Cybersecurity

Penetration Test Report

Rekall Corporation

Penetration Test Report

Student Note: Complete all sections highlighted in yellow.

Confidentiality Statement

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

Table of Contents

Contact Information

Company Name	BJN Enterprises
Contact Name	Brandon Nimer
Contact Title	CEO

Document History

Version	Date	Author(s)	Comments
001	09/20/2023	Brandon Nimer	Getting started on report
002	09/23/2023	Brandon Nimer	Uploading images
003	09/27/2023	Brandon Nimer	Finishing Touches

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.

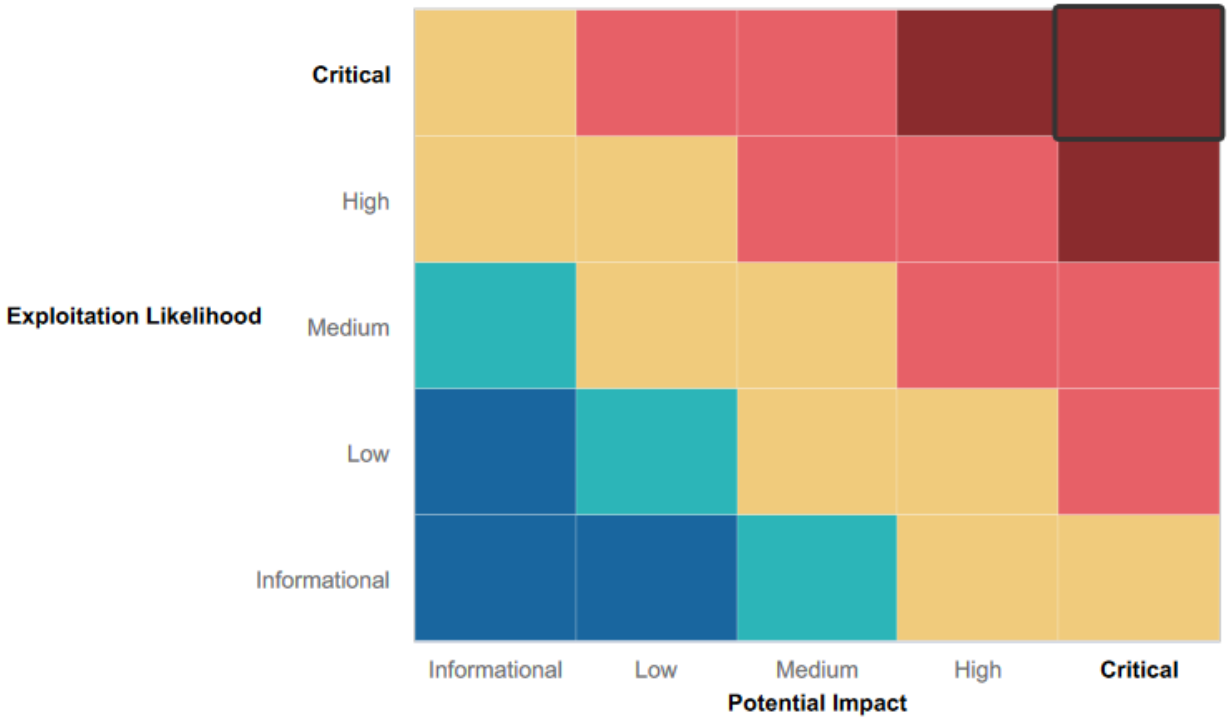
Executive Summary of Findings

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.

- During our exploitation of the Web App, we were able to find a scripting block on the Memory Planner page that initially gave us trouble
- Where you can upload a script.php file on the first file upload, the second one on the website is a little more secure
- The "restricted area" section was blocked until we utilized Burp, showing a basic level of security
- When utilizing metasploit for the various Linux/Windows environments, the team was forced to dig a little deeper to find the exploit that would work
- There are efforts to secure some of the machines, for example SSH not being allowed on certain IPs, certain ports being closed

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.

- Openly available information on public websites, or OSINT tools
- Weak password protection/policies. Too many passwords that are the same as the user name or generic phrases
- A lot of out of date versions of specific tools like Apache
- Data does not have proper permissions, too many times a non admin user is able to view sensitive documents that they should not have access to
- Login credentials and passwords are easily accessible through various users with lower privileges

Executive Summary

BJN Enterprises was contracted to run a penetration test on Rekall Corporation from September 14th, 2023 to September 27th,2023. Senior Pen Tester and CEO of the company, Brandon Nimer was assigned to lead the project. We were given access to Rekall Corporation's Web Application, Linux Servers, and Windows Servers to perform our test. Our goal was to be as thorough as possible and provide a concrete list of vulnerabilities that we were able to exploit in the given time period.

We split the test into three main sections to attack the three different operating systems we were given access to. Our efforts in the first third were dedicated to the Web Application, where the team was able to find a total of 12 vulnerabilities. We started our tests with a number of simulated XSS attacks on the various pages on the Rekall website. Utilizing text boxes on the Welcome, Memory Planner, and comments pages, we were able to input various scripts and prompt responses showing the web application was open to both Stored and Reflected XSS attacks. We were able to conduct similar experiments on the Memory Planner page with a couple Local File Inclusion attacks as well. Moving onto the Login Page, the team was able to input a simple '1=1 command in the passwords field to return sensitive data. Some of the larger exploits came from the Networking.php page, where we were able to inject command strings to reveal sensitive information and directory information. Using the ../ Method, we were able to read the entire etc/passwd file, which contained important login credentials for admin account Melina, which we later used to access the secure admin only section, where we were able to take advantage of Burp to access a secure session.

BJNE next focused their efforts on the Linux side of the test. The first thing we noticed was the amount of readily available information that we can find with simple Domain Dossier searches, where we were able to obtain a username/password. From there, the team ran an aggressive Nmap scan of the subnet which revealed some key vulnerabilities that we were able to leverage Metasploit to exploit. Due to vulnerabilities in Apache Tomcat, Shellshock, Struts, and Drupal, BJNE was able to access 4 separate machines, before also using the credentials we found earlier to SSH into 192.168.13.14.

Finally we conclude our investigation on the Windows side. Similarly to the Linux testing, our first conclusion is the abundance of publicly available information on sites like Github, where we were able to find a user and password to login with. We were able to find a number of open ports that we could exploit using metasploit. Once the team was able to access certain IPs, it was easy for us to search the machine to find new credentials for a possible privilege escalation. We conclude our findings with the administrator credentials, and close out our test.

BJN Enterprises has found in total 31 vulnerabilities for Rekall Corporation to fix. We have given our general summaries of each as well as our general recommendations for remediation. We highly recommend that these are taken seriously and events are put in motion to make changes. This will ensure Rekall Corporation is as secure as possible in the future.

Summary Vulnerability Overview

Vulnerability	Severity
Stored XSS -Welcome Page	Medium
Reflected XSS - Memory Planner	High
Stored XSS - Comments Page	Medium
Sensitive Data Exposure	Low
Local File Inclusion	High
SQL Injection - Login Page	Critical
Sensitive Data Exposure - Robots.txt	Low
Command Injection - Networking.php	Critical
Brute Force - Login page	Critical
PHP injection - Souvenirs	Critical
Session Management - Login Page	Critical
Directory Traversal - Disclaimer	High
Exposed information via OSINT Domain Dossier webpage	Low
Ping of totalrekall.xyz	Low
Nmap scan on subnet	Low
Aggressive Nmap scan	Low
Metasploit Apache Tomcat Exploit -192.168.13.10	Critical
Metasploit Shellshock Exploit cat etc/passwd - 192.168.13.11	Critical
Metasploit Struts Exploit - 192.168.13.12	Critical
Metasploit Drupal Exploit - 192.168.13.13	Critical
SSH into 192.164.13.14	Critical
GitHub Page - Access to Username/password	Low
Nmap scan 172.22.117.0/24 - Using cracked username/password	Critical
FTP - 172.22.117.20	Critical
SLMail Exploit - 172.22.117.20 Port 110	Critical
Windows 10 Task Schedule	Medium
Using Kiwi - 172.22.117.20	High
Accessing Documents in the Public Folder 172.22.117.20	Critical
Metasploit Exploit - 172.22.117.20 , using Kiwi to find ADMBob	Critical
Exploiting the 172.22.117.10 Machine	Critical
Accessing Admin Hashed Password	Critical

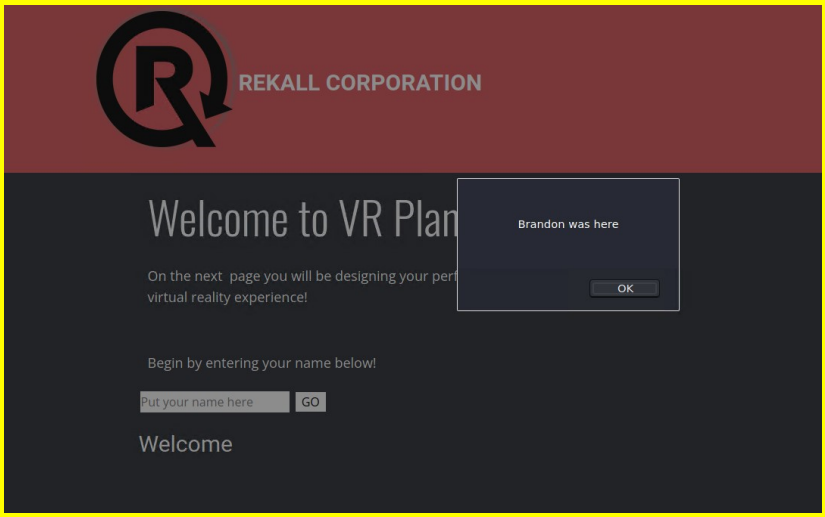
The following summary tables represent an overview of the assessment findings for this penetration test:

Scan Type	Total
Hosts	192.168.13.35 192.168.13.10 192.168.13.11 192.168.13.12 192.168.13.13 192.168.13.14 172.22.117.10 172.22.117.20
Ports	8080 80 21 22 110

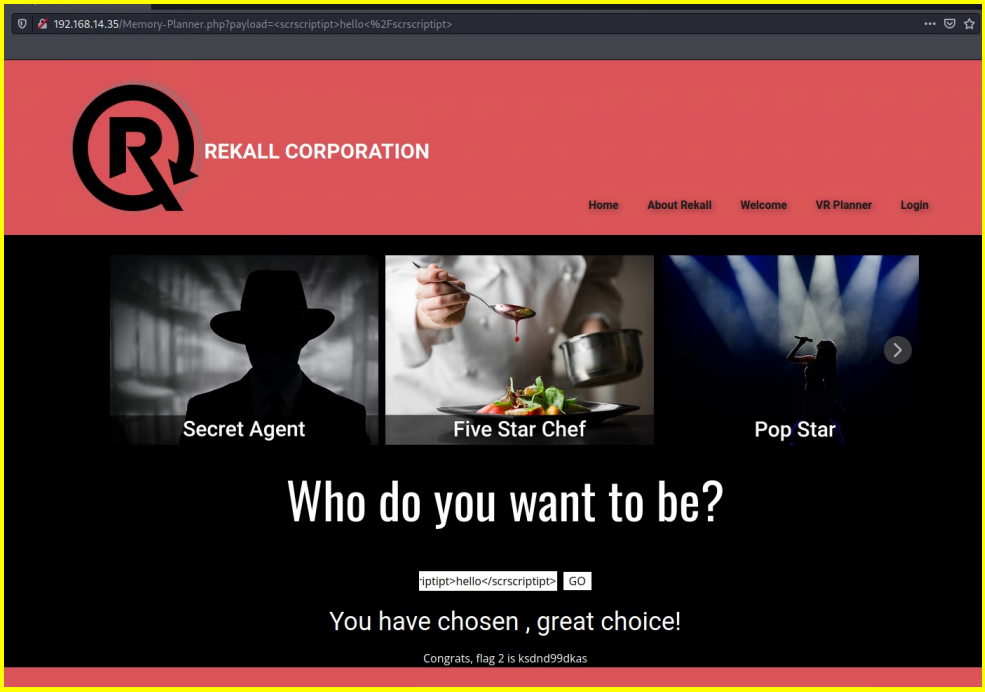
Exploitation Risk	Total
Critical	17
High	4
Medium	3
Low	7

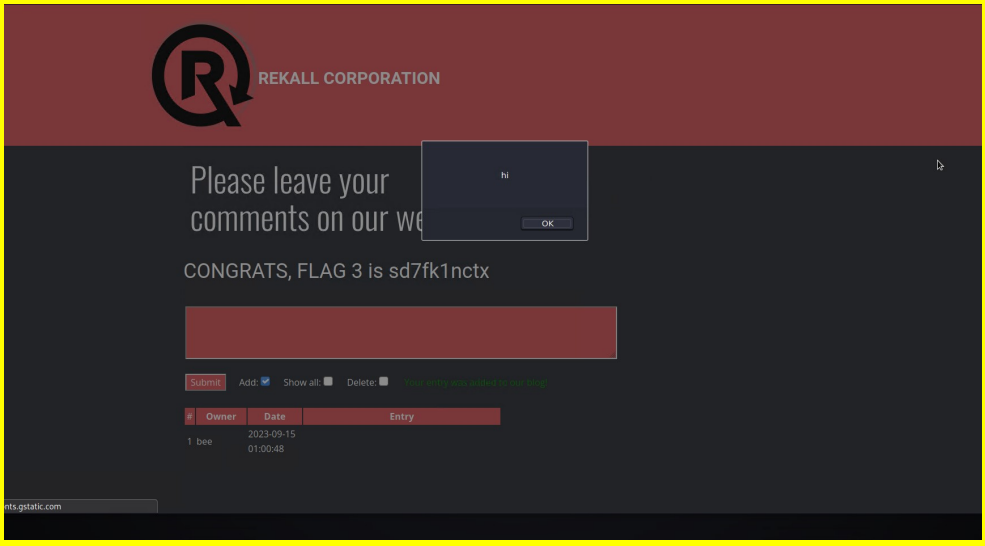
Vulnerability Findings

Vulnerability 1	Findings
Title	Stored XSS
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Medium
Description	Inserting scripts into the Welcome page of the web app to prompt a response <script>alert(Brandon was here)</script>

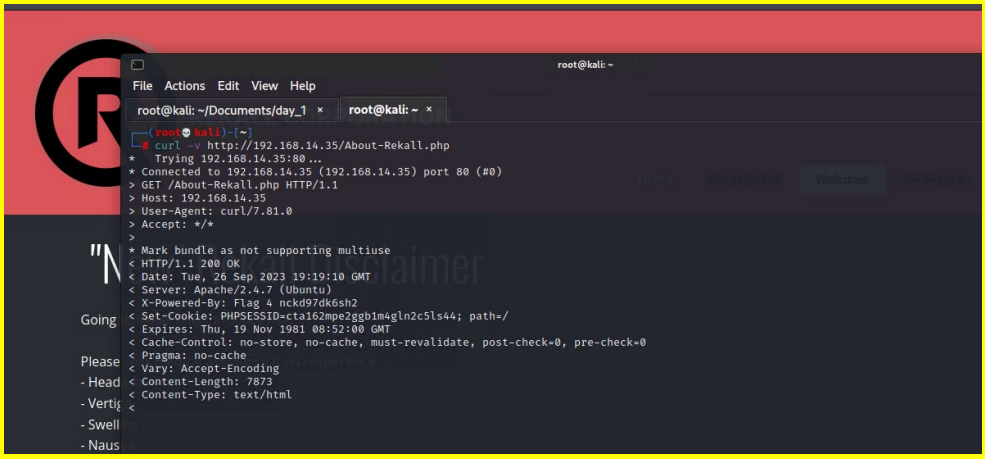
Images	
Affected Hosts	192.168.14.35/Welcome.php
Remediation	Secure handling of user input, or utilyze request blocking to ensure things like <script> cannot be inputted

Vulnerability 2	Findings
Title	Reflected XSS
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	HIgh
Description	Inputting a broken script <scrscriptipt>hello</scriscriptipt> to prompt a response on the Memory Planner page

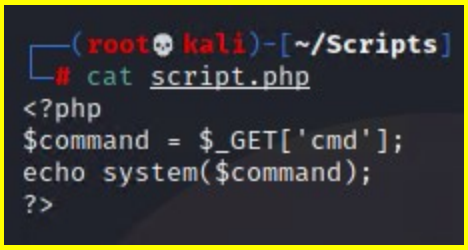
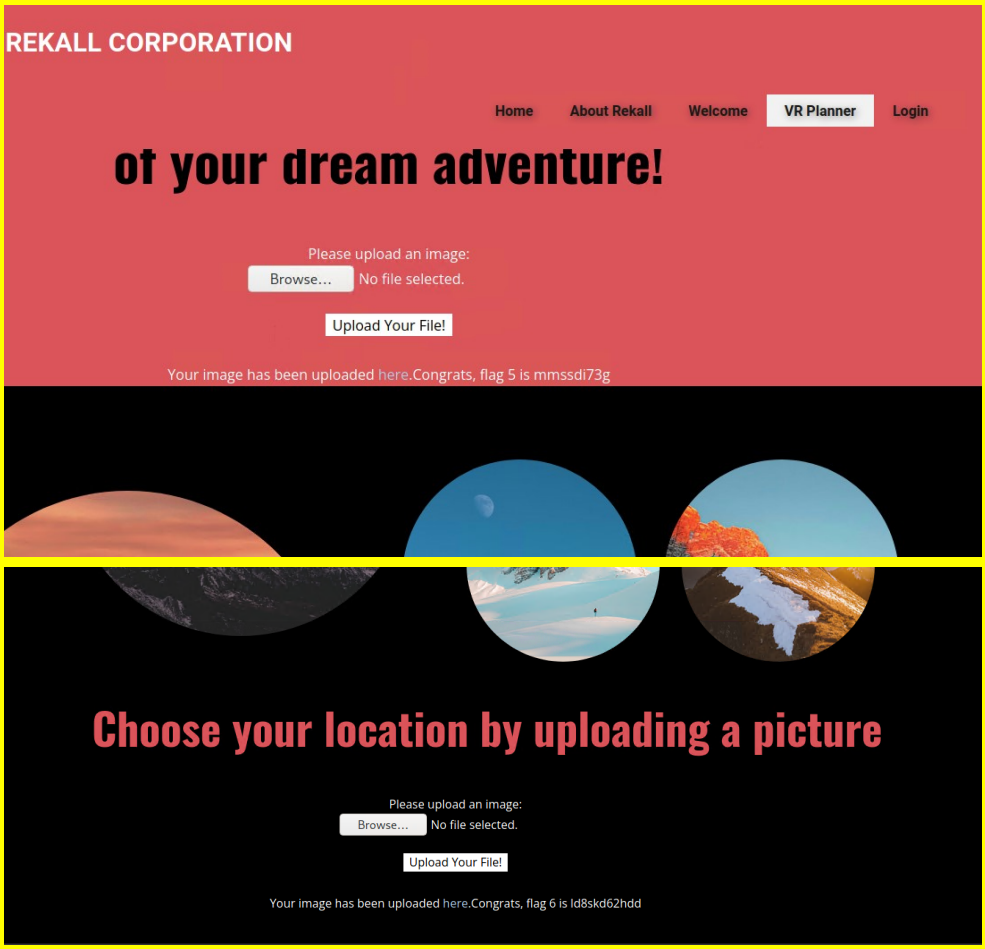
Images	
Affected Hosts	http://192.168.14.35/Memory_Planner.php
Remediation	HTML sanitization, or implement a WAF

Vulnerability 3	Findings
Title	Stored XSS on Comments Page
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Medium
Description	Inputting <script>alert(“Hi”)</script> into the comments box allows a popup to be created displaying the message “Hi”
Images	

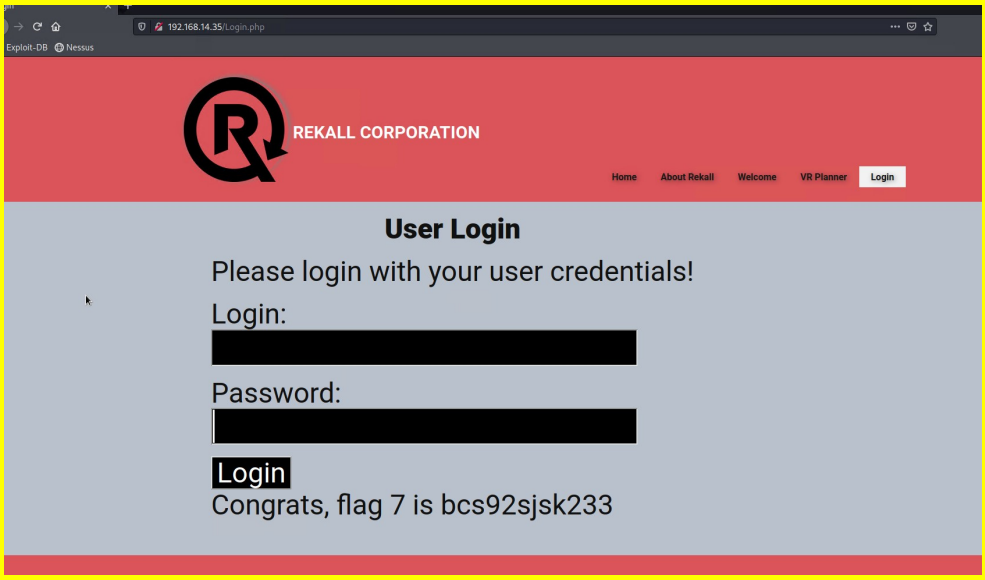
Affected Hosts	http://192.168.14.35/Comments.php
Remediation	Secure handling of user input, or utilyze request blocking to ensure things like <script> cannot be inputted

Vulnerability 4	**Findings**
Title	Sensitive data exposure
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Informational
Description	Running a curl -V command on the About page of Rekall's sight returns sensitive information
Images	
Affected Hosts	http://192.168.14.35/About-Rekall.php
Remediation	Remove sensitive information from HTML code

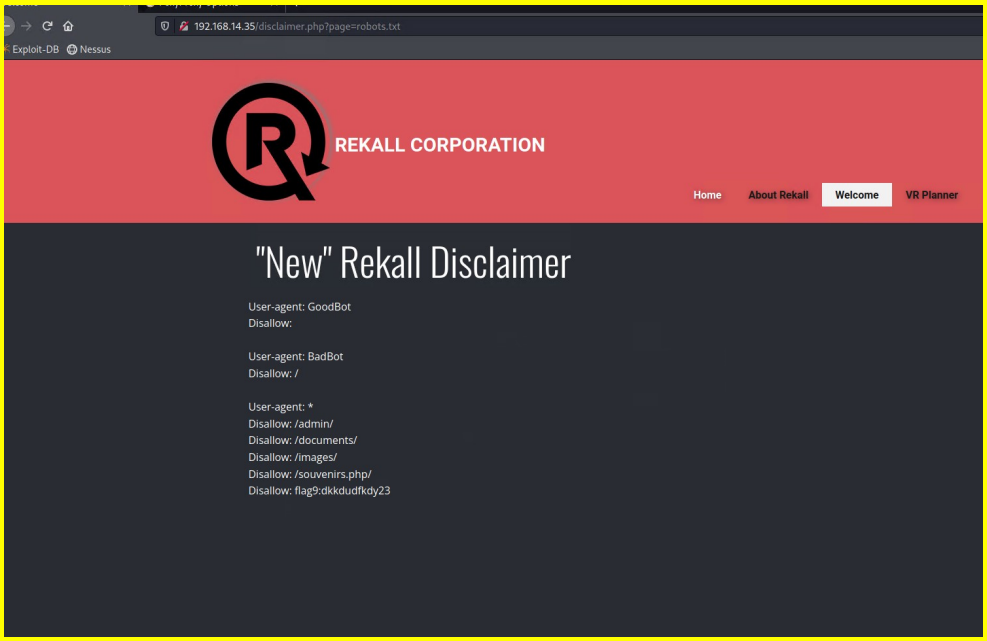
Vulnerability 5	**Findings**
Title	Local file inclusion
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	High
Description	Creating a script.php file with this command allows you to upload it on the memory planner site. If we change the format to .jpg.php, we can use the same file on the second file upload on the page.

Images	 
Affected Hosts	http://192.168.14.35/Memory_Planner.php
Remediation	Eliminatie file inclusion vulnerabilities to avoid passing user-submitted input to any filesystem.

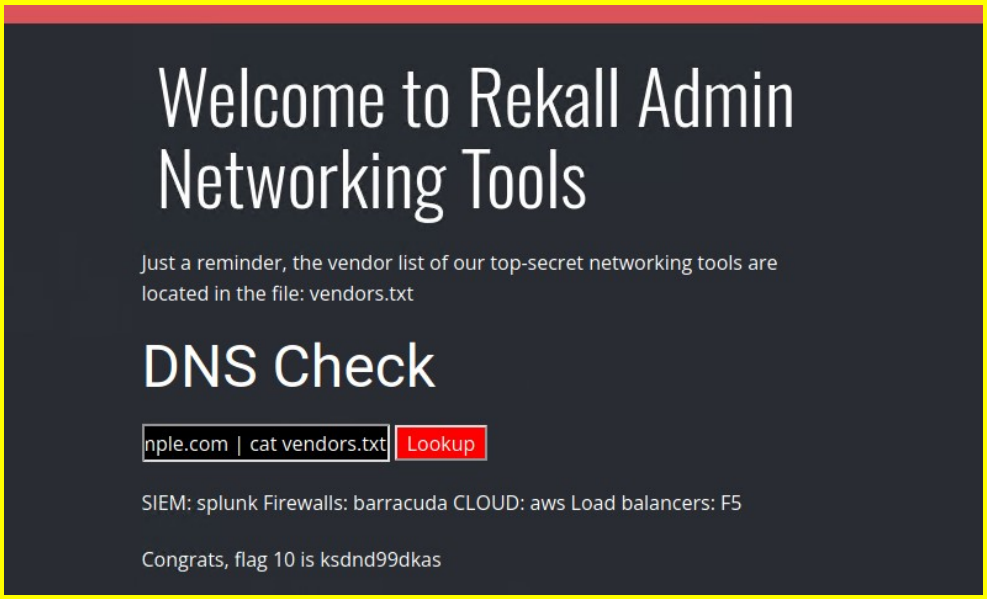
Vulnerability 6	Findings
Title	SQL Injection
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Critical
Description	Using the payload Melina' or '1=1 in the password field prompted the reveal of flag 7

Images	
Affected Hosts	http://192.168.14.35/login.php
Remediation	Use prepared statements and parameterized queries which separate SQL code from user input. This makes it nearly impossible for attackers to inject malicious SQL.

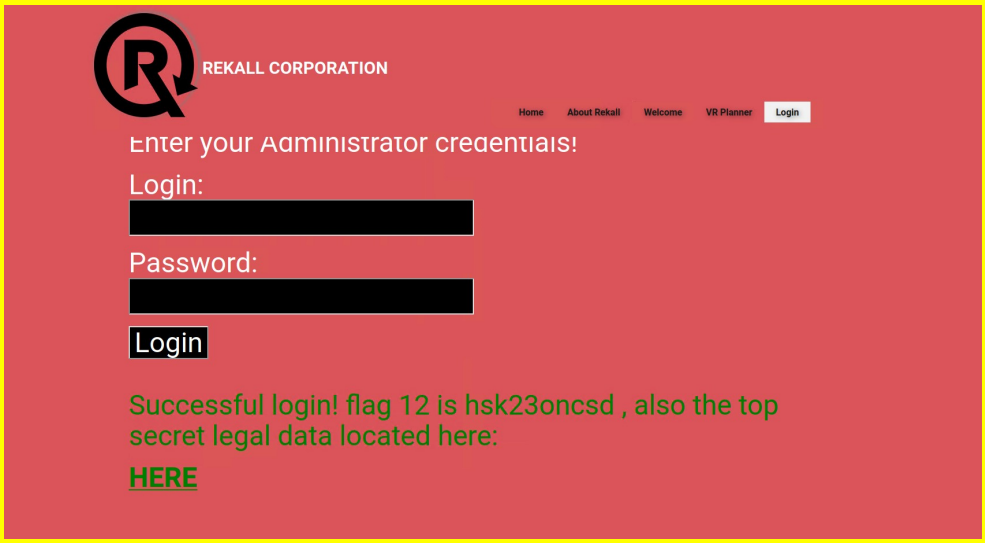
Vulnerability 7	Findings
Title	Sensitive Data - Robots.txt
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Low
Description	On the http://192.168.14.35/disclaimer.php page, you can add a page=robots.txt which displays sensitive information

Images	
Affected Hosts	http://192.168.14.35/disclaimer.php
Remediation	Reduce the amount of sensitive data stored that can be called up, or encrypt data both in transit and at rest

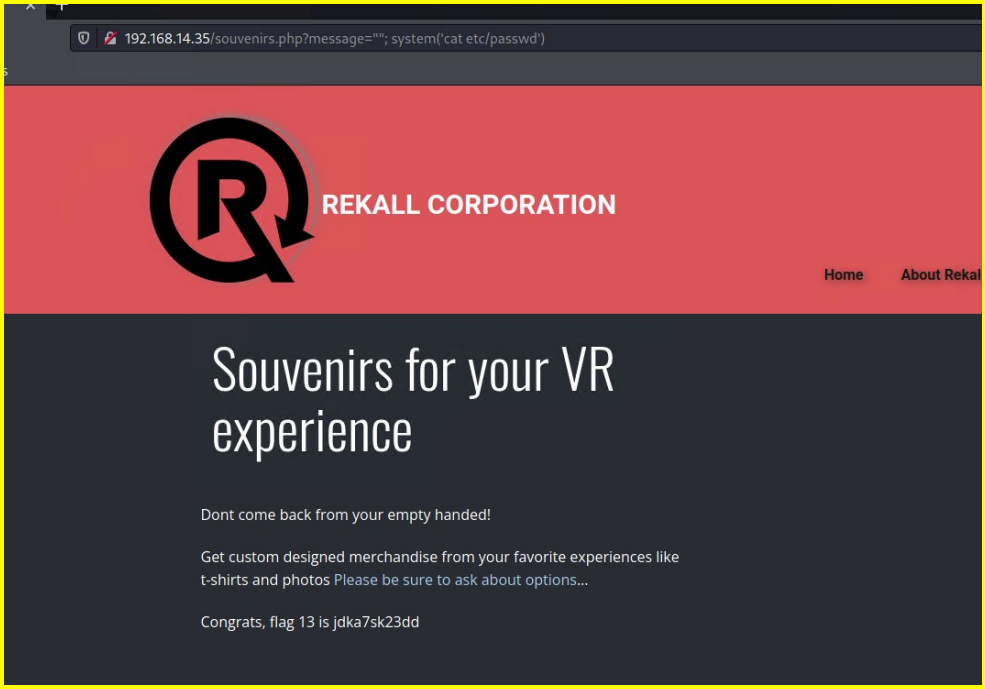
Vulnerability 8	Findings
Title	Command Injection - Networking.php
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Critical
Description	Utilizing the DNS Check and MX Record Checker we can use a pipe command to cat the vendors.txt file. When used on both fields we get the next two flags

Images	 
Affected Hosts	http://192.168.14.35/networking.php
Remediation	Implement strict input validation and sanitization or implement whitelists which would only allow predefined sets of commands/parameters.

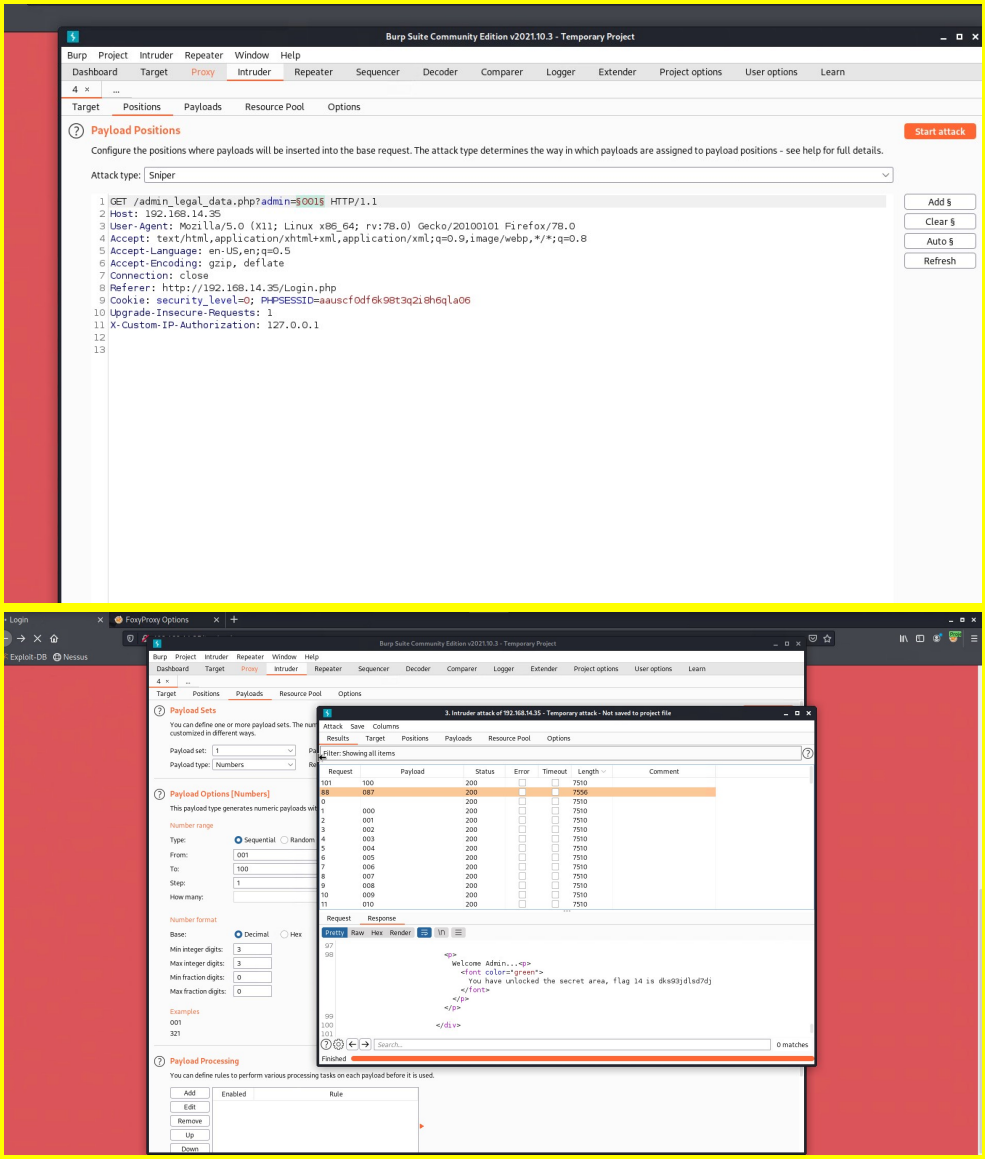
Vulnerability 9	Findings
Title	Brute Force
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Critical
Description	Using the admin creds that we found (Melina, Melina) when utilizing the ../ method which exposed the etc/passwd file.

Images	
Affected Hosts	http://192.168.14.35/login.php
Remediation	Implement stronger password policies and making sure access to the directory is not permitted through methods such as ../

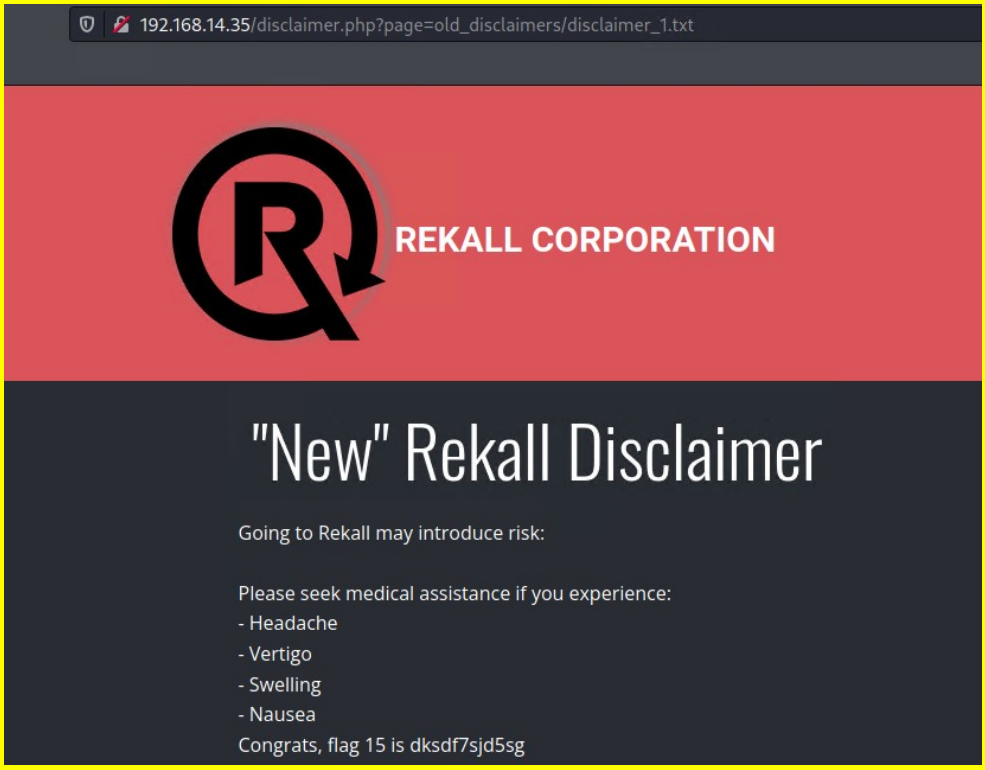
Vulnerability 10	Findings
Title	PHP Injection - Souvenirs
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Critical
Description	Inputting the command message=””;system(‘cat etc/passwd’) on the souvenirs.php page reveals sensitive data

Images	
Affected Hosts	http://192.168.14.35/souvenirs.php
Remediation	Ensure your system's versions are up to date with latest patches and implement security headers in your PHP application

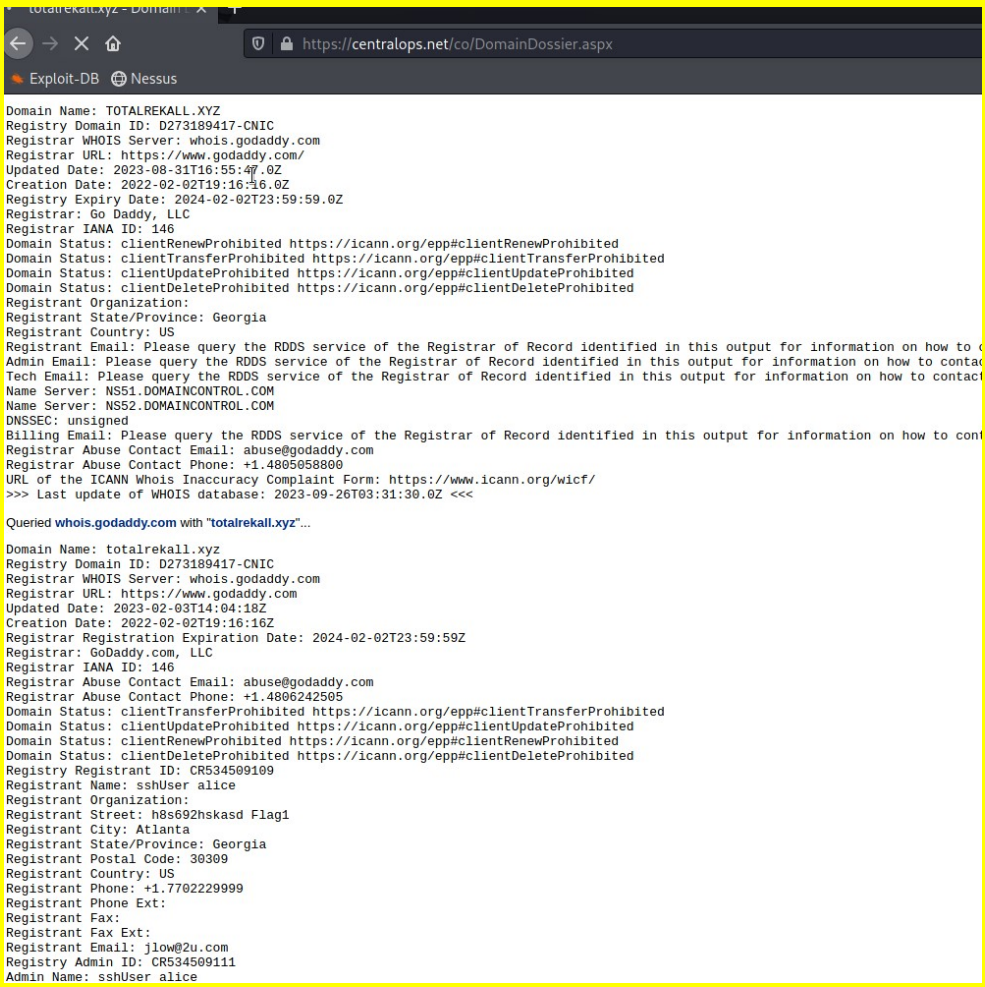
Vulnerability 11	Findings
Title	Session management - Login page
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Critical
Description	Once we login with Melina's credentials we are greeted with a "legal documents restricted area". Using Burp intruder we can test the session ID numbers. We then can see the Session ID is 087, which then allows you to access the restricted area.

Images	
Affected Hosts	http://192.168.14.35/login.php
Remediation	Use secure session management, use HTTPS, generate strong session IDs

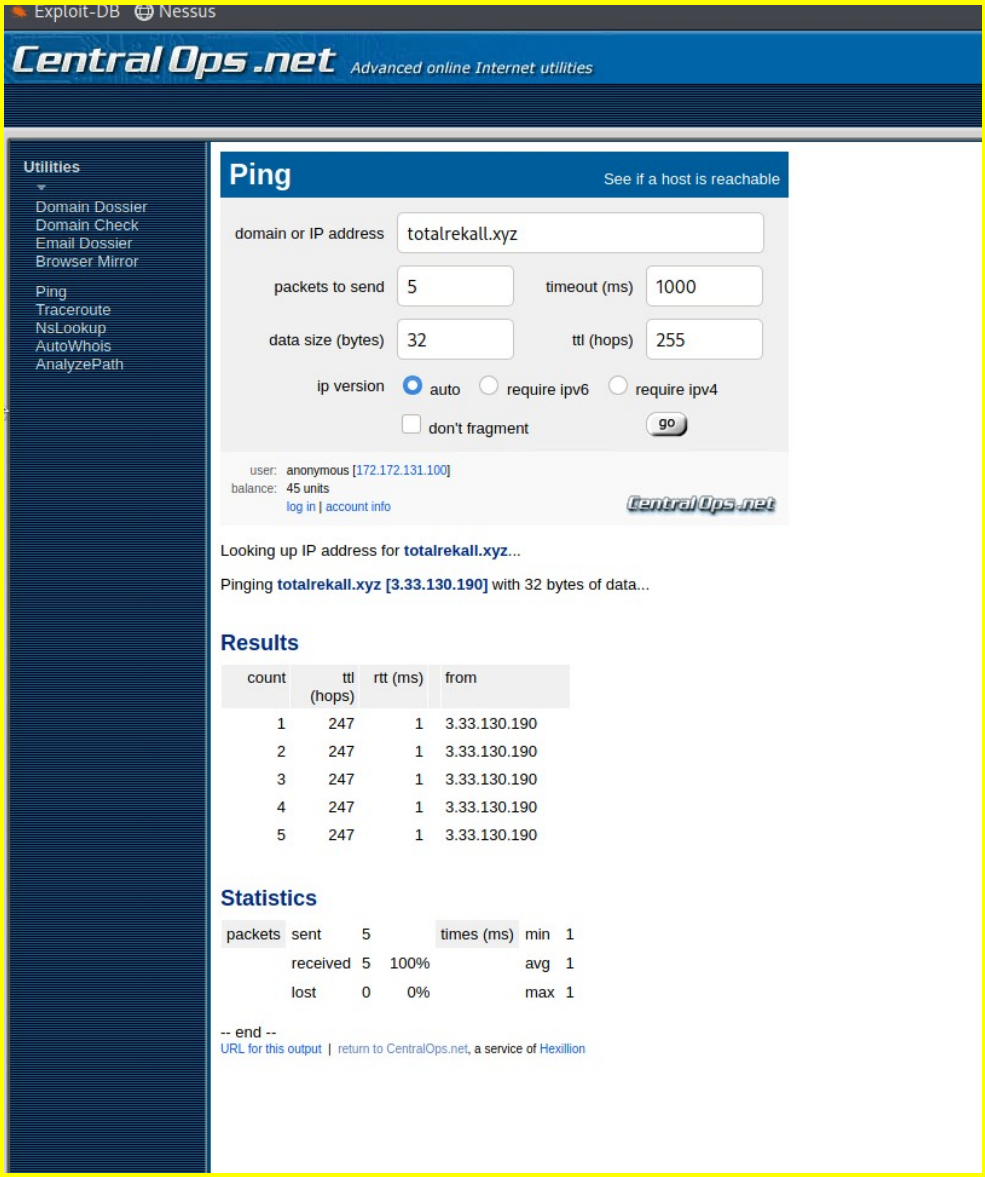
Vulnerability 12	Findings
Title	Directory Traversal - Disclaimer
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	High
Description	On the “DNS Check” page, you can use a command by piping into an ls to view all directories. There you can see a directory called old_disclaimers, which holds the disclaimer_1.txt file. Inputting this into the disclaimer.php page shows old files

Images	
Affected Hosts	http://192.168.14.35/disclaimer.php
Remediation	Input validation and sanitization, as well as using whitelists for allowed inputs

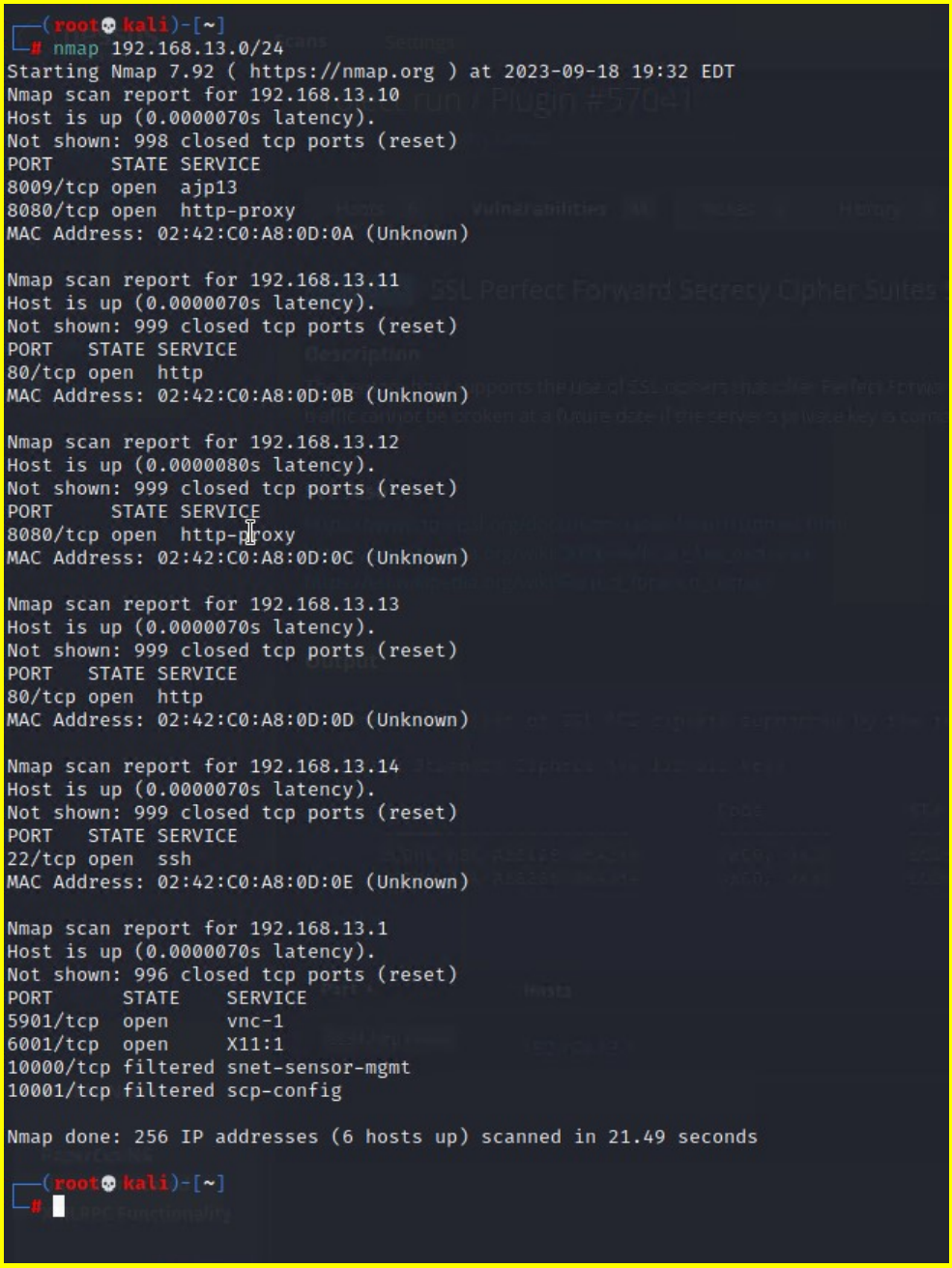
Vulnerability 13	Findings
Title	Exposed information via OSINT Domain Dossier webpage
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Informational
Description	Using publicly available sites you are able to find sensitive data that is easily exposed

Images	
Affected Hosts	totalrekall.xyz
Remediation	Limit the amount of publicly available information, especially if you have things you need to keep hidden

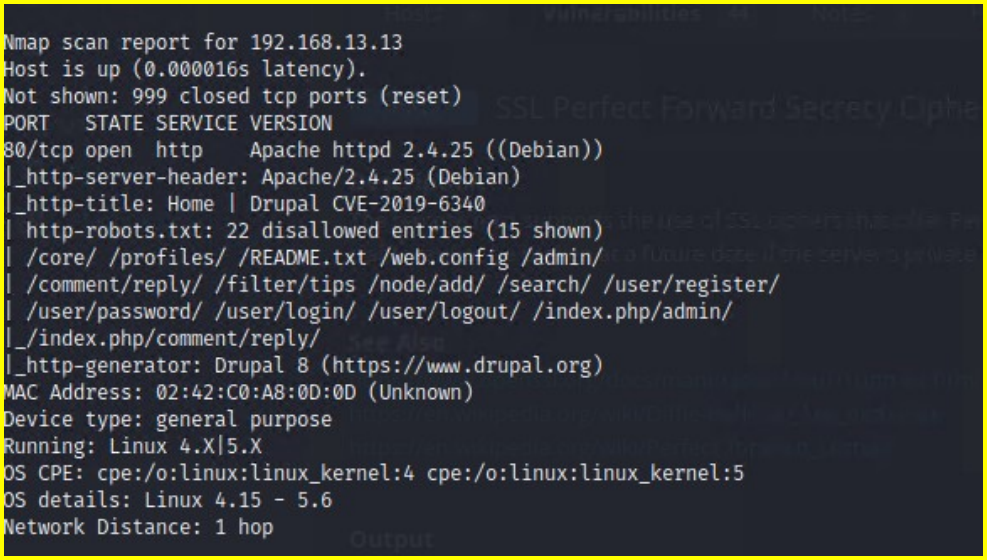
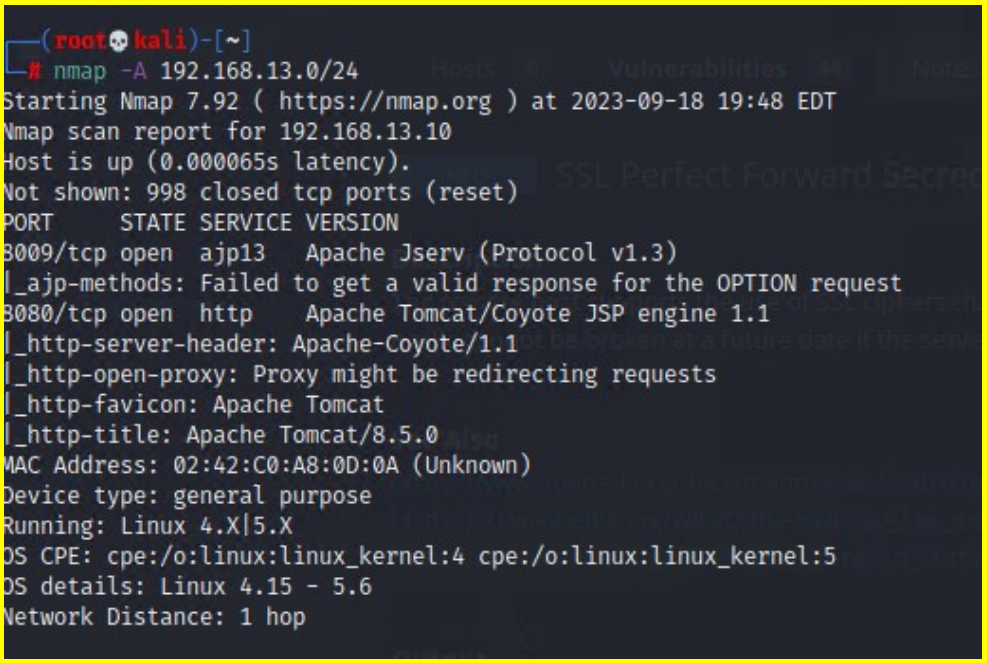
Vulnerability 14	Findings
Title	Sensitive Data
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Informational
Description	Using open source tools

Images	
Affected Hosts	totalrekall.xyz
Remediation	Configure firewall to block ICMP pings

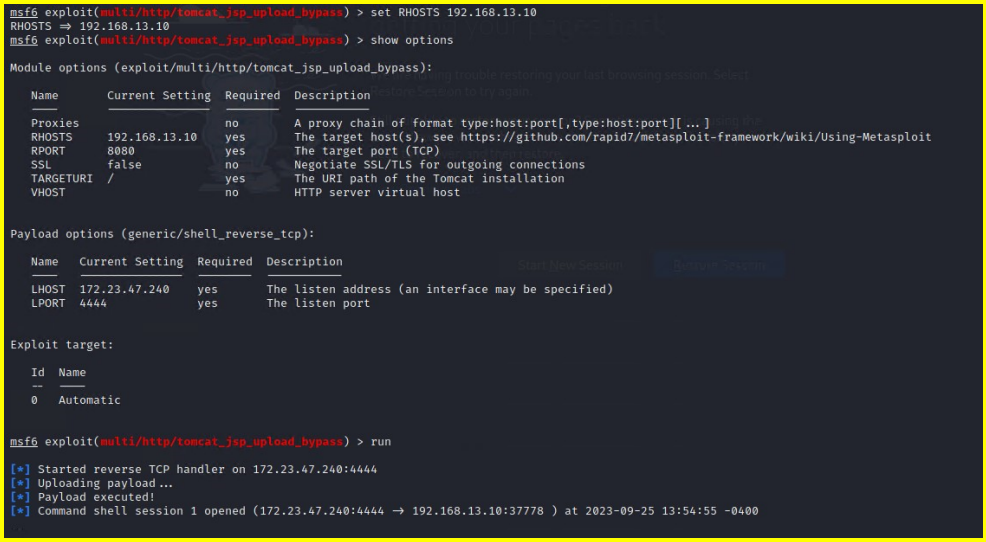
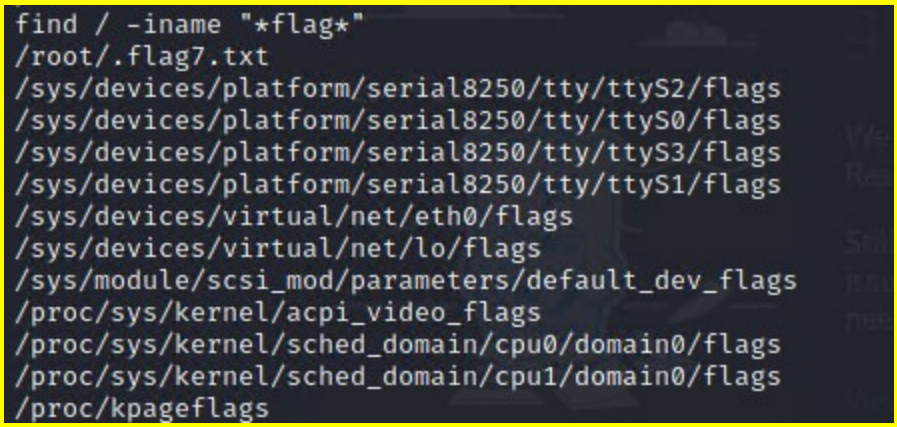
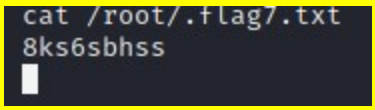
Vulnerability 15	Findings
Title	Nmap scan on Rekall subnet 192.168.13.0/24
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Informational
Description	Running an Nmap scan of the subnet brings back sensitive information

Images	
Affected Hosts	192.168.13.0/24
Remediation	Close unnecessary ports and restrict access

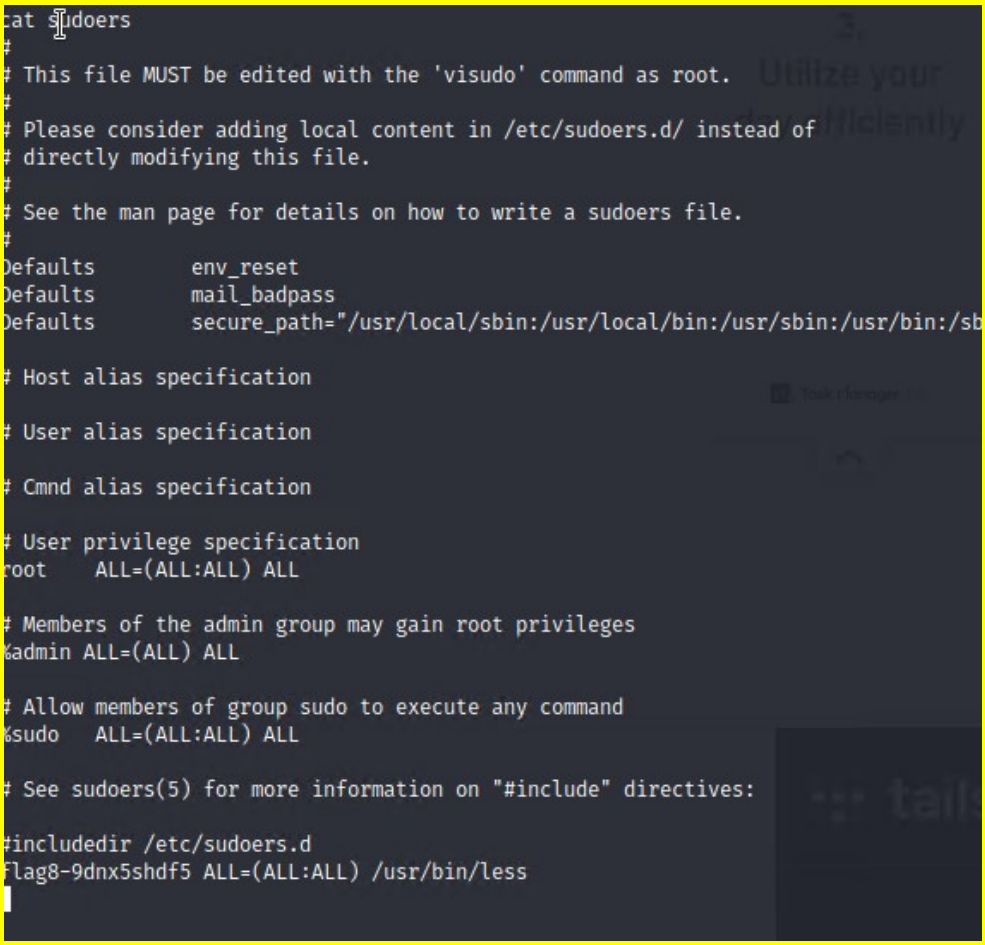
Vulnerability 16	Findings
Title	Aggressive Nmap
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Informational
Description	Using an Nmap -A scan we see that 192.168.13.13 is running Drupal, which

	can lead to a few exploits
Images	 
Affected Hosts	192.168.13.13
Remediation	Make sure Drupal is patched and up to date, ensure all passwords are strong and maybe even implement 2FA

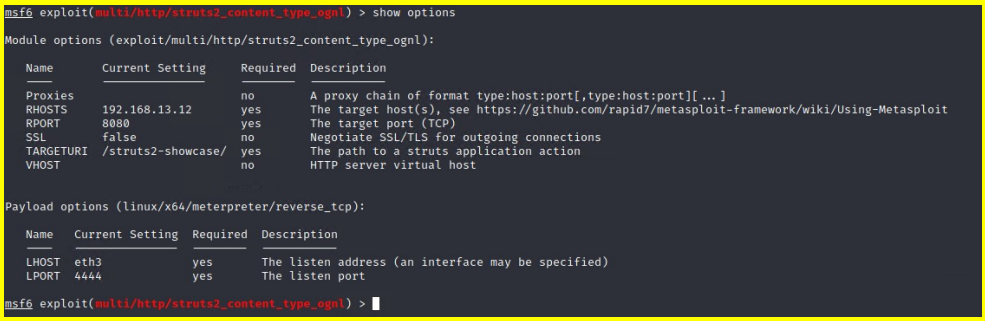
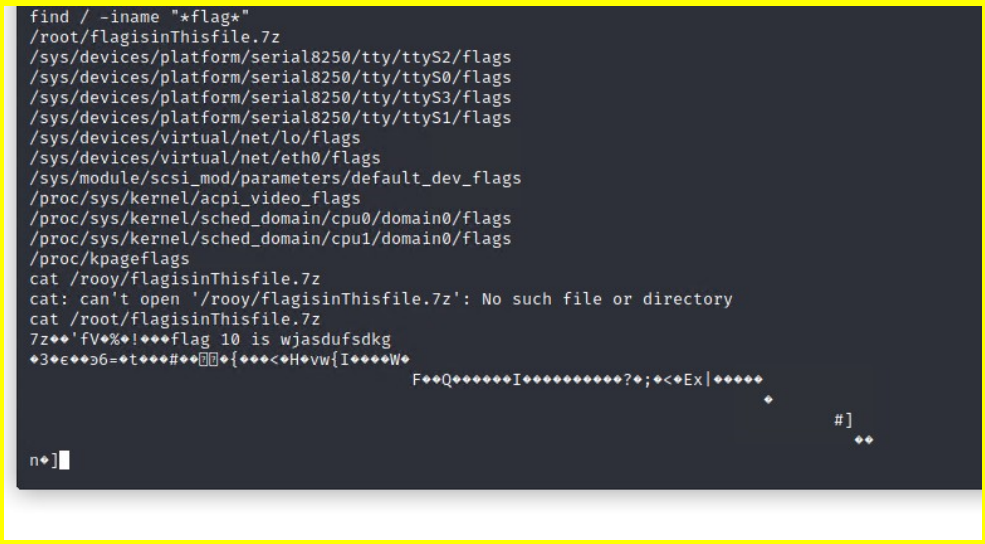
Vulnerability 17	Findings
Title	Metasploit Apache Tomcat Exploit -192.168.13.10
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	Using msf exploit multi/http/tomcat_jsp_upload_bypass on machine

	192.168.13.10, we are able to exploit a vulnerability in Apache Tomcat to gain access to the system. Once in the system we can navigate to find what we need.
Images	  
Affected Hosts	192.168.13.10
Remediation	Update Apache Tomcat to the most recent version to patch this vulnerability

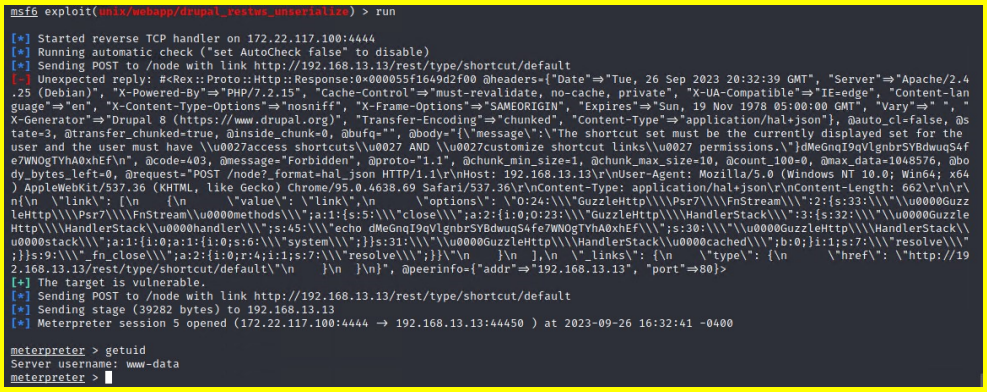
Vulnerability 18	Findings
Title	Metasploit Shellshock Exploit cat sudoers - 192.168.13.11
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	Using the exploit multi/http/apache_mod_cgi_bash_env_exec in metasploit and setting the TARGETURI to /cgi-bin/shockme.cgi you are able to access the 192.168.13.11 machine. Once inside you can cat the sudoers file

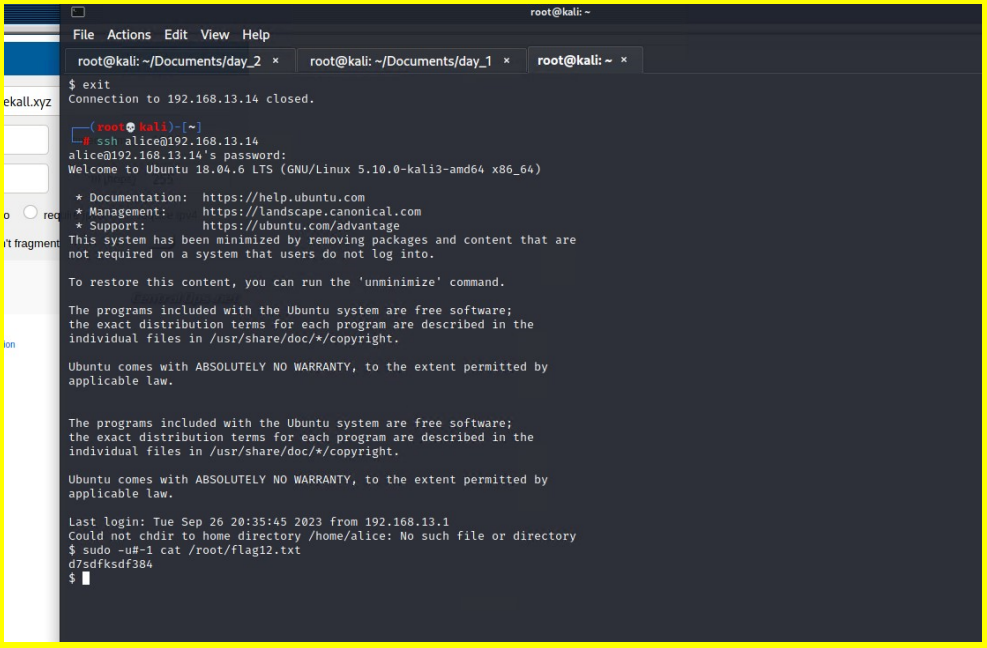
Images	
Affected Hosts	192.168.13.11
Remediation	Limit access to the sudoers file and patch system to account for the Shellshock vulnerability

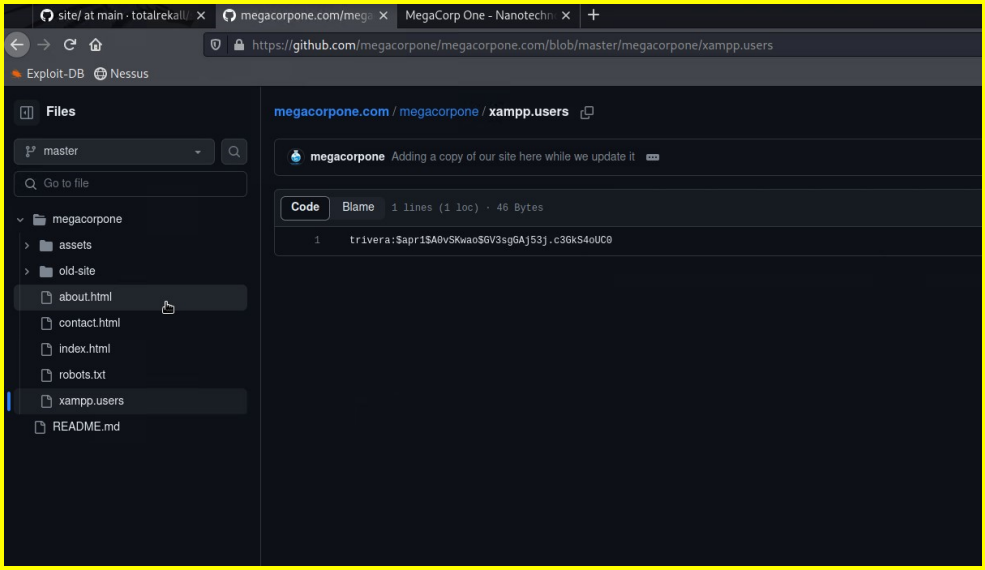
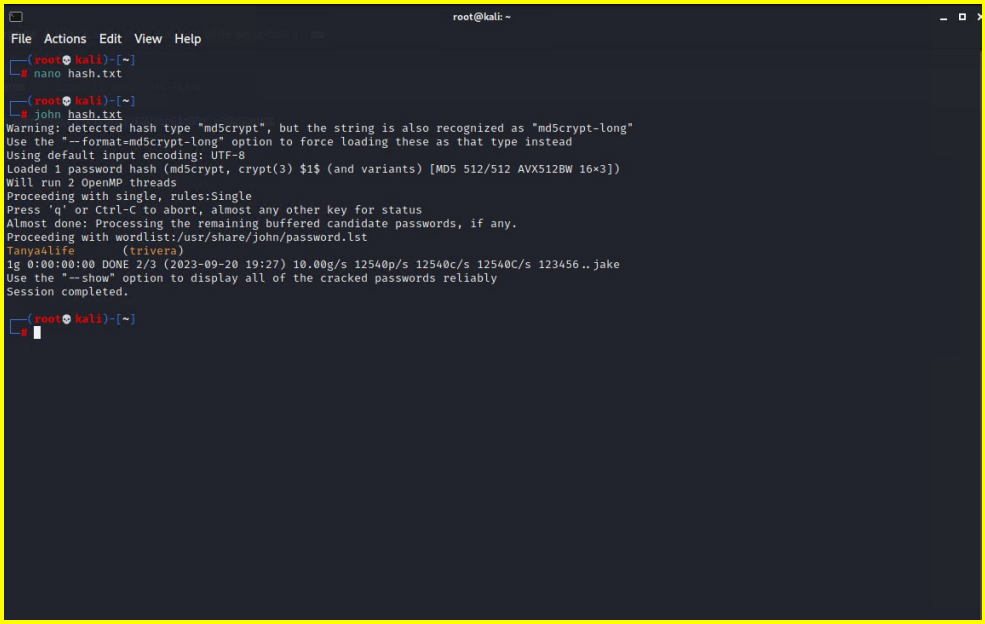
Vulnerability 19	Findings
Title	Metasploit Struts Exploit -192.168.13.12
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	Using exploit multi/http/struts2_content_type_ognl in Metasploit, you can gain access to the 192.168.13.12 machine. Once inside I ran a find command to access the file with the flag, which is in the root directory.

Images	 
Affected Hosts	192.168.13.12
Remediation	Update apache, and restrict privileges of who can and cannot access root

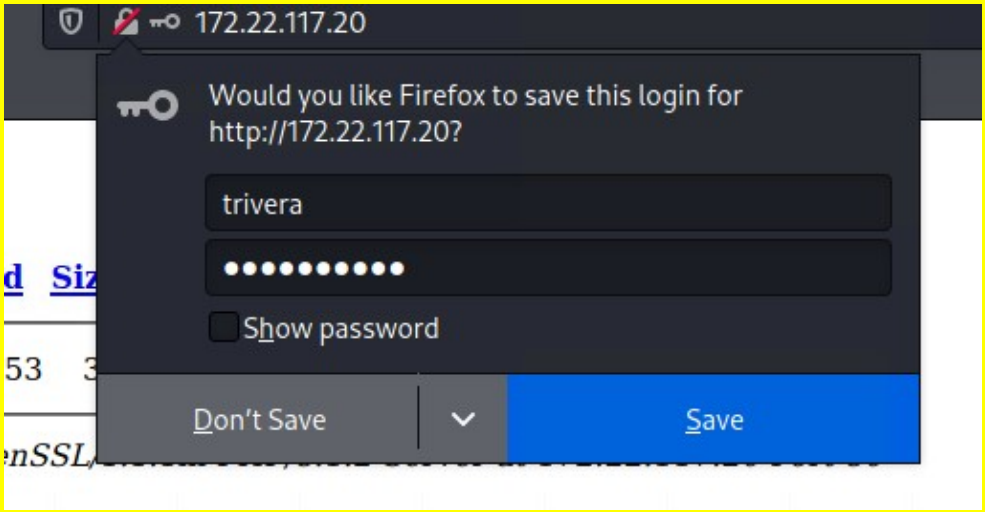
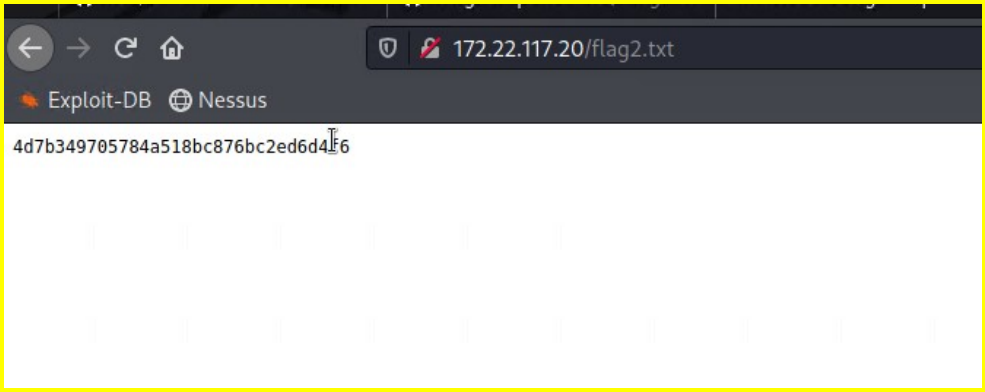
Vulnerability 20	Findings
Title	Metasploit Drupal Exploit - 192.168.13.13
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	Using the Metasploit exploit unix/webapp/drupal_restws_unserialize, we are able to access the 192.169.13.13 machine. When we run getuid we can see that we are logged in as www-data

Images	
Affected Hosts	192.168.13.13
Remediation	Make sure Drupal is running the most recent updates

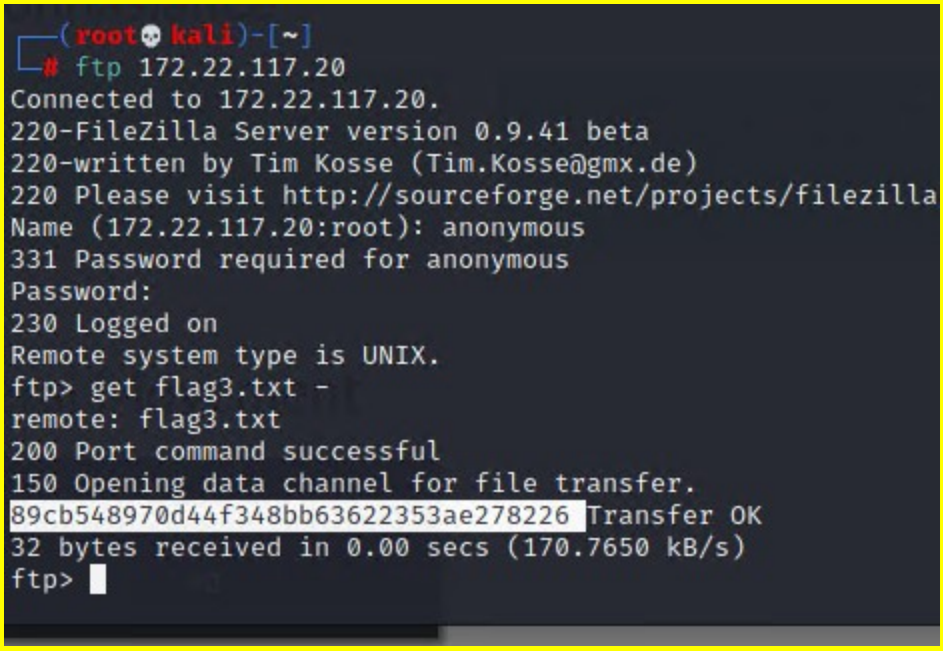
Vulnerability 21	Findings
Title	SSH into 192.164.13.14
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	Using the Alice:Alice login credentials we found in the OSINT step, we are able to login to the 192.168.13.14 machine. Escalating the user's privileges in the system we are able to access the otherwise locked flag12.txt file
Images	
Affected Hosts	192.168.13.14
Remediation	Close port 22 and institute strict password policies. Also ensure private data is not readily available through open source intelligence

Vulnerability 22	Findings
Title	GitHub Page - Access to Username/Password
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Informational
Description	When we browse the
Images	 
Affected Hosts	totalrekall.com Github site
Remediation	Remove sensitive information from publicly accessible github sites, also enforce strict password policies

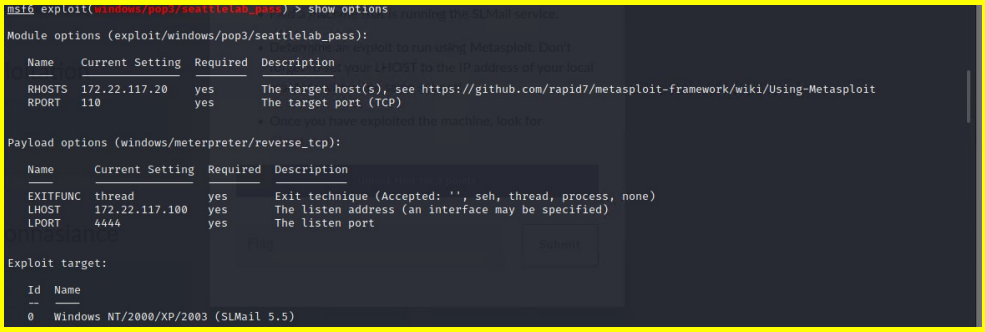
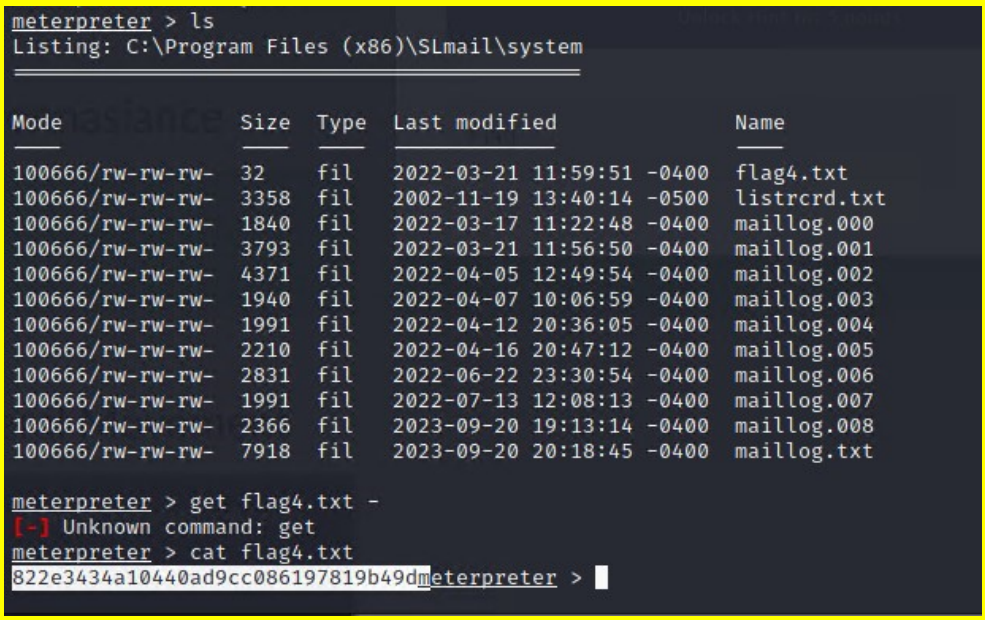
Vulnerability 23	Findings

Title	Nmap scan 172.22.117.0/24 - Using cracked username/password
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Critical
Description	When we run an Nmap scan on the subnet we can see that the .20 IP address has the http port open. Using the username and password we were able to obtain in the last vulnerability, we can access the next flag by going to 172.22.117.20 through the URL.
Images	  

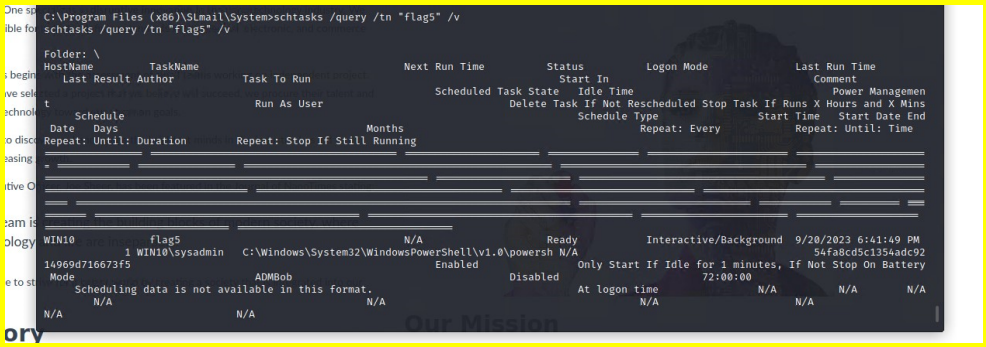
Affected Hosts	172.22.117.20
Remediation	Close the open port and require stronger password policies/2FA

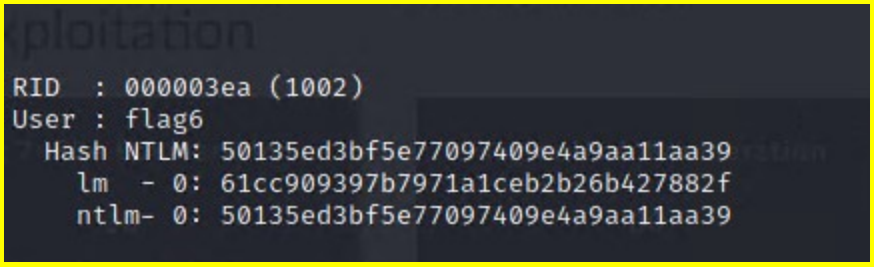
Vulnerability 24	**Findings**
Title	FTP - 172.22.117.20
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Critical
Description	Through our Nmap scan we can see that 172.22.117.20 has the FTP port open and we can also see credentials for anonymous:anonymous, which lets us right into the machine. Using the get command we can find and download the flag.
Images	 
Affected Hosts	172.22.117.20
Remediation	Close the open port and remove generic logins

Vulnerability 25	**Findings**
Title	SLMail Exploit -172.22.117.20 Port 110

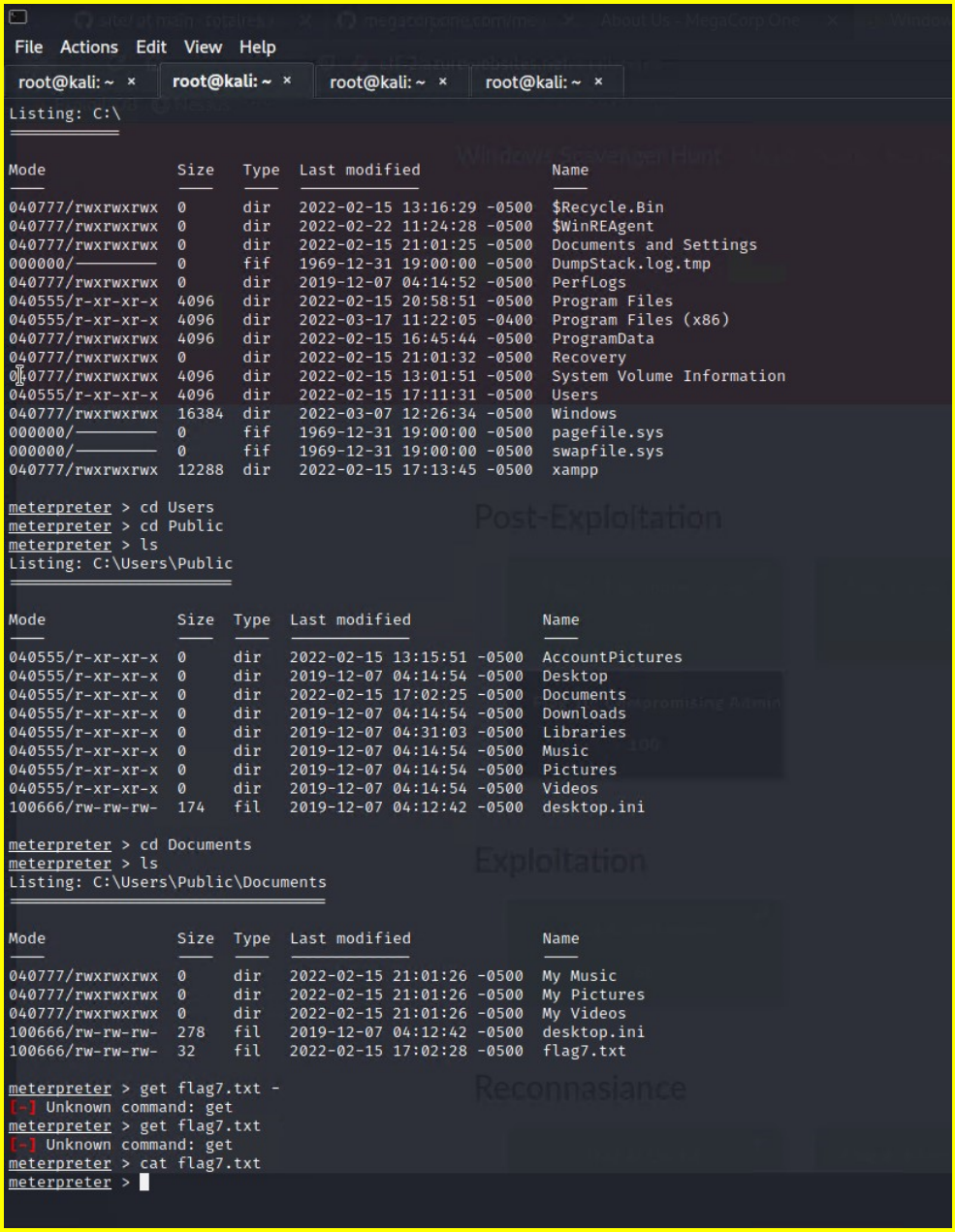
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Critical
Description	Using the Metasploit exploit windows/pop3/seattlelab_pass exploiting a vulnerability in SLMail, we are able to get into 172.22.117.20 through port 110. Once inside we can run a get command to find Flag4
Images	 
Affected Hosts	172.22.117.20
Remediation	Stop and replace SLMail service, restrict port access

Vulnerability 26	Findings
Title	Windows 10 Task Schedule
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Medium
Description	Continuing inside the 172.22.117.20 we can see all of the scheduled tasks. Using the code schtasks /query /tn “flag5” /v we can call up the task with flag5

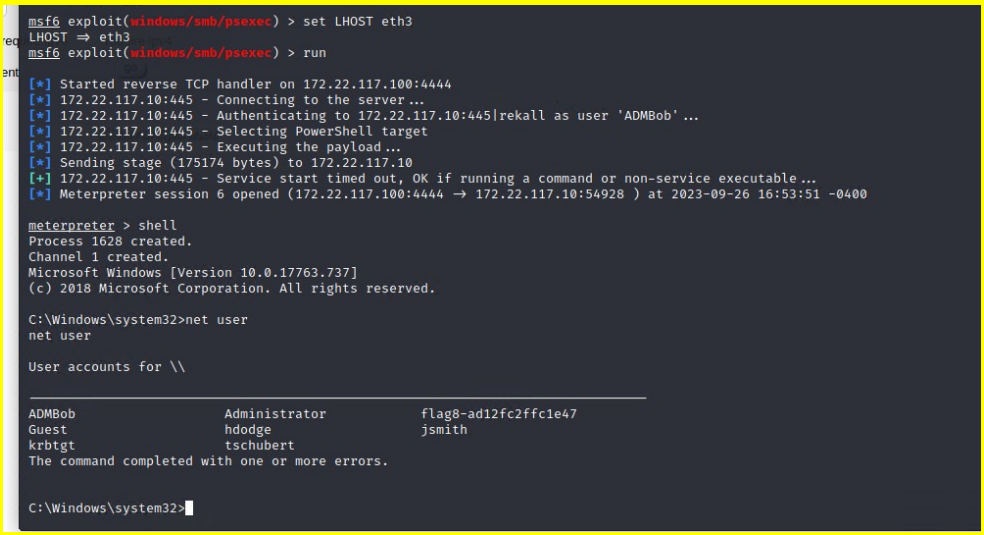
Images	
Affected Hosts	172.22.117.20
Remediation	Restrict permissions to prevent unauthorized access

Vulnerability 27	**Findings**
Title	Using Kiwi - 172.22.117.20
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	High
Description	While in the same machine from the previous two exploits, I loaded Kiwi and ran the lsadump command. We are then able to see the User Flag6 and the hashed password. Using John to crack hash6.txt we get the password Computer!
Images	 
Affected Hosts	172.22.117.20
Remediation	Require specific permissions on specific files and don't allow public access

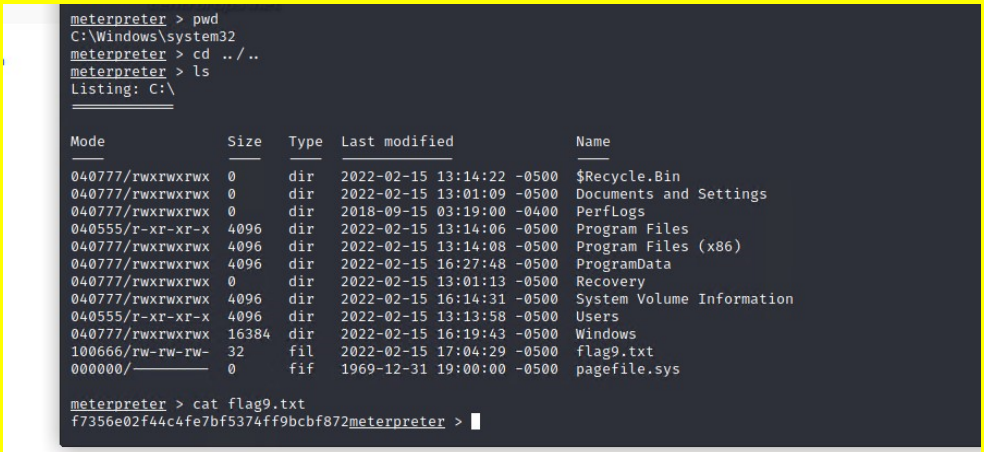
Vulnerability 28	**Findings**
Title	Accessing Documents in the Public Folder 172.22.117.20

Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Critical
Description	On the 172.22.117.20 machine that we already had access to, if we cd into the Public directory, and then into Documents we can find flag7
Images	
Affected Hosts	172.22.117.20
Remediation	Critical files should not be readily available in the Public directory, update permissions on areas that have sensitive information

Vulnerability 29	Findings

Title	Metasploit Exploit - 172.22.117.20 , using Kiwi to find ADMBob
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Critical
Description	Load Kiwi in the Meterpreter session of 172.22.117.20 and run the command lsadump::cache to find ADMBob as well as the hashed password. Cracking the password we can then run the windows/smb/psexec exploit to gain access to the 172.22.117.10 machine
Images	
Affected Hosts	172.22.117.10
Remediation	Set privileges for specific data

Vulnerability 30	Findings
Title	Exploiting the 172.22.117.10 Machine
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Critical
Description	Using the machine that we recently exploited into with ADMBob's credentials, we can search the system to find the file for flag9.txt

Images	
Affected Hosts	172.22.117.10
Remediation	Manage permissions of who can access C:\ as well as ensure data is in correct secure areas

Vulnerability 31	Findings
Title	Accessing Admin Hashed Password
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Critical
Description	Running kiwi on the 172.22.117.10 machine and inputting the dcsync_ntlm administrator command we are able to discover login credentials for the administrator user
Images	
Affected Hosts	172.22.117.10
Remediation	Restrict permissions to only allow specific users to have access to sensitive information, clean data regularly to ensure that there are no leaks like this