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	Cyber Storm, LLC
Contact Name	AMR
Contact Title	Analyst/Pentester

Document History

Version	Date	Author(s)	Comments
001	05/23/2024	AMR	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.

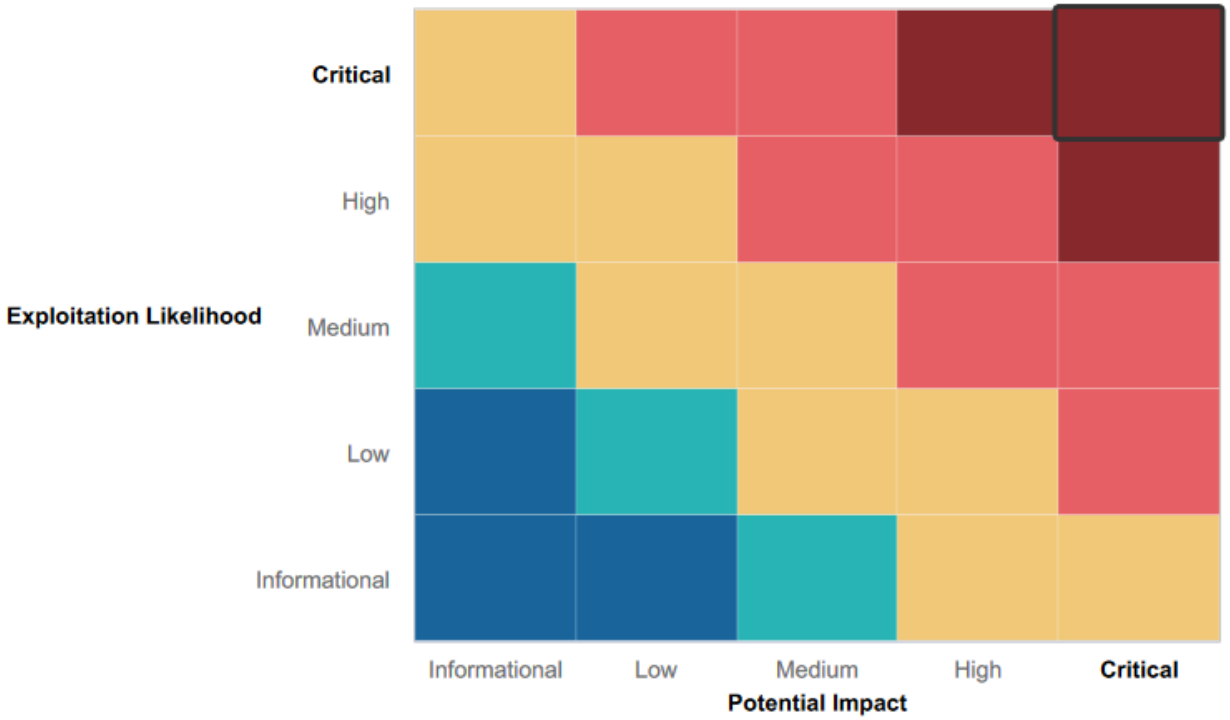
Executive Summary of Findings

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.

- Took several attempts to exploit the command injection
- Multiple exploitation scripts ran against Apache server before locating successful effort

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.

- Many vulnerabilities located on Rekall website
- Open vulnerabilities related to XSS, local file inclusion, and command injections
- Vulnerabilities easily accessible on GitHub Repository

Executive Summary

Cyber Storm LLC performed a comprehensive security assessment for Rekall Corporation, revealing several vulnerabilities: weak passwords, open ports, exposed administrative credentials, XSS vulnerabilities, privilege escalation issues, and vulnerabilities within the Linux and Windows machines.

Our tests revealed 26 vulnerabilities for Rekall Corporations with the most critical vulnerabilities centered around sections of the website allowing unauthorized data input or uploads, potentially leading to theft, manipulation, exploitation, or deletion of customer data. One significant finding was the exposure of administrative credentials via a command injection attack, while updates needed on the Apache server revealed an exploit enabling access to user credential files from a Linux system. Exploiting these vulnerabilities could inflict financial and reputational harm on Rekall Corporation if exploited by malicious actors.

Additionally, we discovered other vulnerabilities, including an exposed password hash on Rekall's public GitHub repository, which we leveraged to breach a Windows10 machine. Rekall's use of outdated email technology poses another vulnerability that requires attention. Furthermore, we identified certain behind-the-scenes settings on the Rekall website facilitating the direction of online robots, recommending adjustments to mitigate potential attacks.

Please see details about each mitigation recommendation in the Vulnerability Findings section of our report.

Thank you for your time and cooperation in this matter. Please feel free to contact us with any questions or concerns.

Summary Vulnerability Overview

Vulnerability	Severity
Reflected Cross Site Scripting XSS	Medium
Stored Cross Site Scripting XSS	Critical
Exclusion Standard Settings Exposure	Critical
Sensitive Data Exposure	Critical
Local File Inclusion	Critical
Command Injection	Critical
Domain Registrar Data Exposure	Medium
DNS Record Exposure	Critical
Certificate Information Exposure	Medium
Nmap Scan	Critical
Drupal (Nmap Result)	High
Apache Struts	Critical
Apache Tomcat Remote Execution	Critical
Shellshock	Critical
Inadequate Permissions/Privilege Escalation to etc/passwd File	Critical
Drupal CVE-2019-6340	Critical
Unprotected User Credentials in GitHub Repository	Critical
HTTP Enumeration/Weak Access Control	High
FTP Anonymous Access Control	High
SLMail Service Version with Vulnerability	High
Improper Permissions on Scheduled Tasks	High
Unprotected NTLM Password Hash	Critical
Sensitive Data Exposure- File Enumeration	High
Cached Credentials- User Enumeration	High
Escalating Access	Critical
Compromising Administrator Credentials and Access	Critical

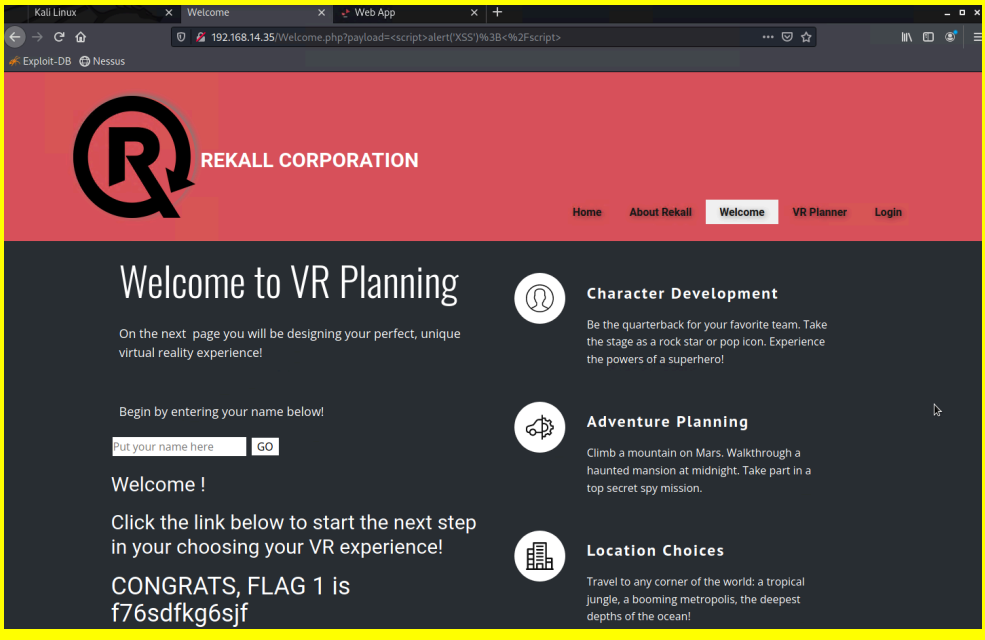
The following summary tables represent an overview of the assessment findings for this penetration test:

Scan Type	Total
Hosts	34.102.136.180 – totalrekall.xyz 192.168.13.10 - Linux 192.168.13.11 - Linux 192.168.13.12 - Linux 192.168.13.13 - Linux 192.168.13.14 - Linux 192.168.13.1 – Linux 172.22.117.20 – Windows10 172.22.117.10 – Windows

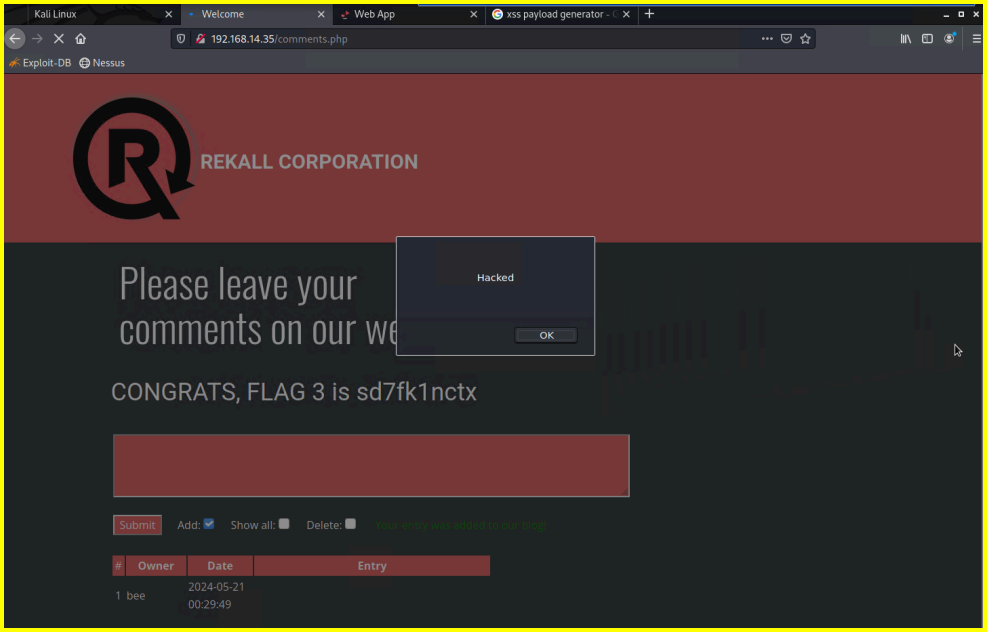
	Domain Controller 172.22.117.100 – Windows host
Ports	80 (HTTP) 21(FTP), 25(SMTP), 110 (POP3), 135 (RPC), 8009 (TCP), 8080

Exploitation Risk	Total
Critical	16
High	7
Medium	3
Low	0

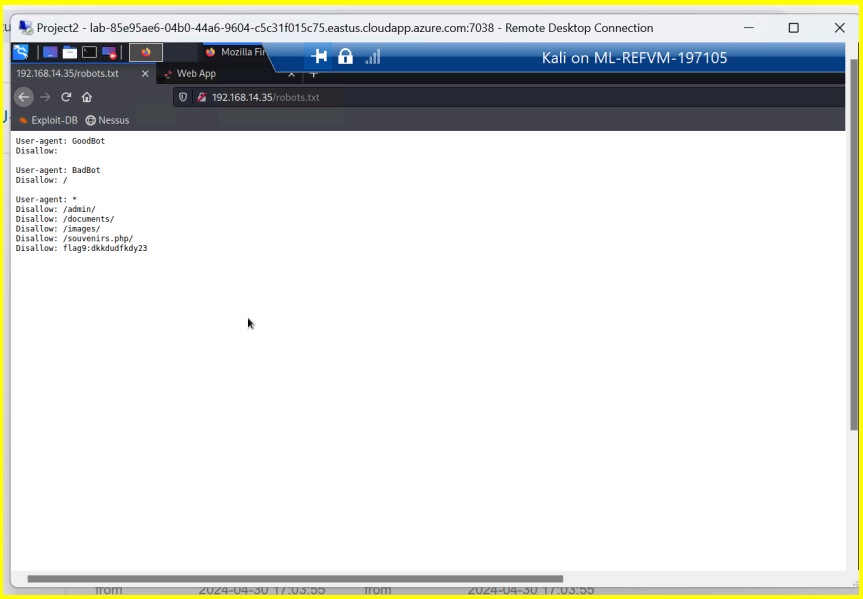
Vulnerability Findings

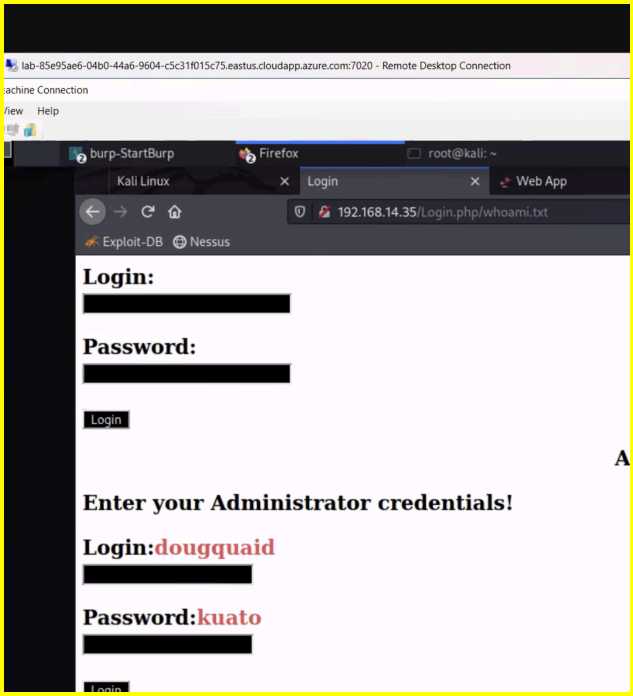
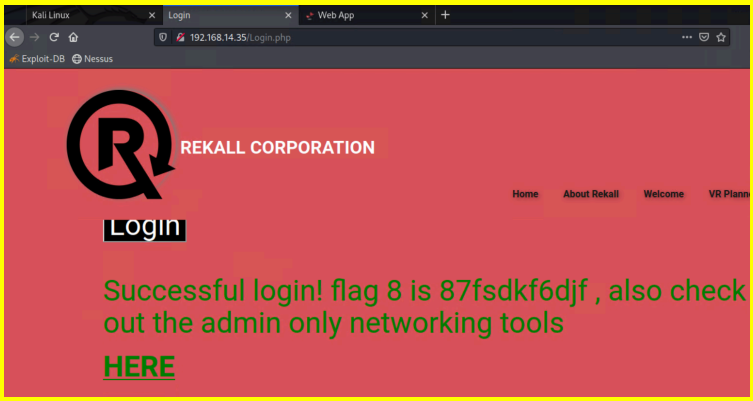
Vulnerability 1	Findings
Title	Reflected Cross SIte Scripting (XSS)
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Medium
Description	Inserted payload on the welcome.php page- <script>alert(“Hi”);</script>
Images	

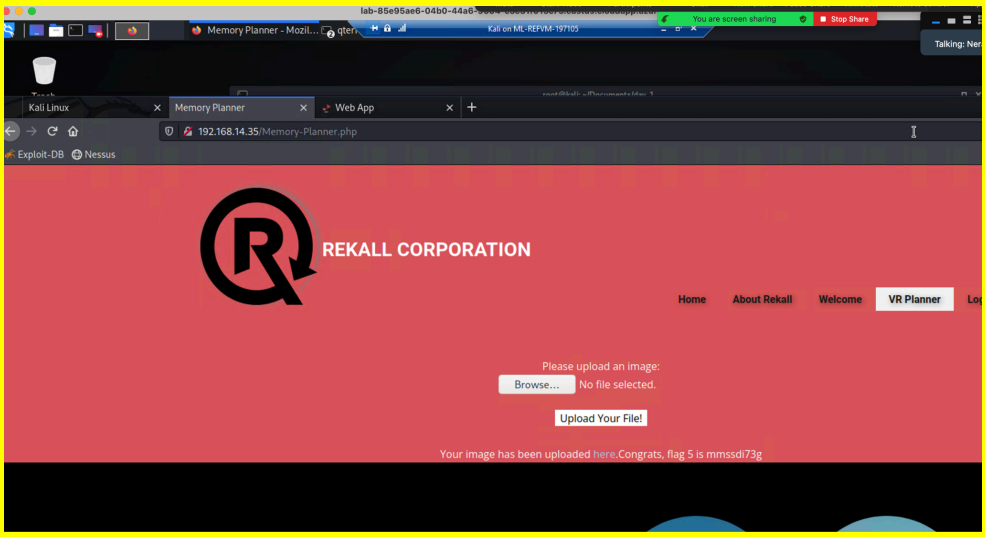
Affected Hosts	192.168.14.35/welcome.php
Remediation	Implement proper input validation and output encoding, especially for user-supplier data.

Vulnerability 2	**Findings**
Title	Stored Cross Site Scripting (XSS)
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Critical
Description	Ran exploit <script>alert(“Hacked”);</script> on the comments.php page.
Images	
Affected Hosts	192.168.14.35/comments.php
Remediation	Use rigorous input validation, output encoding, and content security policies.

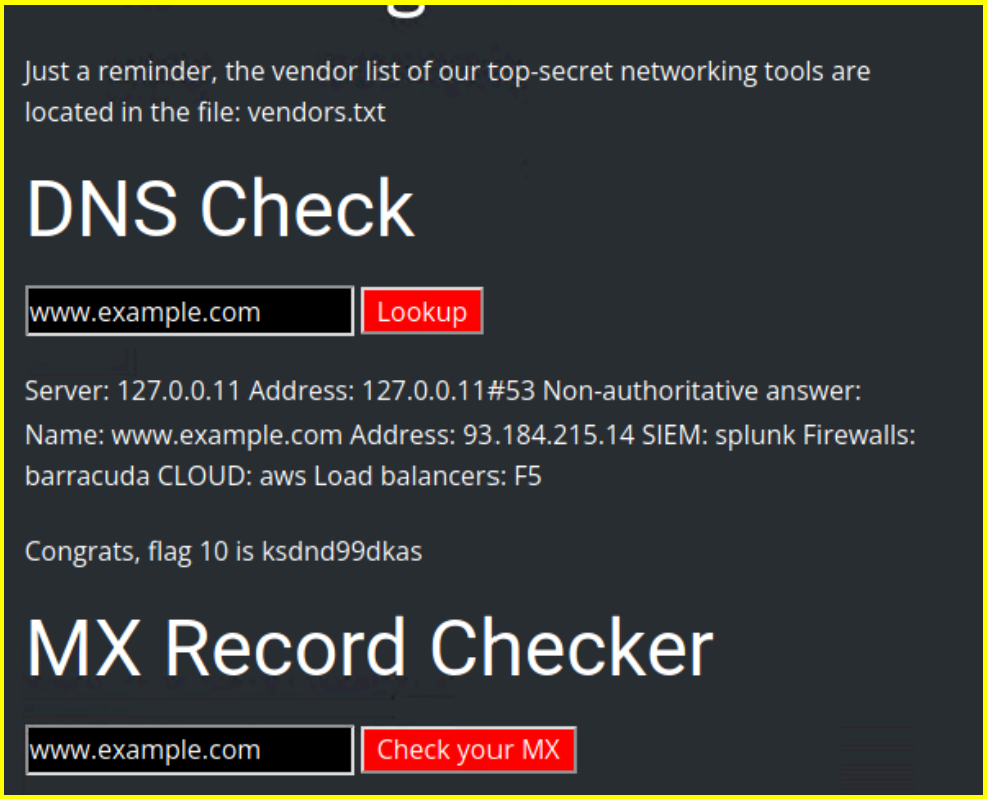
Vulnerability 3	**Findings**
Title	Exclusion Standard Settings Exposure
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Critical
Description	Inserted robots.txt payload into query which resulted in accessible sensitive data.

Images	
Affected Hosts	192.168.14.35/robots.txt
Remediation	Enforce strict access controls and regularly audit permissions to prevent unauthorized changes to exclusion standard settings.

Vulnerability 4	Findings
Title	Sensitive Data Exposure- Administrator Credentials
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Critical
Description	Inserted “whoami” extension into the HTML query structure. Revealed saved administrator credentials.
Images	 
Affected Hosts	192.168.14.35/login.php
Remediation	Encrypt sensitive data in transit and at rest, and implement strong access controls to prevent unauthorized access.

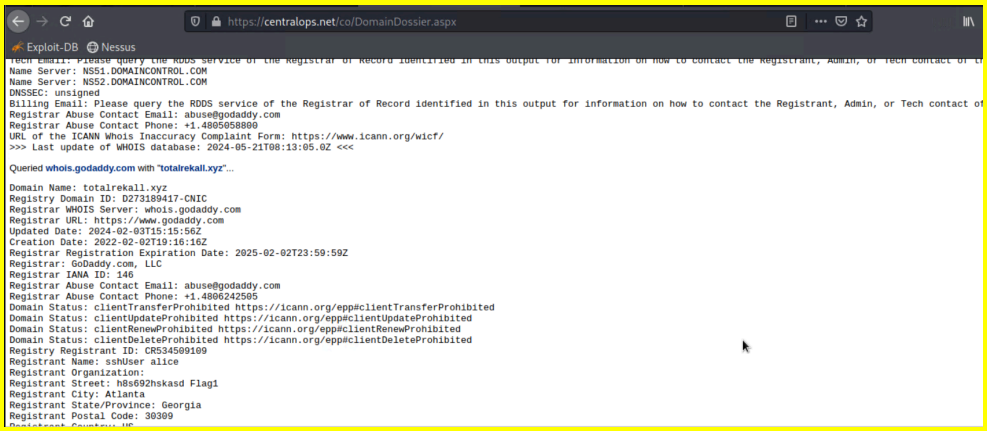
Vulnerability 5	Findings
Title	Local File Inclusion
Type (Web app / Linux OS / WIndows OS)	Web App/Linux OS
Risk Rating	Critical
Description	Uploaded a .php script file into the upload area of the Memory Planner page. The request allows scripts to be run in the backend, malicious or not.
Images	
Affected Hosts	192.168.14.35/mwmory-planner.php
Remediation	Sanitize and validate user inputs to ensure they do not contain path traversal characters, and configure the server to restrict access to critical directories.

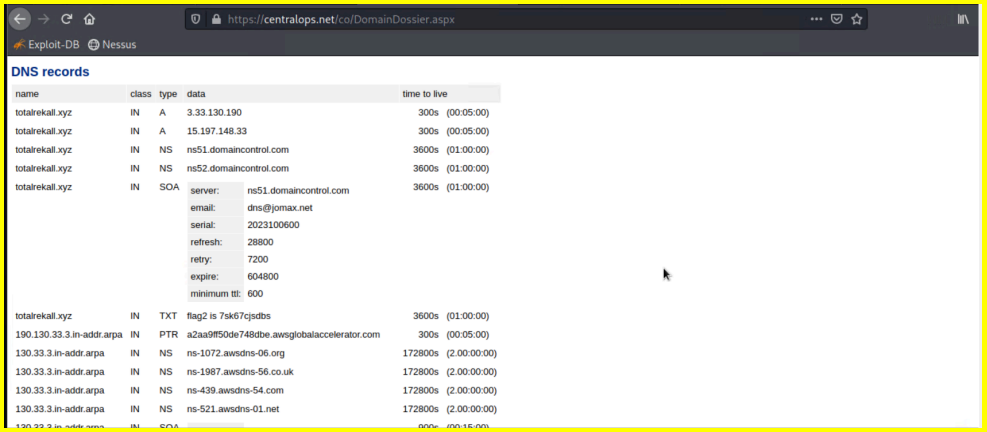
Vulnerability 6	Findings
Title	Command Injection
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Critical
Description	Used payload www.example.com;catvendors.txt. Manipulated the input field in the query designed to execute system commands.

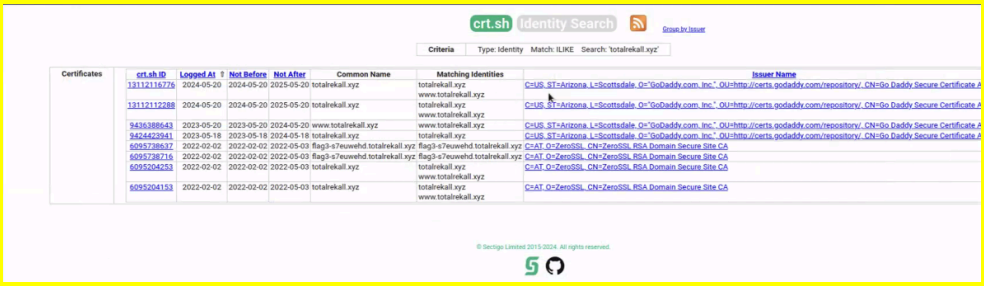
Images	
Affected Hosts	networking.php/vendors.txt
Remediation	Use parameterized queries and avoid using shell commands with user inputs, implementing input validation and least privilege principles.

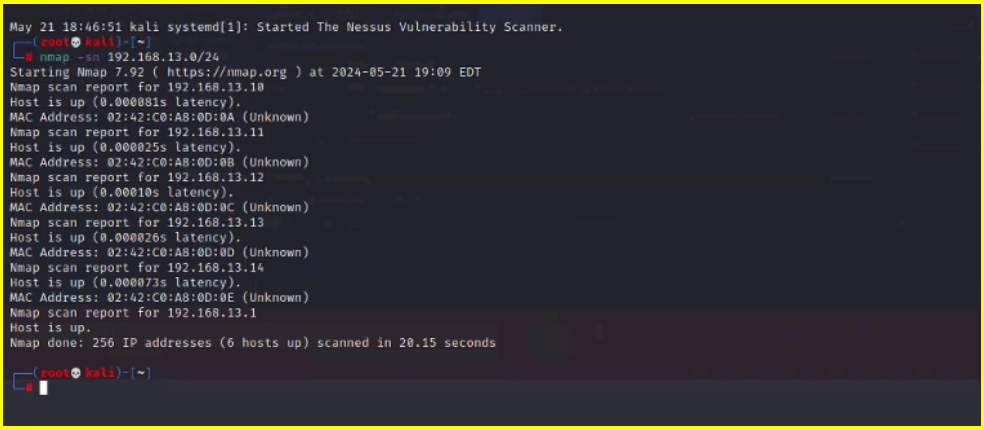
Day 2

Vulnerability 7	Findings
Title	Domain Registrar Data Exposure- Open Source Exposed Data (OSINT)
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Medium
Description	Utilized OSINT tools to explore domain dossier whois records.

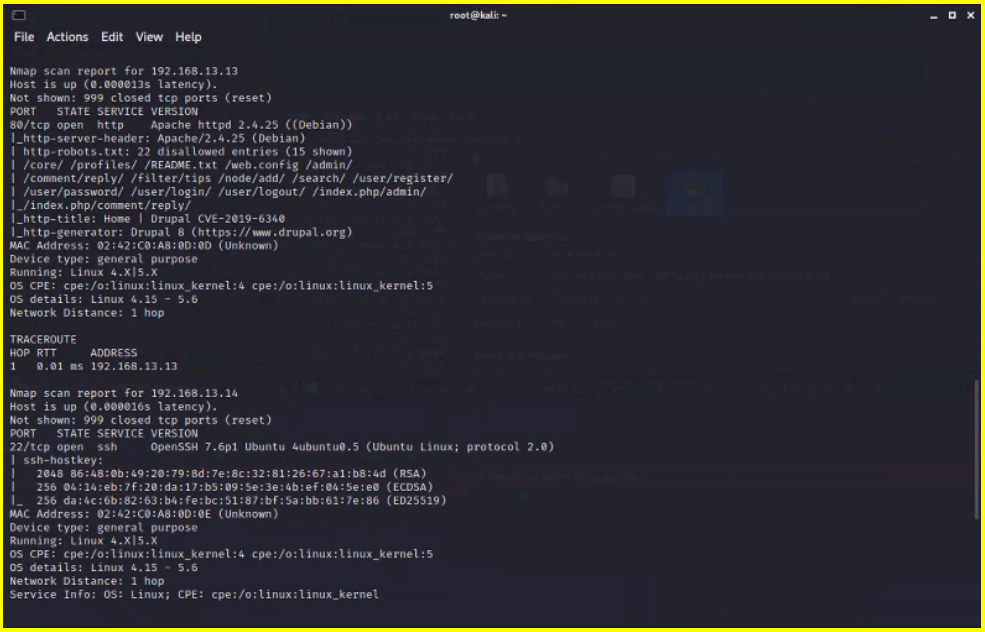
Images	
Affected Hosts	centralops.net/co/DomainDossier.aspx
Remediation	Ensure domain registrar accounts use strong, unique passwords, enable two-factor authentication, and regularly audit contact information and privacy settings.

Vulnerability 8	Findings
Title	DNS Record Exposure
Type (Web app / Linux OS / WIndows OS)	Web App/Linux OS
Risk Rating	Critical
Description	Server is insecurely configured to reveal more information when the IP address is pinged.
Images	
Affected Hosts	totalrekall.xyz centralops.net/co/DomainDossier.aspx
Remediation	Limit public visibility of sensitive DNS records by configuring appropriate DNS security settings and using DNSSEC to protect integrity of DNS data.

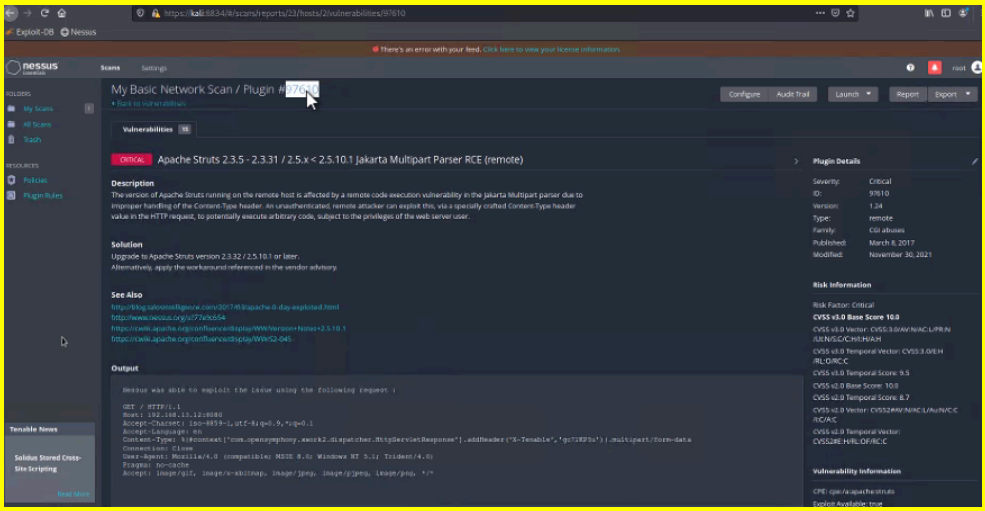
Vulnerability 9	Findings
Title	Certificate Information Exposure- Open Source Exposed Data (OSINT)
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Medium
Description	Explored SSL certificate information.
Images	
Affected Hosts	crt.sh/?q=totalrekall.xyz
Remediation	Regularly review and restrict access to certificate information, implement strong access controls, and use encryption to protect certificate data from unauthorized exposure.

Vulnerability 10	Findings
Title	Nmap Scan
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	Ran Nmap scan and counted the number of hosts which can expose vulnerable devices on the network.
Images	

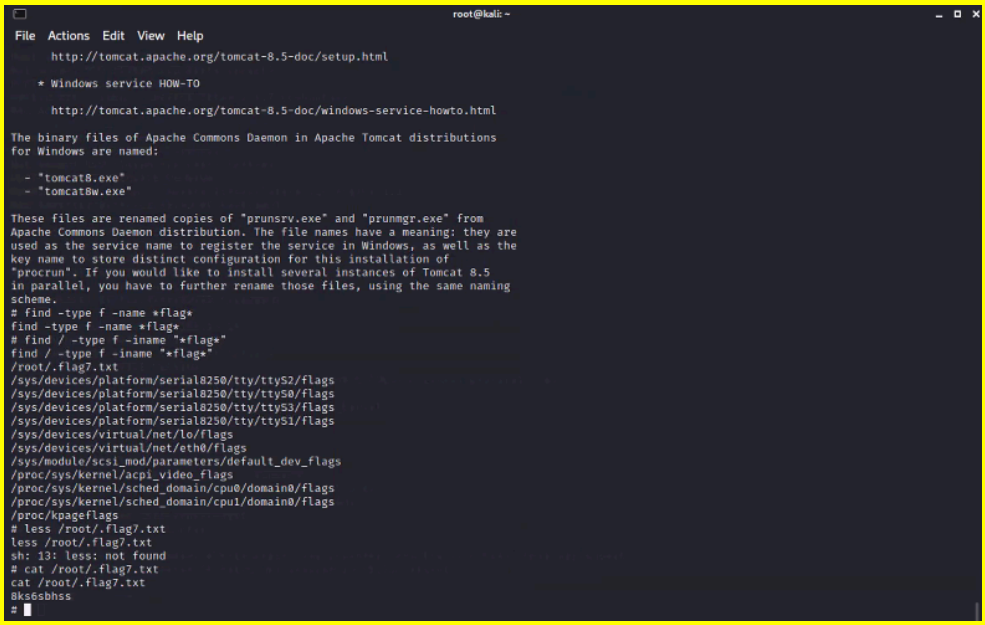
Affected Hosts	192.168.13/24
Remediation	Implement network segmentation, use firewalls to restrict unauthorized scanning, and regularly update and patch systems to mitigate vulnerabilities identified by Nmap scans.

Vulnerability 11	**Findings**
Title	Drupal (Nmap Result)
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	High
Description	Performed aggressive Nmap scan revealing the host that runs Drupal.
Images	
Affected Hosts	192.168.13.13
Remediation	Regularly update Drupal to the latest version, apply security patches promptly, and use security modules to enhance protection against known vulnerabilities.

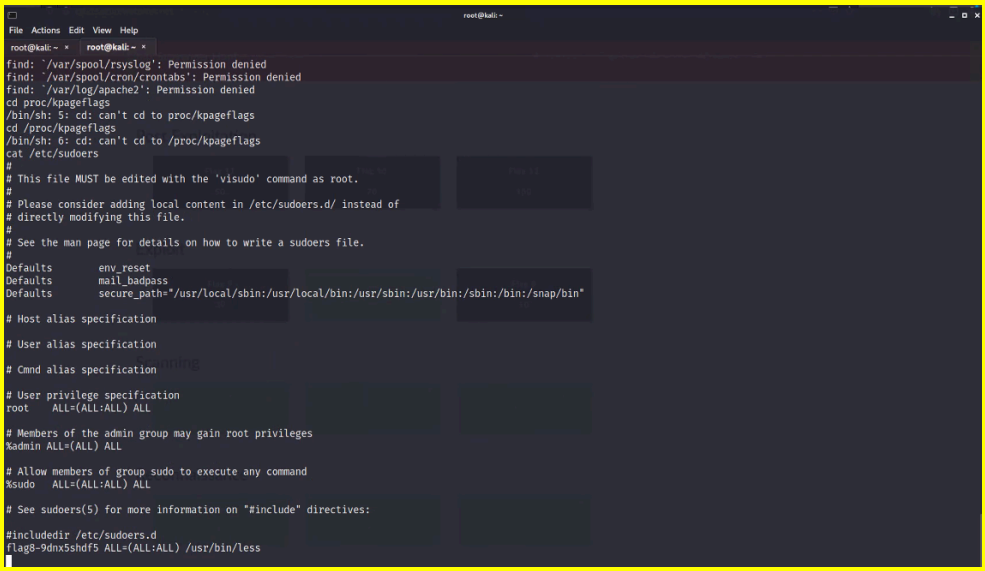
Vulnerability 12	**Findings**
Title	Apache Struts
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical

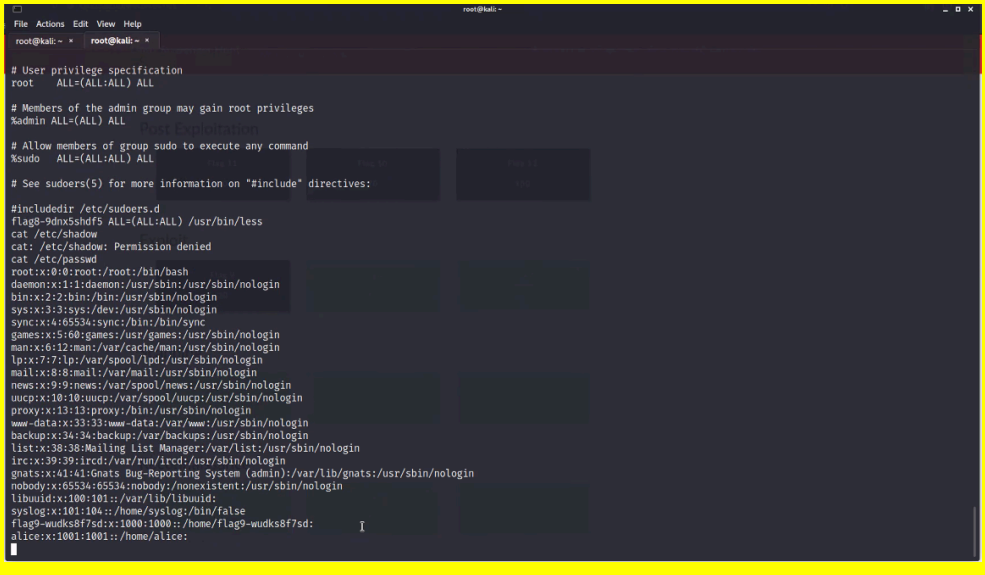
Description	Ran Nessus scan results which identified a critical vulnerability in Apache Struts.
Images	
Affected Hosts	192.168.13.12
Remediation	Upgrade to the latest version of Apache Struts, apply security patches immediately, and configure security settings.

Vulnerability 13	**Findings**
Title	Apache Tomcat Remote Execution
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	Utilized aggressive scan to reveal vulnerable services running on the ports and searched in metasploit for RCE exploit to use for Apache Tomcat.

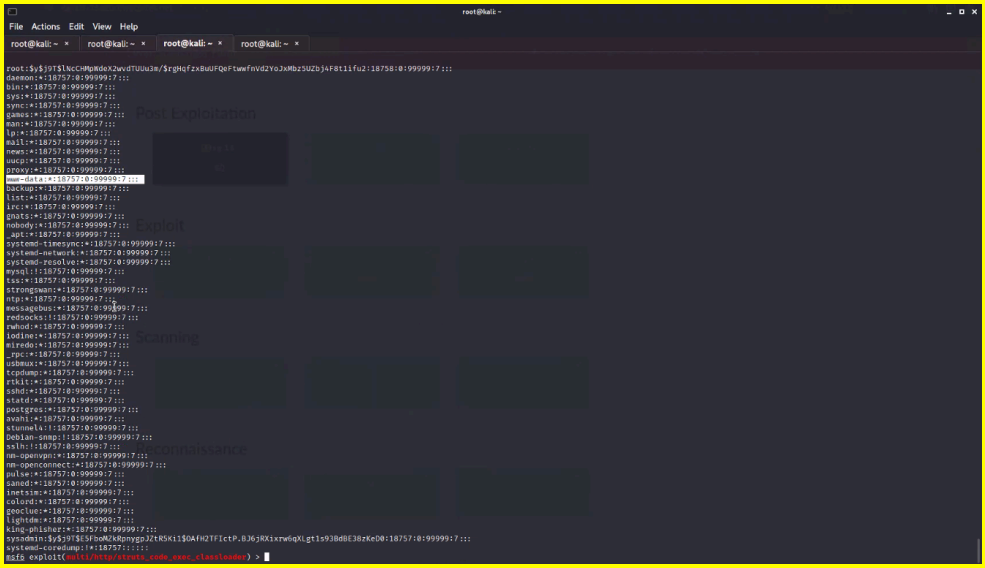
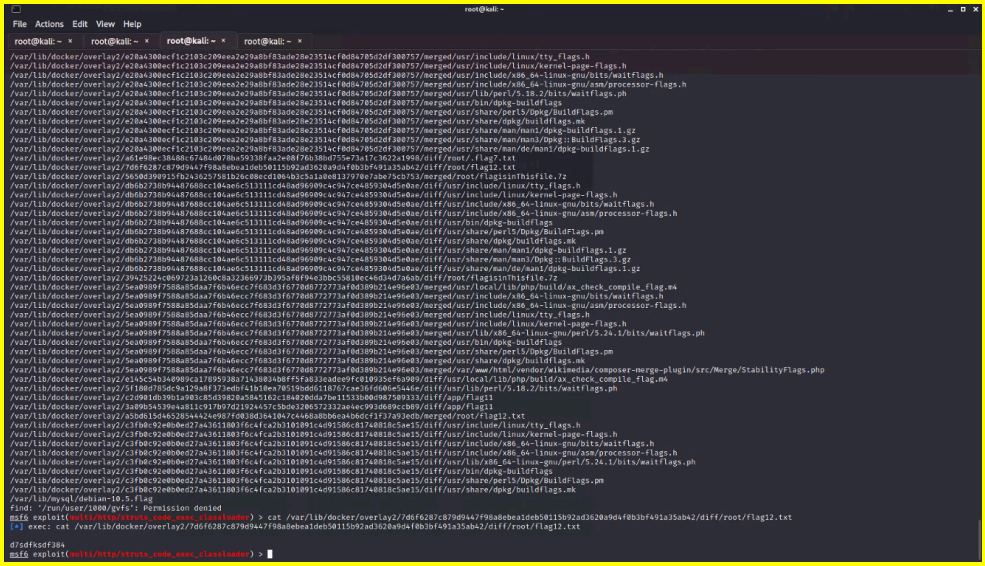
Images	
Affected Hosts	home/etc/root
Remediation	Regularly update Apache Tomcat to the latest version, apply security patches promptly, and configure security settings to restrict access and prevent remote code execution.

Vulnerability 14	Findings
Title	Shellshock
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	Shellshock vulnerability found in web server. Exploited Shellshock using metasploit and ran RHOST and target URI.

Images	
Affected Hosts	etc/sudoers
Remediation	Update Bash to the latest version, apply all relevant patches, and restrict access to potentially vulnerable services to remediate Shellshock vulnerability.

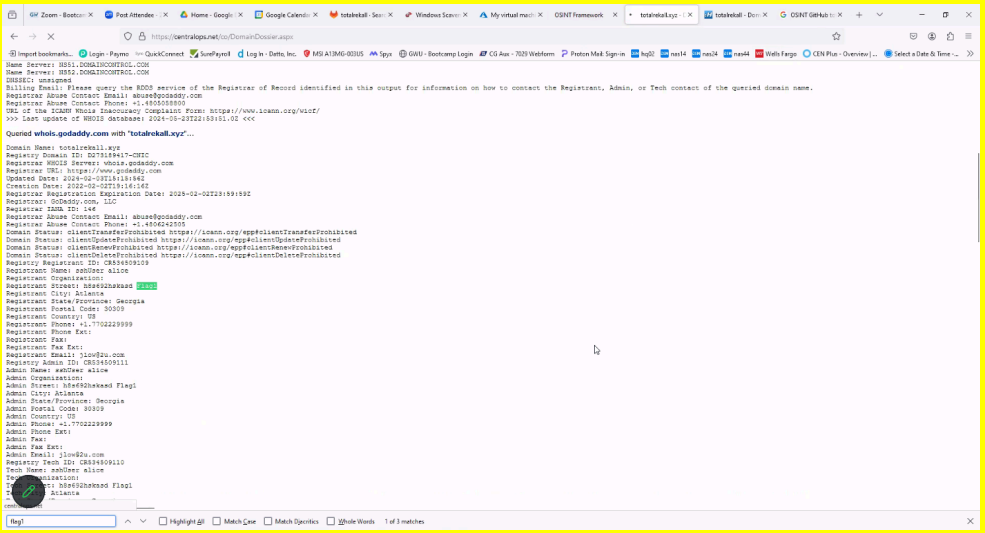
Vulnerability 15	Findings
Title	Inadequate Permissions/Privilege Escalation to etc/passwd file
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	Accessed etc/passwd file and successfully escalated privileges using the credentials that were discovered.
Images	

Affected Hosts	etc/passwd
Remediation	Ensure that sensitive system files like etc/passwd have appropriate permissions set (read-only for non-privileged users) and implement strict access controls to prevent privilege escalation attacks.

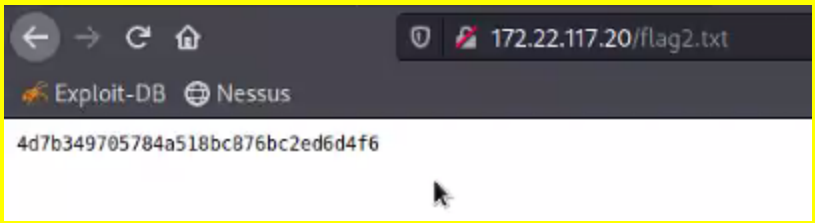
Vulnerability 16	**Findings**
Title	Drupal CVE-2019-6340
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	Ran Drupal exploit drupal_restws_unserialize and then getuid to obtain username.
Images	 

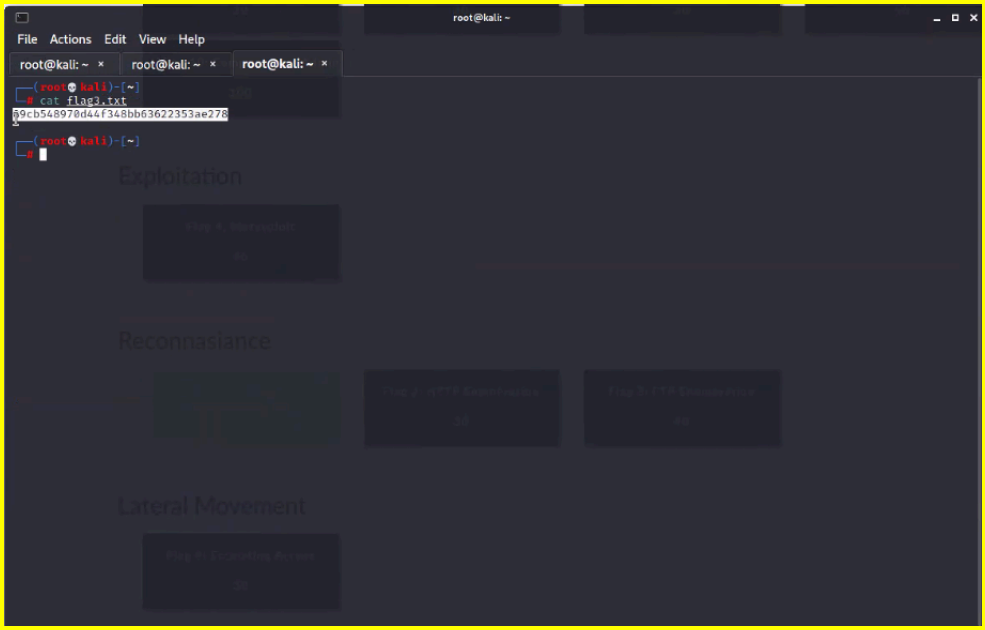
Affected Hosts	192.168.13.13
Remediation	Patch Drupal installations to the latest version, apply the provided security update, and configure proper input validation.

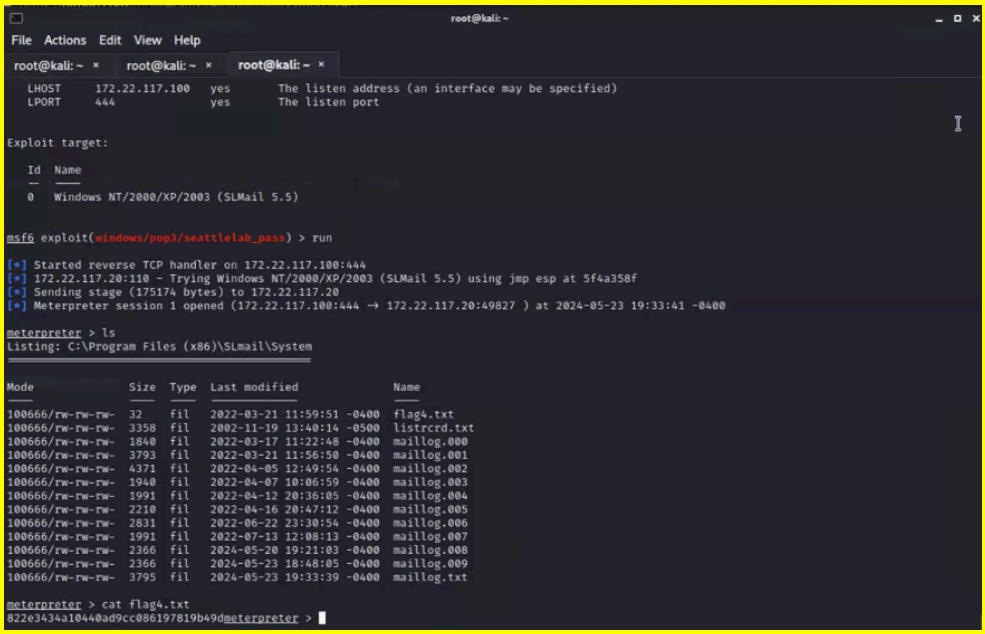
DAY3

Vulnerability 17	Findings
Title	Unprotected User Credentials in GitHub Repository
Type (Web app / Linux OS / WIndows OS)	Web OS
Risk Rating	Critical
Description	Located unprotected credentials by examining the xampp.users page of the GitHub repository.
Images	
Affected Hosts	Totalrekall GitHub and xampp.users
Remediation	Remove the exposed credentials from the repository, rotate the compromised credentials immediately, and use environment variables or secret management tools to securely manage credentials in the future.

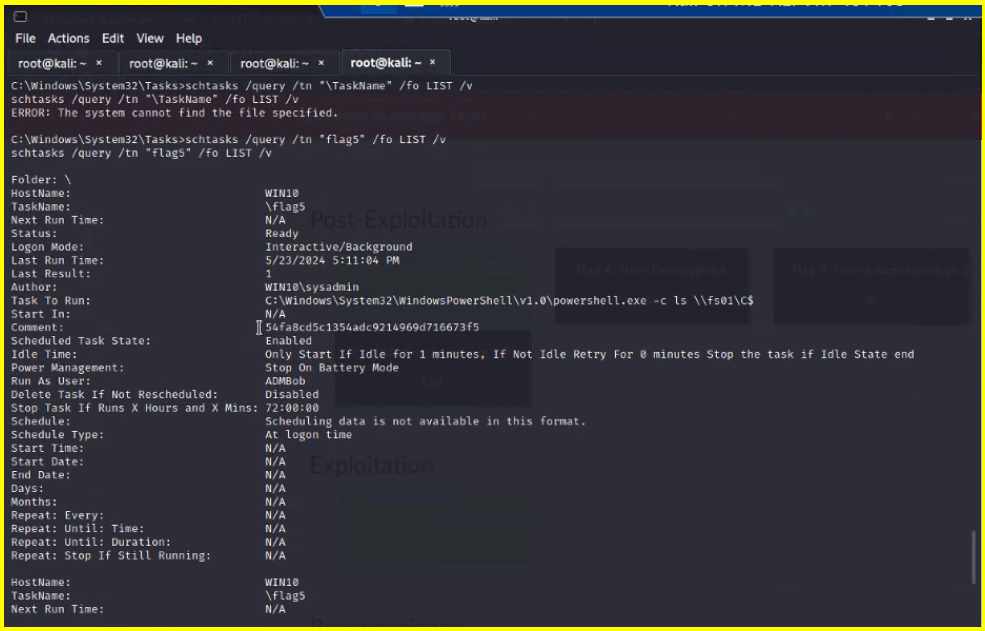
Vulnerability 18	Findings
Title	HTTP Enumeration/Weak Access Control
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	High
Description	The cracked credentials were used to access a secured HTTP server.

Images	
Affected Hosts	172.22.117.20
Remediation	Implement strong authentication and authorization mechanisms, use HTTP's to encrypt data transit, and enforce strict access control policies to mitigate HTTP weak access control vulnerabilities.

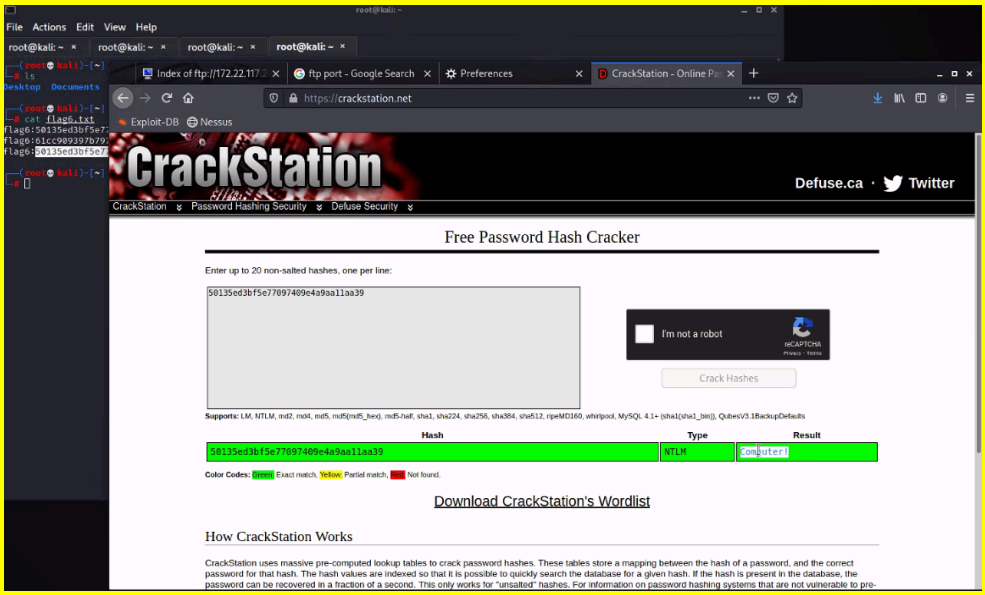
Vulnerability 19	**Findings**
Title	FTP Anonymous Access Allowed
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	High
Description	Logged into FTP anonymously and downloaded and read file.
Images	
Affected Hosts	172.22.117.20
Remediation	Disable anonymous FTP access and require strong authentication to ensure secure access to FTP server.

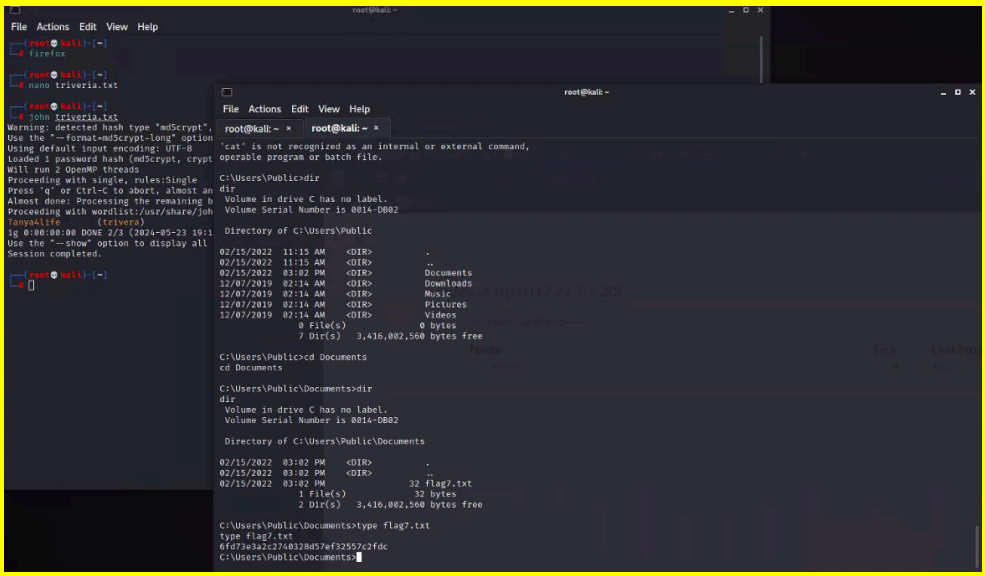
Vulnerability 20	Findings
Title	SLMail Service Version with Vulnerability
Type (Web app / Linux OS / WIndows OS)	Linux OS/Windows OS
Risk Rating	High
Description	Metasploit module exploited the SLMail vulnerability providing a Meterpreter shell that was used.
Images	
Affected Hosts	172.22.117.100 and 172.22.117.20
Remediation	Upgrade SLMail to the latest version, or apply relevant security patches to fix known vulnerabilities in the current version.

Vulnerability 21	Findings
Title	Improper Permissions on Scheduled Tasks
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	High
Description	Inspected the scheduled tasks which revealed data.

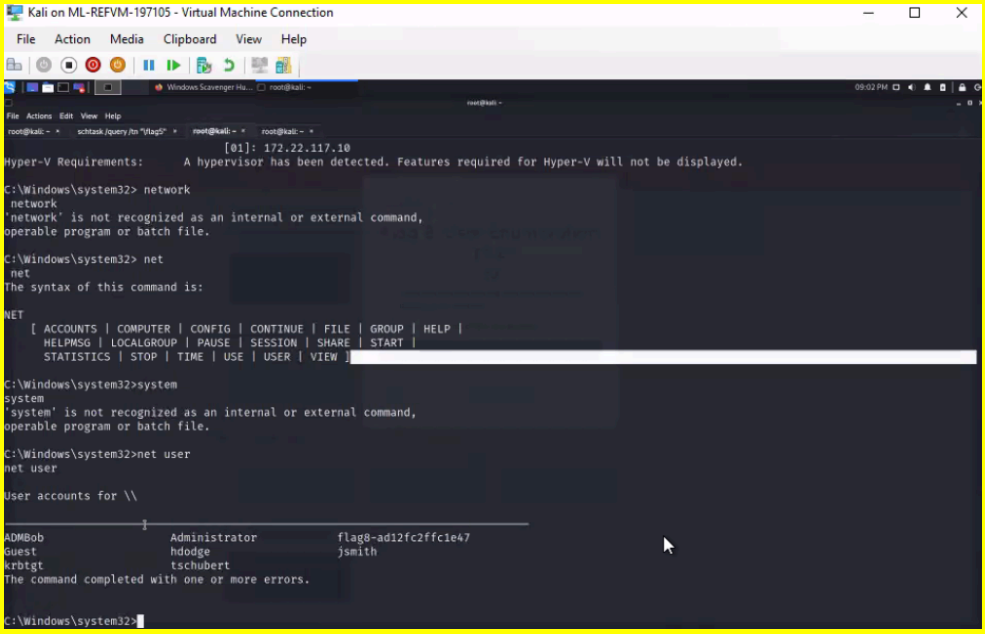
Images	
Affected Hosts	Windows 10
Remediation	Set appropriate permissions on scheduled tasks to ensure only authorized users can create, modify, or execute them

Vulnerability 22	Findings
Title	Unprotected NTLM Password Hash- User Enumeration
Type (Web app / Linux OS / WIndows OS)	Linux OS/Web App
Risk Rating	Critical
Description	Used the kiwi extension in the Meterpreter shell to reveal the hashed NTLM password of a user. This hash was then uploaded into CrackStation where we successfully cracked the text password.

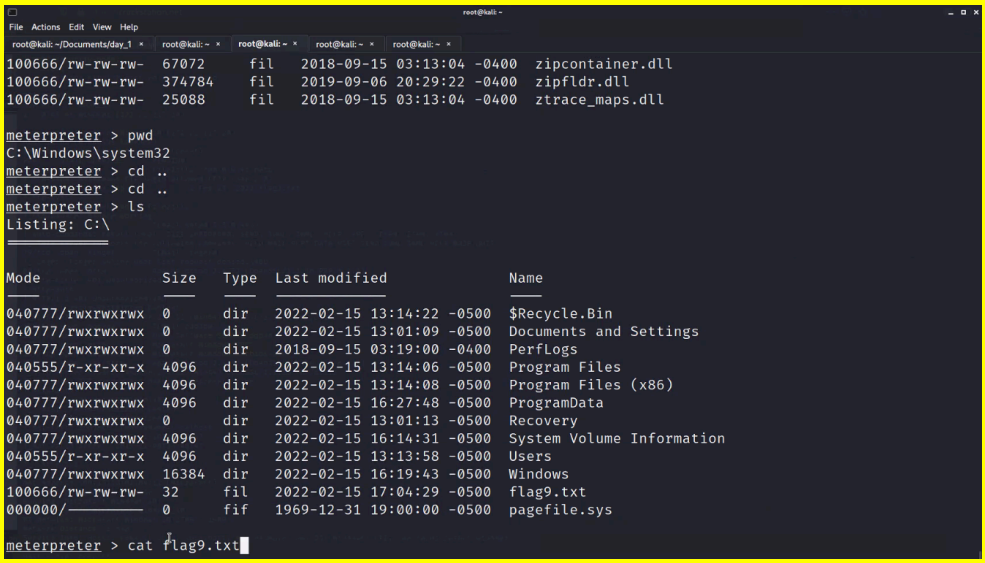
Images	
Affected Hosts	NTLM protocol
Remediation	Store NTLM password hashes securely using strong encryption and limit access to authorized personnel only to prevent unauthorized access.

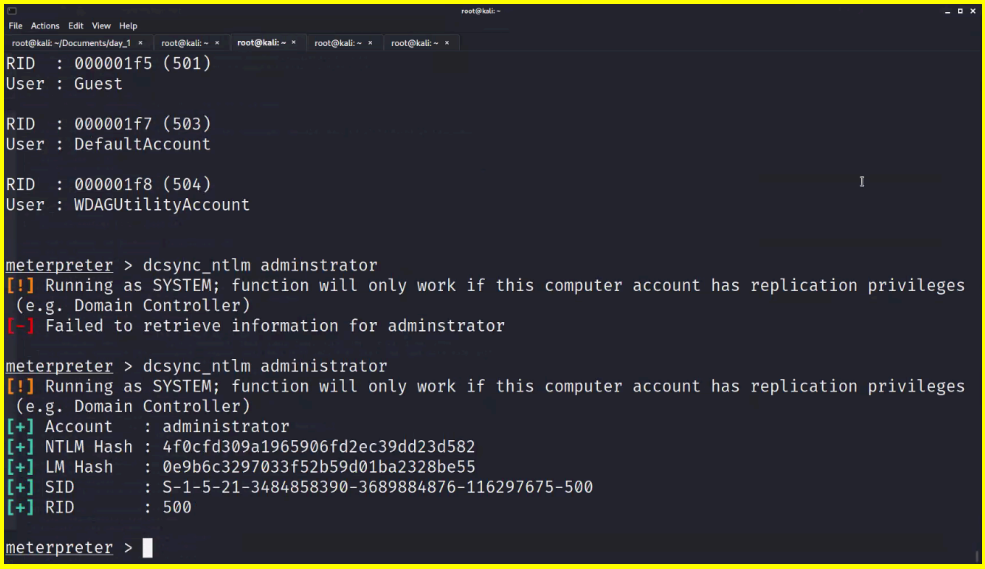
Vulnerability 23	Findings
Title	Sensitive Data Exposure- File Enumeration
Type (Web app / Linux OS / WIndows OS)	Linux OS/Windows OS
Risk Rating	High
Description	Searched the file system of the compromised machine which revealed data.
Images	
Affected Hosts	Windows 10 and C drive

Remediation	Encrypt sensitive data both in transit and at rest, and implement strict access controls to prevent unauthorized access and exposure.

Vulnerability 24	Findings
Title	Cached Credentials- User Enumeration
Type (Web app / Linux OS / WIndows OS)	Linux OS/Windows OS
Risk Rating	High
Description	Kiwi extension in Meterpreter was used to dump cached credentials of an admin (ADMBob). These credentials were then cracked to access the Windows login page of another machine.
Images	
Affected Hosts	Windows 10
Remediation	Disable credential caching or configure policies to securely manage and regularly clear cached credentials to prevent unauthorized access.

Vulnerability 25	Findings
Title	Escalating Access
Type (Web app / Linux OS / WIndows OS)	Linux OS/Windows OS
Risk Rating	Critical
Description	Navigated to the root directory via Meterpreter and read the text file with data.

Images	
Affected Hosts	Windows 10 and C drive
Remediation	Implement the principle of least privilege, enforce multi-factor authentication, and regularly audit permissions to prevent unauthorized access escalation.

Vulnerability 26	Findings
Title	Compromising Administrator Credentials and Access
Type (Web app / Linux OS / WIndows OS)	Linux OS/Windows OS
Risk Rating	Critical
Description	Kiwi extension of Meterpreter used to DCSync the administrator user. NTLM password hash was revealed.
Images	
Affected Hosts	dcsyn_ntlm administrator

Remediation	Enforce strong, unique passwords, enable multi-factor authentication, and conduct regular security audits to protect and monitor administrator credentials and access.