Cybersecurity

Penetration Test Report

Rekall Corporation

Penetration Test Report

Dlock Consulting, LLC

Marty Di
Senior Security Analyst

Confidentiality Statement

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

Table of Contents

Contact Information

Company Name	Dlock Consulting, LLC
Contact Name	Marty Di
Contact Title	Senior Security Analyst

Document History

Version	Date	Author(s)	Comments
001	22.04.2023	Marty Di	
002	23.04.2023	Marty Di	
003	24.04.2023	Marty Di	
004	25.04.2023	Marty Di	
005	26.04.2023	Marty Di	

Introduction

In accordance with Rekall policies, our organization conducts external and internal penetration tests of its networks and systems throughout the year. The purpose of this engagement was to assess the networks' and systems' security and identify potential security flaws by utilizing industry-accepted testing methodology and best practices.

For the testing, we focused on the following:

- Attempting to determine what system-level vulnerabilities could be discovered and exploited with no prior knowledge of the environment or notification to administrators.
- Attempting to exploit vulnerabilities found and access confidential information that may be stored on systems.
- Documenting and reporting on all findings.

All tests took into consideration the actual business processes implemented by the systems and their potential threats; therefore, the results of this assessment reflect a realistic picture of the actual exposure levels to online hackers. This document contains the results of that assessment.

Assessment Objective

The primary goal of this assessment was to provide an analysis of security flaws present in Rekall's web applications, networks, and systems. This assessment was conducted to identify exploitable vulnerabilities and provide actionable recommendations on how to remediate the vulnerabilities to provide a greater level of security for the environment.

We used our proven vulnerability testing methodology to assess all relevant web applications, networks, and systems in scope.

Rekall has outlined the following objectives:

Table 1: Defined Objectives

Objective
Find and exfiltrate any sensitive information within the domain.
Escalate privileges.
Compromise several machines.

Penetration Testing Methodology

Reconnaissance

We begin assessments by checking for any passive (open source) data that may assist the assessors with their tasks. If internal, the assessment team will perform active recon using tools such as Nmap and Bloodhound.

Identification of Vulnerabilities and Services

We use custom, private, and public tools such as Metasploit, hashcat, and Nmap to gain perspective of the network security from a hacker's point of view. These methods provide Rekall with an understanding of the risks that threaten its information, and also the strengths and weaknesses of the current controls protecting those systems. The results were achieved by mapping the network architecture, identifying hosts and services, enumerating network and system-level vulnerabilities, attempting to discover unexpected hosts within the environment, and eliminating false positives that might have arisen from scanning.

Vulnerability Exploitation

Our normal process is to both manually test each identified vulnerability and use automated tools to exploit these issues. Exploitation of a vulnerability is defined as any action we perform that gives us unauthorized access to the system or the sensitive data.

Reporting

Once exploitation is completed and the assessors have completed their objectives, or have done everything possible within the allotted time, the assessment team writes the report, which is the final deliverable to the customer.

Scope

Prior to any assessment activities, Rekall and the assessment team will identify targeted systems with a defined range or list of network IP addresses. The assessment team will work directly with the Rekall POC to determine which network ranges are in-scope for the scheduled assessment.

It is Rekall's responsibility to ensure that IP addresses identified as in-scope are actually controlled by Rekall and are hosted in Rekall-owned facilities (i.e., are not hosted by an external organization). In-scope and excluded IP addresses and ranges are listed below.

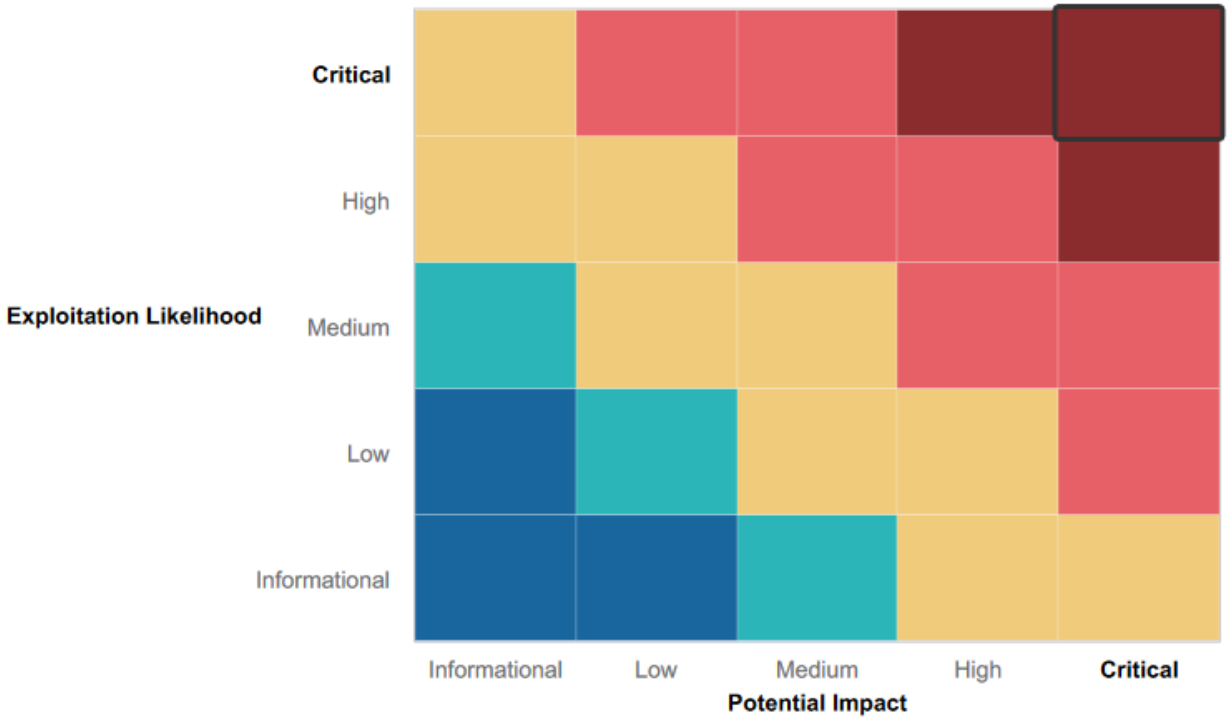
Executive Summary of Findings

Grading Methodology

Each finding was classified according to its severity, reflecting the risk each such vulnerability may pose to the business processes implemented by the application, based on the following criteria:

Critical: Immediate threat to key business processes.
High: Indirect threat to key business processes/threat to secondary business processes.
Medium: Indirect or partial threat to business processes.
Low: No direct threat exists; vulnerability may be leveraged with other vulnerabilities.
Informational: No threat; however, it is data that may be used in a future attack.

As the following grid shows, each threat is assessed in terms of both its potential impact on the business and the likelihood of exploitation:



Summary of Strengths

While the assessment team was successful in finding several vulnerabilities, the team also recognized several strengths within Rekall's environment. These positives highlight the effective countermeasures and defenses that successfully prevented, detected, or denied an attack technique or tactic from occurring.

- Some of the attempted exploits did not function as intended, suggesting that there are some security measures in place.
- Vulnerabilities in the system are mostly quick and inexpensive to resolve.
- Multiple platforms and segregated data pools add extra layers of defense against bad actors.

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.

- The web application is vulnerable to injection (XSS, command and SQL) as most of the user input fields are not sanitized and don't have validation configuration.
- Rekall is vulnerable from public exposure. Html, repositories and other public facing data has critical and sensitive information that makes exploitation likely.
- Multiple services throughout the systems are vulnerable to exploitation due to not being up to date.
- Permissions on multiple users are not appropriately set for the purpose of their use.
- No use of multifactor authentication for user accounts (even those with admin priv).
- Passwords and user credentials are weak and require stronger policies.
- Could not identify the use of an IPS or IDS on any of the platforms.

Executive Summary

Dlock Consulting was commissioned to perform a security assessment on Rekall Corporation's Network commencing on 13th of April and concluding on the 24th of April.
Dlock ran a penetration test to simulate an attack from a bad actor looking to gain administrative level access to Rekall's network.
The goal of this assessment was to discover vulnerabilities and weaknesses in Rekall's infrastructure and to provide recommendations to resolve the discovered exploits.

During this penetration test Dlock discovered vulnerabilities and were able to use these vulnerabilities to access the Rekall's web servers, as well as discover/access user credentials, escalate privileges to administrator level and maintain persistence on both the linux and windows servers.

In total Dlock discovered a total of 19 vulnerability categories across the web application, linux assets and windows assets, with 28 specific vulnerabilities, the largest quantity of these vulnerabilities (total of 8) being due to **public exposure** and **network enumeration**.

If just these 2 areas were remediated there would be a substantial increase in network security.

Over the duration of the penetration test Dlock focused on 3 attack surfaces:

- **The Rekall web application**
- **The Linux Assets**
- **The Windows Assets**

On each of these platforms we found critical vulnerabilities that should be considered a high priority and have immediate action taken.

Dlock commenced the assessment with the web application, where we initially found multiple XSS vulnerabilities on different pages.

As the evaluation continued it was discovered that the web application was also vulnerable to local file injection (LFI), specifically on the planner.php page, which could pose a serious threat if left unchecked.
One of the major concerns for the currently operating web application was discovered during the evaluation of html, in which both username and password credentials were found for the user dougquaid.

```
<p><label for="login">Login:</label><font color="#DB545A">dougquaid</font><br />
<input type="text" id="login" name="login" size="20" /></p>

<p><label for="password">Password:</label><font color="#DB545A">kuato</font><br />
<input type="password" id="password" name="password" size="20" /></p>
```

As we continued the evaluation of the web application we found that most user input fields had some kind of vulnerability, even including the url. This manifested in command injection, sql injection and session hijacking. Each one of these vulnerabilities led to subsequent exploits that entirely compromised the web app, and allowed Dlock to take control and extract data.

Dlock finalized its findings on the web application and moved onto the Linux assets.

To begin this process we began with network enumeration and scanning public data through a variety of means, including but not limited to;

- Nmap scans
- Domain dossier online tool
- crt.sh cert database
- Web browsing

Through these means alone Dlock was able to reveal multiple vulnerabilities, including open ports, ssh user credentials and vulnerable services that were run on the host machines.

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

Domain Name: totalrekall.xyz
Registry Domain ID: D273189417-CNIC
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: https://www.godaddy.com
Updated Date: 2023-02-03T14:04:18Z
Creation Date: 2022-02-02T19:16:16Z
Registrar Registration Expiration Date: 2024-02-02T23:59:59Z
Registrar: GoDaddy.com, LLC
Registrar IANA ID: 146
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: +1.4806242505
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Registry Registrant ID: CR534509109
Registrant Name: sshUser alice
```

Using the available credentials we were able to access the system. Furthermore, Dlock used an alternate method of gaining access in the form of a JSP exploit that targets the Tomcat platform to gain access, which worked successfully, providing Dlock with unauthorized access which we were able to use to change permissions and gain access to a method of achieving persistence.

Dlock moved on to the Windows assets next to assess its vulnerabilities and like the linux system, the first thing to check was whether there was publicly available information that would allow the Windows assets to be compromised. A repository on github.com was discovered which was publicly available, it included a username and a hash which using hash cracking tools was able to be decrypted. Immediately we had credentials to log in with.

```
1 lines (1 sloc)  46 Bytes
  1  trivera:$apr1$A0vSKwao$GV3sgGAj53j.c3GkS4oUC0
```

Through some basic nmapping we also discovered another pathway into the windows system via an anonymous username vulnerability. This allowed Dlock to ftp directly onto the Windows10 machine.

```
Nmap scan report for Windows10 (172.22.117.20)
Host is up (0.00083s latency).
Not shown: 990 closed tcp ports (reset)
PORT    STATE SERVICE       VERSION
21/tcp  open  ftp           FileZilla ftpd 0.9.41 beta
| ftp-syst:
|_  SYST: UNIX emulated by FileZilla
|_ftp-bounce: bounce working!
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
```

As we continued to assess vulnerabilities we discovered an exploitable service in SLMail, which we used to gain system level privileges on the Windows machine, which we then used to verify scheduled tasks, with the potential for adding a task that would provide us with persistence. Dlock used this access to perform an LSASS credential dump, which resulted in user names and NT hashes being made available for cracking.

In summary, all 3 platforms are vulnerable and have critical issues that require immediate attention, as these vulnerabilities threaten Rekall Corporation’s entire network and all of it’s sensitive data.

Summary Vulnerability Overview

Vulnerability	Severity	No of Vulns
Web Application		
1. XSS payload vulnerabilities on several pages (flag 1, 2, 3)	Critical	3
2. LFI inclusion vulnerability on the Memory Planner Page (flag 5, 6)	High	2
3. SQL injection vulnerability on the login.php page (flag 7)	High	1
4. HTML vulnerability - loose data on the login.php page (flag 8)	Critical	1
5. Robots.txt vulnerability - loose data / access (flag 9)	Critical	1
6. Public exposure vulnerability - vendors.txt viewability (flag 10)	High	1
7. Command injection vulnerability - DNS check field (flag 11) splunk vendors.txt	High	1
8. Password vulnerability (flag 12)	Critical	1
9. Session management vulnerability (flag 14)	Critical	1
10. Directory Traversal vulnerability (flag 15)	Critical	1
Linux		
11. Network enumeration / Public exposure (flag 1, 2, 3, 4, 5, 12)	Critical	6
12. JSP exploit vulnerability (flag 7)	Critical	1
13. Access Control - Permissions vulnerability (flag 8, 9)	High	2
Windows		
14. Public exposure vulnerability - Google Dorking (flag 1, 2)	Critical	1
15. Hash password vulnerability (flag 1, 2)	High	1
16. FTP access vulnerability (flag 3)	Critical	1
17. SLMail service vulnerability (flag 4)	Critical	1
18. SCHTASKS vulnerability (flag 5)	Medium	1
19. LSASS Dump vulnerability (flag 6)	Critical	1
Total Vulnerabilities		**28**

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

Web Application

Scan Type	Total
Hosts	192.168..14.35
Ports	80 3306

Exploitation Risk	Total
Critical	8
High	5
Medium	0
Low	0

Linux Assets

Scan Type	Total
Hosts	192.168.13.0/24 192.168.13.10 192.168.13.11 192.168.13.12 192.168.13.13 192.168.13.14
Ports	192.168.13.10 - 8009 192.168.13.10, 192.168.13.12 - 8080 192.168.13.12, 192.168.13.13 - 80 192.168.13.14 - 22

Exploitation Risk	Total
Critical	7
High	2
Medium	0
Low	0

Windows Assets

Scan Type	Total
Hosts	172.22.117.0/24 172.22.117.10 172.22.117.20
Ports	192.168.13.10 - 21 192.168.13.10 - 25 192.168.13.10 - 79 192.168.13.10 - 80 172.22.117.20 - 88 192.168.13.10 - 106 192.168.13.10 - 110 192.168.13.10, 172.22.117.20 - 135

	192.168.13.10, 172.22.117.20 - 139 172.22.117.20 - 389 192.168.13.10 - 443 192.168.13.10, 172.22.117.20 - 445 172.22.117.20 - 464 172.22.117.20 - 593 172.22.117.20 - 636

Exploitation Risk	Total
Critical	4
High	1
Medium	1
Low	0

Vulnerability Findings

Web Application Vulnerabilities

Vulnerability 1	Findings
Title	XSS payload vulnerabilities on several pages (flag 1, 2, 3)
Type (Web app / Linux OS / Windows OS)	Web Application
Risk Rating	Critical

Description	On Rekall's website there are XSS vulnerabilities on the:
	- '/Welcome.php' page in the:
	  - Comments input field - Stored XSS
	  - Name input field - Reflected XSS
	- '/Memory-planner.php' planner page in the choose your character input field - Reflected XSS
	The above listed pages/fields did not properly sanitize user inputs which enabled a variety of XSS payloads to effectively be used and resulted in unauthorized access.

Images	Refer to figures: - 1.1 - 1.2 - 1.3 - 1.4 in the Appendix
Affected Hosts	192.168.14.35
Remediation	- Implement sanitisation lists to prevent reflected or stored XSS. - Encoding the output data would make the extracted data less

	functional. - Devs should use strict mode when building or working on the site to prevent errors. - Use appropriate response headers, specifically 'content-type' headers to ensure that they can't be hijacked for other purposes.

Vulnerability 2	Findings
Title	LFI inclusion vulnerability on the Memory Planner Page (flag 5, 6)
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	**High**
Description	The '/Memory-Planner.php page there is a feature to upload an image which can be exploited to upload a .php script. Ultimately this provides the bad actor a method of running server-side malicious code. This was tested by uploading a non-malicious php cmd script which successfully discovered this vulnerability. The only countermeasure was that the upload field was looking for a .jpeg or similar image file, which is easily subverted.
Images	Refer to figures: - 1.5 - 1.6 in the Appendix
Affected Hosts	192.168.14.35
Remediation	- Saving the files to a secure database instead of the web server would prevent scripts from being run server side. - Assign saved files an id and a set directory, where only the id is available to the user, this would assist with preventing directory traversal.

Vulnerability 3	Findings
Title	SQL injection vulnerability on the login.php page (flag 7)
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	**High**
Description	The /Login.php page was discovered to be vulnerable to SQL injection. This was tested by using the login and password input fields to run a sql

	database query as shown in figure 1.7. note: the image shows the query used in the login field, however it was actually used in the password field and this is just to illustrate the actual query used.
Images	Refer to figures: - 1.7 in the Appendix
Affected Hosts	192.168.14.35
Remediation	- Use prepared statements with variable binding in the Rekall databases. This ensures the input fields distinguished between what is data and what is code and prevents an attacker from being able to hijack the intent of the query. - Avoid the use of dynamic SQL - Allow-list Input validation - construct a robust white and black list set of inputs to prevent exploitative use.

Vulnerability 4	Findings
Title	HTML vulnerability - loose data on the login.php page (flag 8)
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	**Critical**
Description	When looking through the html on the `/Login.php' page sensitive data was found to be exposed in the form of a username and password, as can be seen on figure 1.8 in the appendix.
Images	Refer to figures: - 1.8 - 1.9 in the Appendix
Affected Hosts	192.168.14.35
Remediation	Remediation is simple: - Encrypt all sensitive data and use private keys to extract - Regularly scan your site for keyword sensitivity - Regular website maintenance to clean up any unessential information

Vulnerability 5	Findings
Title	Robots.txt vulnerability - loose data / access (flag 9)

Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	**Critical**
Description	During our evaluation of the ‘robots.txt’ subdomain we discovered sensitive information was being stored there in addition to old website data that could create an attack surface for bad actors. This included the ‘/souvenirs.php’ page which was later used for subsequent exploitation.
Images	Refer to figures: - 1.10 in the Appendix
Affected Hosts	192.168.14.35
Remediation	- Regular website maintenance and scans would resolve this issue - If additional steps are required the implementation of a `disallow` honeypot may result in bad actors being black listed.

Vulnerability 6	**Findings**
Title	Public exposure vulnerability - vendors.txt viewability (flag 10)
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	**High**
Description	As can be seen on figure 1.11 in the appendix, the ‘networking.php’ page revealed there was sensitive data in ‘vendors.txt’. Using this we searched through the ‘/vendors.txt’ which revealed other sensitive information, such as the use of splunk, which was then used in the DNS lookup to gather additional information as shown in figure 1.11 in the appendix.
Images	Refer to figures: - 1.11 in the Appendix
Affected Hosts	192.168.14.35
Remediation	- Ensure that sensitive data is not displayed on publicly available pages

Vulnerability 7	**Findings**
Title	Command injection vulnerability - DNS check field (flag 11) splunk vendors.txt

Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	**High**
Description	The information gathered from vulnerability 6 listed above was used to discover another vulnerability. Using the vendors.txt information we targeted the MX Records lookup field and applied command injection to exploit the input field and gather additional data.
Images	Refer to figures: - 1.12 in the Appendix
Affected Hosts	192.168.14.35
Remediation	- Don't allow system commands from user input - Use stronger input validation - white list and black list syntax - Provide the minimum amount of privilege required for this field to operate as needed. - Ensure all applications are running the most up to date software/patches.

Vulnerability 8	**Findings**
Title	Password vulnerability (flag 12)
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	**Critical**
Description	Using the previous command injection exploit we were able to discover some of the user names of account holders shown in figure 1.13. Using this we navigated to the '/Login.php' page to attempt to guess some typical login credentials. The Melina user account gave us what we needed with a typical password that was actually just the username again. This was a significant step up in privilege as the Melina user accounts UID was 1000 and therefore has additional privileges. Even with the command injection revealing user account information if there had been complex passwords we may not have got this access.
Images	Refer to figures: - 1.13 - 1.14 - 1.15 in the Appendix
Affected Hosts	192.168.14.35

Remediation	- Implement stricter password policies that are more in line with industry standards.
	  - 3 wrong guessed lock the account and require an admin to reset
	  - a successfully login resets the count on the incorrect login attempts
	  - 30 minutes of no log in attempts resets the count on the incorrect login attempts
	  - no less than 8 characters, includes at least one capital, one lowercase, one number and one symbol.
	  - cannot be similar typical or previously used passwords
	  - cannot be the same or similar to the user name

Vulnerability 9	Findings
Title	Session management vulnerability (flag 14)
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	**Critical**
Description	After successfully logging in as Melina, we followed the navigation to a secured page that required administrative level access. Dlock tested the session management by intercepting the traffic using burpsuite and relayed that through the intruder function within the burpsuite application. This let us test the session ids with potentially thousands of variations. As the screenshots will show you a variation was discovered occurring from session 87 and so we modified it on the page to reveal that we now had the access we were aiming for. This vulnerability exposes potentially highly sensitive information and could also give privileges to unauthorized users.
Images	Refer to figures: - 1.16 - 1.17 - 1.18 in the Appendix
Affected Hosts	192.168.14.35
Remediation	- update the web server frame work to current/modern standards to prevent predictable identifier tokens. - Use HTTPS to transfer identifier tokens - Set a short lifespan on the identifier token - terminate the session when the user logs out - Use entropy based ids for sessions

Vulnerability 10	Findings
Title	Directory Traversal vulnerability (flag 15)
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	**Critical**
Description	On the `/disclaimer.php` page Dlock were able to use directory traversal by adding "../../../../../" after the "?page=" in the url. This let us navigate the web servers directory and gave us unauthorized access to key information such as users and groups. See figure 1.20.
Images	Refer to figures: - 1.19 - 1.20 - 1.21 in the Appendix
Affected Hosts	192.168.14.35
Remediation	- Input validation - specify acceptable inputs, black list known malicious inputs. - Prevent user supplied input from validating with web servers unless its an approved input.

Linux Vulnerabilities

Vulnerability 11	Findings
Title	Network enumeration / Public exposure (flag 1, 2, 3, 4, 5, 12)
Type (Web app / Linux OS / WIndows OS)	Linux
Risk Rating	**Critical**
Description	There were a total of 7 specific vulnerabilities that came under the vulnerability category of public exposure / network enumeration for the linux assets. When using 'domain dossier' we gained access to a large portfolio of information including data on open ports, ip addresses, protocols and services. Additionally, this also included the ssh user credentials as shown in figure 2.5 in the appendix. Dlock then moved on to using crt.sh which provided us with information on the certificates used by by totalrekall.xyz. Then we ran an `nmap` to further dig into rekall's network details and discover the host ip addresses. Dlock then moved onto more specific nmap searches to discover if any of the hosts were running services vulnerable to exploit, which we found on 192.168.13.13, which was running drupal.
Images	Refer to figures: - 2.1 - 2.2 - 2.3 - 2.4 - 2.5 in the Appendix
Affected Hosts	192.168.13.10 192.168.13.11 192.168.13.12 192.168.13.13 192.168.13.14
Remediation	- To address exposure of ports, configure your ICMP to only respond if it is coming from an internal or trusted source. - Configure firewall to drop ICMP requests - Configure firewall to treat requests from unknown sources as potential threats - Regularly update your information, credentials and services so that any publicly available information is out of date and ineffective.

Vulnerability 12	Findings
Title	JSP exploit vulnerability (flag 7)
Type (Web app / Linux OS / WIndows OS)	Linux
Risk Rating	**Critical**
Description	Using an tomcat_jsp RCE exploit in metasploit Dlock were able gain access to 192.168.13.10. From here Dlock had unauthorized privileges and access to sensitive files that if desired we could have exfiltrated.
Images	Refer to figures: - 2.6 - 2.7 - 2.8 in the Appendix
Affected Hosts	192.168.13.10
Remediation	- This is a known vulnerability (CVE-2019-0232) and has been patched - recommend immediate update of Apache Tomcat to the latest version

Vulnerability 13	Findings
Title	Access Control - Permissions vulnerability (flag 8, 9)
Type (Web app / Linux OS / WIndows OS)	Linux
Risk Rating	**High**
Description	There is an issue with the access control of the www-data account being able to manipulate the sudoers file, which led to permanent adjustments to privileges and account control.
Images	Refer to figures: - 2.9 - 2.10 in the Appendix
Affected Hosts	192.168.13.11
Remediation	- Implement policy of user accounts only having access for essential

	functions - policy of least privilege. This would prevent all but the necessary accounts from having access to integral files such as sudoers.

Windows Vulnerabilities

Vulnerability 14	Findings
Title	Public exposure vulnerability, Google Dorking (flag 1, 2)
Type (Web app / Linux OS / WIndows OS)	Windows
Risk Rating	**Critical**
Description	As we moved focus on to the windows assets, we checked through Google dorking whether there were any online repositories with neglected information that might assist us with penetrating the Rekall network. Through this method Dlock found a left over repository on github.com owned by totalrekall which included a username and a hash. Dlock used 'John the Ripper', a well known hash cracking tool, to decrypt the hash. These credentials were then used to log in and exfiltrate data.
Images	Refer to figures: - 3.1 - 3.3 in the Appendix
Affected Hosts	172.22.117.20
Remediation	- Change credentials routinely so that exposed information such as the git repository does not pose a significant threat. - avoid exposing any passwords, usernames or credentials to the publicly available internet, even if it is hashed or encrypted.

Vulnerability 15	Findings
Title	Hash password vulnerability (flag 1, 2)
Type (Web app / Linux OS / WIndows OS)	Windows
Risk Rating	**High**
Description	Dlock were able to use 'John' , a well known hash cracking tool, to decrypt the hash discovered in the repository found on github.com.
Images	Refer to figures: - 3.2 in the Appendix

Affected Hosts	172.22.117.20
Remediation	- More complex passwords could reduce the likelihood it being cracked and would increase the time taken to crack. Passwords that are less logical and that are formulated with more entropy would be more resilient.

Vulnerability 16	**Findings**
Title	FTP access vulnerability (flag 3)
Type (Web app / Linux OS / WIndows OS)	Windows
Risk Rating	**Critical**
Description	An FTP vulnerability was made apparent through a basic nmap scan, as shown in figure 3.4 the scan reveals that Anonymous can be used to ftp into the machine. This allowed unauthenticated and unauthorized access
Images	Refer to figures: - 3.4 - 3.5 in the Appendix
Affected Hosts	172.22.117.20
Remediation	- Adjust the security parameters for FTP to only allow authenticated and authorized users.

Vulnerability 17	**Findings**
Title	SLMail service vulnerability (flag 4)
Type (Web app / Linux OS / WIndows OS)	Windows
Risk Rating	**Critical**
Description	There exists a known exploit in metasploit to utilize the SLMail service to gain System level access to the machine through manipulating the buffer overflow.
Images	Refer to figures: - 3.6

	- 3.7 in the Appendix
Affected Hosts	172.22.117.20
Remediation	- Review whether there is an alternative to using SLMail service - Update to the latest version - SLMail does not require a system level account, downgrade to a low privilege account.

Vulnerability 18	**Findings**
Title	SCHTASKS vulnerability (flag 5)
Type (Web app / Linux OS / WIndows OS)	Windows
Risk Rating	**Medium**
Description	After acquiring system level access Dlock checked the user privileges to create and manage scheduled tasks through 'SCHTASKS'. Dlock was able to create and manage tasks, even to the point of being able to set up a script that allowed for remote access.
Images	Refer to figures: - 3.8 in the Appendix
Affected Hosts	172.22.117.20
Remediation	- Perform regular SCHTASK scans to discover any suspicious tasks, primarily when and what they run.

Vulnerability 19	**Findings**
Title	LSASS Dump vulnerability (flag 6)
Type (Web app / Linux OS / WIndows OS)	Windows
Risk Rating	**Critical**
Description	Dlock conducted an LSASS dump on the Windows 10 machine to exfiltrate credentials. This successfully provided an NT formatted hash which once again was cracked by using the 'John' tool.

Images	Refer to figures: - 3.9 - 3.10 in the Appendix
Affected Hosts	172.22.117.20
Remediation	- Enable protected mode - only other protected mode processes can run LSASS - Accelerate LSASS Memory Wipe - Run a credential guard manager - Limit cred caching

MITRE ATT&CK Navigator Map

The below MITRE ATT&CK map outlines the different tools, tactics and techniques that Dlock Consulting used during its network assessment (penetration test) of Rekall Corporation.

Legend:

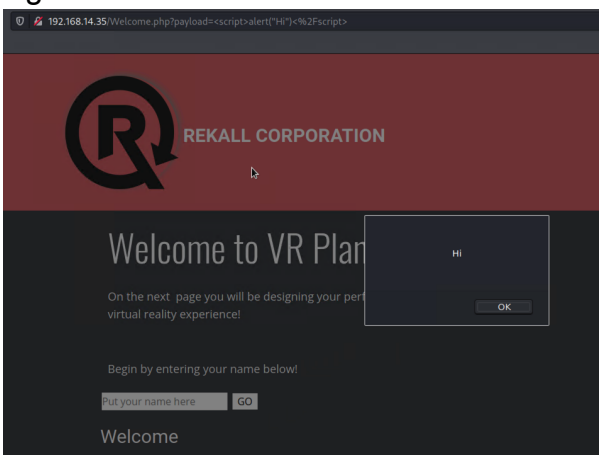
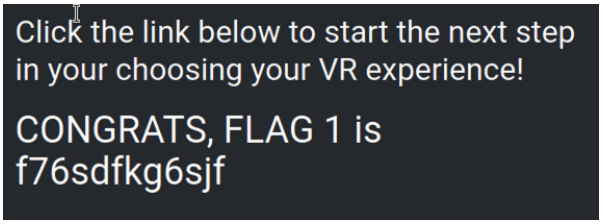
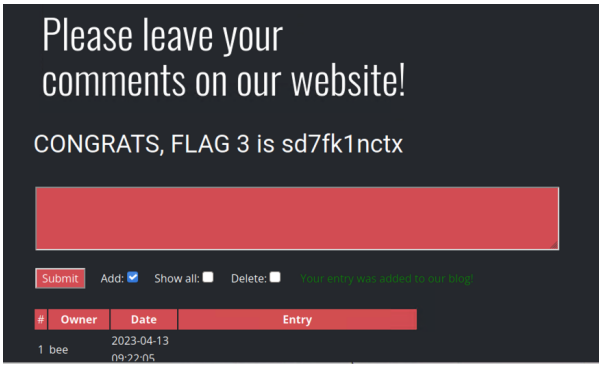
- Performed
- Not performed

Json link - https://drive.google.com/file/d/1T0CG8wjr9-DhEIEoLh6hhFmCC1Hbztbb/view?usp=share_link

Excel link - https://docs.google.com/spreadsheets/d/1N0lSvcIeSeRO1OWKhfBnHhfNhxzPoEWb/edit?usp=share_link&ouid=102975770986536585299&rtpof=true&sd=true

Appendix

Web Application

Flags 1, 2, 3 - XSS	Figure 1.1  Figure 1.2  Figure 1.3  Figure 1.4 
Flags 5, 6 - LFI	Figure 1.5

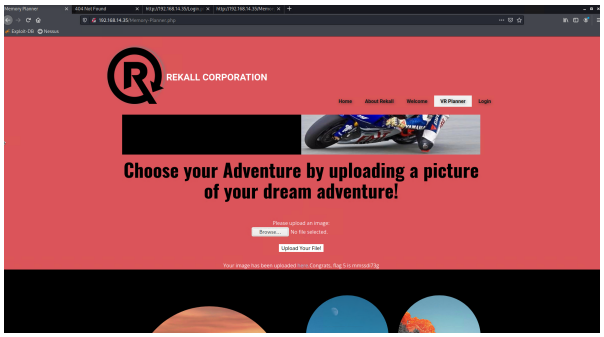
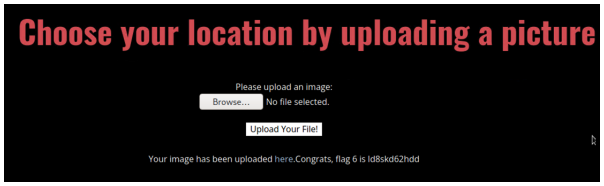
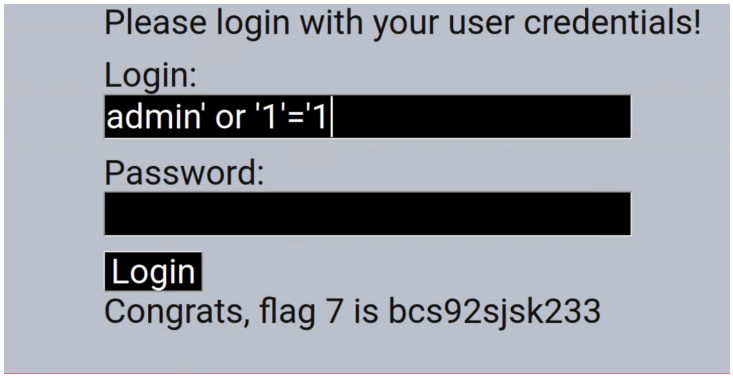


Figure 1.6



Flag 7 - SQL

Figure 1.7

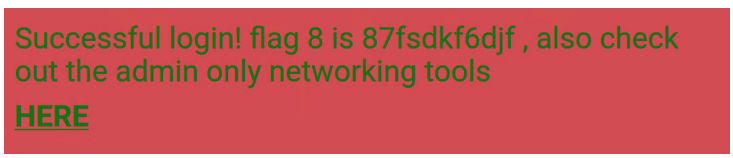


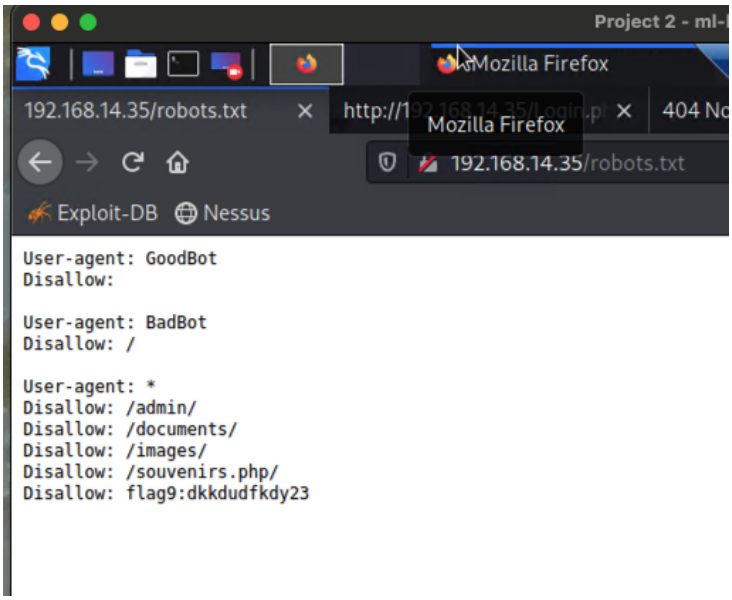
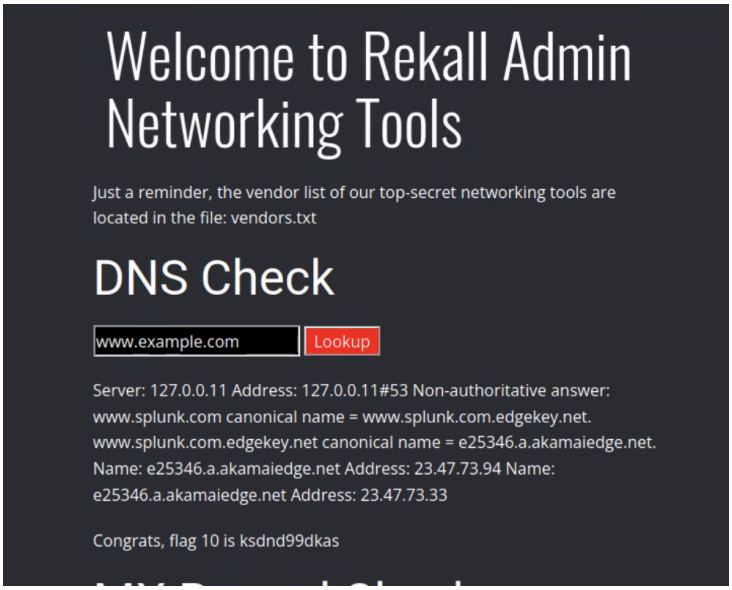
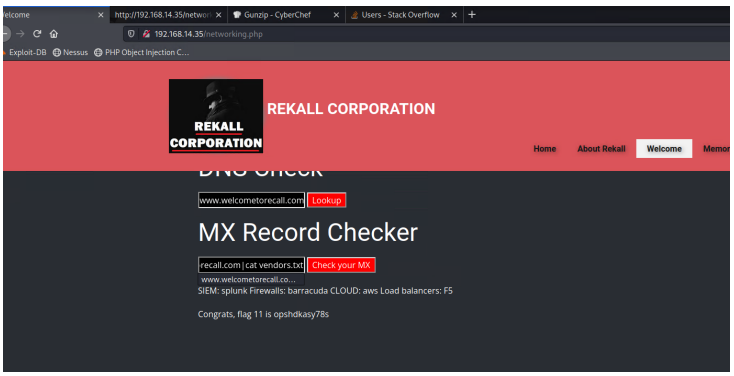
Flag 8 - HTML

Figure 1.8

```
color: white;
}
</style>
    <form action="/Login.php" method="POST">
        <p><label for="login">Login:</label><font color="#DB545A">dougquaid</font><br />
        <input type="text" id="login" name="login" size="20" /></p>
        <p><label for="password">Password:</label><font color="#DB545A">kuato</font><br />
        <input type="password" id="password" name="password" size="20" /></p>
        <button type="submit" name="form" value="submit" background-color="black">Login</button>
    </form>
    </br >
</div>
```

Figure 1.9



Flag 9 - ‘robots.txt’	Figure 1.10 
Flag 10 - Public Exposure	Figure 1.11 
Flag 11 - Command Injection	Figure 1.12 

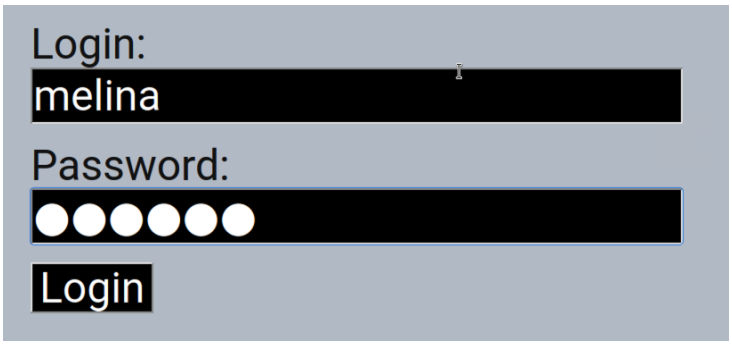
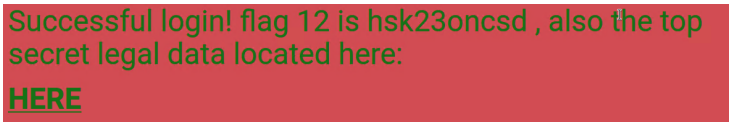
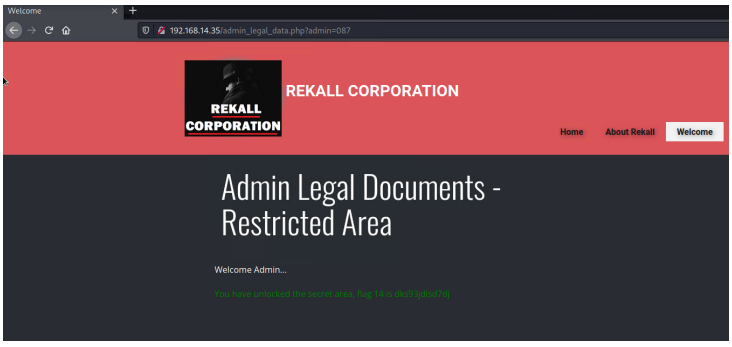
Flag 12 - Weak Password Policy	Figure 1.13  Figure 1.14  Figure 1.15 
Flag 14 - Session Management	Figure 1.16 

Figure 1.17

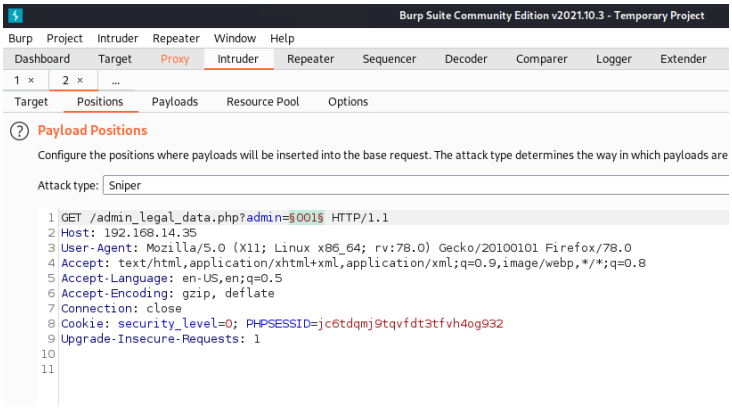
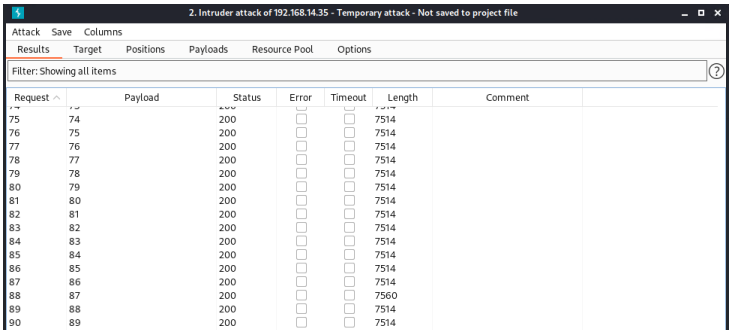


Figure 1.18



Flag 15 - Directory Traversal

Figure 1.19

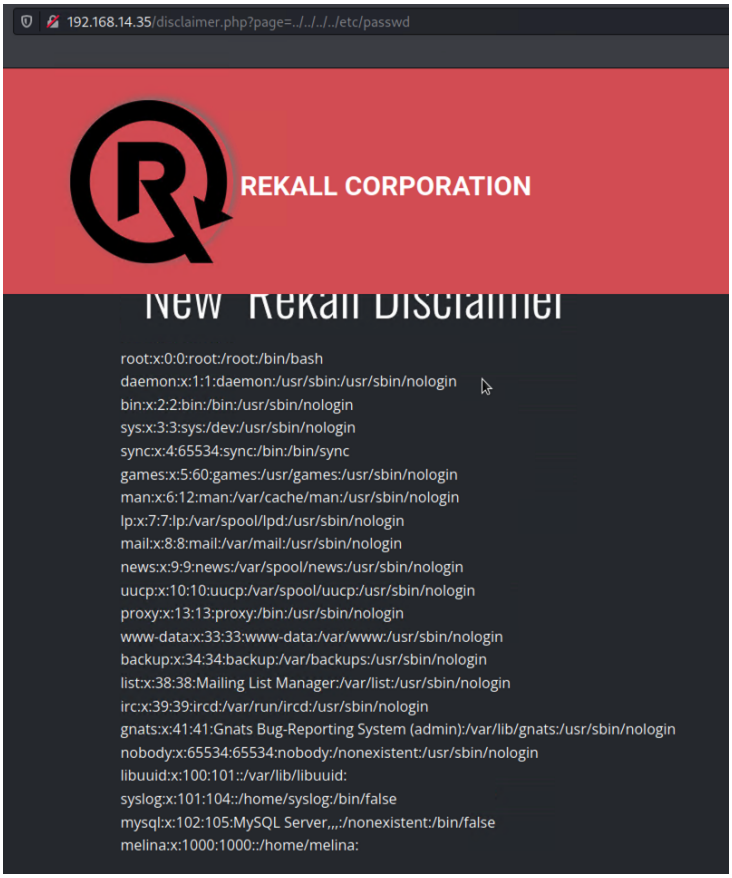
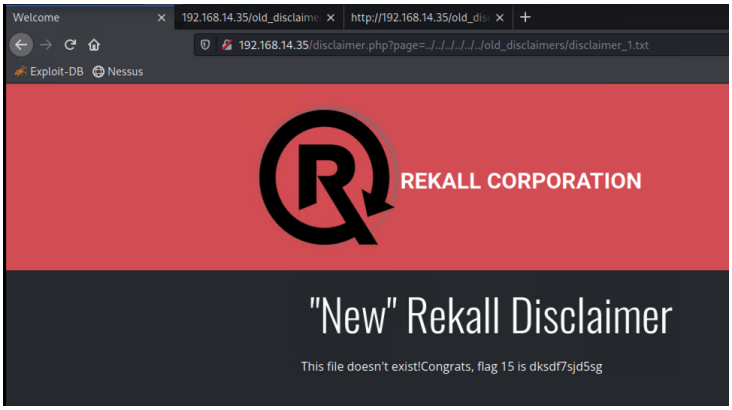


	Figure 1.20  Figure 1.21 
Linux	
Flags 1, 2, 3, 4, 5, 12	Figure 2.1

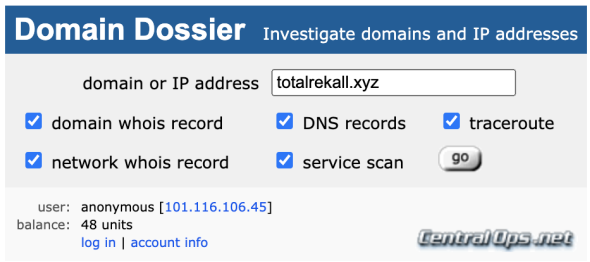


Figure 2.2

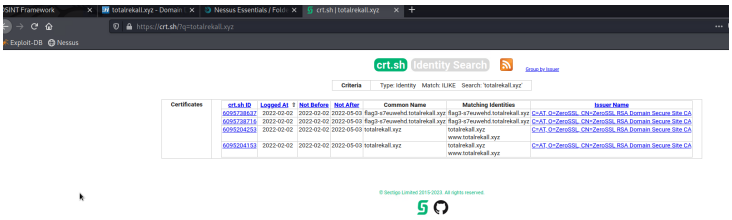


Figure 2.3

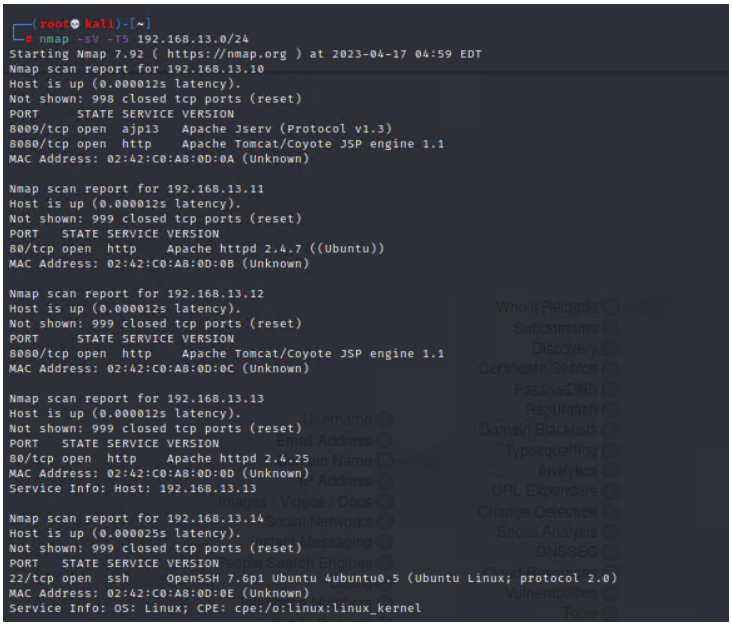


Figure 2.4

```
┌──(root💀kali)-[~]
└─# sudo nmap -Pn -T5 -A -O 192.168.13.13
Starting Nmap 7.92 ( https://nmap.org ) at 2023-04-17 05:03 EDT
Nmap scan report for 192.168.13.13
Host is up (0.000074s 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   0.07 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 20.91 seconds
```

Figure 2.5

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

Domain Name: totalrekall.xyz
Registry Domain ID: D273189417-CNIC
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: https://www.godaddy.com
Updated Date: 2023-02-03T14:04:18Z
Creation Date: 2022-02-02T19:16:16Z
Registrar Registration Expiration Date: 2024-02-02T23:59:59Z
Registrar: GoDaddy.com, LLC
Registrar IANA ID: 146
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: +1.4806242505
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Registry Registrant ID: CR534509109
Registrant Name: sshUser alice
Registrant Organization:
Registrant Street: h8s692hskasd Flag1
Registrant City: Atlanta
Registrant State/Province: Georgia
Registrant Postal Code: 30309
Registrant Country: US
Registrant Phone: +1.7702229999
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=totalrekall.xyz
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: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=totalrekall.xyz
Registry Tech ID: CR534509110
Tech Name: sshUser alice
Tech Organization:
Tech Street: h8s692hskasd Flag1
Tech City: Atlanta
```

Flag 7

Figure 2.6

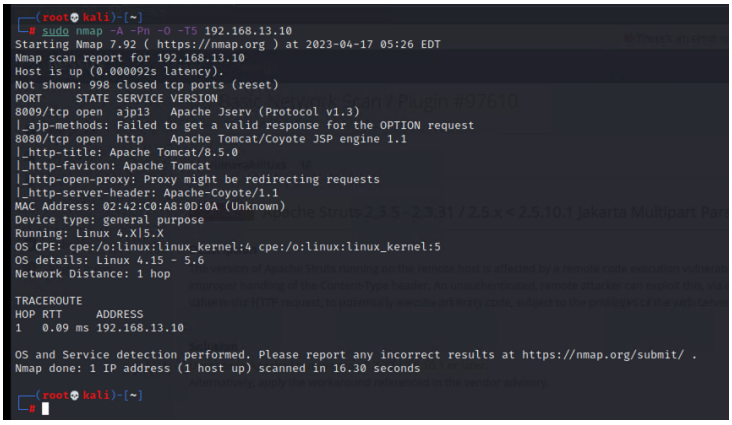


Figure 2.7

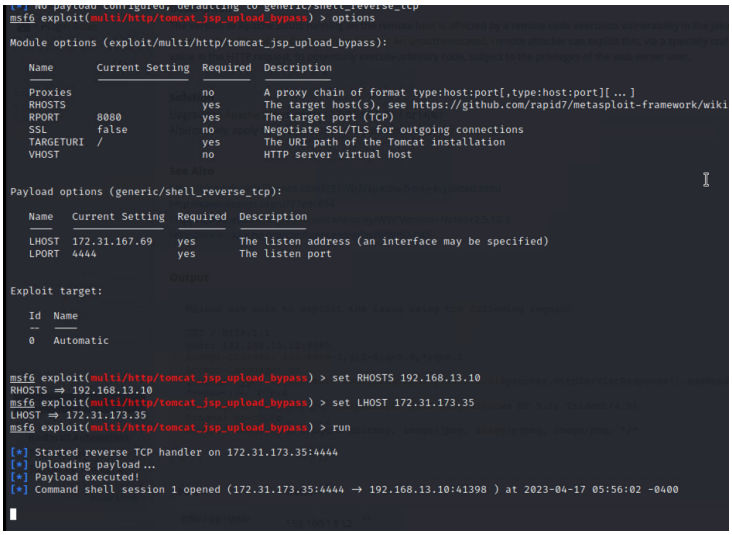
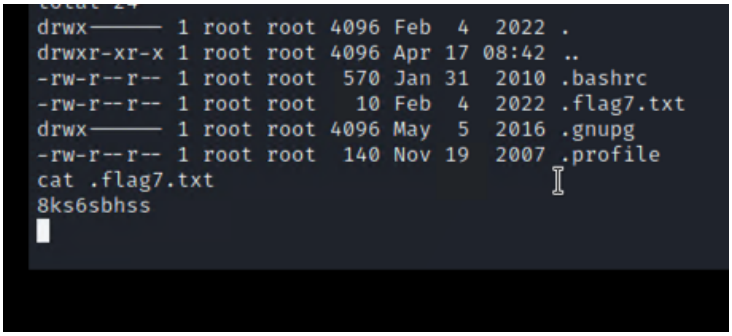
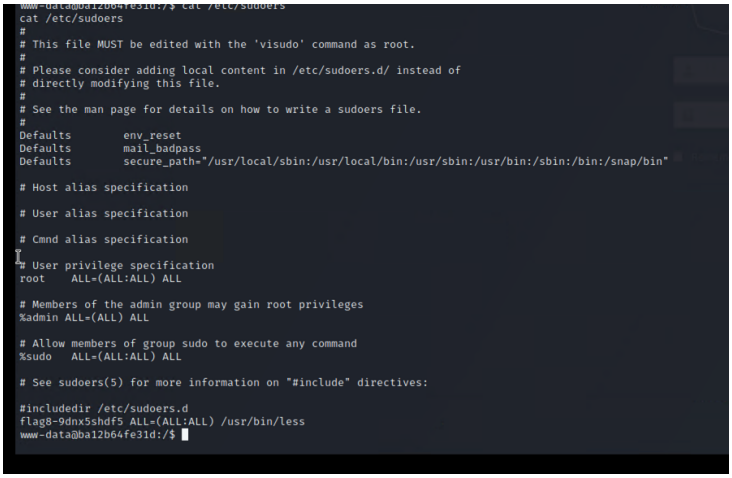
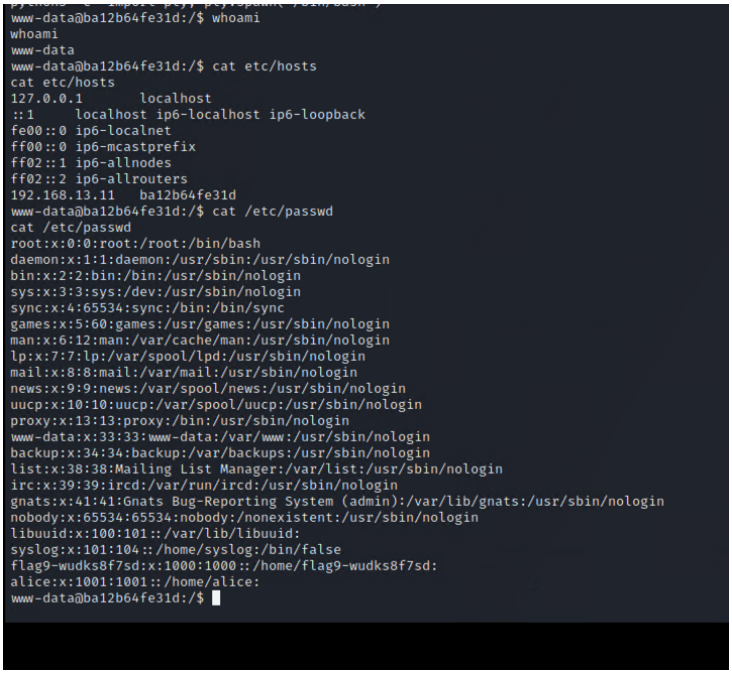
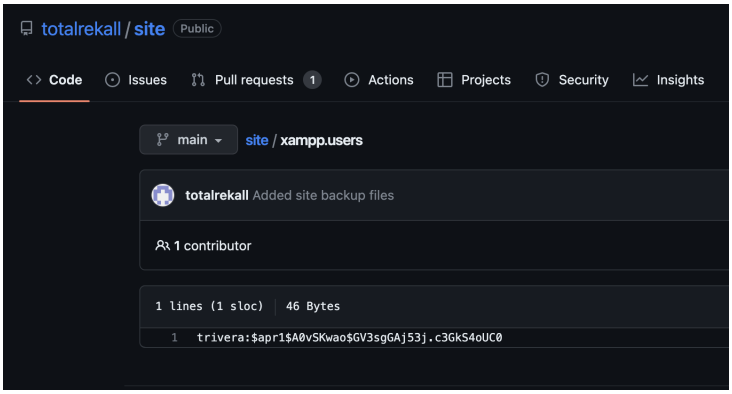


Figure 2.8



Flag 8 - Access Control	Figure 2.9  Figure 2.10 

Windows

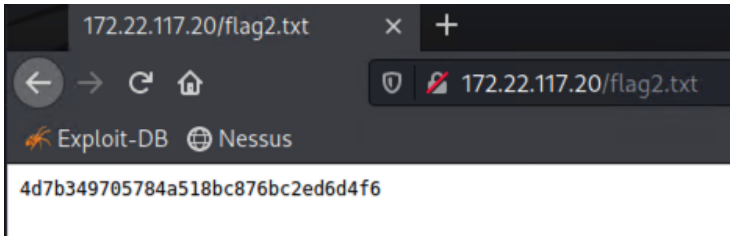
Flag 1, 2 - Public Exposure - Google Dorking	Figure 3.1  Figure 3.2

```
File  Actions  Edit  View  Help
root@kali: ~ ×   root@kali: ~ ×
┌──(root㉿kali)-[~]
└─# nano hash.txt

┌──(root㉿kali)-[~]
└─# john hash.txt
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ (and variants) [MD5 256/256 AVX2 8×3])
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 30 candidates buffered for the current salt, minimum 48 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Tanya4life       (trivera)
1g 0:00:00:00 DONE 2/3 (2023-04-18 05:12) 6.250g/s 6837p/s 6837c/s 6837C/s 123456..hammer
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

┌──(root㉿kali)-[~]
└─#
```

Figure 3.3



Flag 3 - FTP

Figure 3.4

```
Nmap scan report for Windows10 (172.22.117.20)
Host is up (0.00083s latency).
Not shown: 990 closed tcp ports (reset)
PORT    STATE SERVICE       VERSION
21/tcp  open  ftp           FileZilla ftpd 0.9.41 beta
| ftp-syst:
|_  SYST: UNIX emulated by FileZilla
|_ftp-bounce: bounce working!
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-r--r--r-- 1 ftp ftp              32 Feb 15  2022 flag3.txt
25/tcp  open  smtp          SLmail smtpd 5.5.0.4433
| smtp-commands: rekall.local, SIZE 100000000, SEND, SOML, SAML, HELP, VRFY, EXPN, ETRN, XTRN
|_ This server supports the following commands. HELO MAIL RCPT DATA RSET SEND SOML SAML HELP NOOP QUIT
79/tcp  open  finger        SLMail 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-title: 401 Unauthorized
| 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
106/tcp open  pop3pw        SLMail pop3pw
110/tcp open  pop3          BVRP Software SLMAIL pop3d
135/tcp open  msrpc         Microsoft Windows RPC
139/tcp open  netbios-ssn   Microsoft Windows netbios-ssn
443/tcp open  ssl/http      Apache httpd 2.4.52 (OpenSSL/1.1.1m PHP/8.1.2)
|_ssl-date: TLS randomness does not represent time
|_http-server-header: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/8.1.2
| ssl-cert: Subject: commonName=localhost
```

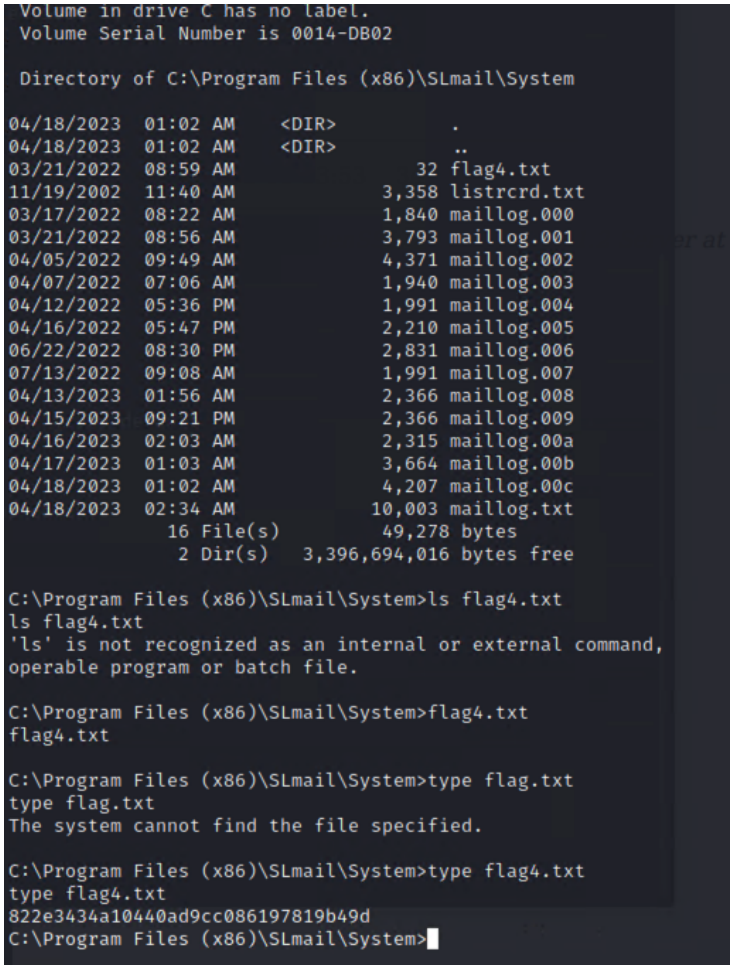
Figure 3.5

```
┌──(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> cat flag3.txt
?Invalid 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
226 Transfer OK
ftp> cat flag3.txt
?Invalid command
ftp> get flag3.txt
local: flag3.txt remote: flag3.txt
200 Port command successful
150 Opening data channel for file transfer.
226 Transfer OK
32 bytes received in 0.00 secs (47.4924 kB/s)
ftp> exti
?Invalid command
ftp> exit
221 Goodbye

┌──(root㉿kali)-[~]
└─# ls
Desktop    Downloads   file3.jpg  'LinEnum.jpg (copy 1).jpg.php'   Music     Public    Templates
Documents  file2.jpg   flag3.txt   LinEnum.sh                      Pictures  Scripts   Videos

┌──(root㉿kali)-[~]
└─# cat flag3.txt
89cb548970d44f348bb63622353ae278

┌──(root㉿kali)-[~]
└─#
```

Flag 4 - SLMail	Figure 3.6  Figure 3.7 
Flag 5 - SCHTASKS	Figure 3.8

Flag 6 - LSASS

Figure 3.9

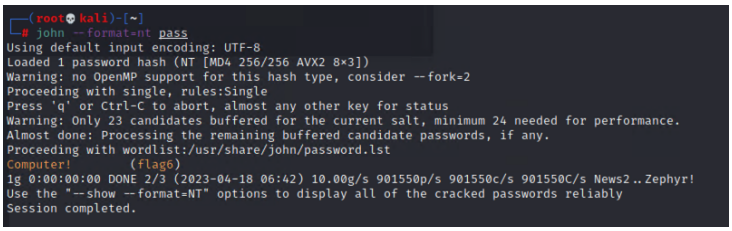


Figure 3.10