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

Contact Information

Company Name	The Acme Pen Testing Lab LLC
Contact Name	Jaco Kirsten
Contact Title	Chief Pen Tester and Bottlewasher

Document History

Version	Date	Author(s)	Comments
001	10/21/2022	Jaco Kirsten	Final

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.

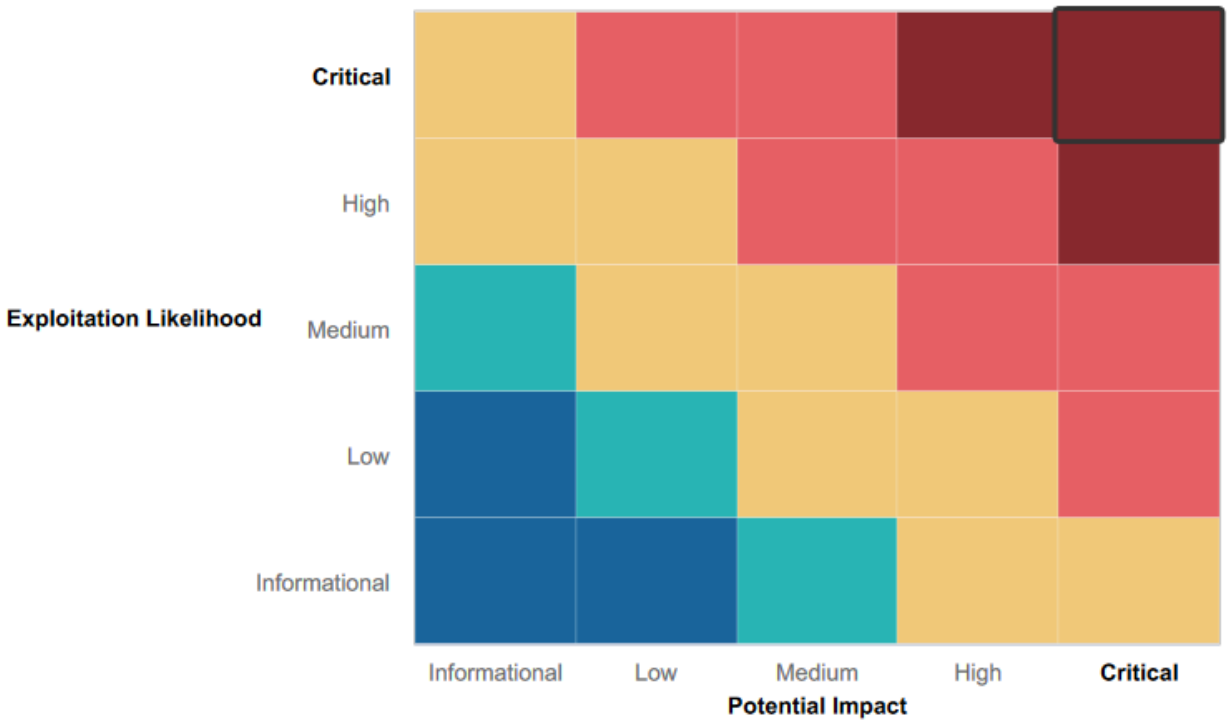
Executive Summary of Findings

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.

- The input validation areas block some malicious scripts.
- Encrypted passwords
-

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.

- Too much valuable information available through open source intelligence.
- Weak passwords and unsecure credentials
- Open ports

Vulnerability to the following:

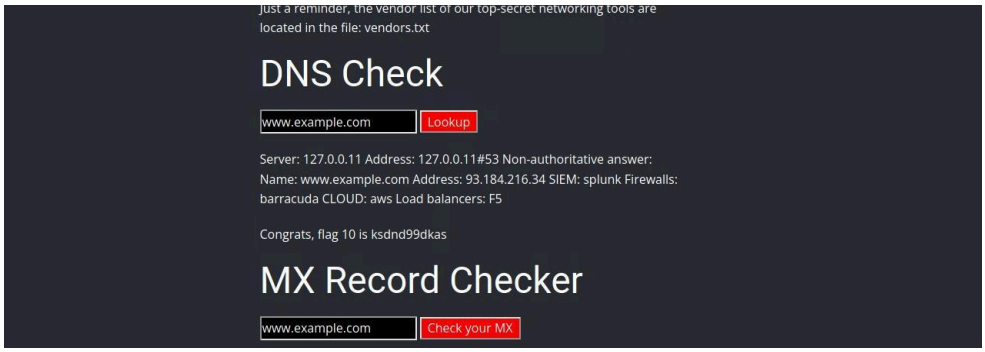
- Cross-site scripting on web app
- SQL injection on web app
- Local file inclusion on web app
- Command injection on web app
- Brute forcing on web app
- Remote code execution
- Arbitrary code execution
- User enumeration

Executive Summary

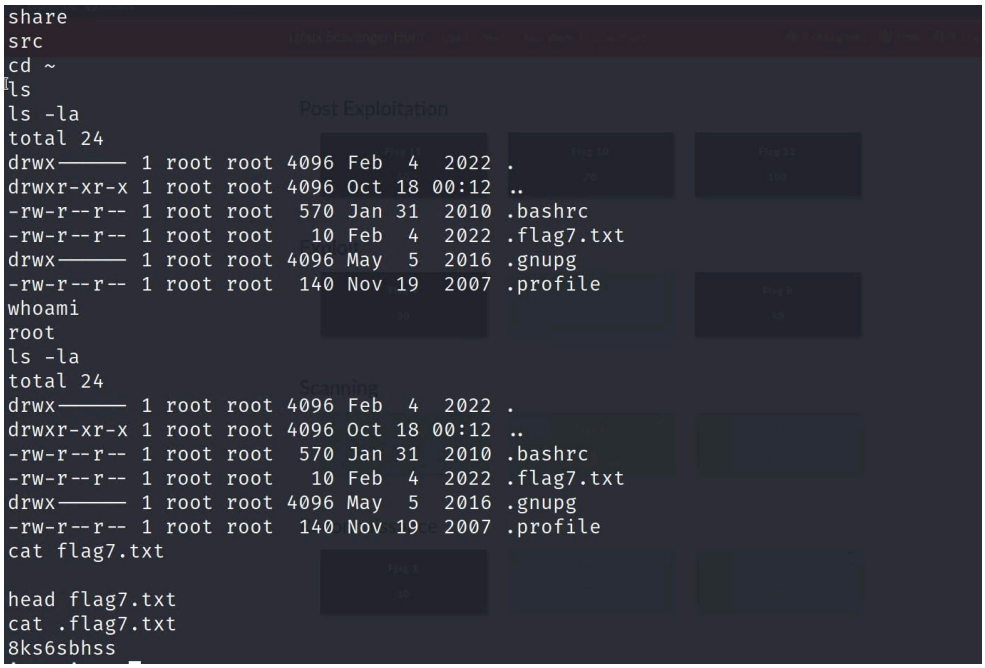
We performed an indepth penetration test of the following components of Totalrekall: The web app, as well as the Linux and Windows servers.

We started by trying to gather as much open source intelligence as we could gain. It turned out that there were indeed some valuable information that could be gleaned this way - and which allowed us a way into some of the servers.

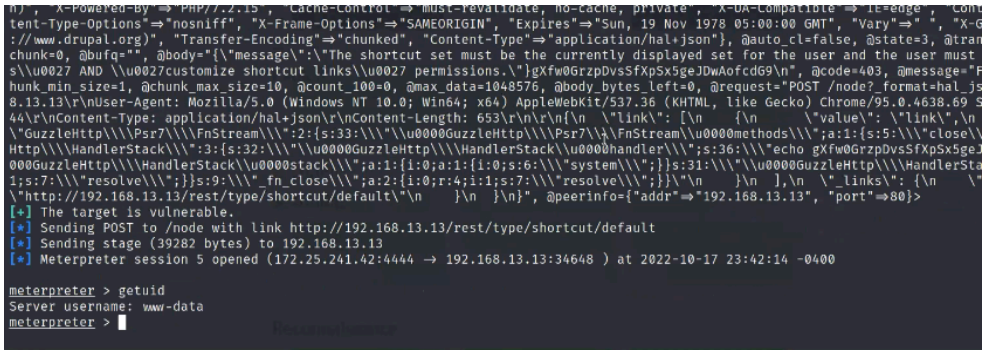
On the web app there were a number of ways in which we could compromise the security and gain access to privileged information. See screenshot:



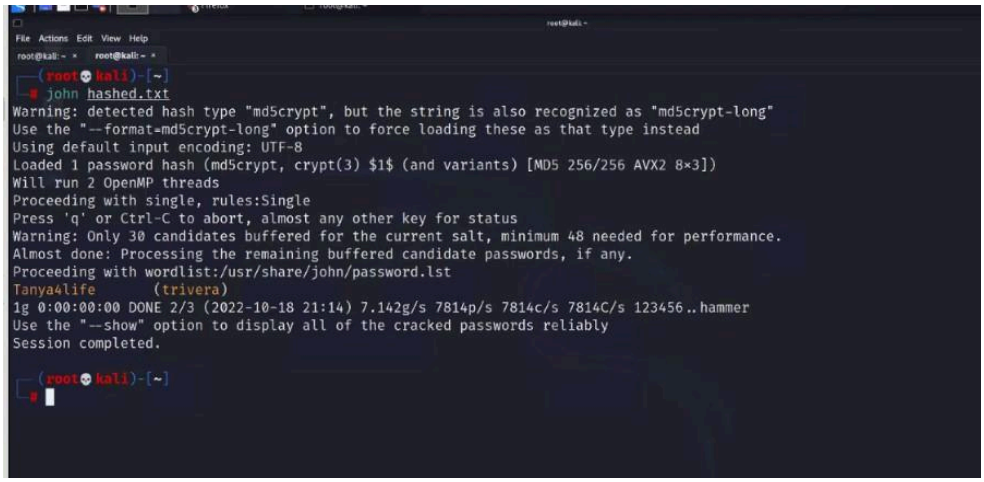
We were able to ascertain that quite a number of ports on the Linux machines were open. Through the use of Metasploit, we were able to deploy a number of exploits that allowed us a concerning level of access to the system, including that of root user. See screenshot:



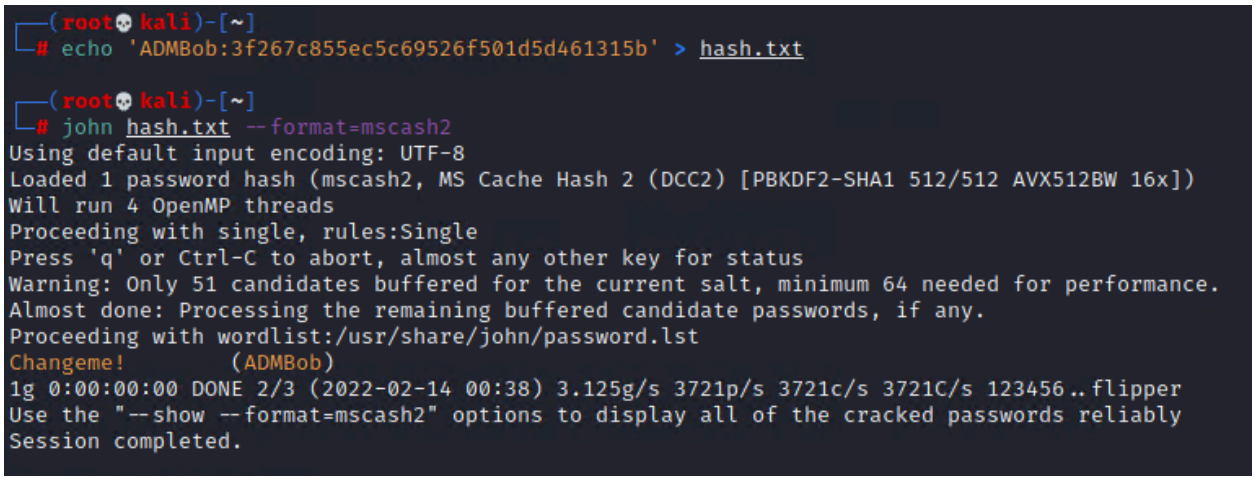
We also ran a couple of other exploits, succeeding in gaining access to sensitive directories such as /etc/sudoers and /root/, as well as targeting the machines with reverse shells - a technique whereby your machines communicate with ours, making it very hard for your information security department to detect it. See screenshot:



We were able to gain relatively easy access to the Windows machines, by cracking an encoded password found on a public website. See screenshot:



After doing an nmap scan on the Windows machines, we found numerous ports open. Through Metasploit we were once again able to access these machines, from where we accessed a number of highly sensitive files and directories. Through user enumeration we gained further access to root/admin directories. See screenshot:



Summary Vulnerability Overview

Vulnerability	Severity
XSS	Low
Sensitive data exposure	Low
Local file inclusion	Medium
SQL injection	Medium
Command injection	High
Brute force attack	Critical
PHP Injection	High
Session Management	High
Directory Traversal	High
Sensitive data exposure	High
Apache Tomcat Remote Code Execution Vulnerability (CVE-2017-12617)	Critical
Shellshock Remote Code Execution Vulnerability (CVE-2014-7169)	Critical
Struts Remote Code Execution Vulnerability (CVE-2017-5638)	Critical
Drupal Remote Code Execution Vulnerability: CVE-2019-6340	Critical
Sudo Vulnerability - CVE-2019-14287	Critical
Compromising SLMail - CVE-1999-0272	Critical
Elevation of privilege - CVE-2021-1733	Critical

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

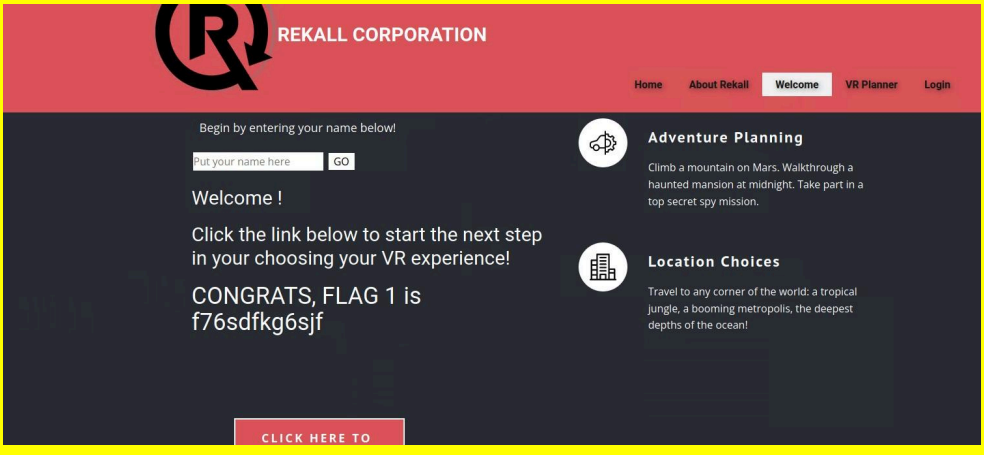
Scan Type	Total
Hosts	5 Linux, Windows 3
Ports	Linux: 80, 443, 5901, 6001, 10000, 10001.

	Windows: 21, 25, 79, 80, 106,110

Exploitation Risk	Total
Critical	8
High	5
Medium	2
Low	2

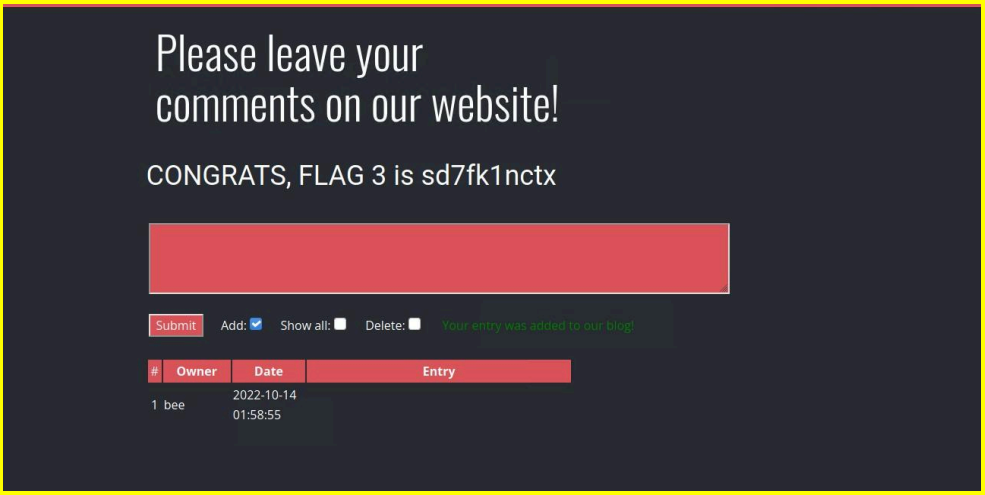
Vulnerability Findings

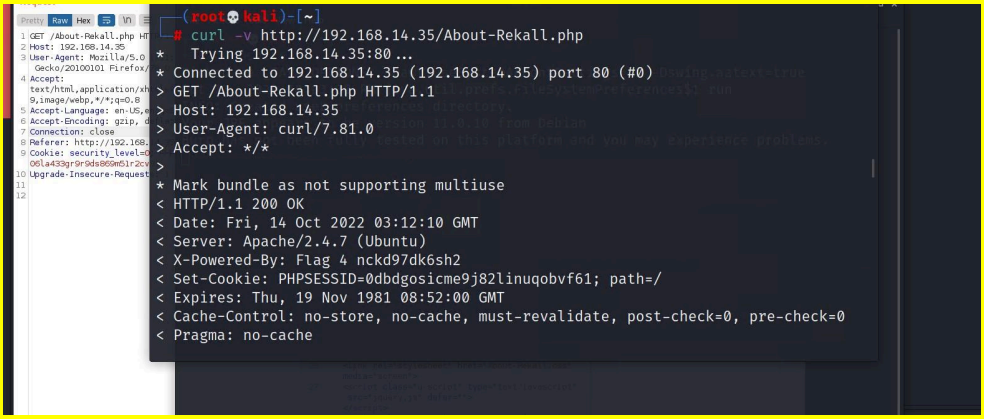
Web Application vulnerabilities

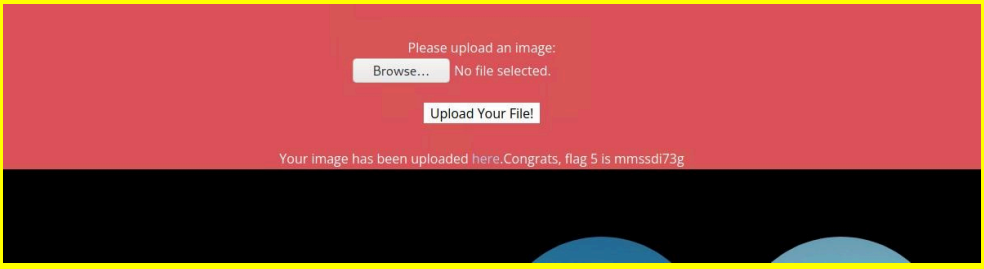
Vulnerability 1	Findings
Title	XSS reflected on Welcome page
Type	Web app
Risk Rating	Low
Description	We successfully entered an XSS payload into the “Enter your name here field.”
Images	
Affected Hosts	totalrekall.xyz
Remediation	Ensure best input validation possible

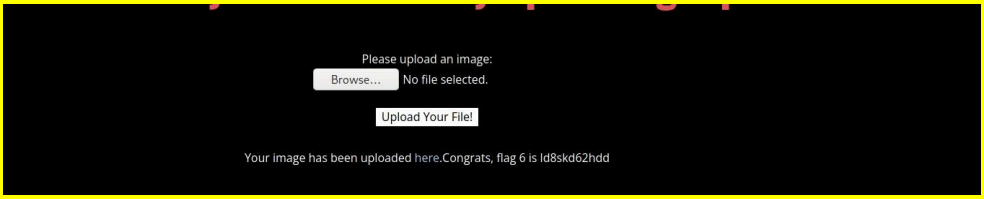
Vulnerability 2	Findings
Title	XSS reflected on Memory-Planner page.
Type	Web app

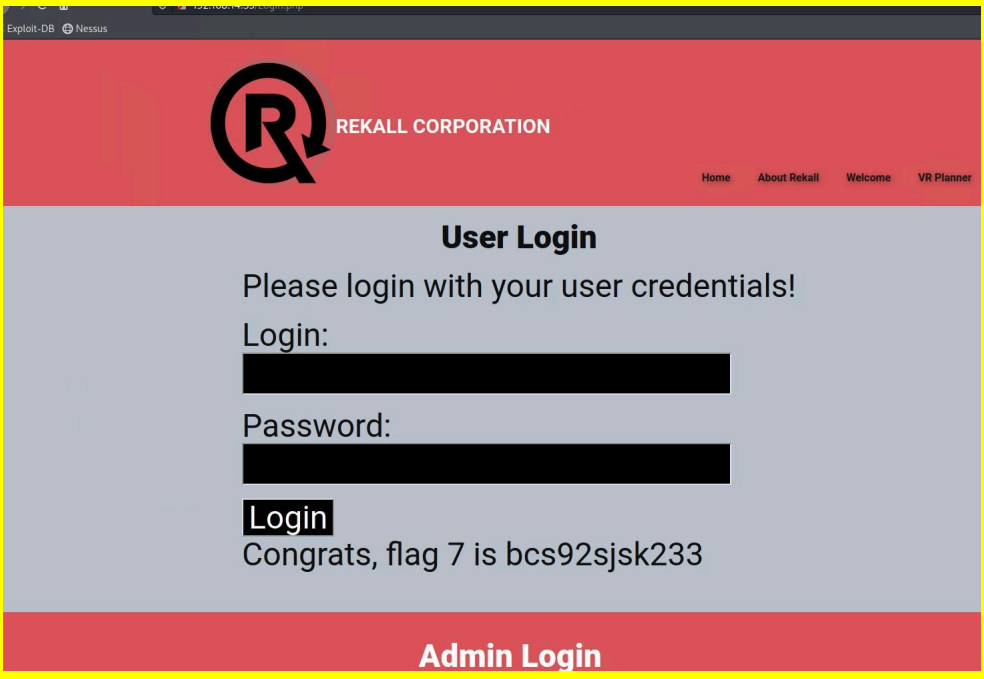
Risk Rating	Low
Description	We successfully entered an XSS payload into the "Choose Your Character" field on the Memory-Planner page, resulting in a pop up appearing. The input validation automatically protects against the word "script" to prevent malicious payloads running, but we got around it by wrapping "script" in "scriscriptpt".
Images	
Affected Hosts	totalrekall.xyz
Remediation	Ensure best input validation possible

Vulnerability 3	**Findings**
Title	XSS stored in the Comments page.
Type	Web app
Risk Rating	Low
Description	We entered a simple Javascript payload into the "Please leave your comments here" field, resulting in a pop-up appearing
Images	
Affected Hosts	totalrekall.xyz
Remediation	Ensure best input validation possible

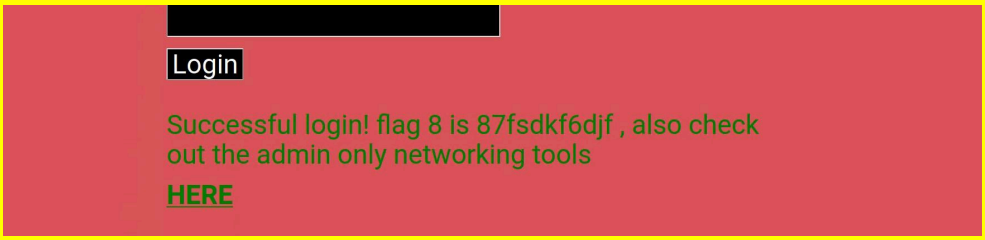
Vulnerability 4	Findings
Title	Sensitive data exposure on the About-Rekall page.
Type	Web app
Risk Rating	Low
Description	In Kal-Linux we used a Curl request to look at the HTTP traffic and was easily able to view sensitive data.
Images	
Affected Hosts	192.168.14.35
Remediation	Sensitive data should be encrypted

Vulnerability 5	Findings
Title	Local file inclusion on Memory-Planner field.
Type	Web app
Risk Rating	Medium
Description	We were able to upload a .php file to the TotalRekall site.
Images	
Affected Hosts	totalrekall.xyz
Remediation	Sanitize user-supplied inputs

Vulnerability 6	Findings
Title	Local file inclusion
Type	Web app
Risk Rating	Medium
Description	Input validation looks for .jpg files, so we cloaked our malicious script by adding .jpg to the filename. This allowed the script to bypass the check.
Images	
Affected Hosts	totalrekall.xyz
Remediation	Ensure best input validation possible

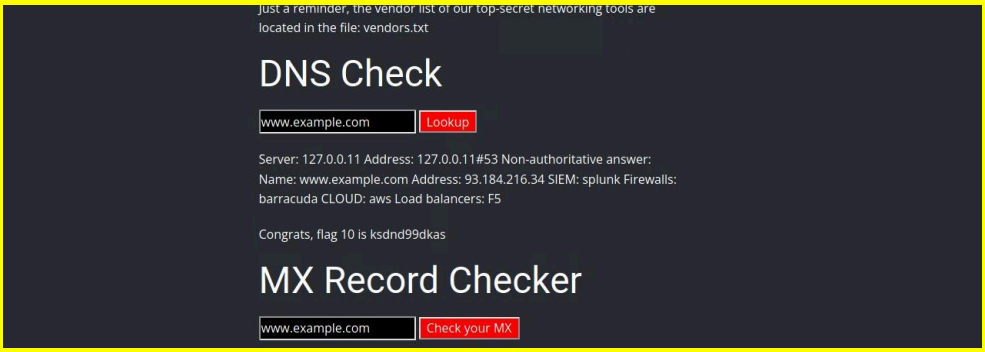
Vulnerability 7	Findings
Title	SQL injection in the Login page.
Type	Web app
Risk Rating	Medium
Description	We were successful with inserting an SQL payload into the login page.
Images	
Affected Hosts	Ensure best input validation possible

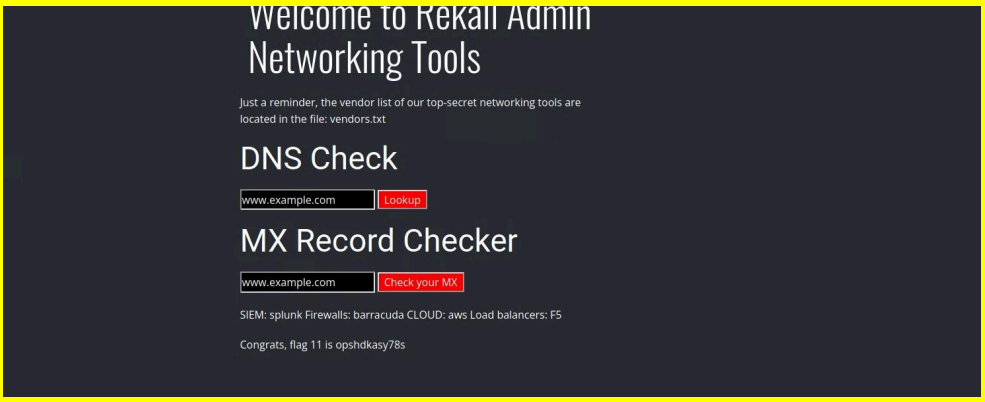
Remediation	

Vulnerability 8	Findings
Title	Sensitive data exposure
Type	Web app
Risk Rating	High
Description	Not only are both the username and password in the HTML code, but one can also view them by simply highlighting fields on the web page with a cursor.
Images	
Affected Hosts	totalrekall.xyz
Remediation	Better encryption

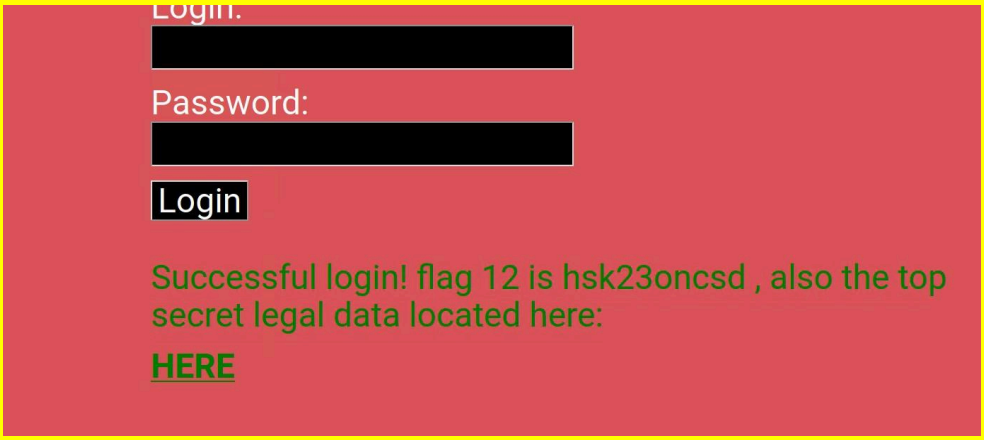
Vulnerability 9	Findings
Title	Sensitive data exposure
Type	Web app
Risk Rating	Low
Description	By simply replacing Login.php in the URL with ‘robots.txt’ we were able to access sensitive information.
Images	
Affected Hosts	totalrekall.xyz

Remediation	Better encryption

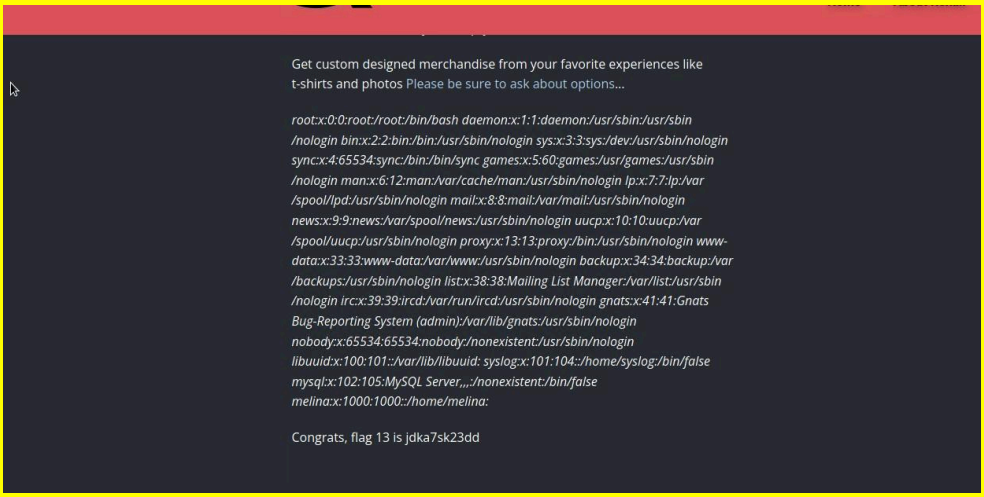
Vulnerability 10	Findings
Title	Command injection
Type	Web app
Risk Rating	High
Description	We were able to insert commands into www.welcometorecall.com and view sensitive information.
Images	
Affected Hosts	totalrekall.xyz
Remediation	Ensure best input validation possible

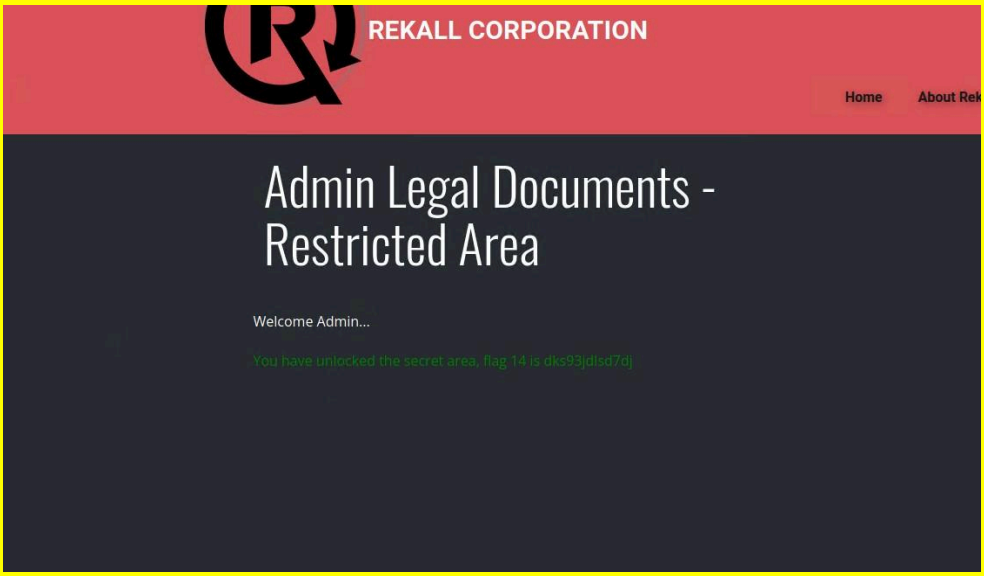
Vulnerability 11	Findings
Title	Command injection
Type	Web app
Risk Rating	High
Description	We were once again able to access sensitive data by injecting commands into input fields
Images	

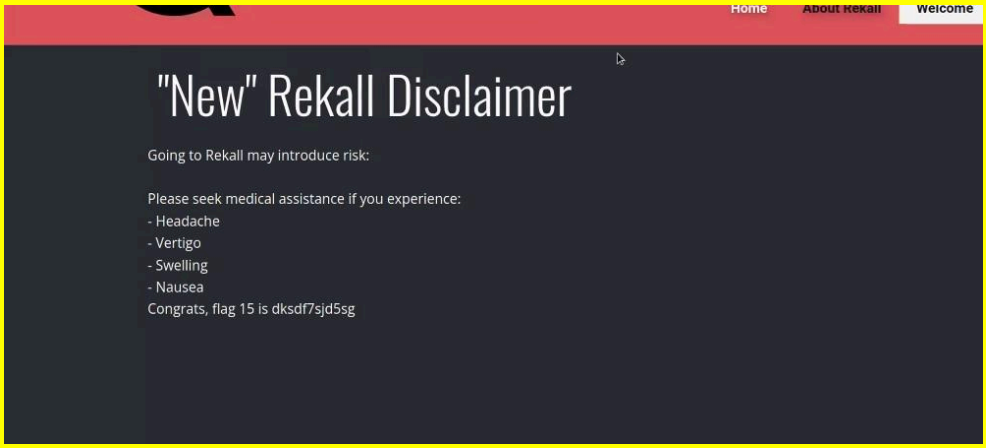
Affected Hosts	totalrekall.xyz
Remediation	

Vulnerability 12	Findings
Title	Brute force attack
Type	Web app
Risk Rating	Critical
Description	We were able to use vulnerabilities 10 and 11 to view the /etc/passwd file. This allowed us to get a username and password for an admin.
Images	
Affected Hosts	totalrekall.xyz
Remediation	Limit failed login attempts, limit logins from a specific IP address, 2FA, make root user inaccessible via SSH.

Vulnerability 13	Findings
Title	PHP injection
Type	Web app
Risk Rating	High
Description	This hidden webpage was identified in the robots.txt file found in exploit 9. The page is then exploited by changing the URL to include a malicious payload.

Images	
Affected Hosts	totalrekall.xyz
Remediation	Use a php php security linter, code serialization, use a SAST tool to identify code injection issues.

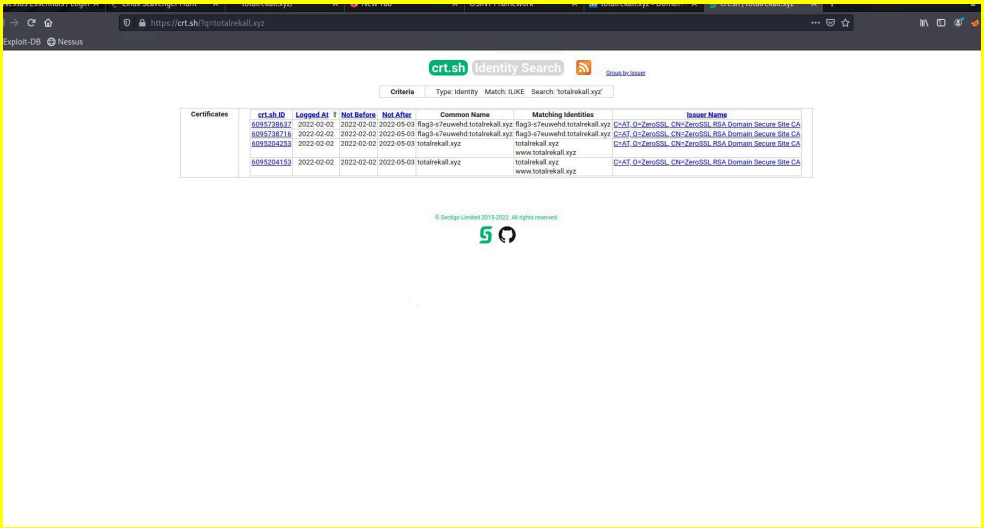
Vulnerability 14	Findings
Title	Session Management
Type:	Web app
Risk Rating	High
Description	After performing exploit 12 we discovered a link to a page. Using Burp Suite we were able to discover a particular high value session.
Images	
Affected Hosts	totalrekall.xyz
Remediation	Use an up-to-date web-server framework to generate and manage the session identifier token.

Vulnerability 15	Findings
Title	Directory traversal
Type	Web app
Risk Rating	High
Description	Using the information from exploits 10 and 11 we were able to view older directories and change site information from a current disclaimer to and older version.
Images	
Affected Hosts	totalrekall.xyz
Remediation	Keep web server and operating system updated. Validate user input before processing. Non superusers should only have read-only rights. Run web server from a separate disk from system disk.

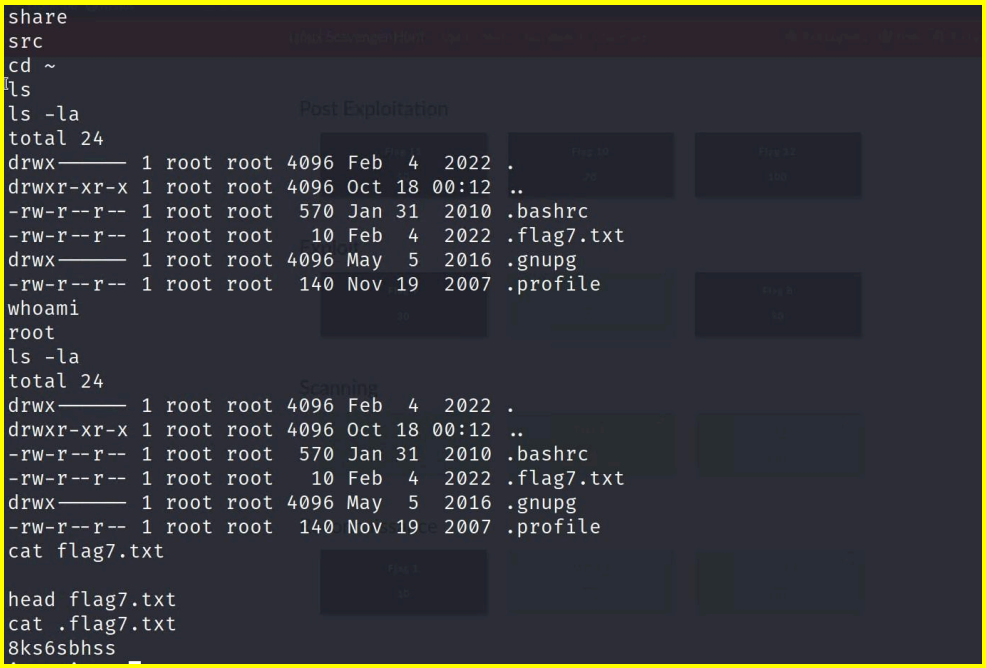
Linux vulnerabilities:

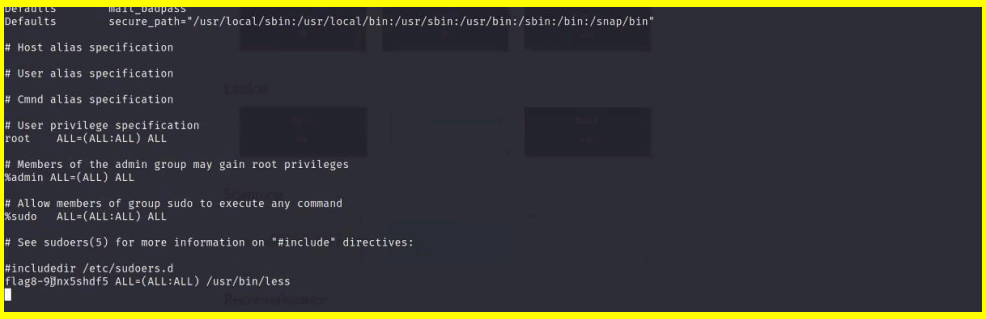
Vulnerability 1	Findings
Title	Sensitive data exposure
Type	Linux OS
Risk Rating	Low
Description	We were able to view confidential data about totalrekall.xyz through open source investigation.

Images	
Affected Hosts	totalrekall.xyz
Remediation	Limit open source information.

Vulnerability 2	Findings
Title	Sensitive data exposure
Type	Linux OS
Risk Rating	Low
Description	We were able to get access to sensitive data by simply searching for totalrekall.xyz on crt.sh
Images	
Affected Hosts	totalrekall.xyz
Remediation	Try to limit open source data exposure where possible.

Vulnerability 3	Findings
Title	Apache Tomcat Remote Code Execution Vulnerability (CVE-2017-12617)

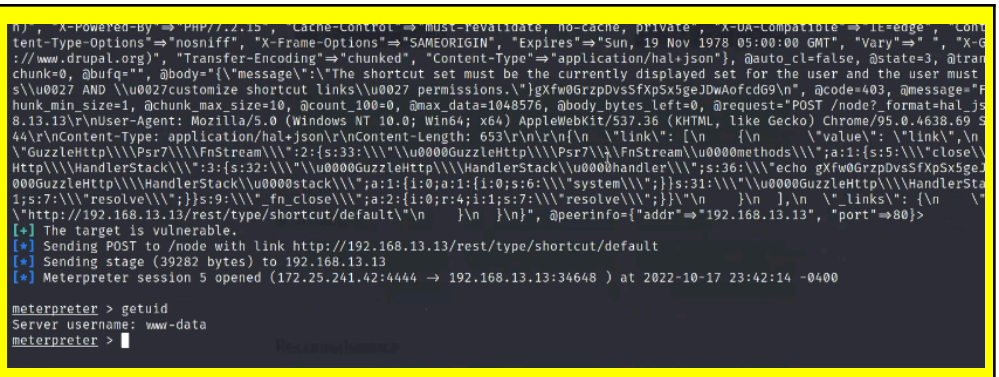
Type	Linux OS
Risk Rating	Critical
Description	With Metasploit we were able to use an exploit to create a reverse shell on a machine. This gave us root access to the machine.
Images	
Affected Hosts	192.168.13.10
Remediation	Update all security patches

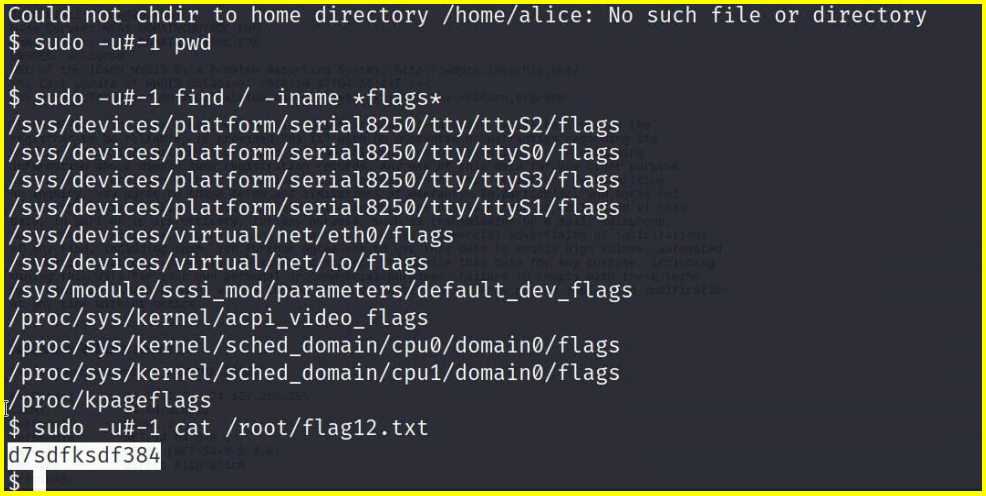
Vulnerability 4	Findings
Title	Shellshock - CVE-2014-7169
Type	Linux OS
Risk Rating	Critical
Description	We were able to run a Shellshock exploit with Metasploit. We then used a shell to get access to the /etc/sudoers directory.
Images	

Affected Hosts	192.168.13.11
Remediation	Update all security patches

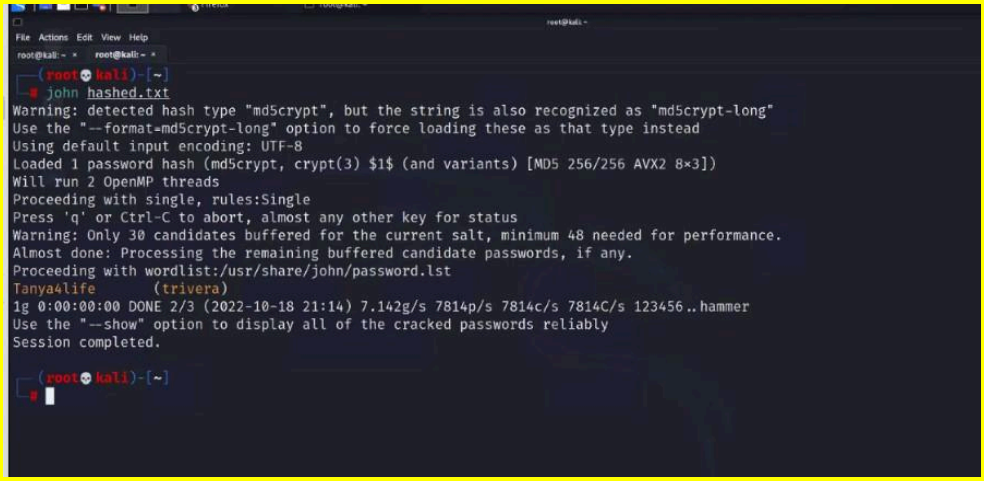
Vulnerability 5	Findings
Title	Struts - CVE-2017-5638
Type	Linux OS
Risk Rating	Critical
Description	We determined via a Nessus scan that this host was vulnerable to Struts. Using Metasploit, we used a Struts exploit to create a Meterpreter shell and gain access to the /root/ directory from which we extracted a file.
Images	
Affected Hosts	192.168.13.12
Remediation	Update all security patches

Vulnerability 6	Findings
Title	Drupal - CVE-2019-6340
Type	Linux OS
Risk Rating	Critial
Description	Through Metasploit we used a Drupal exploit to create a Meterpreter shell.

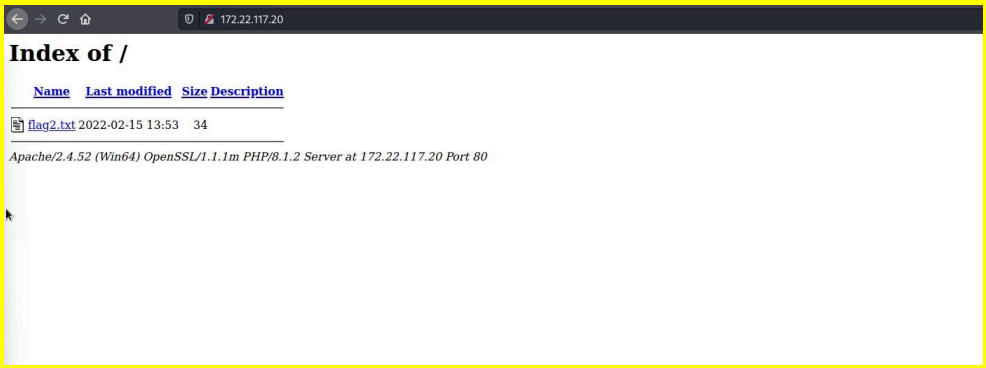
Images	
Affected Hosts	192.168.13.13
Remediation	Update all security patches

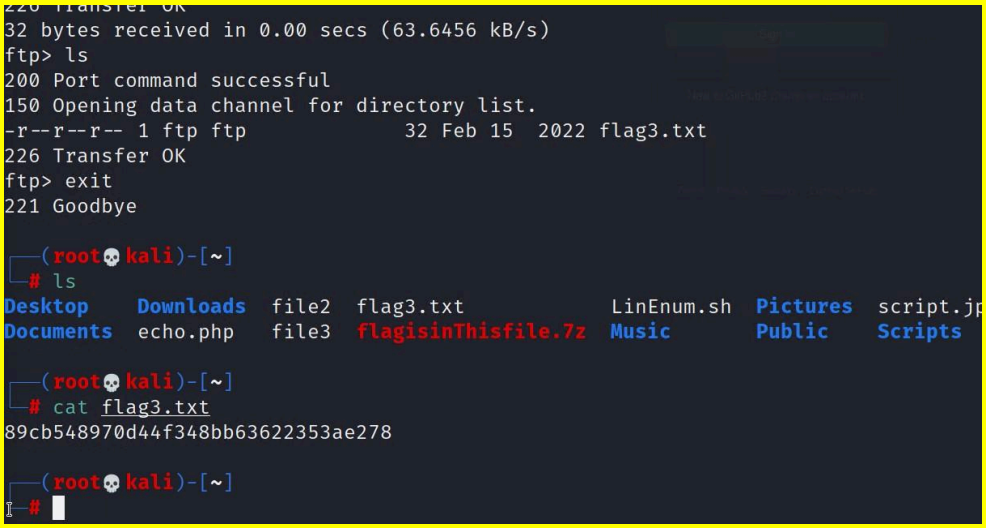
Vulnerability 7	Findings
Title	Sudo Vulnerability - CVE-2019-14287
Type	Linux OS
Risk Rating	Critical
Description	We were able to SSH into the server using credentials we gained through OSINT research, as well as guessing the password of the user ‘Alice’ - which turned out to be ‘alice.’We then conducted privilege escalation to access a file that only the root user should have access to.
Images	
Affected Hosts	192.168.13.14
Remediation	Update all security patches

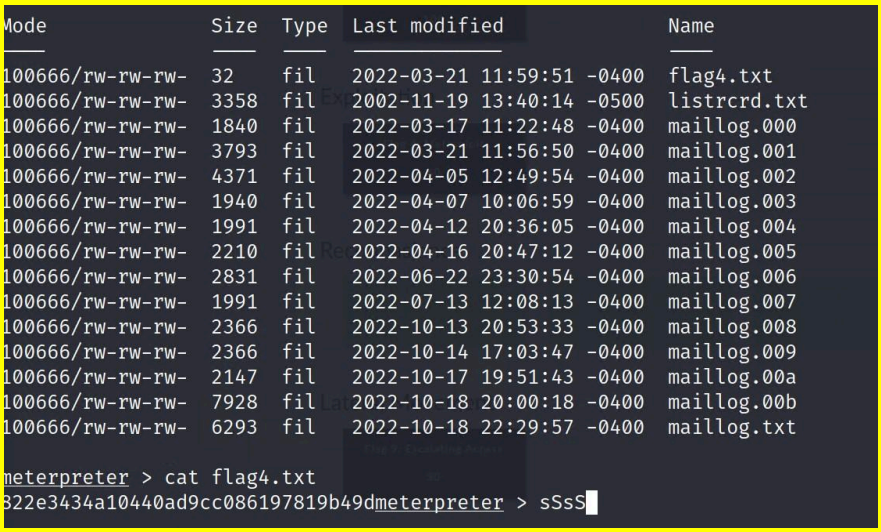
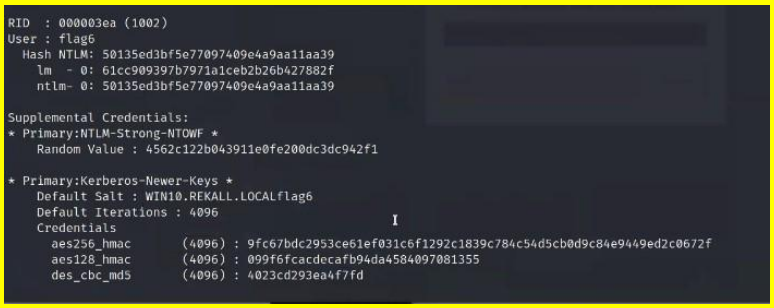
Windows Vulnerabilities

Vulnerability 1	Findings
Title	Unsecure credentials
Type	Windows
Risk Rating	High
Description	We were able to quickly crack the password for user trivera, a weakly encoded version that was easily obtained on Totalrekall's Github repository.
Images	
Affected Hosts	
Remediation	Don't store passwords - even encrypted ones - on a public platform.

Vulnerability 2	Findings
Title	Open port 80
Type	Windows
Risk Rating	High
Description	Using an nmap scan, we found an open http port (80) on one machine. Using its IP address and the cracked username and password from Vulnerability 1, we were able to gain access to a file with code.

Images	
Affected Hosts	172.22.117.20
Remediation	Close port 80

Vulnerability 3	Findings
Title	Open port 21
Type	Windows
Risk Rating	Critical
Description	An nmap scan showed an open ftp port (21). It also showed that anonymous access is possible to the ftp server. This was accessed to discover a certain file.
Images	
Affected Hosts	172.22.117.20
Remediation	Close port 21

Vulnerability 4	Findings
Title	Compromising SLMail - CVE-1999-0272
Type	Windows
Risk Rating	Critical
Description	Through our nmap scan we discovered open ports (25 and 110) on which the SLMail service is running. Using Searchsploit on Metasploit we found a module to exploit the target and establish a reverse Meterpreter shell on 172.22.117.20. This allowed access to system files where we located flag4.txt. After this, we dropped a command shell within Meterpreter to access the directory with all scheduled tasks.
Images	 

```
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   2022-10-13 20:53:33 -0400  maillog.008
100666/rw-rw-rw-  2366  fil   2022-10-14 17:03:47 -0400  maillog.009
100666/rw-rw-rw-  2147  fil   2022-10-17 19:51:43 -0400  maillog.00a
100666/rw-rw-rw-  7928  fil   2022-10-18 20:00:18 -0400  maillog.00b
100666/rw-rw-rw-  6293  fil   2022-10-18 22:29:57 -0400  maillog.txt

meterpreter > cat flag4.txt
822e3434a10440ad9cc086197819b49dmeterpreter > sSsS
```

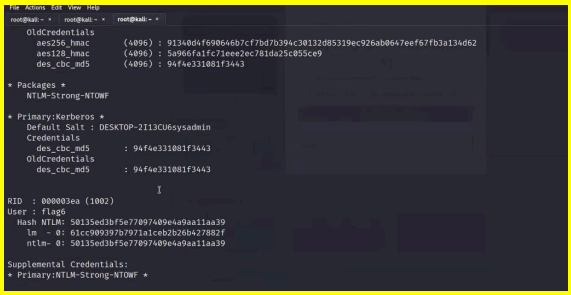
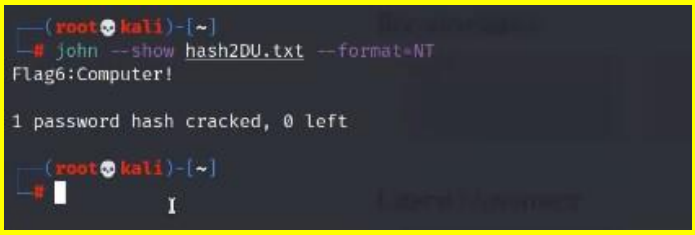
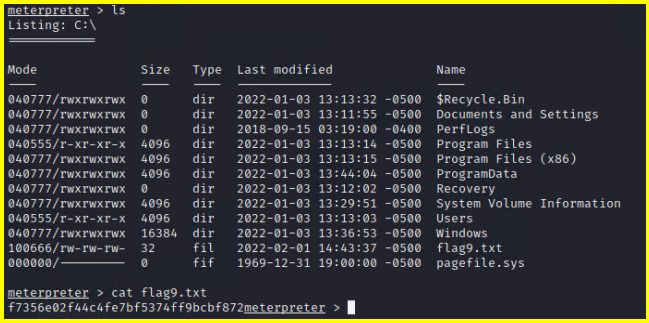
```
RID  : 000003ea (1002)
User : flag6
  Hash NTLM: 50135ed3bf5e77097409e4a9aa11aa39
    lm  - 0: 61cc909397b7971a1ceb2b26b427882f
    ntlm- 0: 50135ed3bf5e77097409e4a9aa11aa39

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) : 099f6fcacdecafb94da4584097081355
      des_cbc_md5       (4096) : 4023cd293ea4f7fd
```

Affected Hosts	172.22.117.20
Remediation	Close port 110.

Vulnerability 5	Findings
Title	Elevation of privilege - CVE-2021-1733
Type	Windows
Risk Rating	Critical
Description	After the SLMail exploit, we loaded kiwi in the Meterpreter shell. This allowed us to perform user enumeration and check for both local and domain users. We then managed to crack the password of a few users. One of them has access to the Server2019 machine (172.22.117.10). By using his credentials and employing the PsExec module in Metasploit, we created a new shell on this computer - and gained access to its root, or C:\ drive.

Images	   
Affected Hosts	172.22.117.20 and 172.22.117.10
Remediation	Update all security patches