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	Orange Hats
Contact Name	Jason Vaz
Contact Title	Pentester

Document History

Version	Date	Author(s)	Comments
001	02/20/2025	Jason Vaz	Web App Exploits
002	02/20/2025	Jason Vaz	Linux Server Exploits
003	02/20/2025	Jason Vaz	Windows Server Exploits
004	02/20/2025	Jason Vaz	Executive Summary
005	02/20/2025	Jason Vaz	Vulnerability Overview
006	02/20/2025	Jason Vaz	Vulnerability Findings

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.

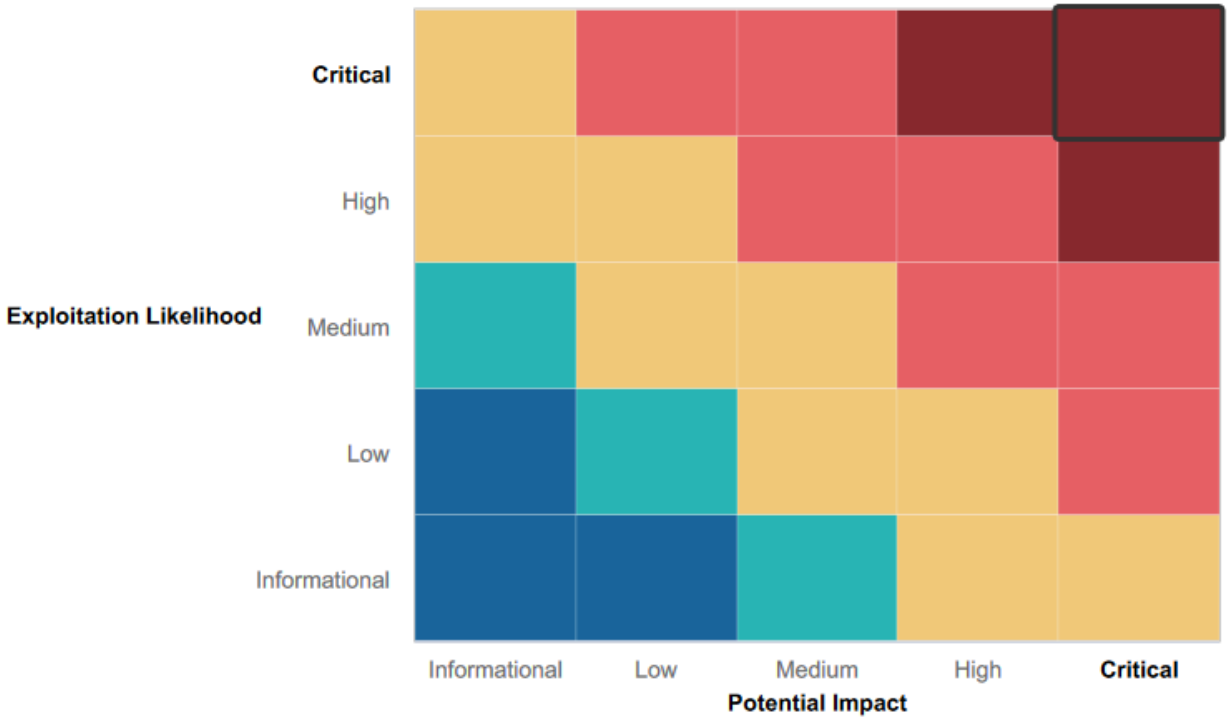
Executive Summary of Findings

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.

- **A comprehensive DDoS mitigation strategy** is implemented to maintain network availability and prevent service disruptions.
- **Network architecture mapping** ensures that no vulnerable open-source data is exposed, reducing the risk of unauthorized penetration.
- **Advanced security tools** such as Metasploit, Hashcat, and Nmap are utilized to detect and prevent unauthorized access attempts.
- **A proactive security approach** is adopted, balancing both defensive and offensive strategies to anticipate and counter emerging threats.
- **Ongoing penetration testing** is conducted to continuously identify, assess, and remediate vulnerabilities, strengthening overall security resilience.

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.

- **XSS and SQL Injection Vulnerabilities:** The web application is susceptible to Cross-Site Scripting (XSS) and SQL injection, allowing attackers to execute malicious scripts and manipulate database queries.
- **Exposure of Credentials in Source Code:** User credentials are stored in the HTML source code, making them easily accessible to unauthorized users.
- **Outdated Apache Web Server:** The Apache web server is running an outdated version, exposing it to multiple known exploits that could compromise system security.
- **Vulnerable SLMail Server:** The SLMail server contains security flaws that allow remote exploitation, potentially granting attackers unauthorized shell access.
- **Risk of Password Hash Cracking:** Unauthorized access to password hashes creates an opportunity for attackers to crack passwords and escalate privileges.
- **Public Disclosure of Server Address:** The physical address of Rekall's server is publicly available, increasing the risk of targeted cyberattacks.
- **Credential Exposure in IP Lookup:** Credentials are revealed during IP lookup queries, potentially leading to unauthorized access.
- **Network Vulnerabilities in IP Range:** Rekall's IP addresses display security weaknesses, such as open ports and other vulnerabilities, when scanned.
- **Open Ports Allow Unauthorized Access:** Unsecured open ports permit file enumeration and unauthorized access, increasing the likelihood of data breaches.

Executive Summary

During the penetration testing of Rekall's IT assets, Orange Hats was able to identify multiple vulnerabilities, including several Critical ones that could have a potentially catastrophic impact on Rekall's revenue or reputation. Orange Hats successfully infiltrated Rekall's assets, exfiltrated sensitive data, and escalated privileges within systems, as outlined below.

Web Application Assessment

Orange Hats began testing Rekall's Web Application, which was found to be vulnerable to a Reflected XSS attack, allowing malicious scripts to run on the homepage. The Web App also showed a vulnerability to Local File Inclusion, where files could be uploaded from the VR Planner webpage. An XSS Stored vulnerability was discovered on the Comments page, permitting scripting code execution. SQL Injection attacks were found to be possible on the Login.php toolbar, while the Networking.php page was susceptible to a Command Injection attack.

Data Exposure

Open-source data was exposed and could be viewed using OSINT, with a stored certificate revealed by searching crt.sh. Shockingly, user login credentials were found in plain text within the HTML source code of the Login.php page, easily visible by simply highlighting the page in a web browser. The file robots.txt was also exposed and readily accessible. Research uncovered user credentials in a GitHub repository, leading to unauthorized access to the web host's files and directories. Additionally, the Apache server was found to be out-of-date with a Struts vulnerability.

Linux Environment Evaluation

In the Linux environment, Orange Hats identified five publicly exposed and vulnerable IP addresses, one of which was running Drupal. Stolen credentials were used to access a host and escalate privileges to root. A common known shell RCE execution vulnerability was discovered using Meterpreter, and the sudoers file was accessible through a Shellshock exploit in Metasploit.

Windows Environment Evaluation

Next, the Windows OS environment was tested, revealing that FTP Port 21 and Port 110 (used for SLMail service) were open and vulnerable. Metasploit was used to identify these vulnerabilities, gain access to a password hash file, and crack it, allowing for the creation of a reverse shell. Scheduled tasks were easily visible in the Windows 10 Task Scheduler, and Metepreter could be used to display directories on public Windows directories.

Conclusions

In conclusion, these vulnerabilities could be maliciously exploited, causing severe damage to both the assets and overall business functionality. Orange Hats has provided detailed recommendations to mitigate each of these vulnerabilities, preventing potential harm and loss.

Summary Vulnerability Overview

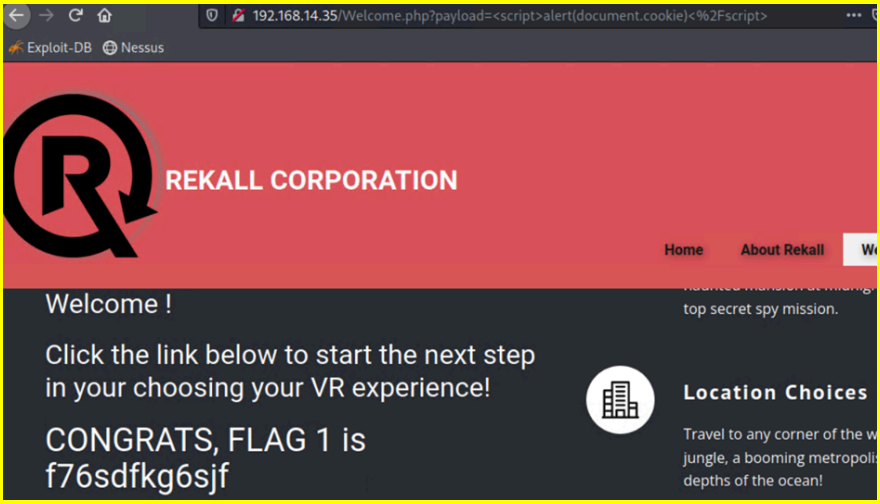
Vulnerability	Severity
XSS Reflected	Medium
Local File Inclusion	Critical
XSS Stored	Critical
SQL Injection	Critical
Command Injection	Critical
FTP Enumeration	Critical
SLMail Exploit	Critical
Sensitive Data/Credentials Dump	Critical
Open Source Exposes Data	Medium
Certificate Search Vis crt.sh	Medium
Nmap Scan Result	Critical
Aggressive Nmap Scan	Critical
User Credentials Exposure	Critical
Sensitive Data Exposure	Medium
Nessus Scan	Medium
Privilege Escalation	Critical
Meterpreter shell RCE execution (CVE 2017-5638)	Critical
Shellshock on Web Server (Port 80)	Critical
Username and Password Hash in Repo	Critical
Port Scon of Subnet	Critical
Windows 10 Machine Task Scheduler	Medium
Public Directory Search	Medium

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

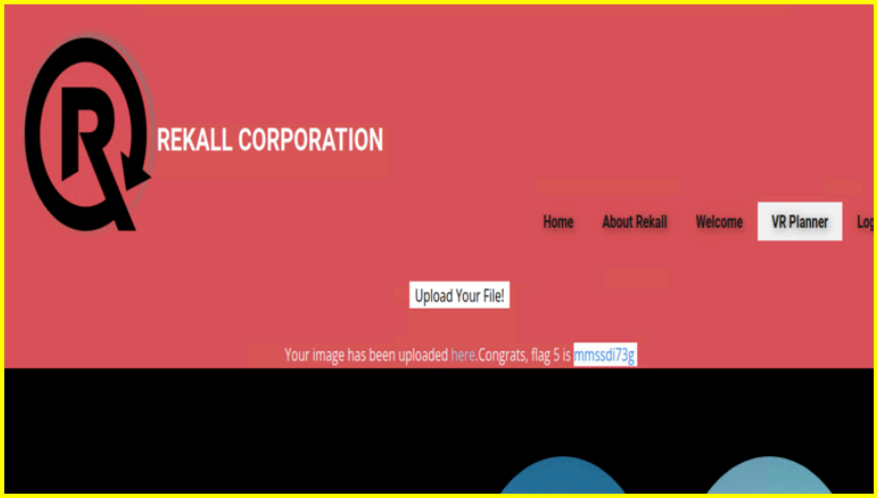
Scan Type	Total
Hosts	192.168.13.10, 192.168.13.11, 192.168.13.12, 192.168.13.13, 192.168.13.14,192.168.14.35, 172.22.117.20, 172.22.117.10
Ports	21, 22 80, 106,110

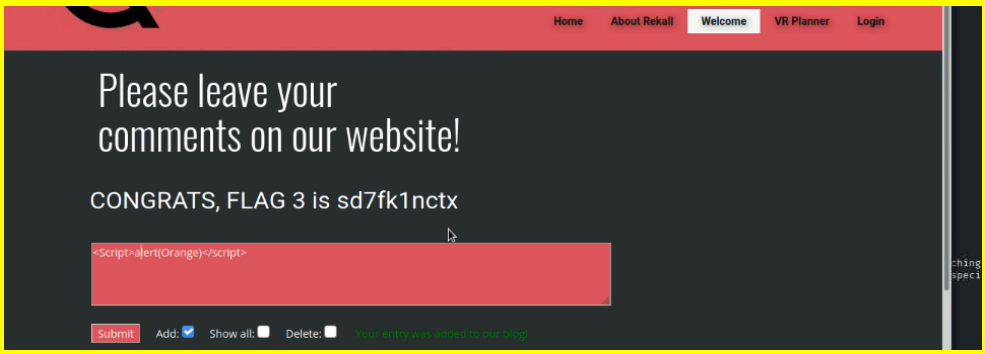
Exploitation Risk	Total
Critical	15
High	0
Medium	7
Low	0

Vulnerability Findings

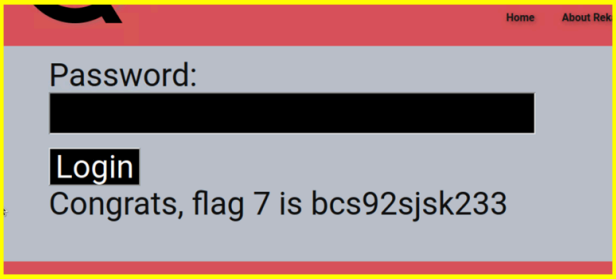
Vulnerability 1	Findings
Title	XSS Reflected
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	**Medium**
Description	Malicious script successfully reflected on host home page **<script>alert(Document.cookie)</script>**
Images	
Affected Hosts	192.168.14.35
Remediation	Input Validation

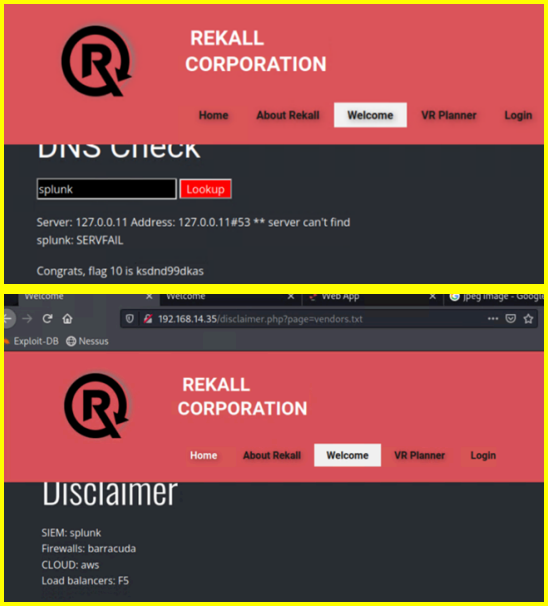
Vulnerability 2	Findings
Title	Local File Inclusion
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	**Critical**
Description	successfully uploaded a .php file by changing the name of the file to end with .jpg on the VR planner page

Images	
Affected Hosts	192.168.14.35
Remediation	Prevent direct appending of file paths; if possible, restrict the API to allow inclusion only from a specified directory and its subdirectories.

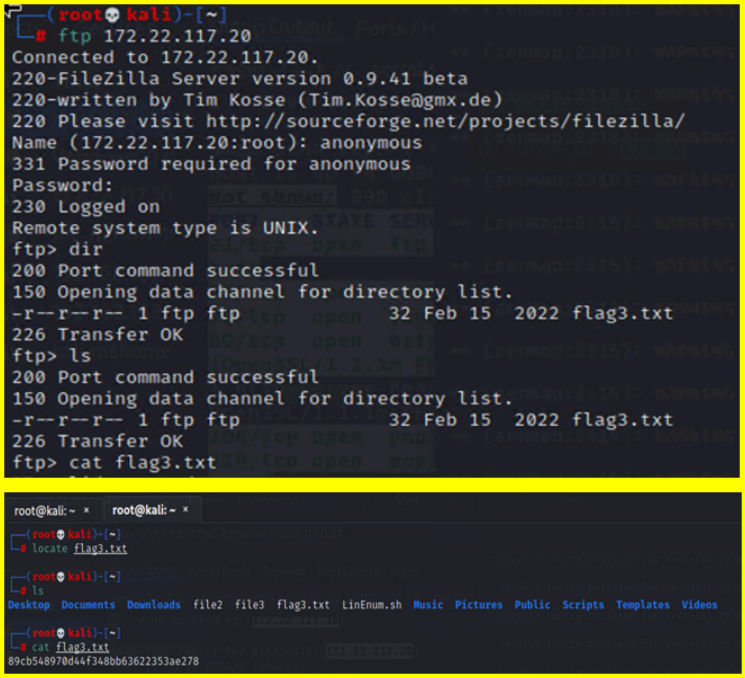
Vulnerability 3	Findings
Title	XSS Stored
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	**Critical**
Description	While accessing /Comments page, entered <script>alert(“Orange”)</script> to reveal Flag 3
Images	
Affected Hosts	192.168.14.35
Remediation	Implement XSS protection to disallow injection of script code in comment section of website, or remove comment sections of website completely and substitute with a directly link to a google review

Vulnerability 4	Findings
Title	SQL Injection

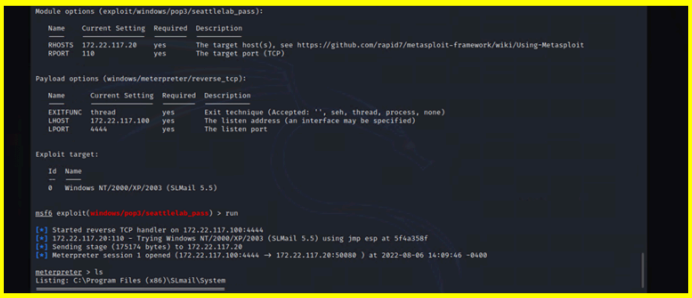
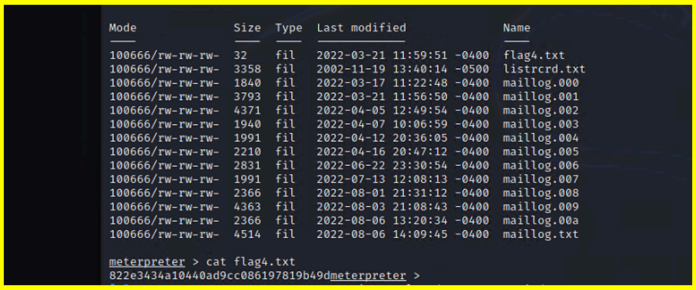
Type (Web app / Linux OS / Windows OS)	Web APP
Risk Rating	**Critical**
Description	While accessing /Login.php page, payload **(Name or "1=1")** was entered in toolbar intended for password successfully resulting in exploit
Images	
Affected Hosts	192.168.14.35
Remediation	Limit the ability web app to accept direct input and/or implement character escaping

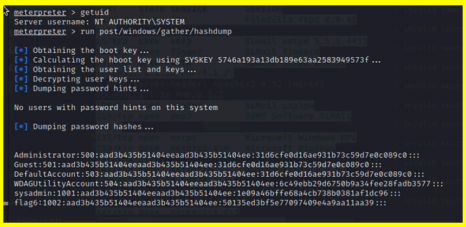
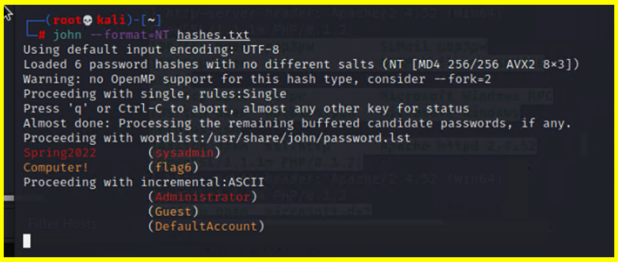
Vulnerability 5	**Findings**
Title	Command Injection
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	**Critical**
Description	Navigation allowed from /Networking.php to 192.168.14.35/disclaimer.php?page=vendors.txt via 192.168.14.35/networking.php Able to input "splunk" inside of toolbar intended for DNS Check
Images	

Affected Hosts	192.168.14.35
Remediation	Implement input validation unintended access

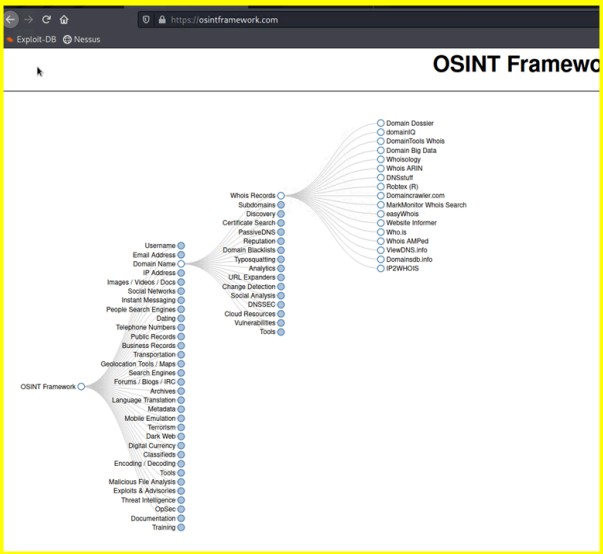
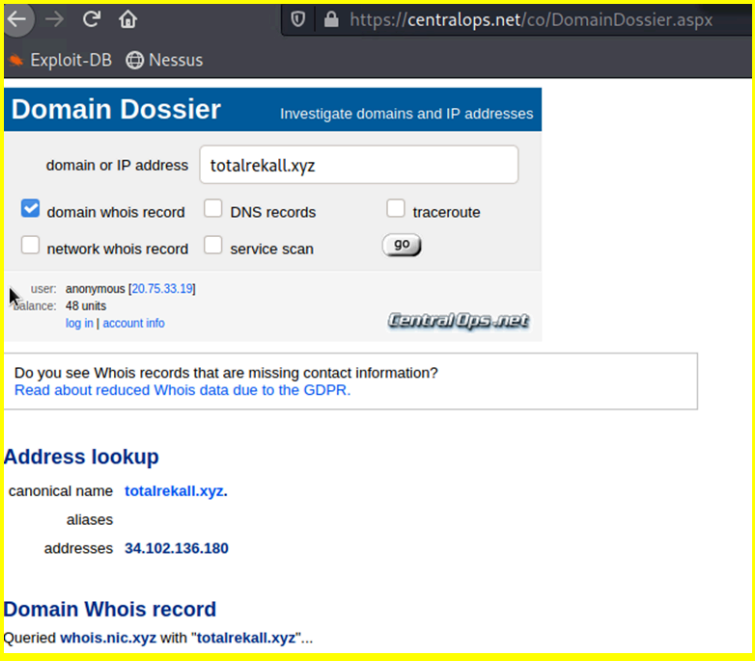
Vulnerability 6	Findings
Title	FTP Enumeration
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	**Critical**
Description	Open Port 21 allows for FTP enumeration through FTP connection on host IP which resulted in successful transfer and access/download of vulnerable files
Images	
Affected Hosts	172.22.117.20
Remediation	Restrict access to Port 21

Vulnerability 7	Findings
Title	SLMail Exploit
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	**Critical**
Description	Vulnerability in SLMail due to open port 110 was successfully exploited through use of windows/pop3/seattlelab_pass exploit within Metasploit which resulted in successful Meterpreter session

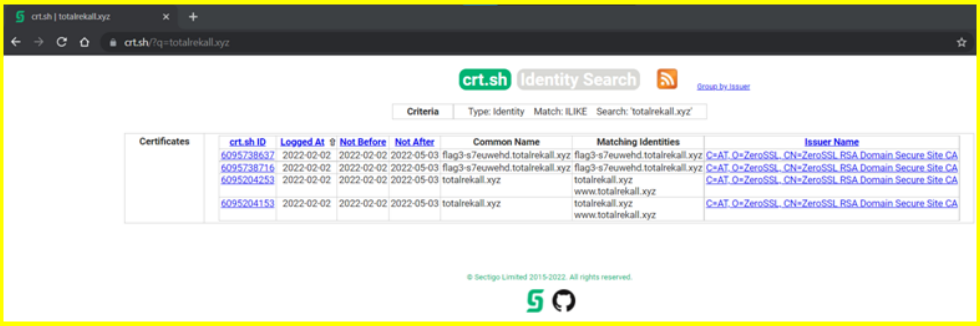
Images	 
Affected Hosts	172.22.117.20
Remediation	Restrict access to Port 110, disuse SLMai as it is outdated and vulnerable mail server software, making it a security risk. A better alternative would be a modern, secure, and actively maintained mail server

Vulnerability 8	Findings
Title	Sensitive Data/Credentials Dump
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	**Critical**
Description	Continued use of previous successful exploit via Metasploit/Meterpreter session; access to vulnerable passwords file obtained, followed by successful hash dump within post/windows/gather/hashdump. Passwords cracked using john, resulting in successful access to credentials and creation of a reverse shell.
Images	 

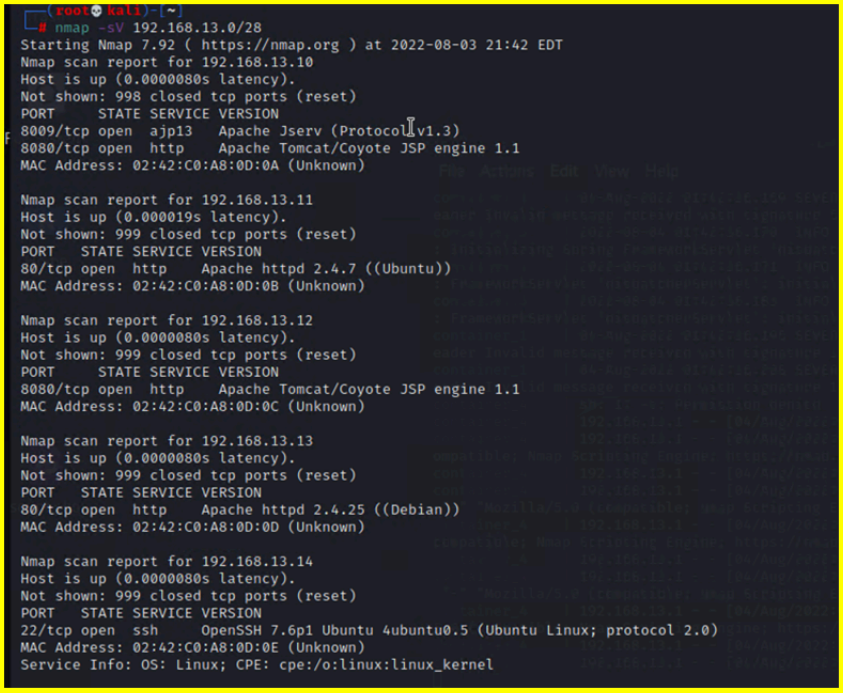
Affected Hosts	172.22.117.20
Remediation	Restrict access to vulnerable files by updating permissions on files and user permissions; move files to an non-public domain

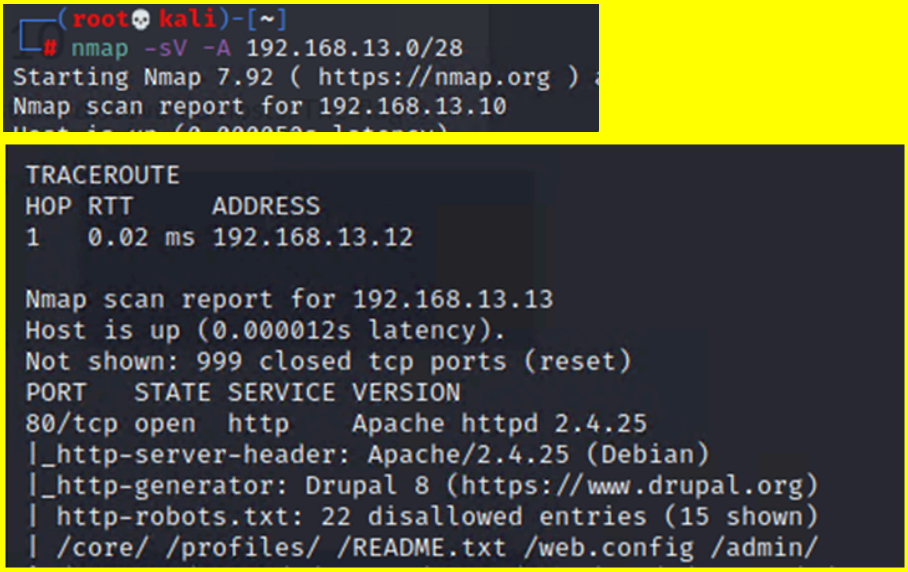
Vulnerability 9	**Findings**
Title	Open source exposed data
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	**Medium**
Description	On the Domain Dossier webpage, viewed the WHOIS data with OSINT for Total rekall.xyz to access sensitive information
Images	 

Affected Hosts	https://centralops.net/co/DomainDossier.aspx
Remediation	Ensure no sensitive data is being shared publicly, clean up WHOIS records

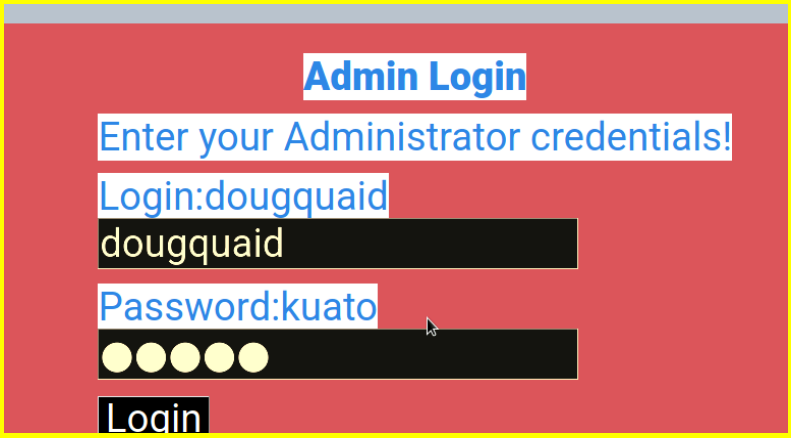
Vulnerability 10	**Findings**
Title	Certificate Search via crt.sh
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	**Medium**
Description	Searched for totalrekall.xyz on crt.sh, found stored certificate
Images	
Affected Hosts	34.102.136.180
Remediation	Protect information from being exposed by the crt.sh site

Vulnerability 11	**Findings**
Title	Nmap Scan Result
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	**Critical**
Description	An Nmap scan on 192.168.13.0/24 revealed 5 hosts are visible with exposed IP's

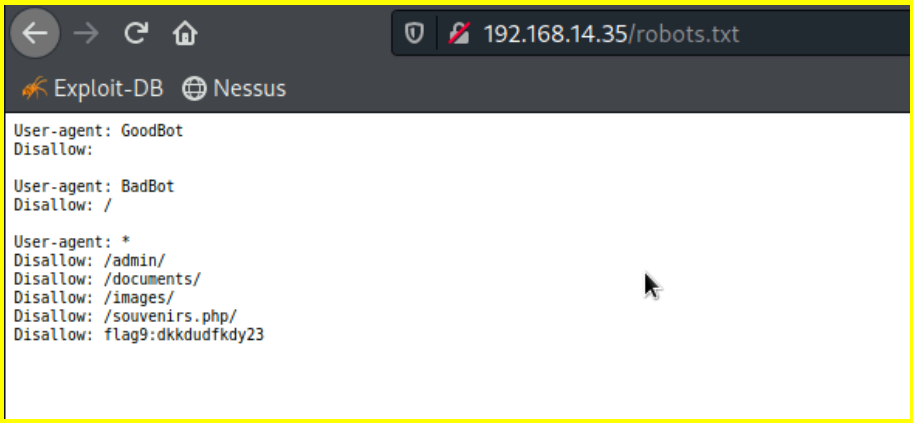
Images	
Affected Hosts	192.168.13.10, 192.168.13.11, 192.168.13.12, 192.168.13.13, 192.168.13.14
Remediation	Implement IP blocking for unauthorized users

Vulnerability 12	Findings
Title	Aggressive Nmap Scan
Type (Web app / Linux OS / Windows OS)	Linux
Risk Rating	**Critical**
Description	Ran aggressive Nmap scan (Nmap -A 192.168.13.0/28) to discover host running Drupal
Images	

Affected Hosts	192.178.13.12
Remediation	Block probes, restrict information returned, slow down the aggressive Nmap scan, and/or return misleading information

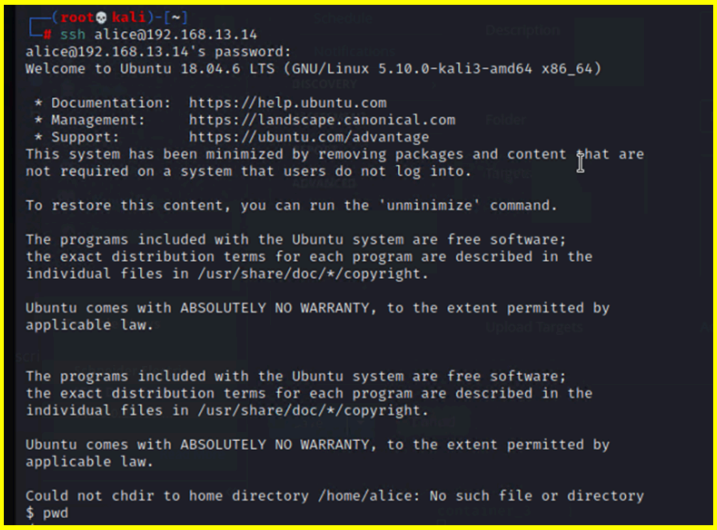
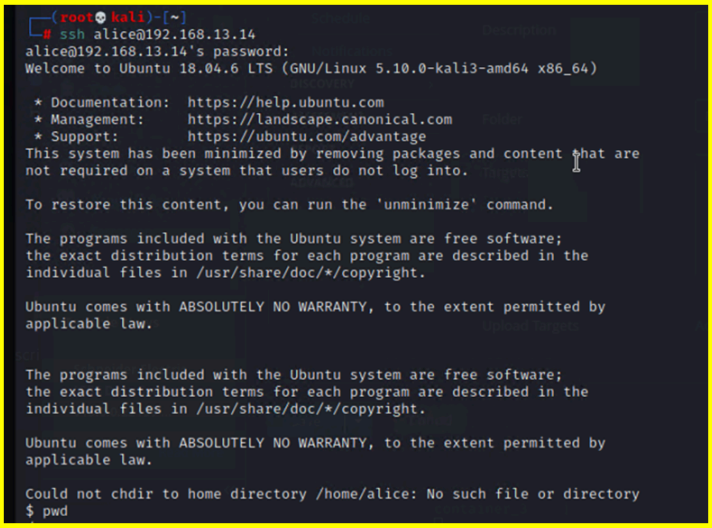
Vulnerability 13	Findings
Title	User Credentials Exposure
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	**Critical**
Description	User credentials are visible within HTML of the Login.php and when highlighting page in a web browser
Images	
Affected Hosts	192.168.14.35
Remediation	Delete this information from the HTML, implement 2-factor authentication for enhanced security

Vulnerability 14	Findings
Title	Sensitive Data Exposure
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	**Medium**
Description	Unrestricted access to robots.txt page

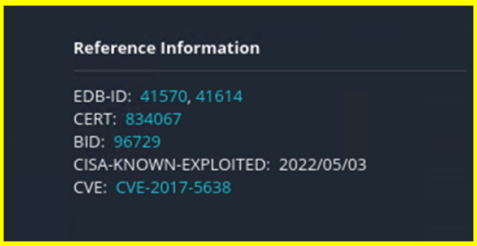
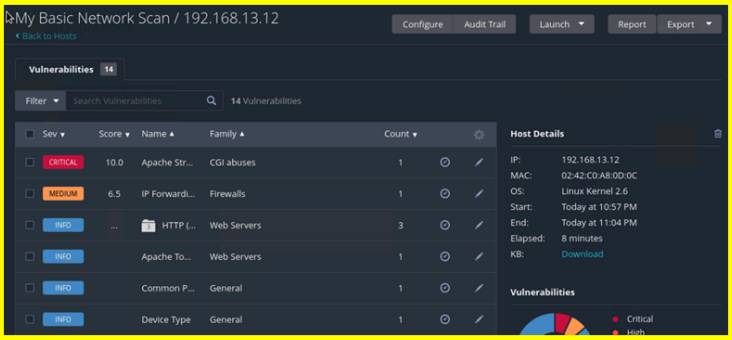
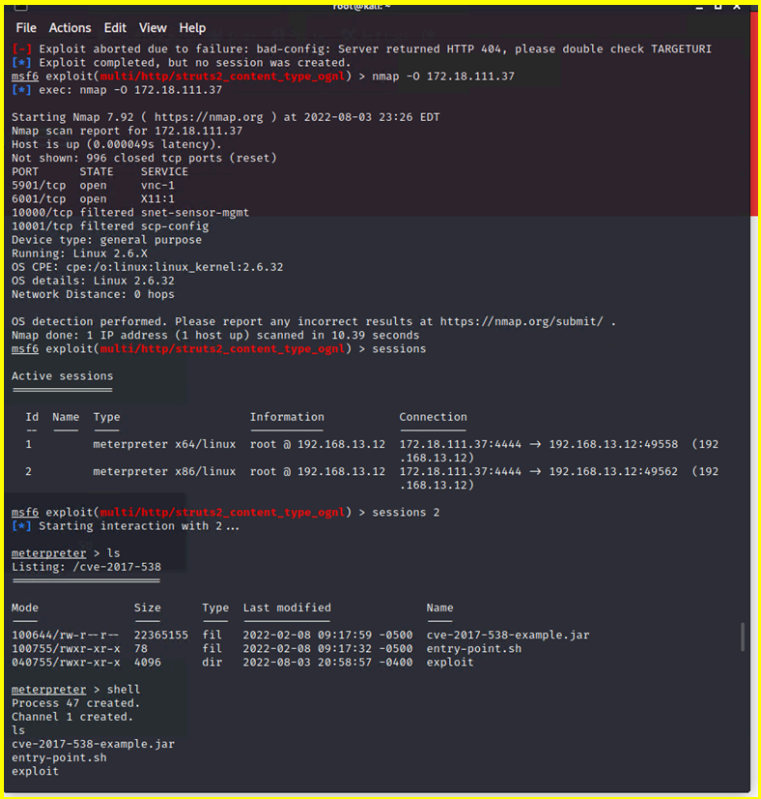
Images	
Affected Hosts	192.168.14.35
Remediation	Restrict access to robots.txt to authorized users

Vulnerability 15	Findings
Title	Nessus scan
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	**Medium**
Description	Nessus scan revealed Apache Struts vulnerability
Images	
Affected Hosts	192.168.13.12
Remediation	Perform regular updates on Apache

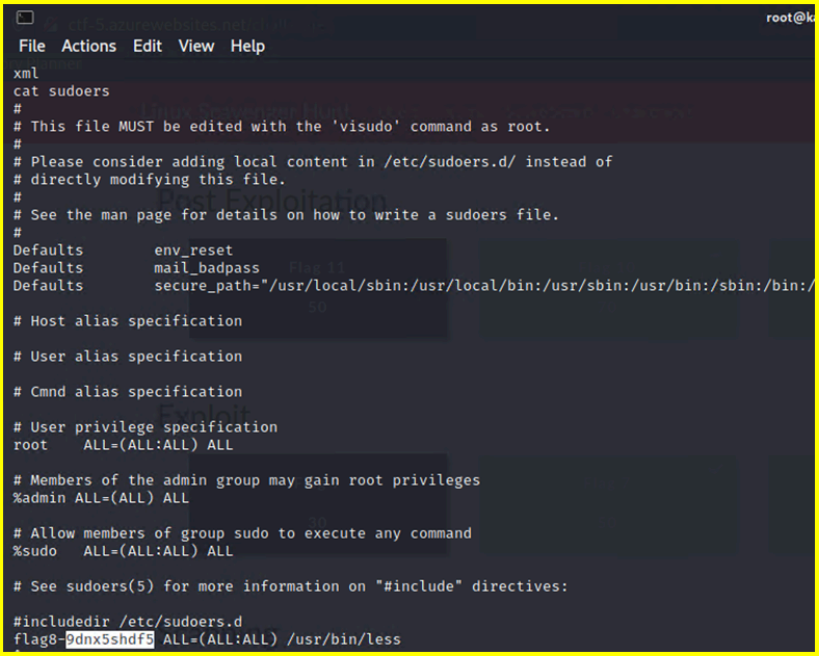
Vulnerability 16	Findings
Title	Privilege Escalation
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	**Critical**
Description	Able to escalate privileges via SSH from stolen credentials

Images	 
Affected Hosts	192.168.13.14
Remediation	Close port 22, enforce stronger credentials, and/or implement 2-factor authentication

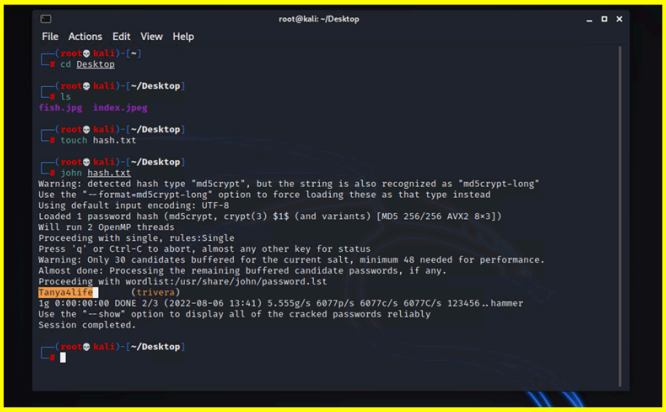
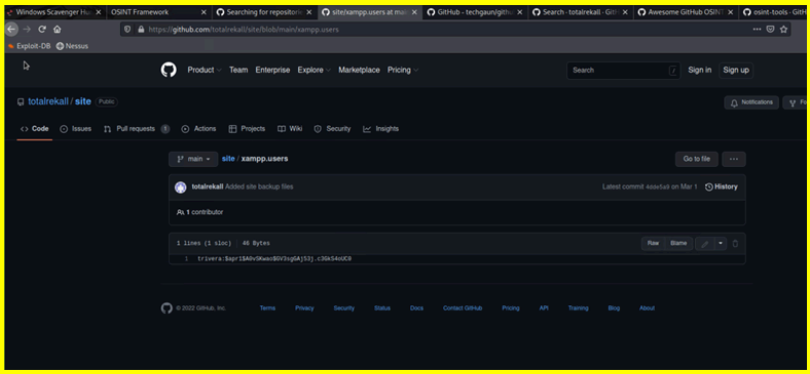
Vulnerability 17	Findings
Title	Meterpreter shell RCE execution (CVE 2017-5638)
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	**Critical**
Description	With Meterpreter, used multi/http/struts2_content_type_ognl exploit with PAYLOAD= linux/x86/shell_reverse_tcp

Images	  
Affected Hosts	192.168.13.12
Remediation	Apply updates per vendor instructions

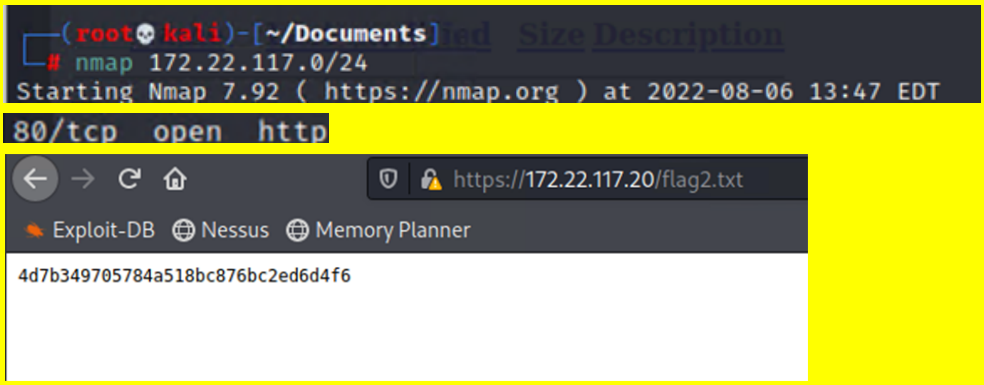
Vulnerability 18	Findings
Title	Shellshock on Web Server (Port 80)
Type (Web app / Linux OS / Windows OS)	Linux OS

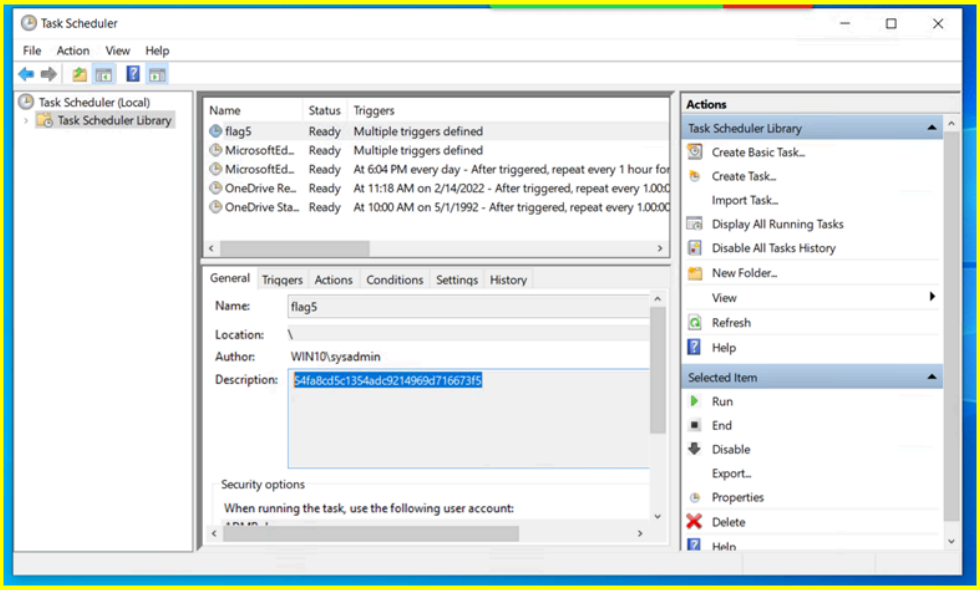
Risk Rating	**Critical**
Description	Used exploit (multi/http/apache_mod_cgi_bash_env_exec) set TARGETURI /cgi-bin/shockme.cgi shell Navigate to /etc/sudoers for root privileges file
Images	
Affected Hosts	192.168.13.14
Remediation	orarom ALL = ALL, !/bin/su

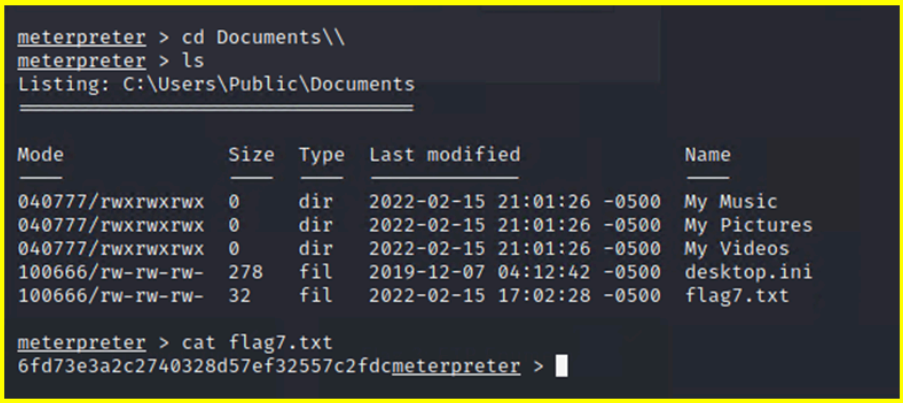
Vulnerability 19	Findings
Title	Username and Password Hash in Repo
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	**Critical**
Description	Using credentials found in Github repo, was able to crack password and gain access

Images	 
Affected Hosts	Total Rekall web server
Remediation	Restrict access and remove credentials from Github

Vulnerability 20	Findings
Title	Port Scon of Subnet
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	**Critical**
Description	Using credentials gained from Github repo to login, there was a single file there named flag2.txt containing the flag Method/Payload to Exploit: Nmap 172.22.117.0/24 172.22.117.20 has port 80 open Opened 172.22.117.20 in a web browser Provide credentials from Flag 1 (trivera Tanya4life) to log in File flag2.txt is located in root directory

Images	
Affected Hosts	172.22.117.20
Remediation	Require stronger credentials and or 2-factor authentication

Vulnerability 21	**Findings**
Title	Windows 10 Machine Task Scheduler
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	**Medium**
Description	Within the Windows 10 machine, able to view details of scheduled tasks
Images	
Affected Hosts	172.22.117.20
Remediation	Change permissions of accounts to restrict unauthorized access

Vulnerability 22	Findings
Title	Public Directory Search
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	**Medium**
Description	Navigating to the Users\Public\Documents directory, used the ls command in Meterpreter to display files
Images	
Affected Hosts	172.22.117.20
Remediation	Move sensitive files to more secure areas and/or restrict unauthorized access