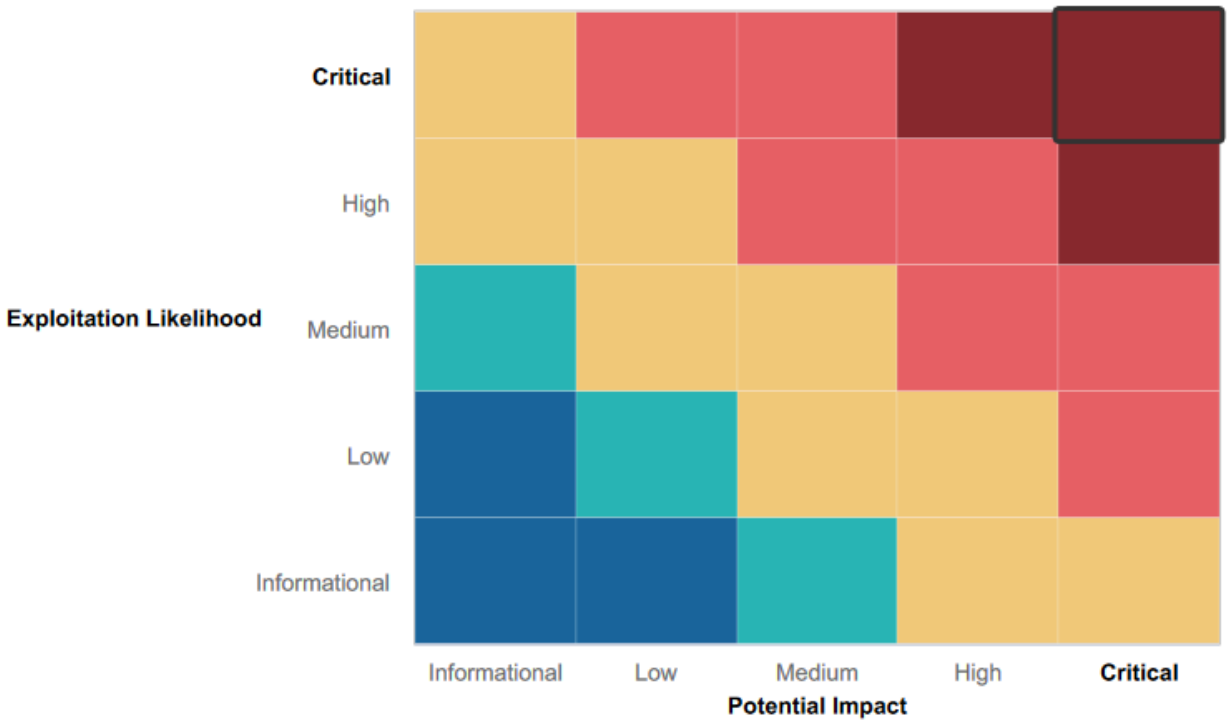
Executive Summary of Findings

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.

- Instances of Login Protections
- Numerous Ports Closed (that would otherwise be vulnerable to attacks)
- Instances of 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.

- Reflected XSS Attack Susceptibility
- Local File Inclusion
- Exposed WHOIS Domain Record
- Sensitive Information within DNS Record Registration, DNS Registration, and SSL Certificate Registration
- Weak Protections against Zenmap and Nmap scans
- Several Outdated Services
- Privilege Escalation within the Windows OS
- Username and Password Credentials within Public Github Repository
- Outdated FTP Protocol

Executive Summary

Web Application

Within the Web Application, numerous elements were found to be susceptible to attacks. Regarding text fields requiring user input, the potential for manipulation by a bad actor were deemed to be prevalent. When testing numerous text fields, the end goal was to cause the site to produce unintended popups leading to the reveal of sensitive information (flags). While this may be, the potential for code injection, remote execution, and other far devastating attacks leading to potential sensitive system file exposure, cookie and user session hijacking, the leaking of employee and user accounts, and more is still very possible should a bad actor intrude if the necessary service upgrades, framework changes, and other means of prevention/ countermeasures are not taken into consideration and enacted immediately.

Linux System

In regards to the DNS, domain, and SSL certificate registration(s), extremely sensitive information can be found using widely available, free to use websites and tools. This can and will inevitably lead to a potential bad actor gaining access to multiple internal systems. Should this be the case, a bad actor could and would most likely exert the means to hinder internal system(s) performance along with manipulating internal data structure as well as internal files ranging from system files to sensitive employee/business/user documents stored on such systems.

Multiple vulnerabilities found in outdated services leave a door for a potential bad actor to remotely access these systems, escalating their privileges to root (similar to Administrative privileges), executing internal programs, and imbedding unintended software and executables.

Along with this, several open ports that should not be required to be in the state that they are in order for various functions to run have been discovered. Such ports were discovered through scanning tools which are widely available to the public. The same tools were also used to find multiple exposed IP addresses, some of which are tied to sensitive internal systems. The services used to support these IPs are either outdated or have been replaced by newer services.

This must be addressed as soon as possible.

Windows System

Similar to the issues outlined in the Linux System, multiple services have been found to be running with outdated versions. Most, if not all, of such services can be exposed using publicly available scanning tools. This has the potential for a bad actor to invade these systems (similar to the Linux system) and cause lasting damage to internal systems.

Sensitive information regarding user accounts and other internal files have been found in publicly available Github repositories. It is recommended that the site be contacted for the removal of these repositories.

Overall

Serious inquiry is needed to address the numerous issues across the Web application, Linux Server, and Windows Server. The impact of an attack on any of these fronts can (but are not limited to):

-User/Employee/Business information being leaked or manipulated
-Remote execution of external/internal programs and services not intended by design
-Backdoor Access
-Surveillance by unknown parties
-Degradation of hardware
-Reputational damage and potential lawsuits

Summary Vulnerability Overview

Vulnerability	Severity
Web App	
Flag 1 Reflected XSS Payload	Medium
Flag 2 Bypassed Reflected XSS Payload	Medium
Flag 3 Reflected XSS Payload	Medium
Flag 5 Local File Inclusion	High
Linux OS	
Flag 1 Exposed WHOIS Domain Record	Low
Flag 2 Sensitive Information within DNS Record Registration	Low
Flag 3 Sensitive Information Exposed within SSL Certificate	Low
Flag 4 Exposed IPs revealed by Zenmap Scan	Medium
Flag 5 Outdated Drupal Service	Hlgh
Flag 6 Critical Vulnerability of Apache service Discovered through Nessus	Critical
Flag 7 Outdated Apache Tomcat Service	Critical
Flag 8 Outdated “Shellshock” Apache Service	Critical
Flag 9 Outdated “Shellshock” Apache Service (continued)	Critical
Flag 10 Outdated Apache Struts Service	Critical
Flag 11 Outdated Drupal Service	Critical
Flag 12 Exposed Username Information/Priviledge Escalation	Critical
Windows OS	
Flag 1 Github Repository with Sensitive Data	Low
Flag 2 Exposed Hosts Against Nmap Scan	Medium
Flag 3 NSE Script for FTP	Critical
Flag 4 Outdated SLMail Service	Critical

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

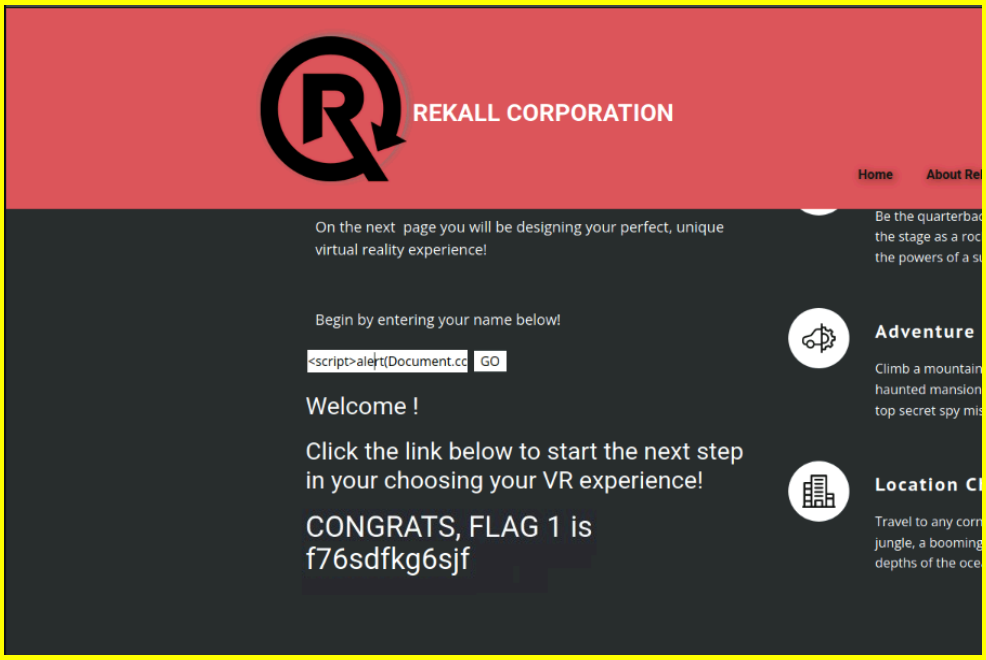
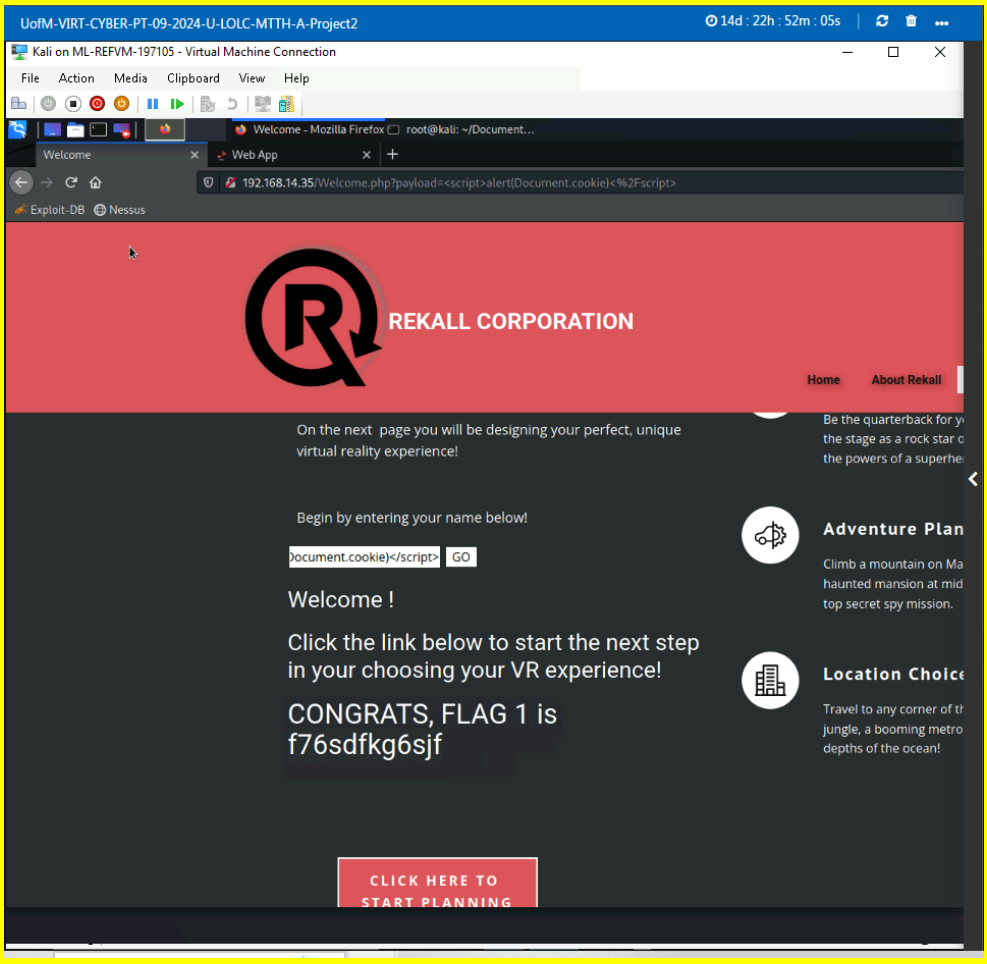
Scan Type	Total
Hosts	8
Ports	10

Exploitation Risk	Total
Critical	9
High	2
Medium	5

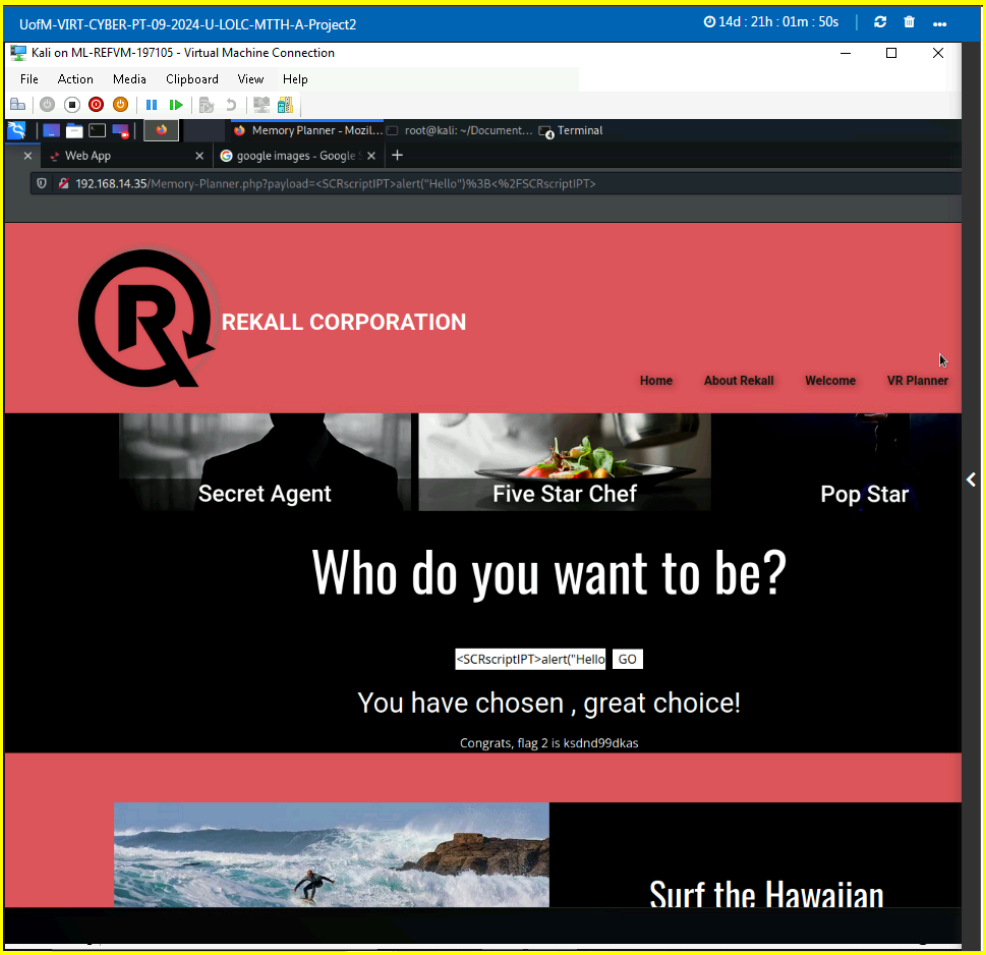
Low	4

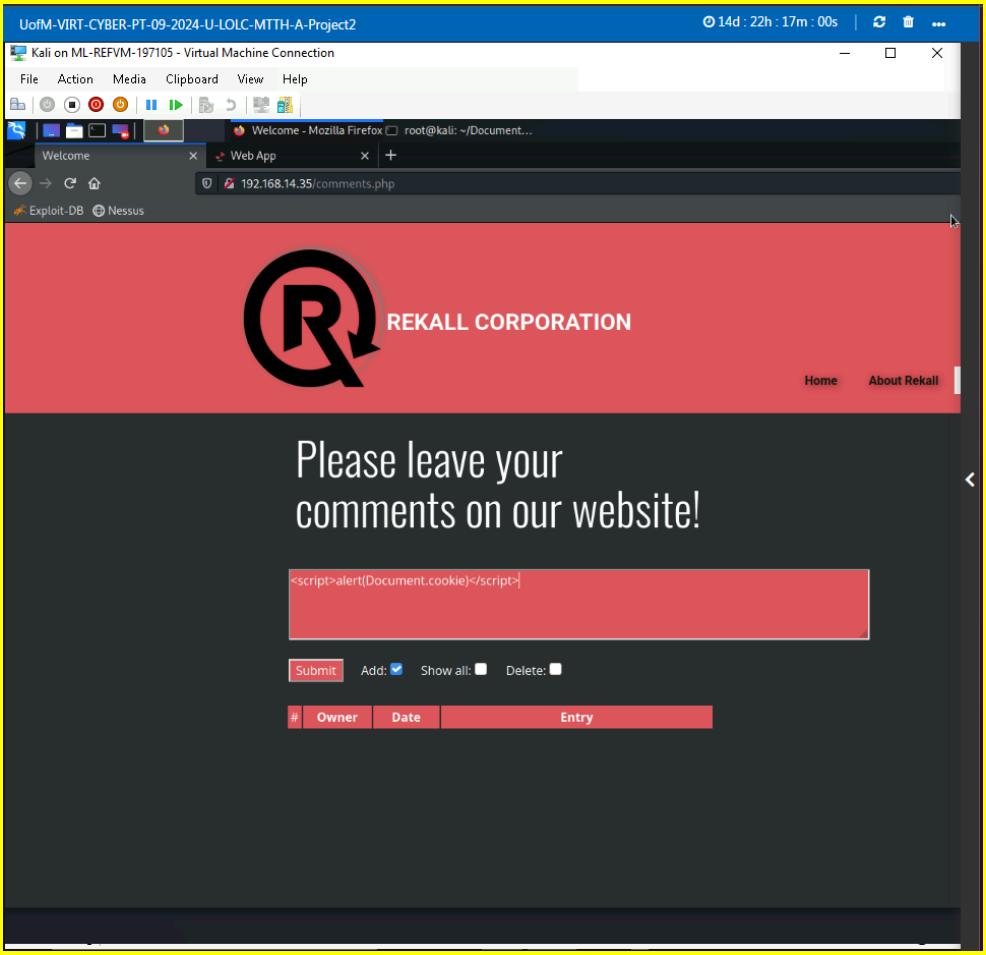
Vulnerability Findings

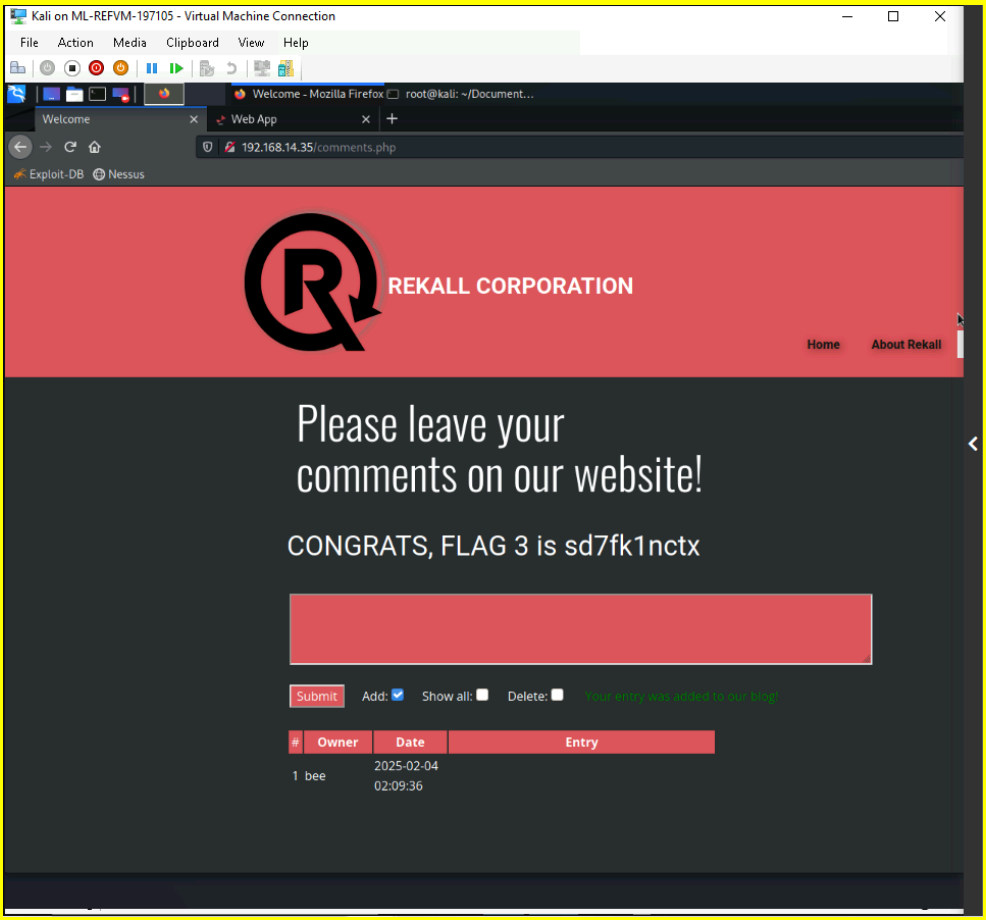
Vulnerability 1	Findings
Title	Reflected XSS Payload Attack Flag 1 Day 1
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	Medium
Description	On the Welcome.php portion of the Total Rekall website, successfully implemented a Reflected XSS Payload onto the text field titled “Put Your Name Here” using this script: <script>alert(Document.cookie)</script> to cause an unintended popup to reveal flag 1.

Images	 
Affected Hosts	192.168.14.35/Welcome.php
Remediation	Sanitizing user input by restricting specific characters/symbols (such as <,>,?,!,', and ". If such characters/symbols are introduced to the textfield, reject the input. Along with this, restrict phrases such as "script" or other standard HTML tags. ChatGPT suggests to consider switching from inline JavaScript to

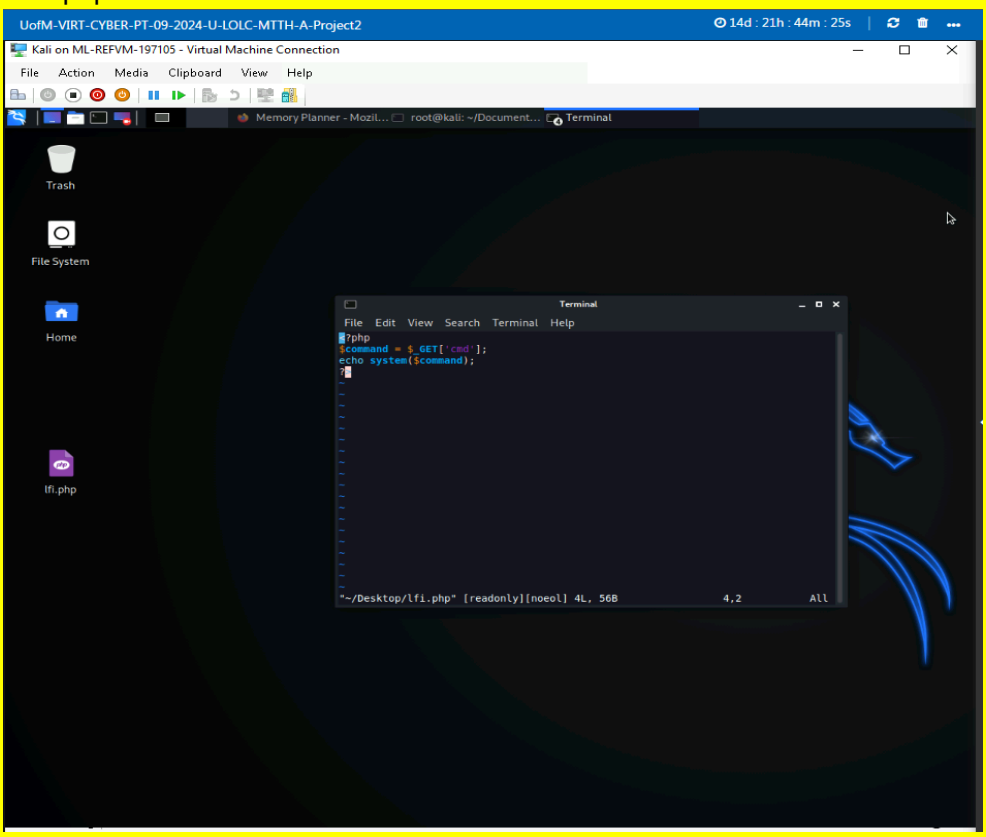
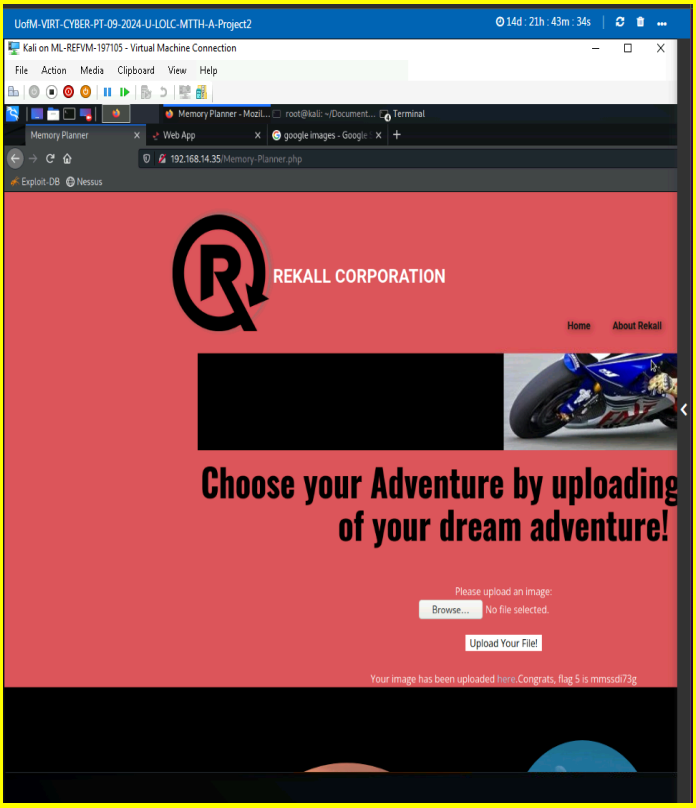
	using external JavaScript files and keeping them separate from user-generated content.

Vulnerability 2	Findings
Title	Bypassed Reflected XSS Payload Attack Flag 2 Day 1
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Medium
Description	In the Memory.php portion of the Total Rekall website, successfully bypassed input sanitization through placing a Reflected XSS Payload with modified tags using this script: <SCRscriptIPT>alert("Hello");<SCRscriptIPT> onto the “Who do you want to be?” textfield to cause an unintended popup revealing flag 2.
Images	
Affected Hosts	192.168.14.35/Memory-Planner.php
Remediation	Sanitizing user inputs by restricting characters/symbols as well as phrases associated with common HTML tags. Consider restricting input to alphanumeric and numeric characters. ChatGPT suggests implementing Content Security Policies to define what resources can be loaded and executed on the user-end of the website.

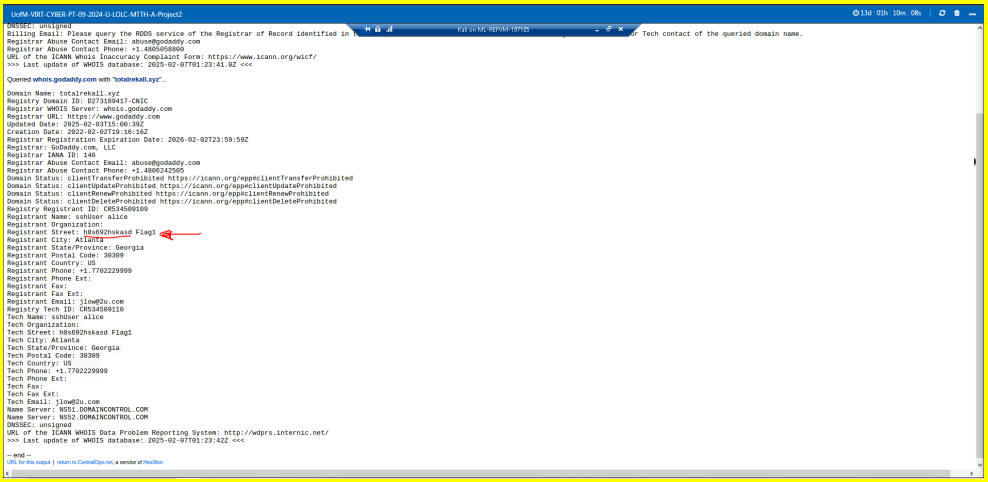
Vulnerability 3	Findings
Title	Reflected XSS Payload Flag 3 Day 1
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Medium
Description	Implemented a Reflected XSS Payload onto the Comments.php portion of the Total Rekall website by using this script: <script>alert(Document.cookie)</script> to cause an unintended popup to reveal flag 3.
Images	

	
Affected Hosts	192.168.14.35/comments.php
Remediation	Similar to previous XSS Payload attacks mentioned on this report, sanitizing user inputs by restricting characters/symbols as well as phrases associated with common HTML tags. Consider restricting input to alphanumeric and numeric characters. ChatGPT suggests implementing Content Security Policies to define what resources can be loaded and executed on the user-end of the website.

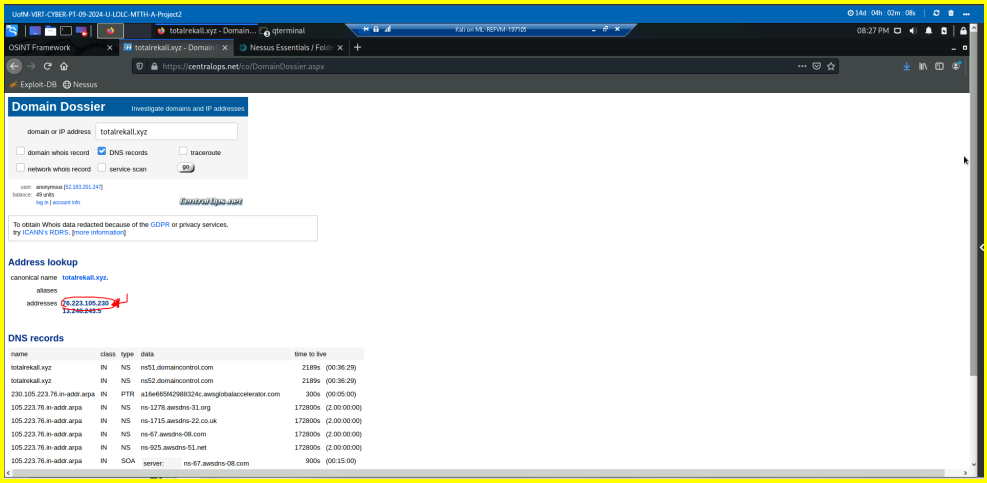
Vulnerability 4	Findings
Title	Flag 5 Day 1
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	High
Description	Abused a Local File Inclusion Exploit (LFI) in the second field of the Memory-Planner.php portion of the Total Rekall site by uploading a .php file containing this script with the same structure to cause an unintended popup revealing flag 5: <?php $command = $_GET[‘cmd’]; echo system($command); ?>

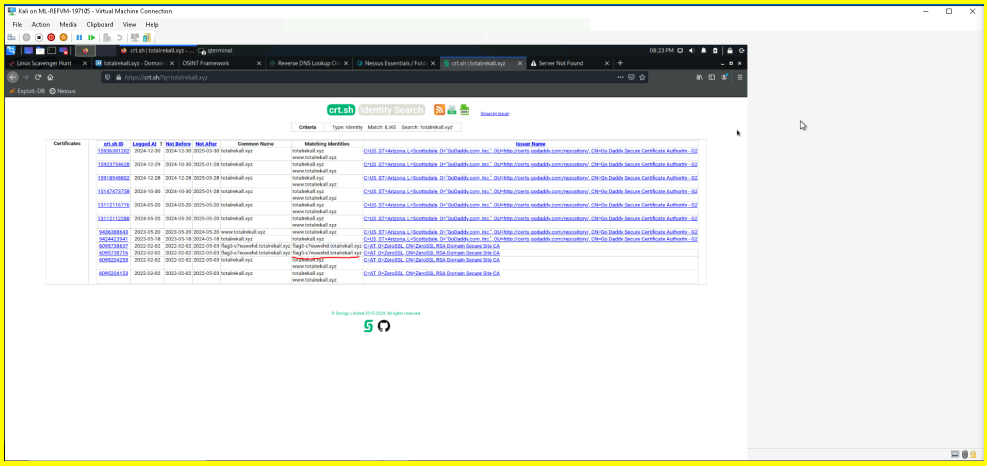
Images	The .php file used:  Result: 
Affected Hosts	192.168.14.35/Memory-Planner.php

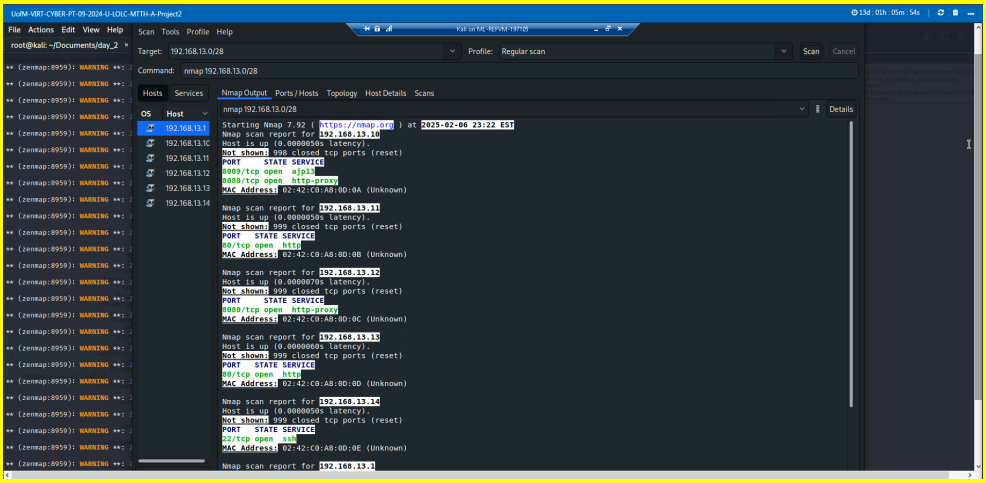
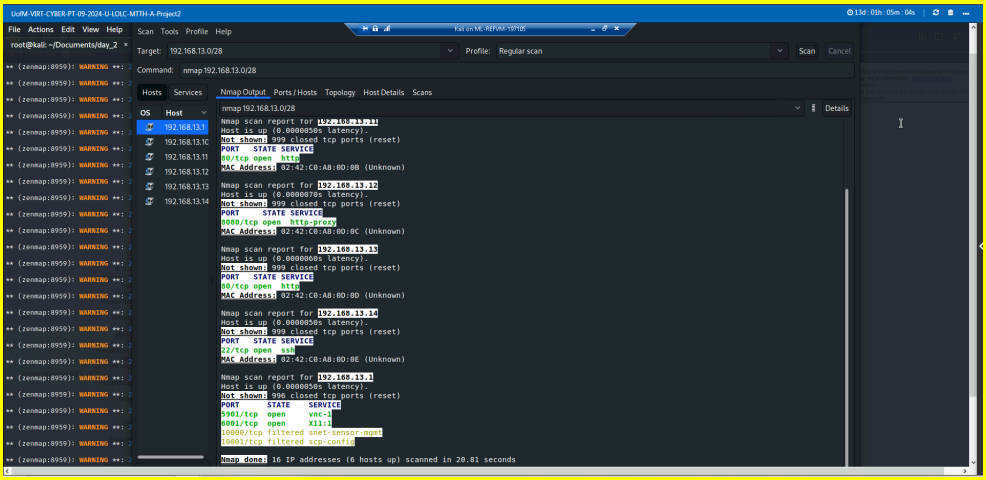
Remediation	ChatGPT suggests restricting file paths by ensuring that any user input into such file paths is strictly validated. This can be done by only allowing a predefined set of sage file paths or whitelisting specific filenames. User input should not allow sequences such as "../" which can allow attackers to go through the directory structure and access files, especially sensitive files.

Vulnerability 5	Findings
Title	Exposed WHOIS domain record Flag 1 Day 2
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Low
Description	Successfully searched for sensitive data regarding the domain of the Total Rekall site leveraging the Domain Dossier tool from the OSINT Framework page.
Images	
Affected Hosts	192.168.14.35
Remediation	Enable WHOIS privacy as most domain registrars offer this to hide sensitive information about the domain. While registering the domain, avoid listing sensitive and internal information.

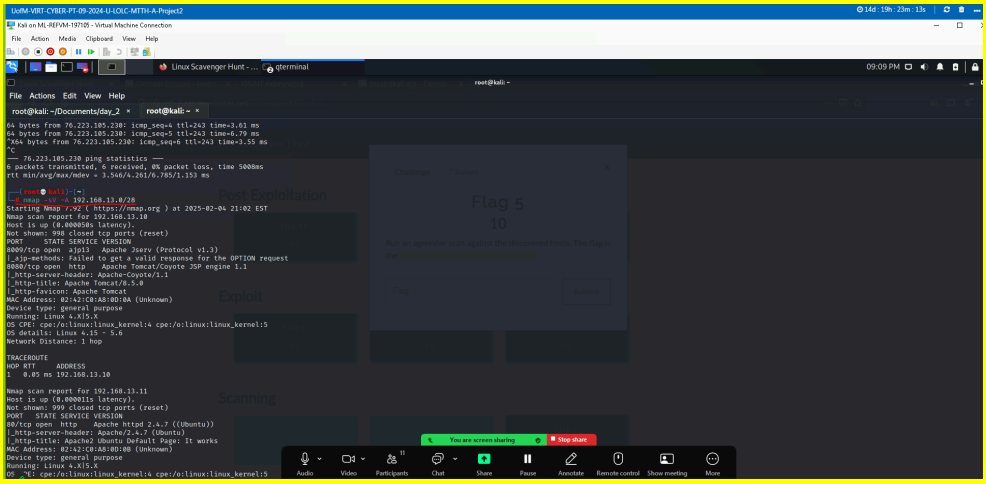
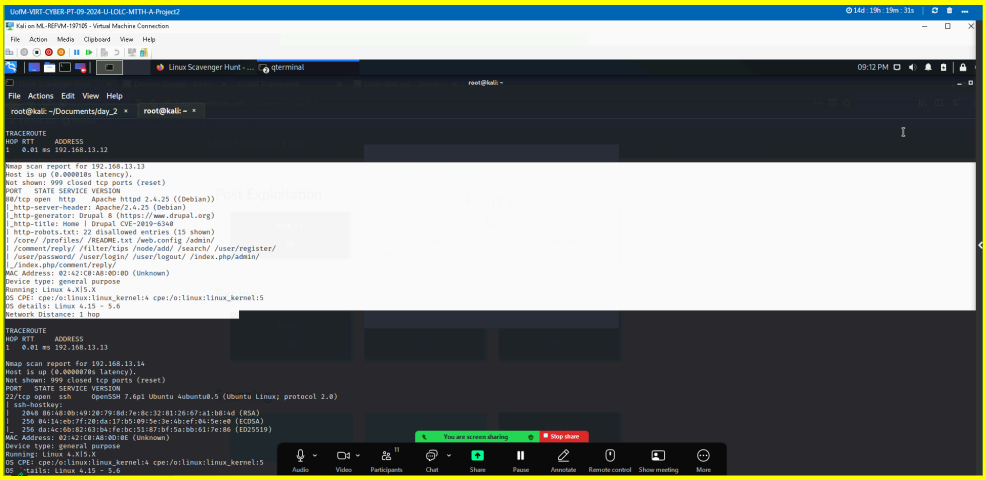
Vulnerability 6	Findings
Title	Exposed information regarding DNS Record of the Total Rekall site Flag 2 Day 2
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Low
Description	Leveraged the Domain Dossier tool within the OSINT framework page to search for DNS information on the Total Rekall site.

Images	
Affected Hosts	192.168.14.35
Remediation	Consider using CNAME records that point to other domains rather than listing the direct A record of sensitive domains. According to ChatGPT, some providers like Cloudflare and Amazon Route 53 offer DNS services that obscure certain DNS records as well as offering additional layers of privacy and hiding/minimizing the exposure of sensitive records.

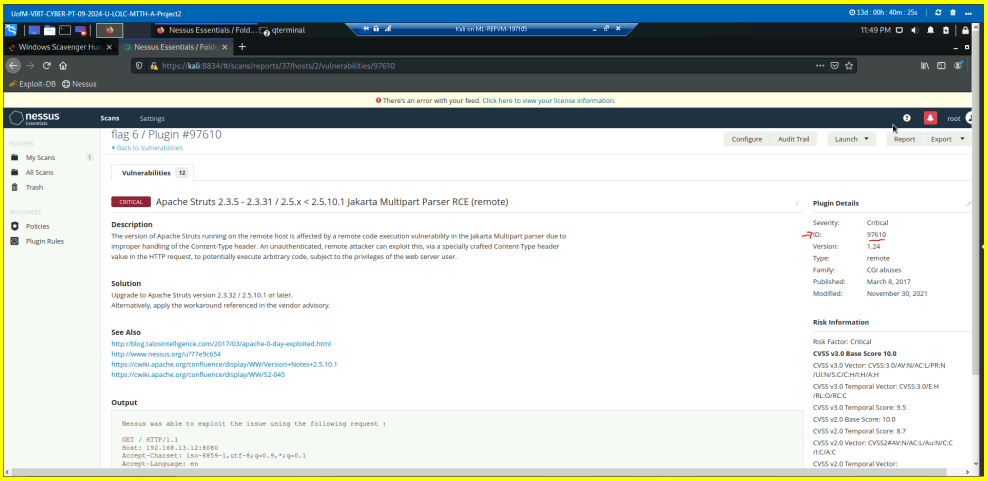
Vulnerability 7	**Findings**
Title	Exposed information regarding the SSL certificate of the Total Rekall site Flag 3 Day 2
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Low
Description	Utlized the “crt.sh” tool from the OSINT framework page to find sensitive information regarding the SSL certificate of the Total Rekall website.
Images	
Affected Hosts	192.168.14.35
Remediation	Consider using a private or an internal certificate authority.

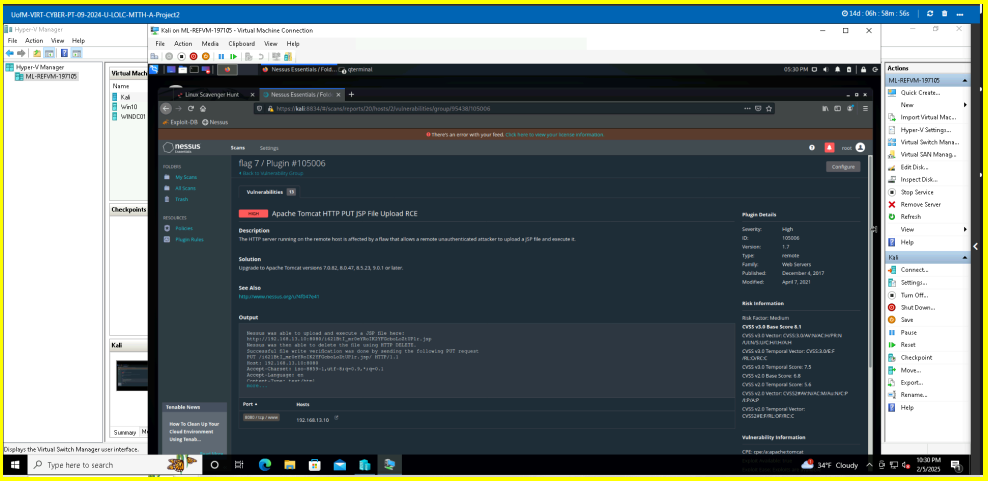
Vulnerability 8	Findings
Title	Flag 4 Day 2
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Medium
Description	Ran a Zenmap scan (using this cider notation: 192.168.13.0/28) to search for exposed host IPs.
Images	 
Affected Hosts	192.168.13.10, 192.168.13.11, 192.168.13.12, 192.168.13.13, 192.168.13.14, 192.138.13.1
Remediation	According to ChatGPT, using intrusion detection/prevention systems can detect and block such scans. It also suggests configuring firewalls and other perimeter security devices to rate-limit or block excessive traffic from sources performing aggressive scans.

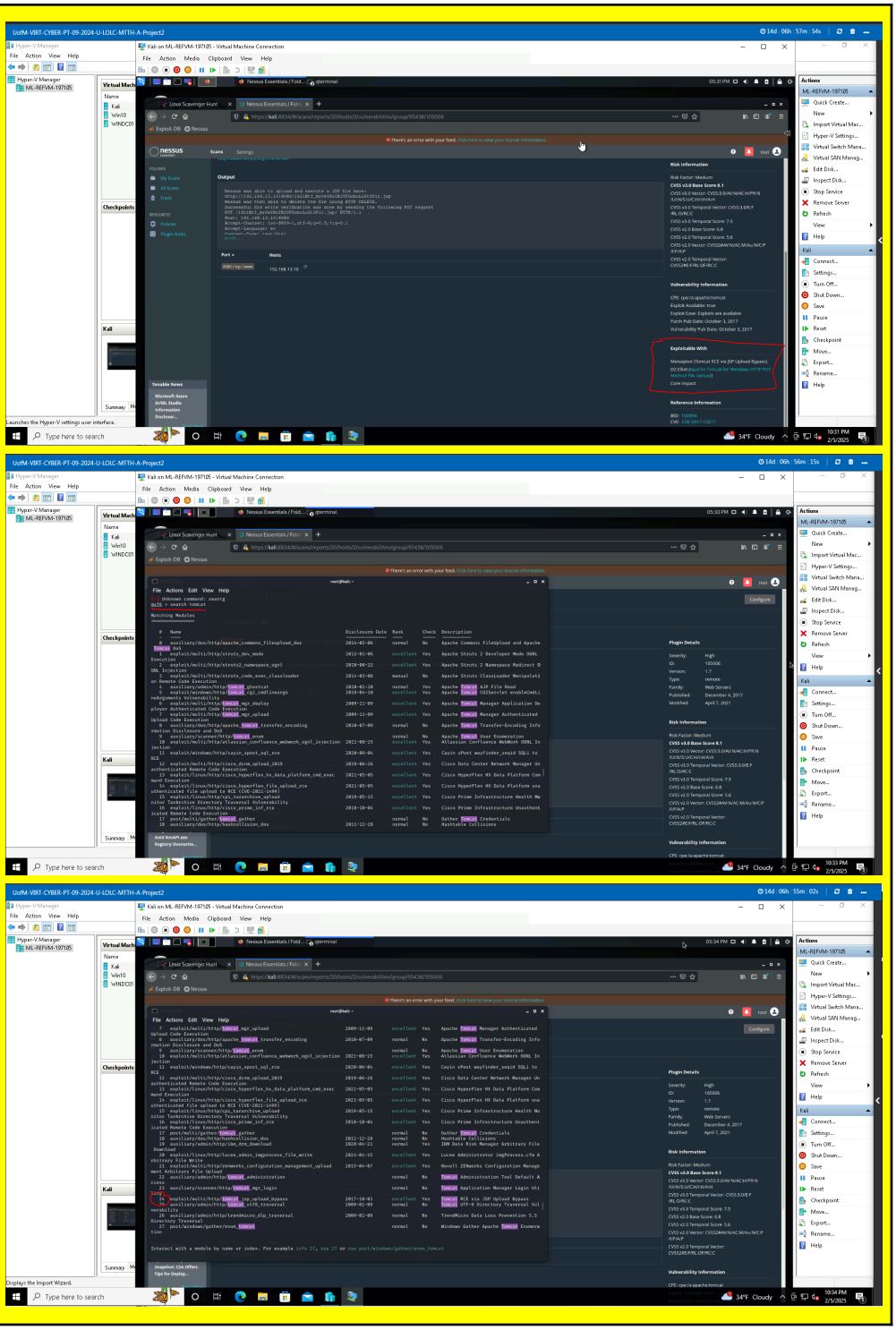
Vulnerability 9	Findings
Title	Drupal Service Flag 5 Day 2

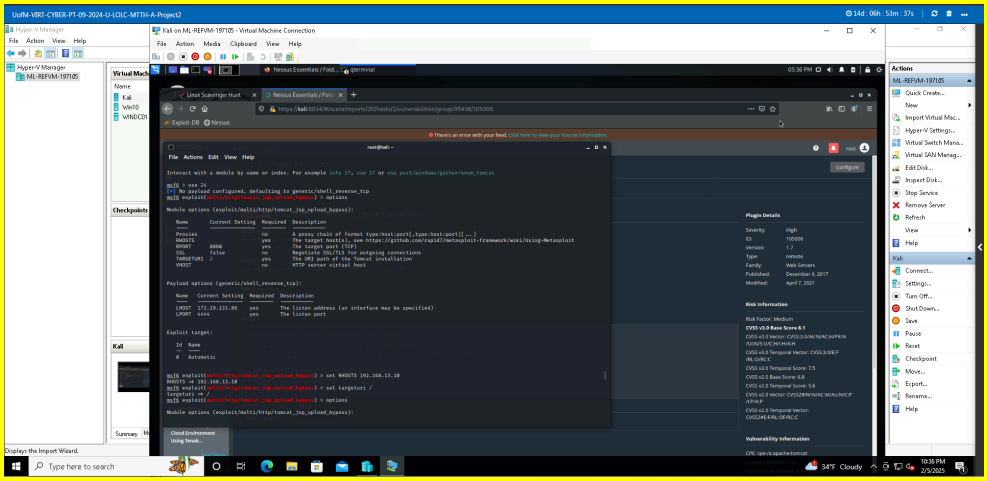
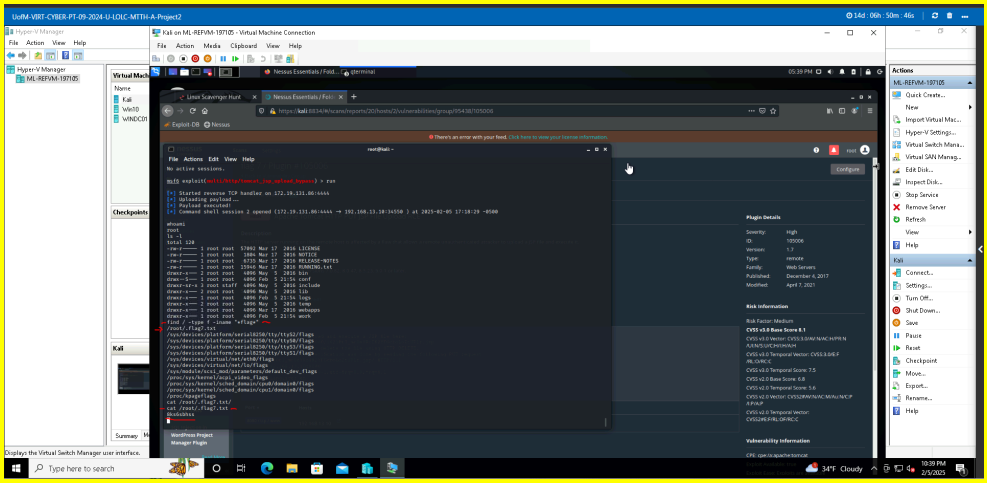
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	High
Description	Ran an aggressive nmap scan (against this IP with cider notation: 192.168.13.0/28) to search and find an exposed host IP that was running with the Drupal service with a known CVE vulnerability.
Images	 
Affected Hosts	192.168.13.13
Remediation	Upgrading the Drupal service to its most up to date version to avoid an attacker exploiting any known vulnerabilities on the version depicted. One could also deploy measures and tactics to counteract abuse of any known vulnerabilities on the current version depicted

Vulnerability 10	**Findings**
Title	Nessus Scan Flag 6 Day 2
Type (Web app / Linux OS / WIndows OS)	Linux OS

Risk Rating	Critical
Description	Ran a Nessus scan on the IP 192.168.13.12 to find the ID number of a known critical vulnerability (Jakarta Multipart RCE).
Images	
Affected Hosts	192.168.13.12
Remediation	Consider upgrading to the latest version. If that is not possible, research the vulnerability and deploy countermeasures to prevent a potential attack.

Vulnerability 11	**Findings**
Title	Flag 7 Day 2
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	Utilized a RCE exploit to
Images	

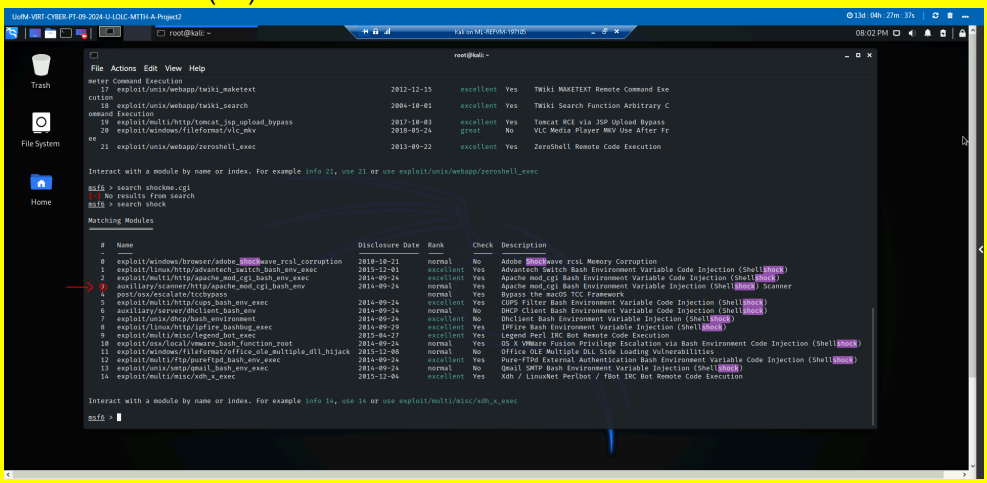


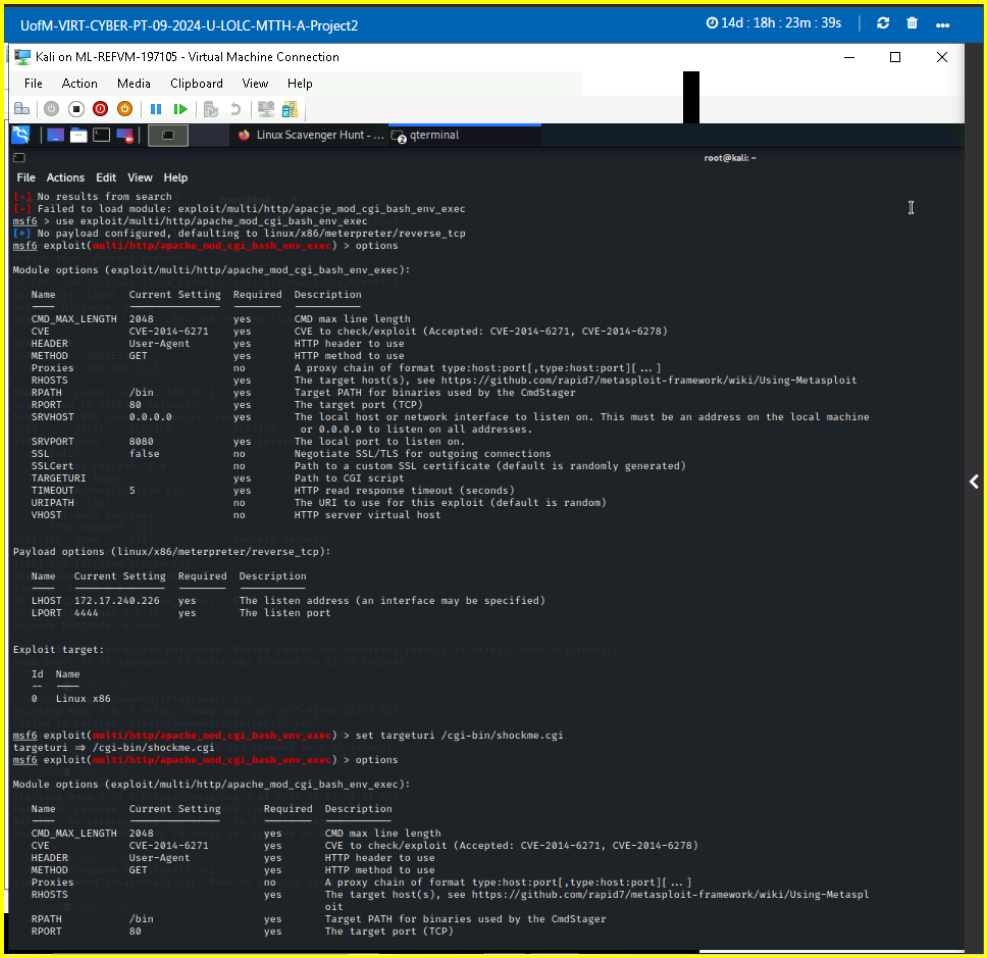
	 
Affected Hosts	192.168.13.10
Remediation	Upgrade the Tomcat service to the most current version available to avoid a potential attack.

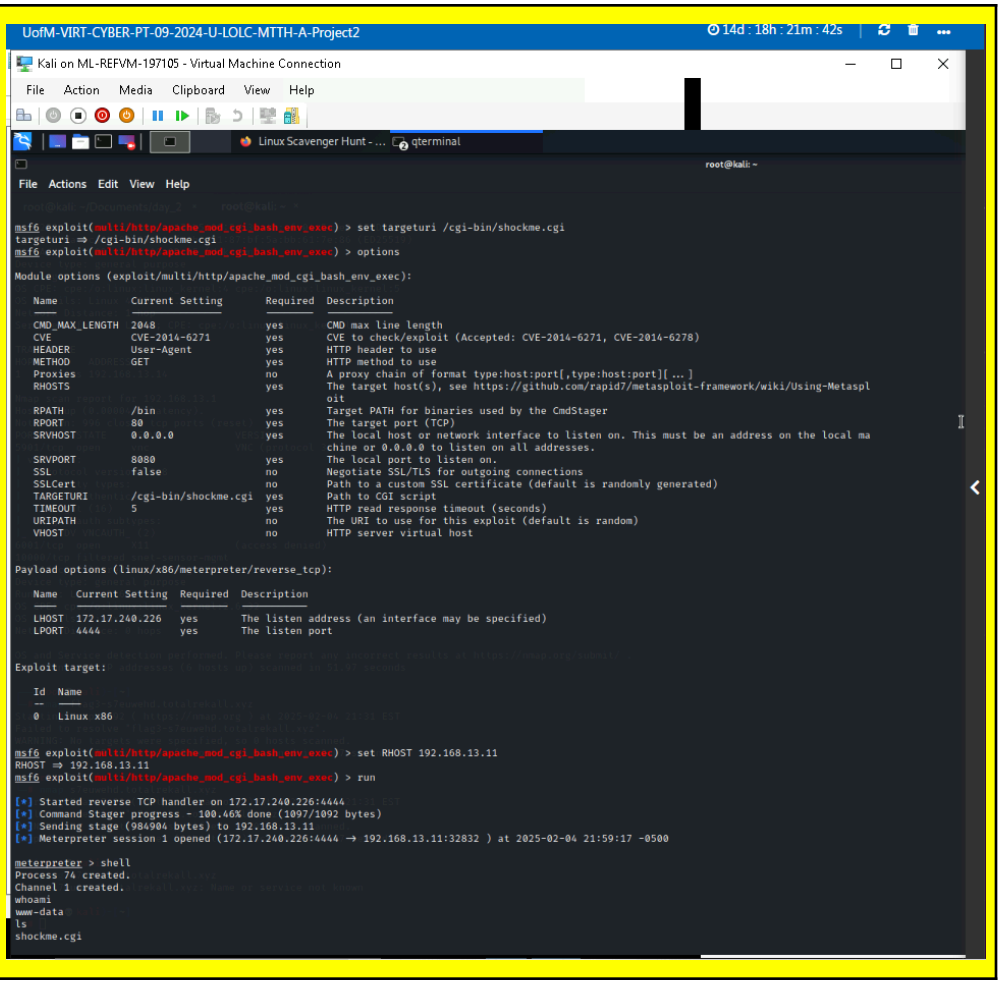
Vulnerability 12	**Findings**
Title	Flag 8 Day 2
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	Used the Apache mod_cgi Bash Environment Variable Code Injection (Shellshock) exploit to gain access to the 192.168.13.11 host IP to gain access to the /etc/sudoers file. Once inside, the “cat” command was utilized to show the sudoers file, revealing flag 8.

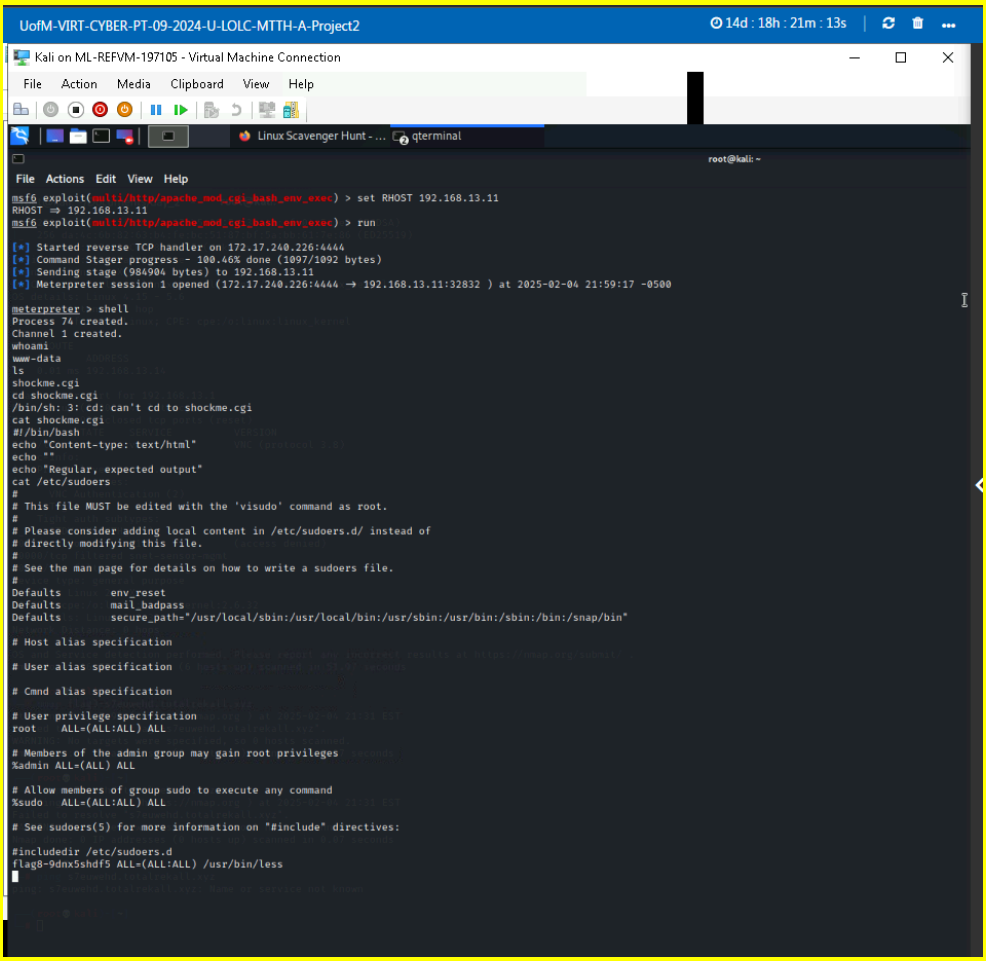
Images

(Disregard the marking on the first image, it was made to highlight the exploit used, however the highlight that was used and should have been marked is the one above it (#2)

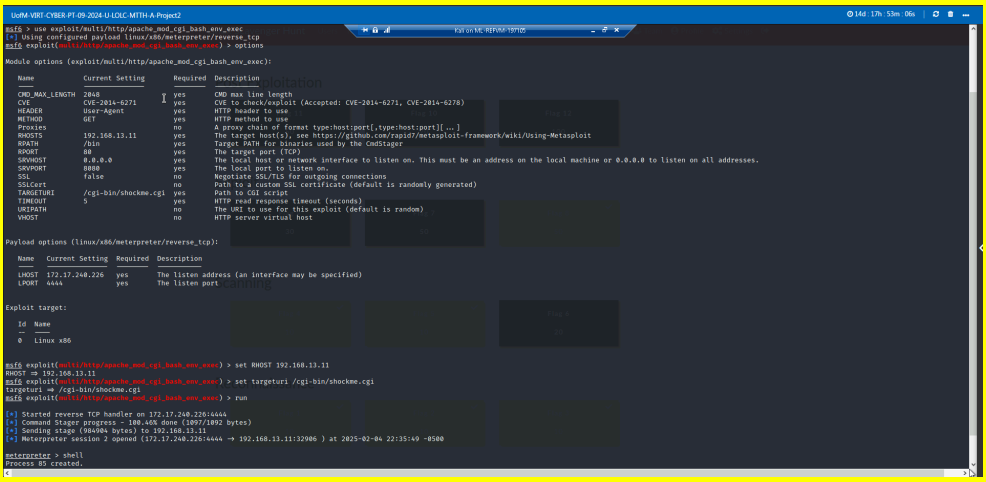
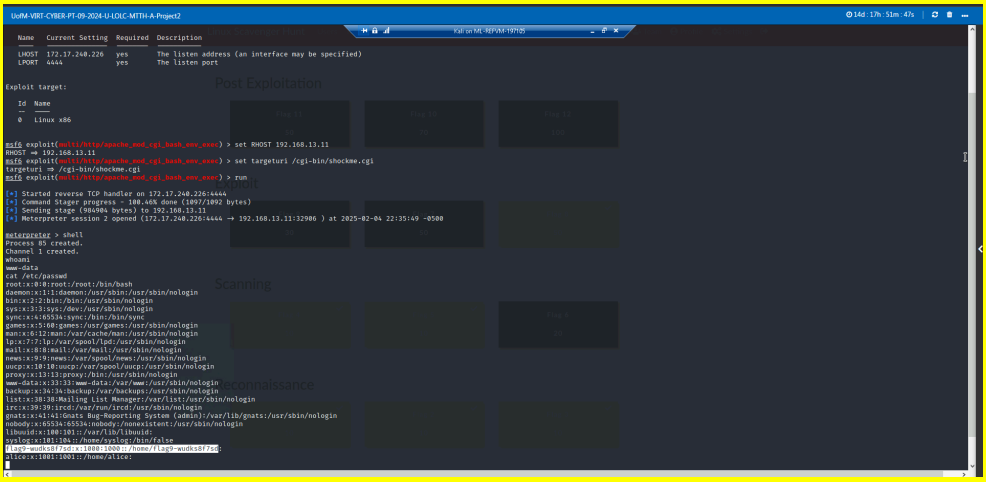






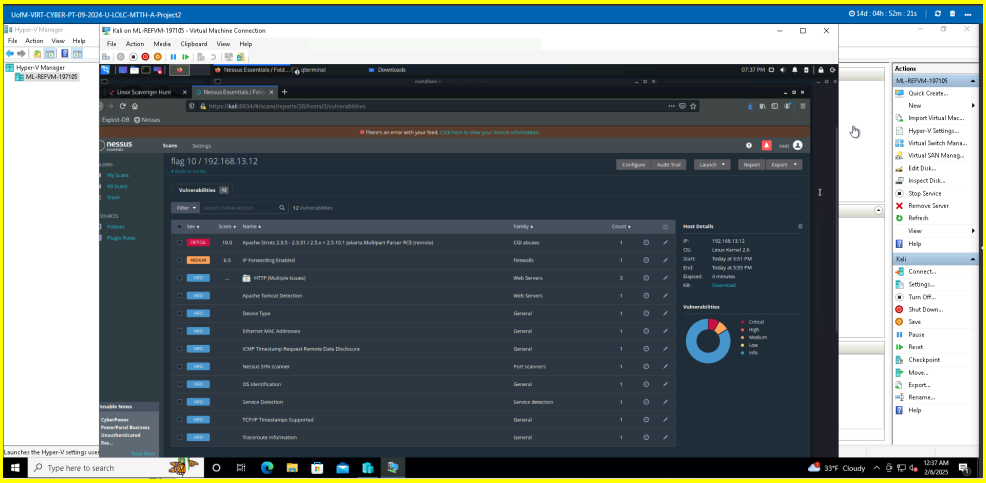
	
Affected Hosts	192.168.13.11
Remediation	Upgrade the Apache service that is used to run the host IP listed in order to prevent any potential attacks.

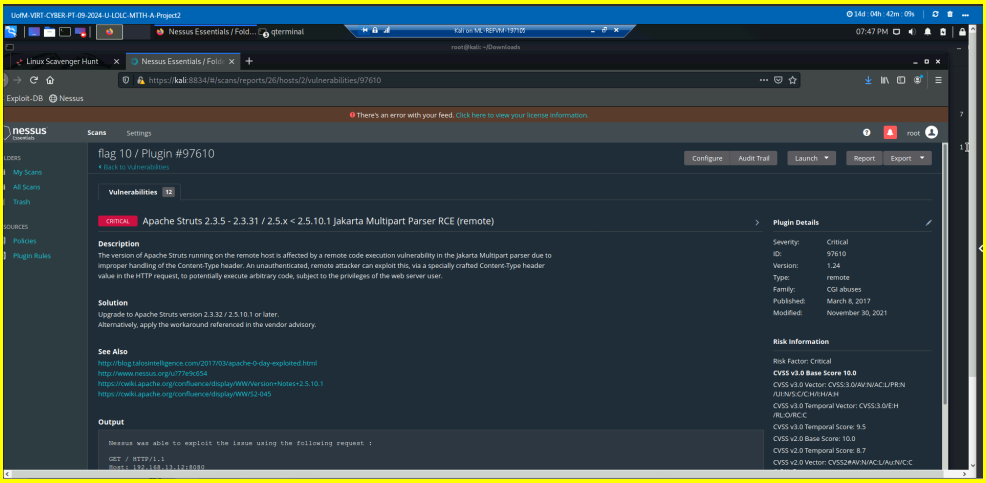
Vulnerability 13	Findings
Title	Flag 9 Day 2
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	Utilizing the same exploit from the previous vulnerability listed onto the same host IP, the “cat” command was used to show the contents of the /etc/passwd file, revealing flag 9.

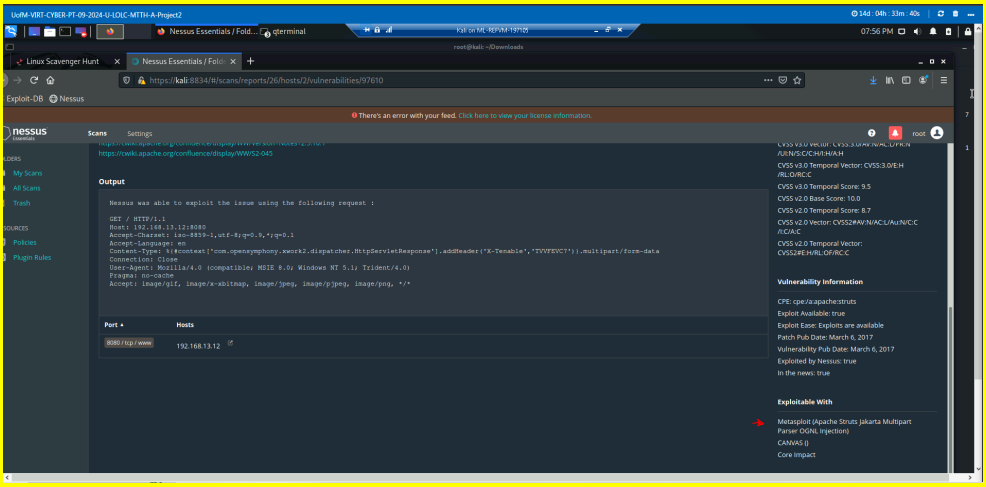
Images	 
Affected Hosts	192.168.13.11
Remediation	Upgrade the Apache service that is used to run the host IP listed in order to prevent any potential attacks.

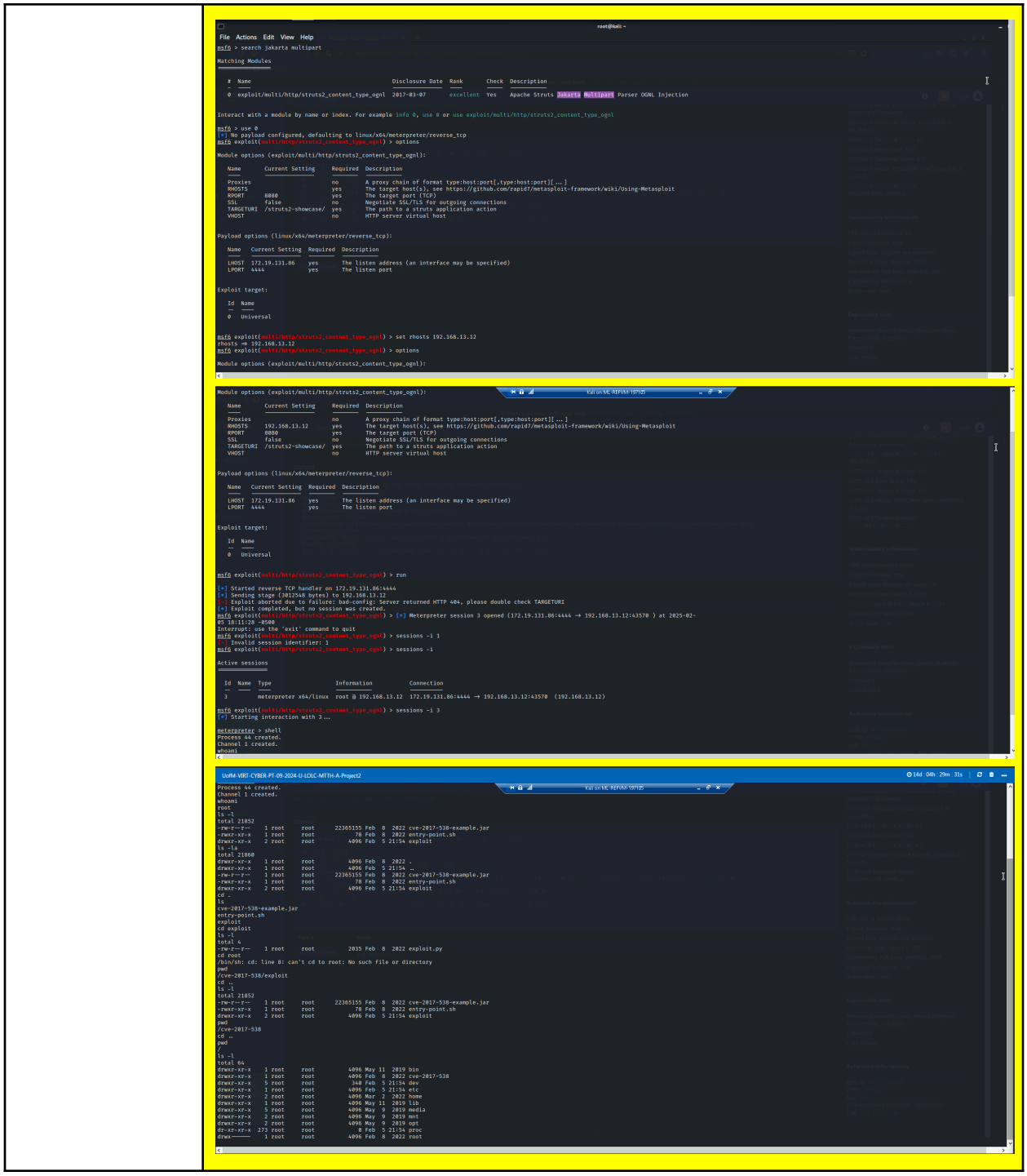
Vulnerability 14	Findings
Title	Flag 10 Day 2
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	Nessus was used against the 192.168.13.12 host IP to identify any RCE exploits. The Apache Struts Jakarta Multipart Parser OGNL Injection exploit was then used to gain access to the host IP listed. Once inside the system, A .zip file was found within the /root directory titled “flagisinThisfolder.zip”. After the file was downloaded to the local machine and unzipped, flag 10 was revealed.

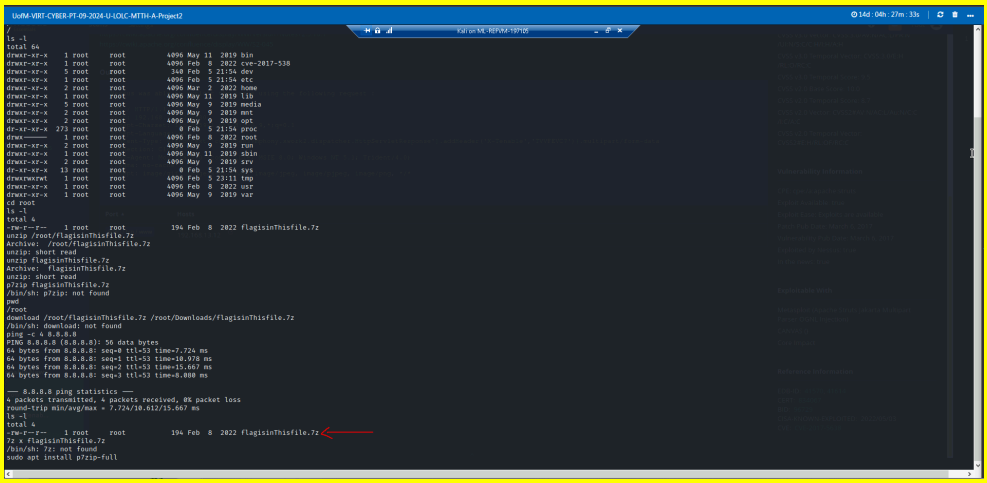
Images

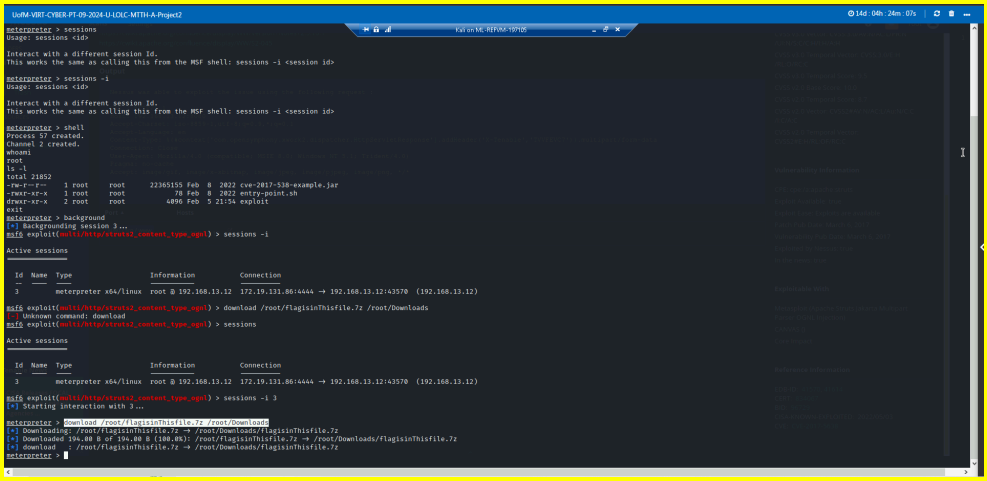


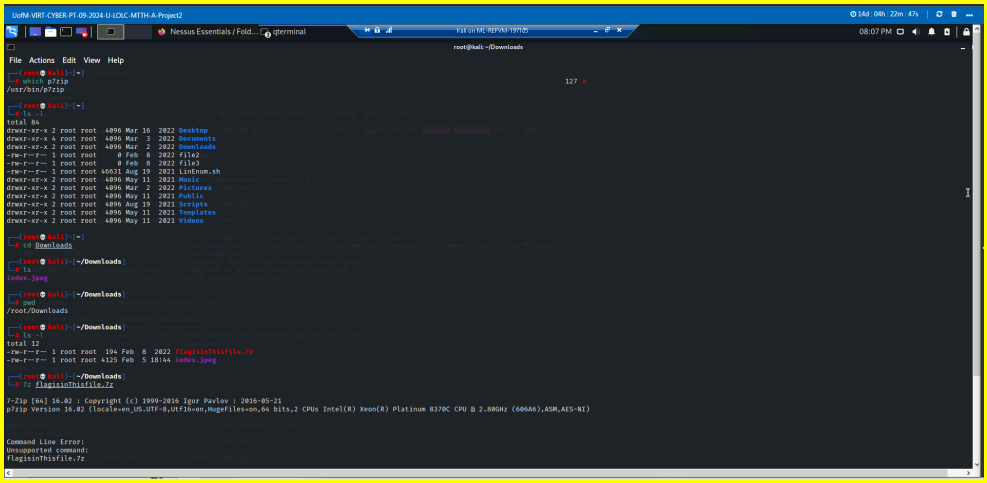


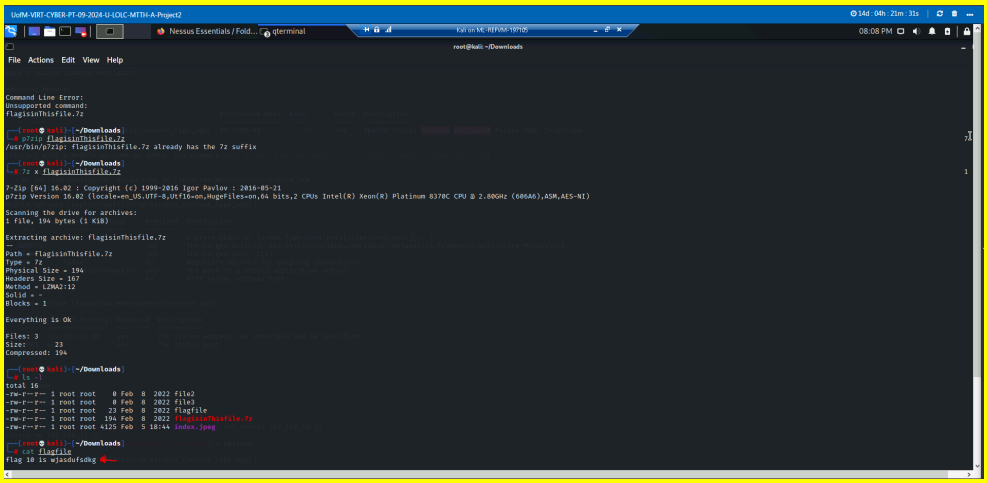


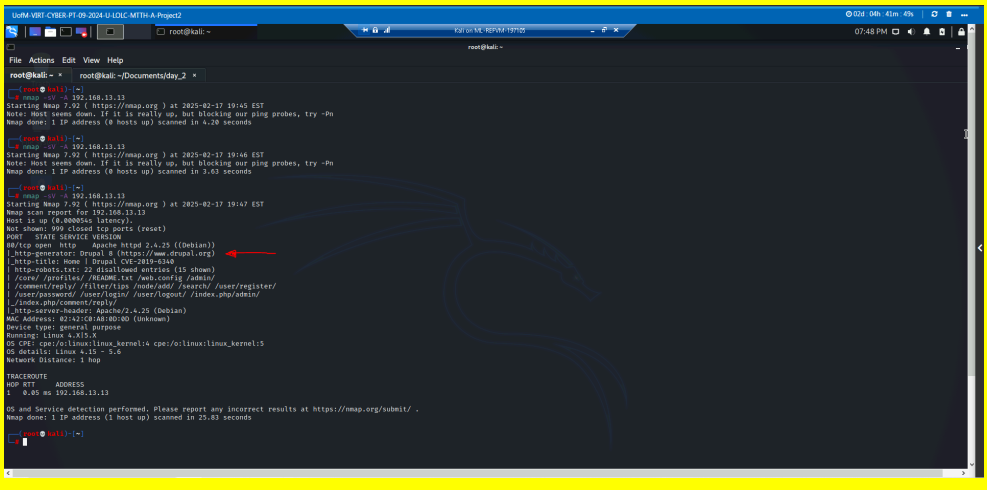


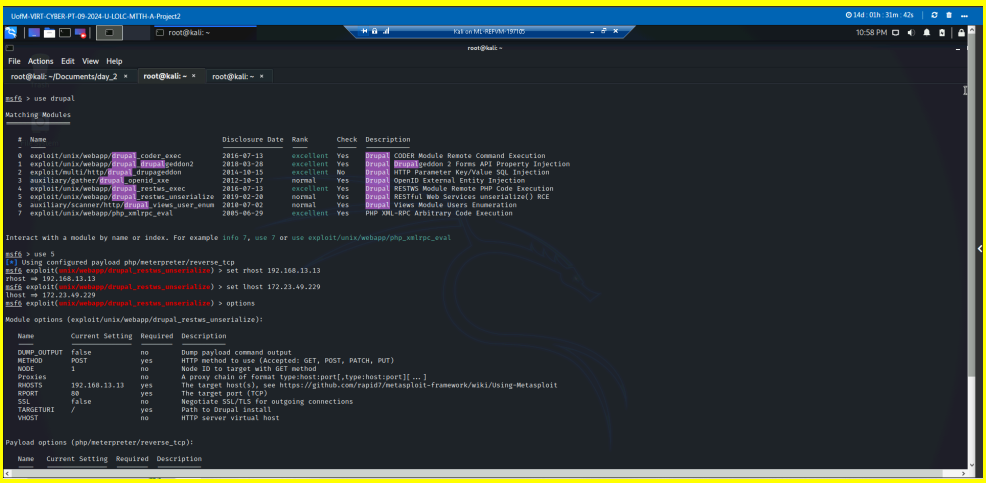


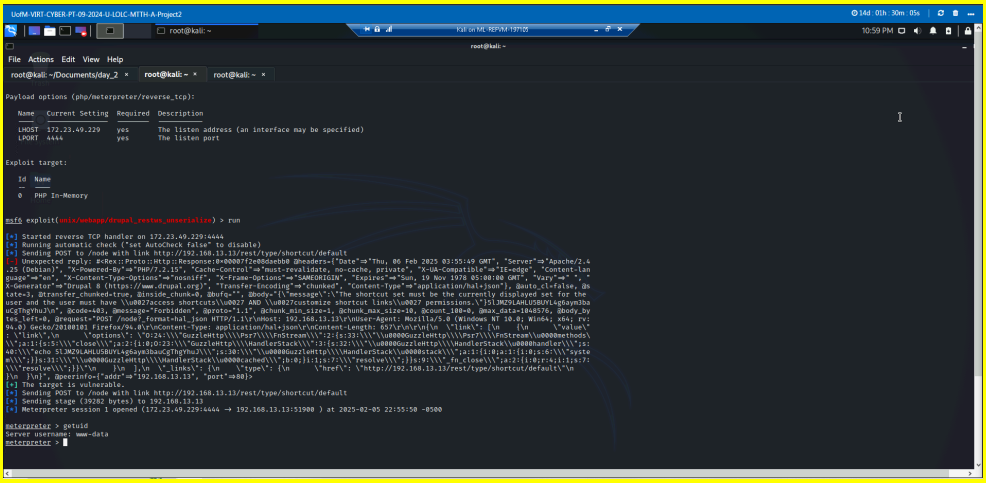




	
Affected Hosts	192.168.13.12
Remediation	Update the Apache service used to run the IP listed to avoid any potential attacks.

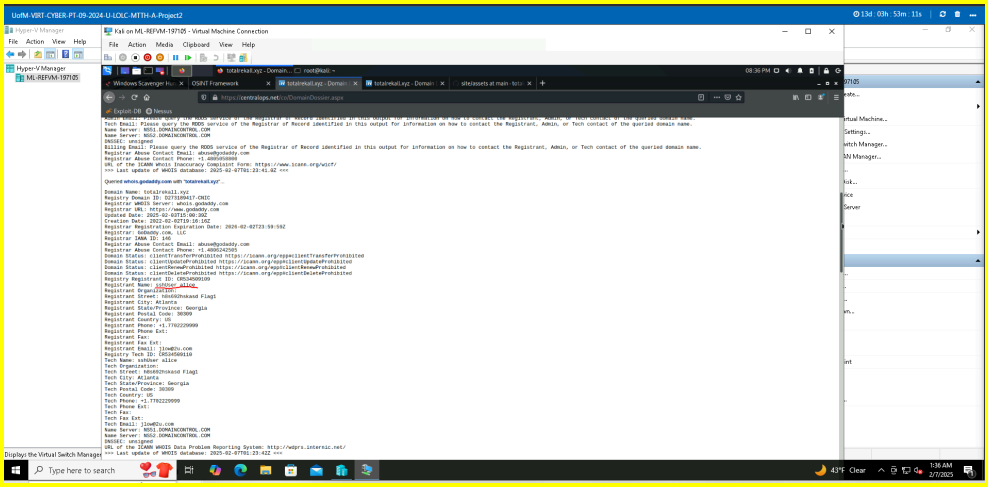
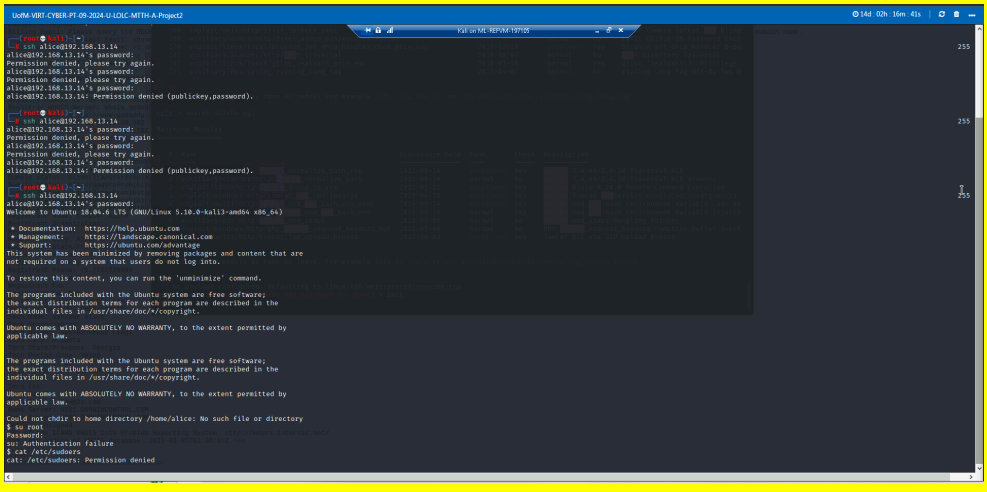
Vulnerability 15	**Findings**
Title	Flag 11 Day 2
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	Using Nmap on the host IP 192.168.13.13, it was discovered that the service used to run the host IP was Drupal 8. After researching the service to find any known vulnerabilities, the Drupal RESTful Web Services unserialize() RCE exploit was used to gain access to the IP. The command used to determine the server username was getuid.
Images	

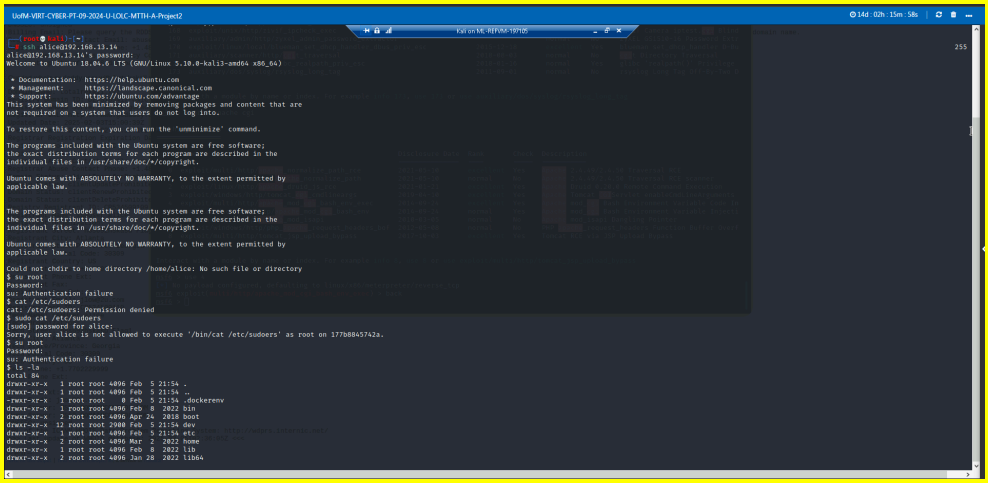
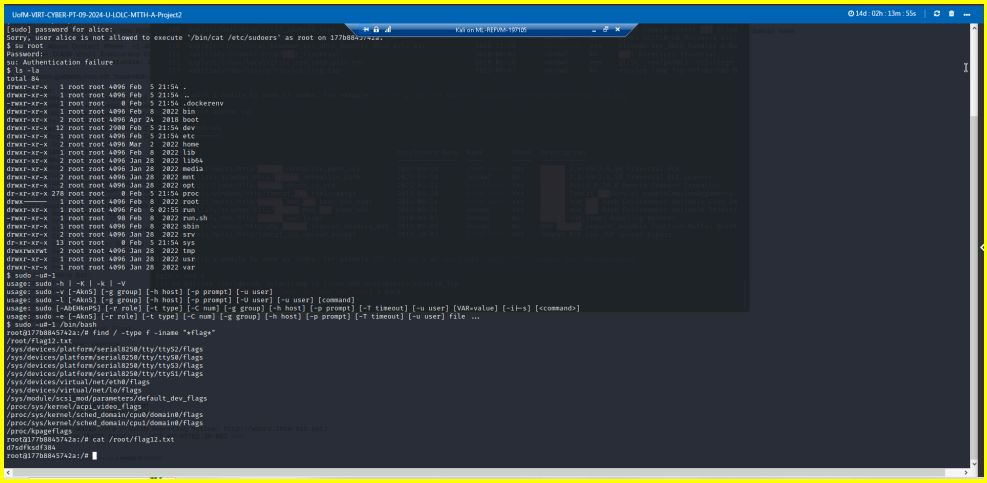




Affected Hosts	192.168.13.13
Remediation	Upgrade the Drupal service to the latest firmware version to prevent any potential attacks.

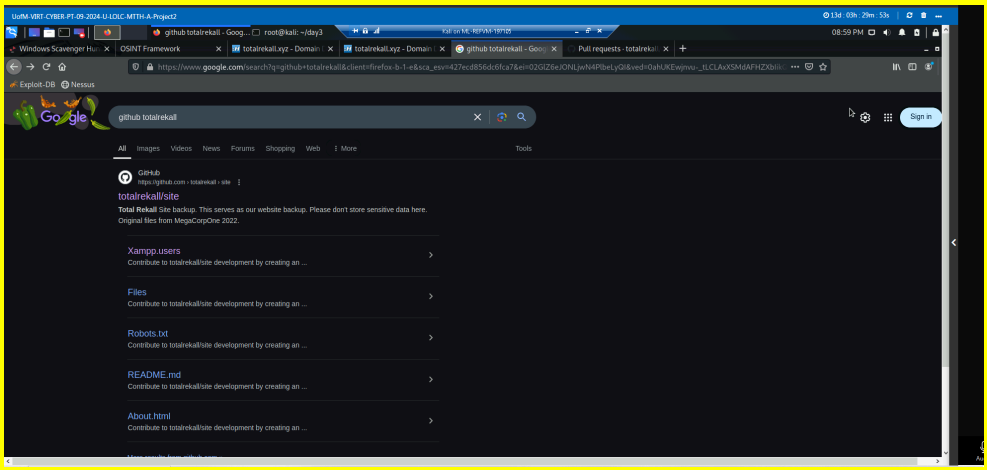
Vulnerability 16	Findings
Title	Flag 12 Day 2
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	Upon reviewing the WHOIS domain record for the Total Rekall site from the Domain Dossier tool (totalrekall.xyz), a potential username listed under the “Tech Name” field (ssh User alice). Then, the “ssh” command was used to connect to the host IP as the user (ssh alice@192.168.13.14). After several attempts, a simple password was used (alice) leading to a successful breach into the IP as the user. Once inside and after some research through Github and Reddit forums, the command ***sudo -u#-1 /bin/bash*** was used to escalate to a root user. As the root user, the command: find / -type f -iname “*flag*“ was

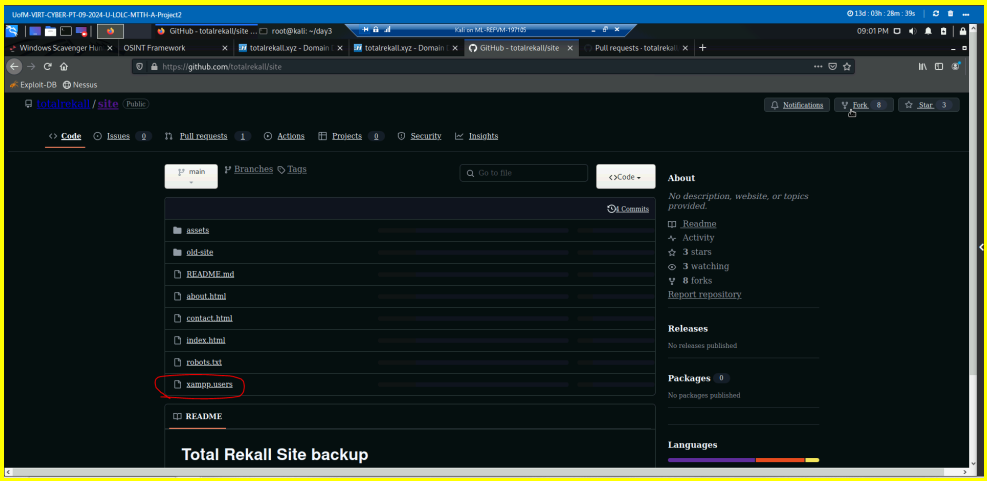
	used to search the system for any files containing the word “flag”. The result of the command showed that there indeed was a file called “flag12.txt” listed in the /root directory. The command cat /root/flag12.txt returned the contents of the text file, revealing flag 12.
Images	  

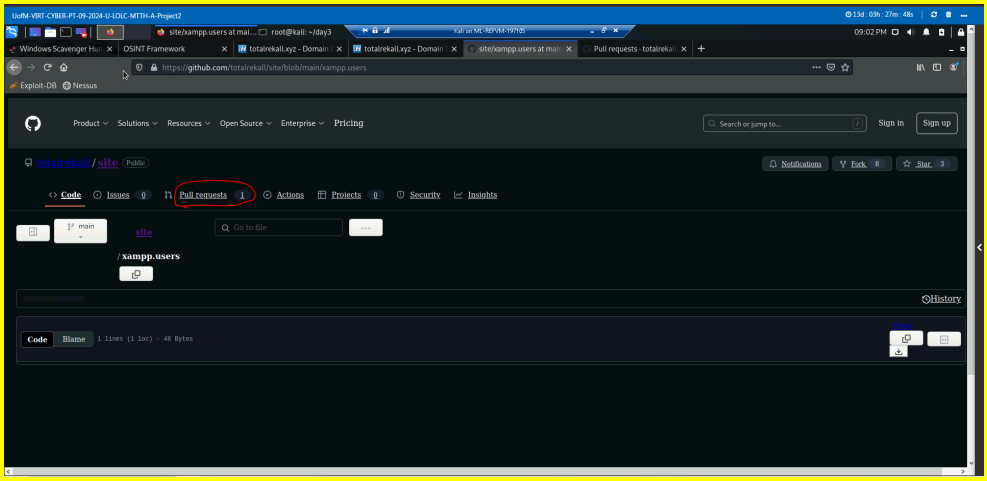
	 
Affected Hosts	192.168.13.14
Remediation	Removing sensitive information from the current DNS record if the DNS record can not be registered under a provider like Cloudflare and Amazon Route 53 which can offer DNS services that obscure certain DNS records as well as offering additional layers of privacy and hiding/minimizing the exposure of sensitive records. Enforcing stricter, more complex username and password policies to all ssh accounts.

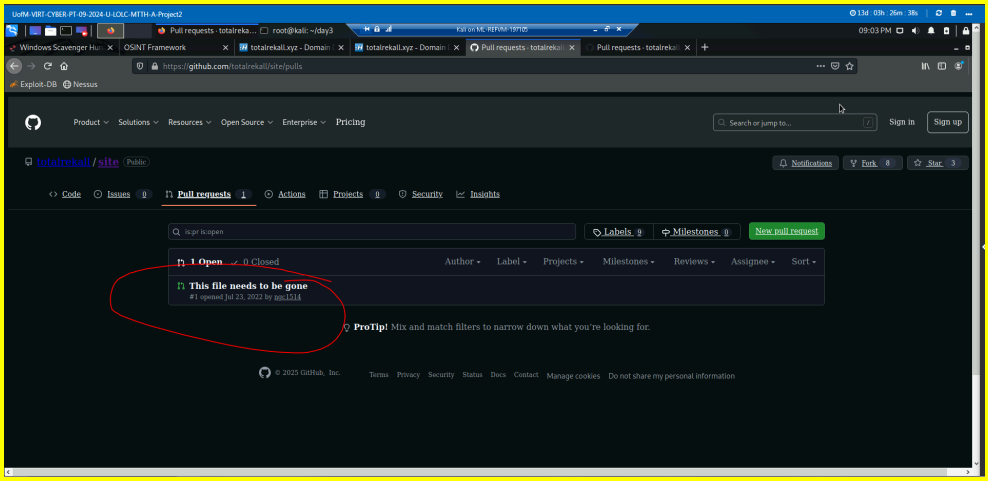
Vulnerability 17	Findings
Title	Flag 1 Day 3
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Low
Description	Upon googling “github totalrekall” and navigating through various links, a username and password bash was found. Upon entering both into a text file and using the command “john” to crack the password, the password was found.

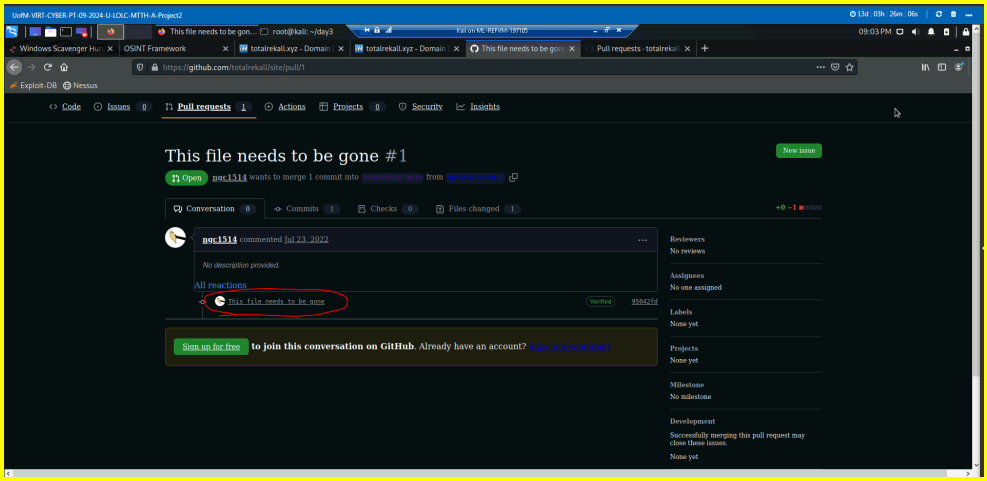
Images

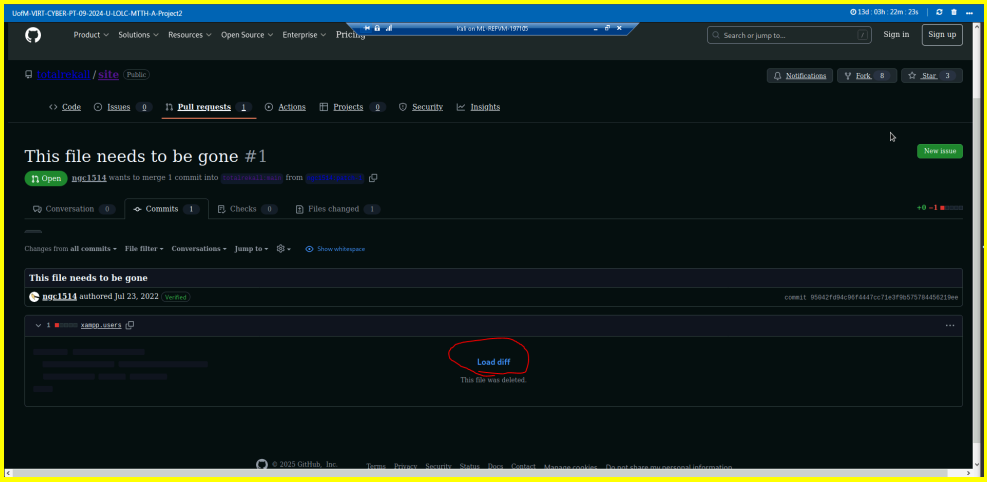


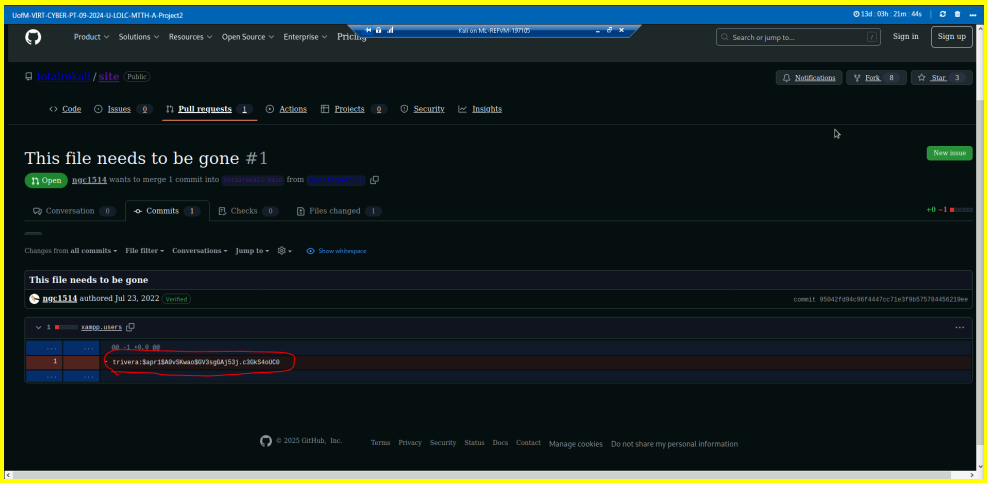


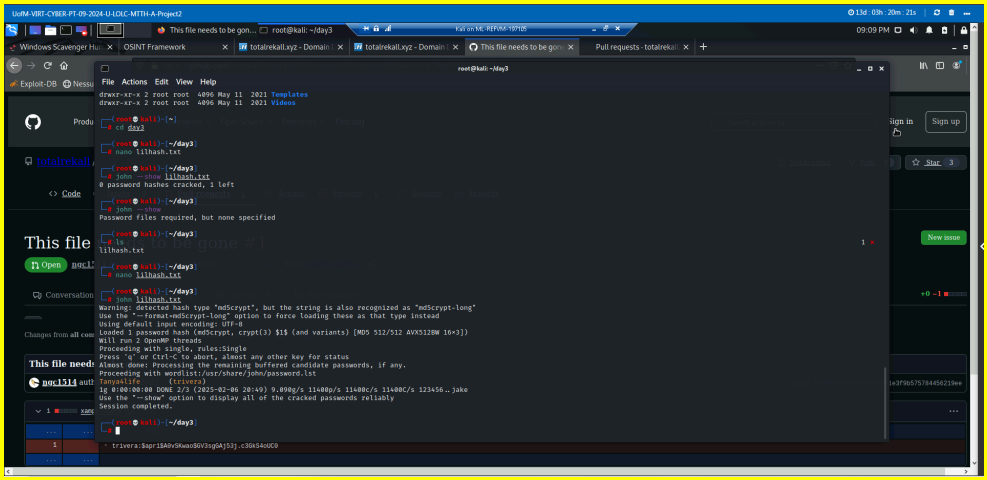








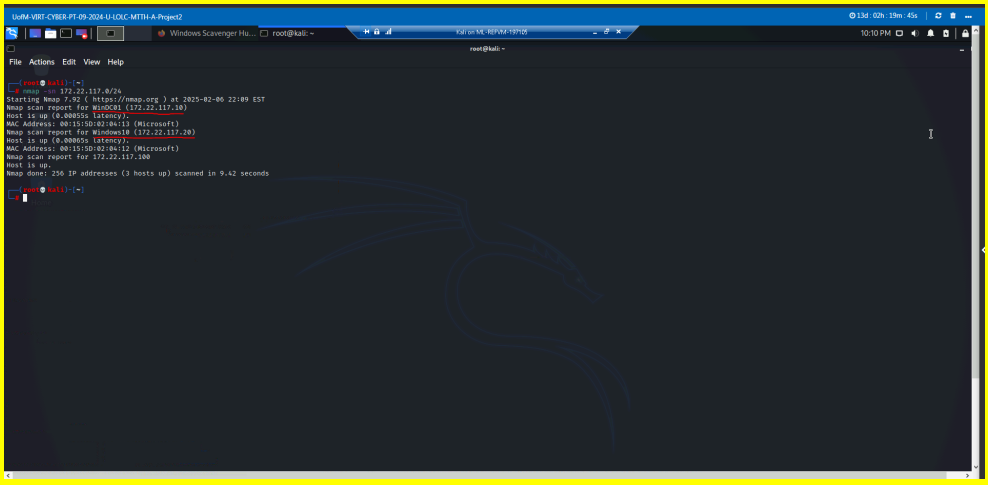


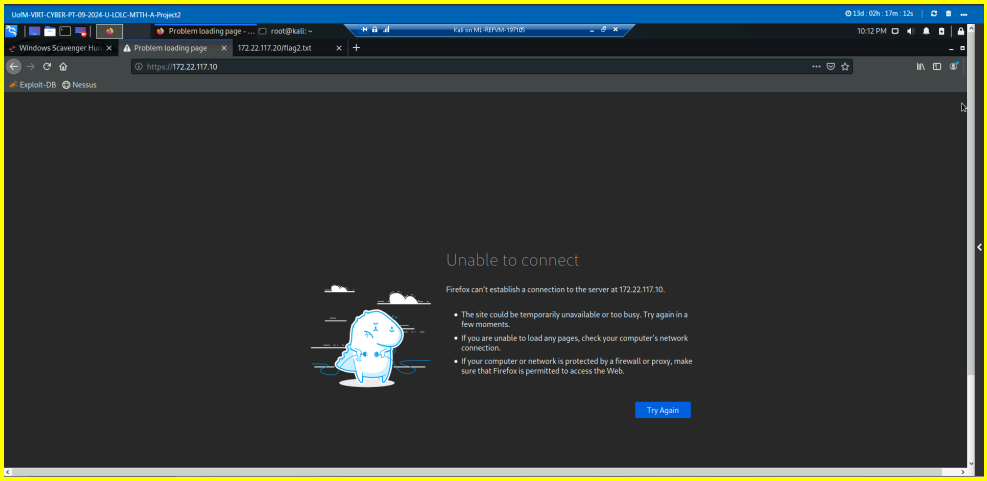


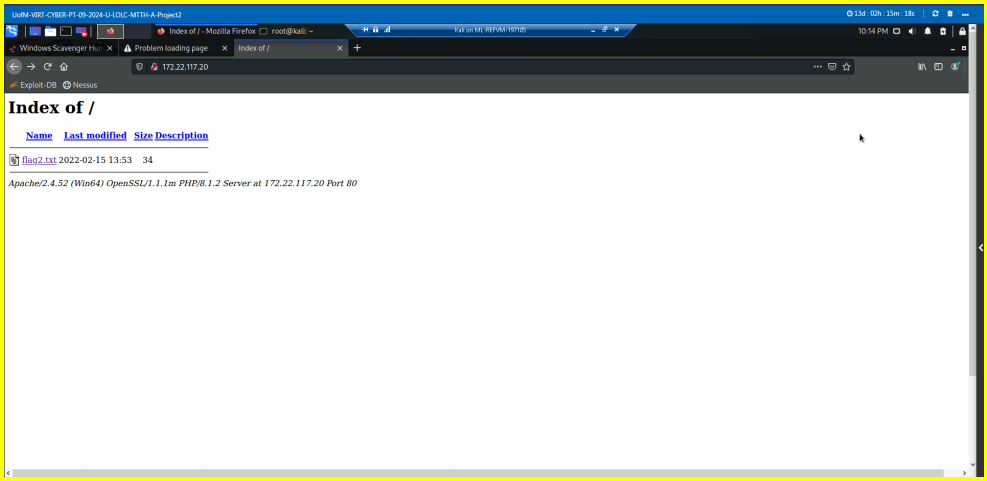
Affected Hosts	The Total Rekall page (totalrekall.xyz)
Remediation	Removing the Github page entirely.

Vulnerability 18	Findings
Title	(Flag 2 Day 3)
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Medium
Description	Using Nmap against the Windows network subnet (172.22.117.0/24), two internal server IPs were found (172.22.117.10 and 172.22.117.20). While entering the first IP yielded no result, the second led to a page displaying a file titled “flag2.txt”, revealing flag 2.

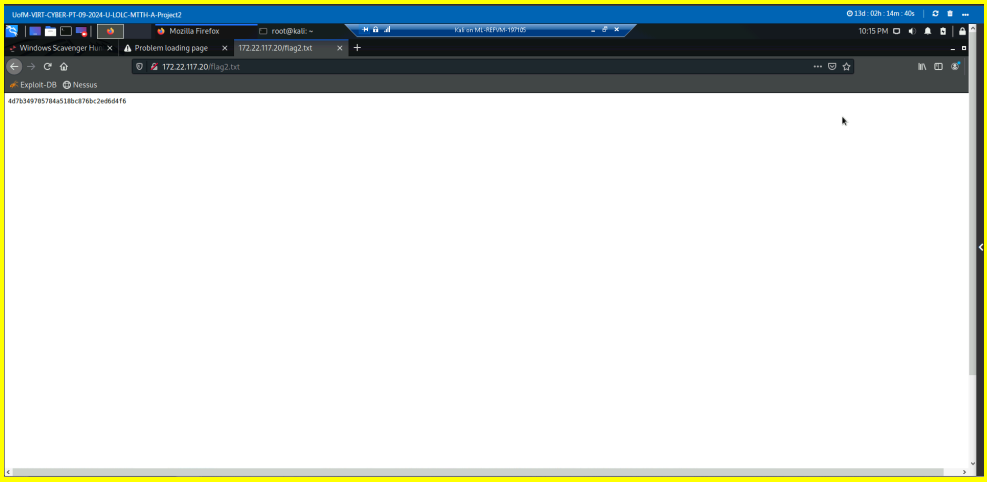
Images

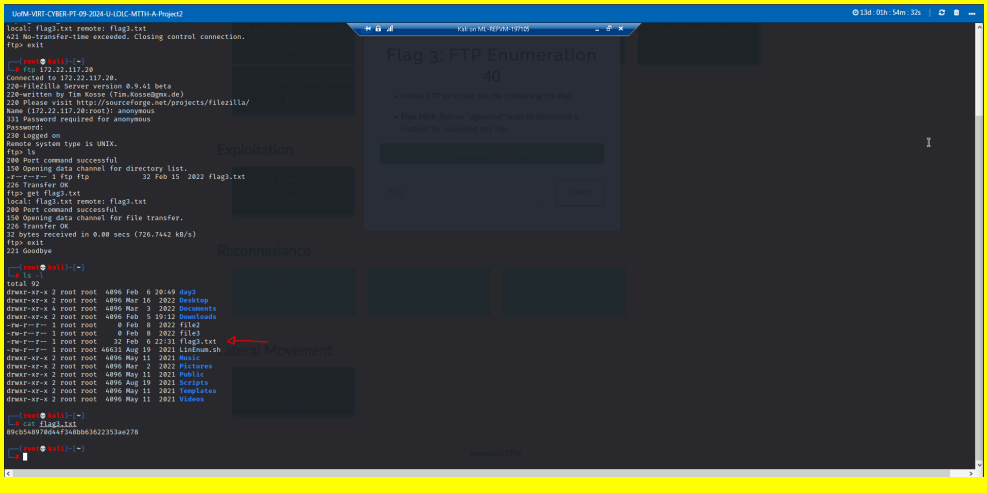




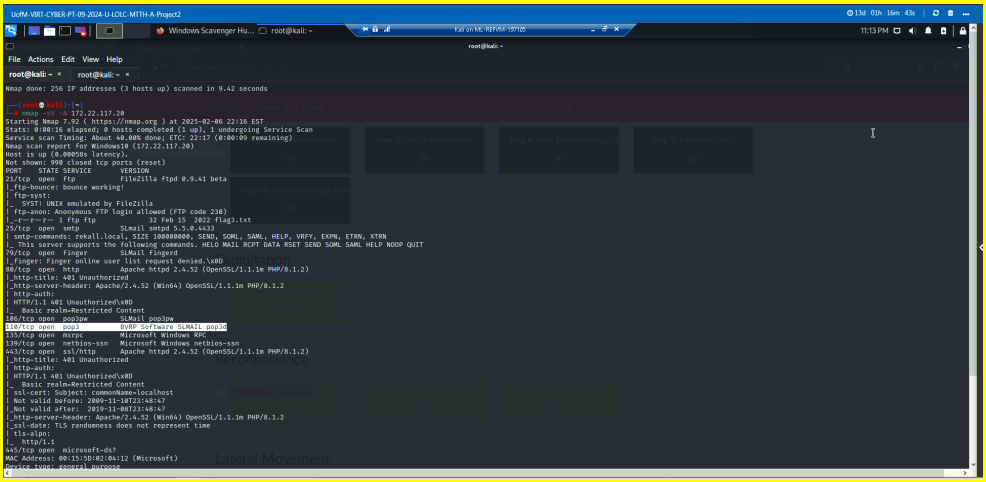
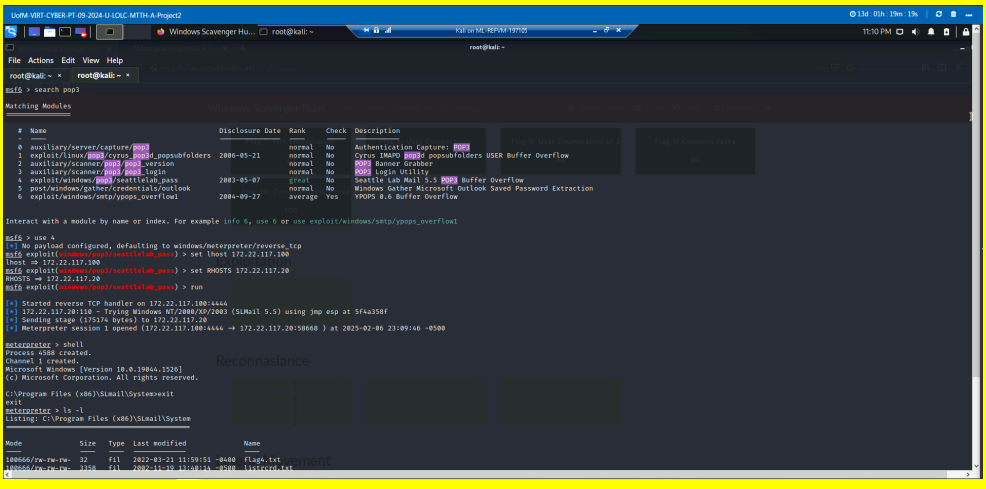


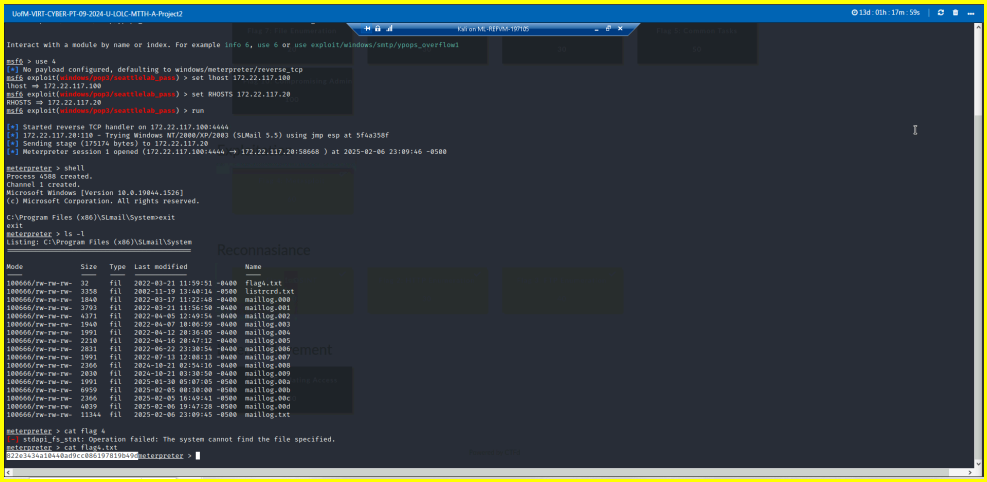
(I was unable to recreate the prompt that required the trivera username and Tanya4life password for a screenshot)

	
Affected Hosts	172.22.117.10, 172.22.117.20
Remediation	According to ChatGPT, the best remediation to this kind of attack is network segmentation. This is the practice of dividing a computer network into smaller, isolated segments or sub-networks.

Vulnerability 19	**Findings**
Title	(Flag 3 Day 3)
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Medium
Description	Using the “ftp” command to establish a connection to the IP 172.22.117.20, the username “anonymous” and password “Tanya4life” was used to gain access to the IP via FTP protocol. Once inside, the command “ls -l” was used to show all contents within the immediate directory, revealing a file titled: “flag3.txt”. The “cat” command was used to show the contents of the file, revealing flag 3.
Images	

Affected Hosts	172.22.117.20
Remediation	ChatGPT recommends removing the ability to use Anonymous Access.

Vulnerability 20	**Findings**
Title	(Flag 4 Day 3)
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Critical
Description	After using Nmap to aggressively scan the IP 172.222.117.20, it was revealed that the IP was running an outdated version of the SLMail service. Upon using the Seattle Lab Mail 5.5 POP3 Buffer Overflow exploit to successfully gain access to the IP, the command “ls -l” revealed a file within the immediate directory titled “flag4.txt”. The “cat” command was then used to show the contents of the file, revealing flag 4.
Images	 

	
Affected Hosts	172.22117.20
Remediation	Upgrading the SLMail service to prevent any potential attacks. ChatGPT recommends hardening the service by disabling unused services, limiting permissions, and enabling detailed logging to detect any attempts of unauthorized access.