Cybersecurity

Penetration Test Report

Rekall Corporation

Penetration Test Report

BC Security

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	BC Security
Contact Name	Benjamin Chavez
Contact Title	Head Pentester

Document History

Version	Date	Author(s)	Comments
001	03/03/2025	Benjamin Chavez	Started Outline
002	03/05/2025	Benjamin Chavez	Added Screenshots from days 1 and 2
003	03/07/2025	Benjamin Chavez	Added more detail and day 3 info
004	03/09/2025	Benjamin Chavez	Revisions and edits
005	03/10/2025	Benjamin Chavez	Revisions and edits
006	03/12/2025	Benjamin Chavez	Final report

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.

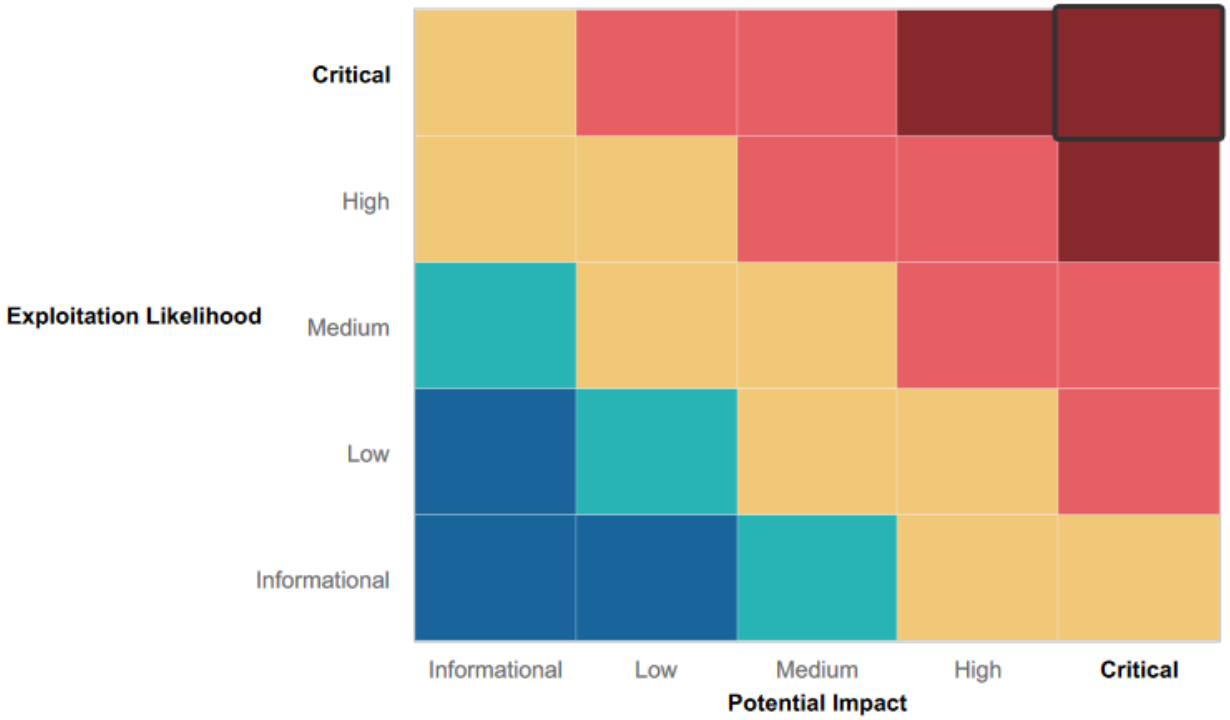
Executive Summary of Findings

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.

- Rekall Corp has a plan and strategy to fend off and mitigate DDoS attacks to ensure the network stays online.
    - This is not only good for day to day operations, but prevents harm to TotalRekall's reputation.
        - CIA Triad seems to be taken into account.
- Network utilizes tools such as Metasploit and Nmap.
    - These tools can be used to prevent unauthorized access to the network.
- Site not vulnerable to base level SQL injection strategies.
    - Some fields on the website are not vulnerable to basic <script></script> Javascript exploits, needed to at least use Input Validation or even XSS (Cross-Site Scripting)
- Hired an outside company to conduct this pentest, checking for vulnerabilities to be corrected and mitigate any outside attacks on company data.

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 website is highly susceptible to script injections and other high level risks associated with webpages.
    - Most fields on the website are vulnerable to some form of XSS or Javascript injection.
        - SQL payload injections yield compromising information, such as NAME or '1=1'' exploits.
    - Admin credentials can be easily viewed on the page's source code by viewing the tab in developer tools.
    - Can also view confidential info by viewing the robots.txt file.
- The web server itself uses an outdated version of Apache which is vulnerable to multiple exploits, critical to update this to prevent and outside threats.
    - As well the SLMail server is vulnerable to exploits which allow access to shell.
    - An attacker can access unencrypted password hashes that allow those hashes to be cracked, thus having an attacker escalate privileges.
        - These attacks are possible due to TotalRekall.xyz credentials and other compromising info being accessible with IP lookups and github repositories.
    - Open ports can be found leading to unauthorized access.

Executive Summary

Over the course of BC Security's Pentest of Rekall Corp and all the servers associated with it, the team was able to successfully identify and discover numerous vulnerabilities, including multiple critical vulnerabilities that could have a potentially expensive and catastrophic impact on not only finance and day to day operations of Rekall Corp, but also reputational damage as well. After going over scope and knowing at what level our pentesters were able to do in terms of permissions, we were given the go ahead to conduct a full pentest that includes the ability to infiltrate assets, escalate privileges, and live of the land of the Total Rekall Corp and totalrekall.xyz.

On day 1, BC Security (henceforth referred to as BCS) tested Total Rekall's Web Applications first. We did what we think is a thorough look into vulnerabilities. We discovered the website is vulnerable to Local File Inclusion, XSS Stored and Reflected, Command Injection, as well as SQL Injections. Very alarmingly there are admin credentials stored in HTTP source code, being able to be viewed in developer tools, which needs to be addressed as soon as humanly possible to avoid data breaches. As well as this the robot.txt is easily viewable on the main website.

BCS was also able to find on the web publicly a github repository, which again, alarmingly contained a username and a hashed password which we were able to easily crack, giving us access to other parts of the system. There was also open source data exposed and viewable using OSINT. Other publicly viewable info includes the certificates located on crt.sh, which needs to be rectified.

Once BCS divulged into the Linux systems, our team was able to discover 5 different IP addresses and their ports, and out of these found services that we discovered could be exploitable. One of the hosts we discovered was running the Drupal service, and using found and cracked credentials were able to gain access within shells to gather more data to escalate our privileges. Using a Shellshock exploit we were able to discover a vulnerability that was able to put us into root, as well as being able to access Sudo.

On our final days we divulged our efforts into the Windows OS systems, and doing more scans using our tools we were able to determine there was an easily accessible FTP server, and an SLMail service on Port 110 that should be closed as soon as possible. Using credentials we found on the systems we were able to exploit the open Port on 110 and gain access onto the system, again finding more credentials, more hashes, and being able to further gain access into the environment until we were able to become a SYSTEM user.

While this is a brief summary by BCS, these vulnerabilities on their own could be enough to do some serious damage to Total Rekall, both to your assets and reputation. BCS has included below a detailed summary and recommended remediations of many critical, high, medium, and low vulnerabilities you can now use to mitigate potential damage from malicious actors looking to cause damage.

Summary Vulnerability Overview

Vulnerability	Severity
Local File Inclusion	Critical
Command Injection	Critical
SQL Injection	Critical
Admin Credentials Stored in HTML Source	Critical
GitHub Username and Password Hash	Critical
Nmap Scan	Critical
Nmap Scan Finding Visible IP's	Critical
Shellshock on Web Server (Port 80)	Critical
User Credential Exposure	Critical
Apache Struts (CVE-2017-5638)	Critical
Drupal (CVE-2019-6340)	Critical
SLMail Port 110 Exploited with Metasploit (SeattleMail)	Critical
Privilege Escalation	Critical
Kiwi Password Hashes	Critical
Open Source Exposed Data	High
Aggressive Nmap Scan	High
Apache Struts Discovery with Nessus	High
Port 21 FTP Open	High
Windows Task Scheduler	High
Sensitive Data Exposure in Public Data	High
XSS Reflected	Medium
XSS Stored	Medium
Certificate Searched on crt.sh	Low
Robots.txt	Low

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

Scan Type	Total
Hosts	172.22.117.20 172.22.117.10 192.168.13.10 192.168.13.11 192.168.13.12 192.168.13.13 192.168.13.14 192.168.14.35

Ports	21 22 80 110 8080

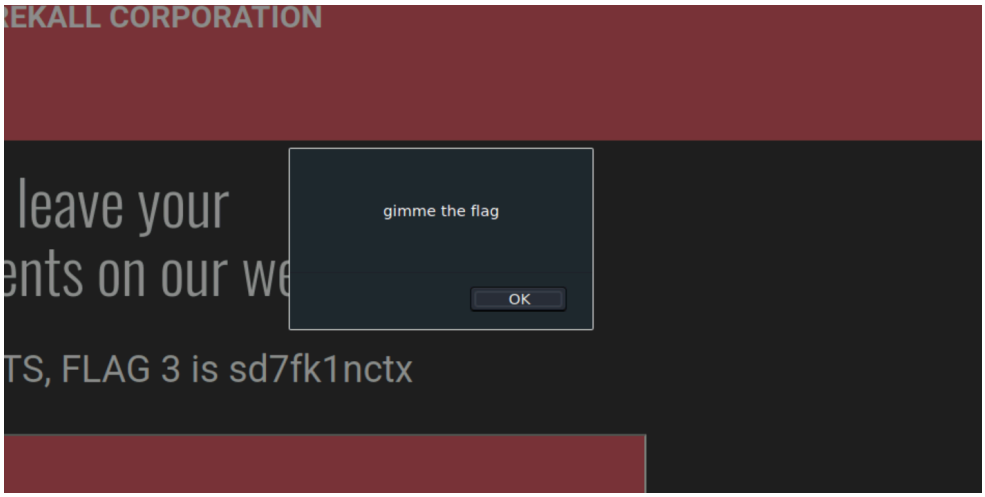
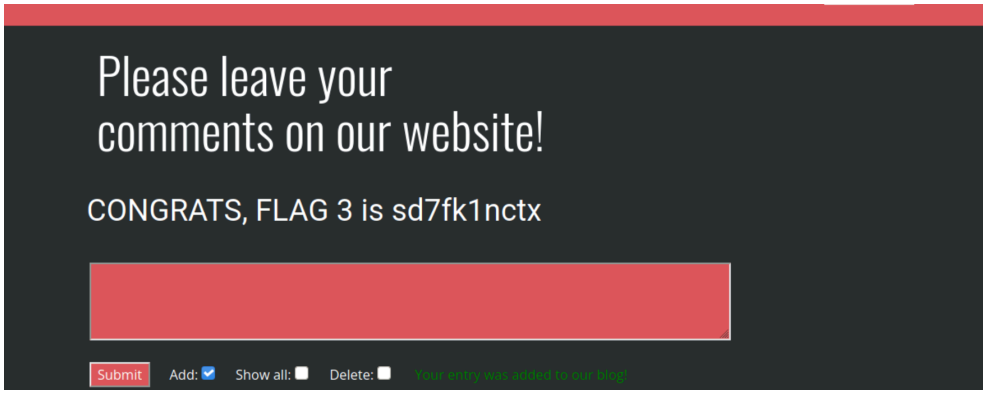
Exploitation Risk	Total
Critical	14
High	6
Medium	2
Low	2

Vulnerability Findings

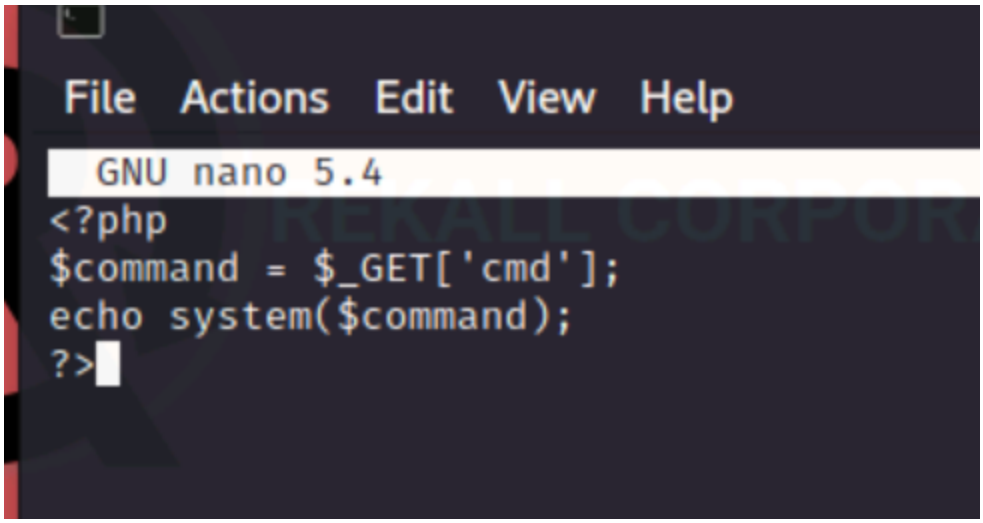
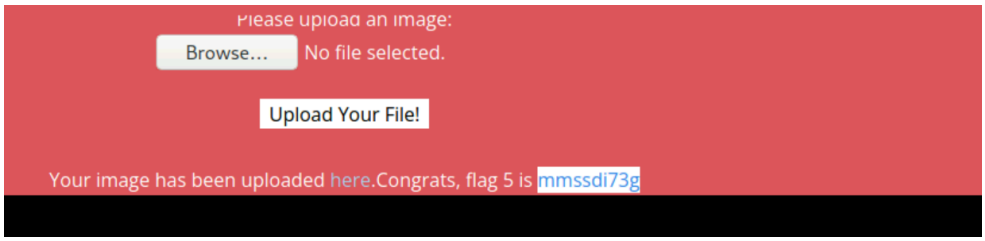
Vulnerability 1	Findings
Title	XSS Reflected
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Medium
Description	Malicious script was successfully used on the Rekall site. Script that was used was <script>alert(“gimme the flag”)</script>
Images	

	
Affected Hosts	192.168.14.35
Remediation	Implement some form of Input Validation

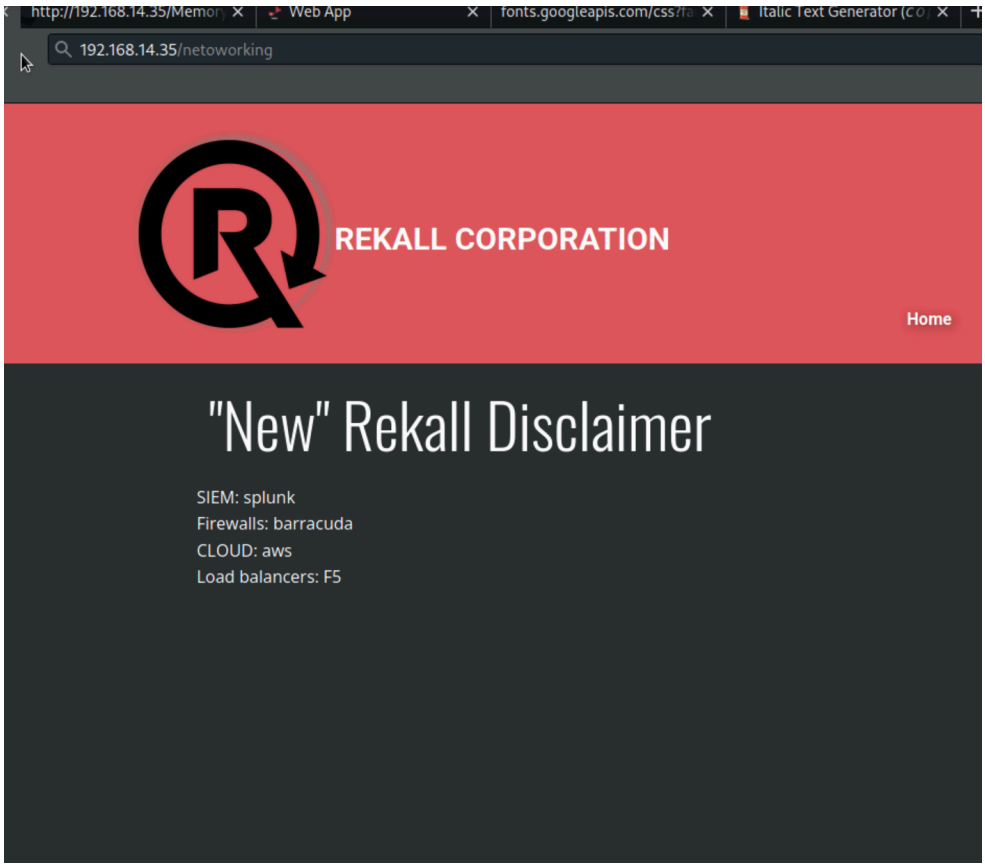
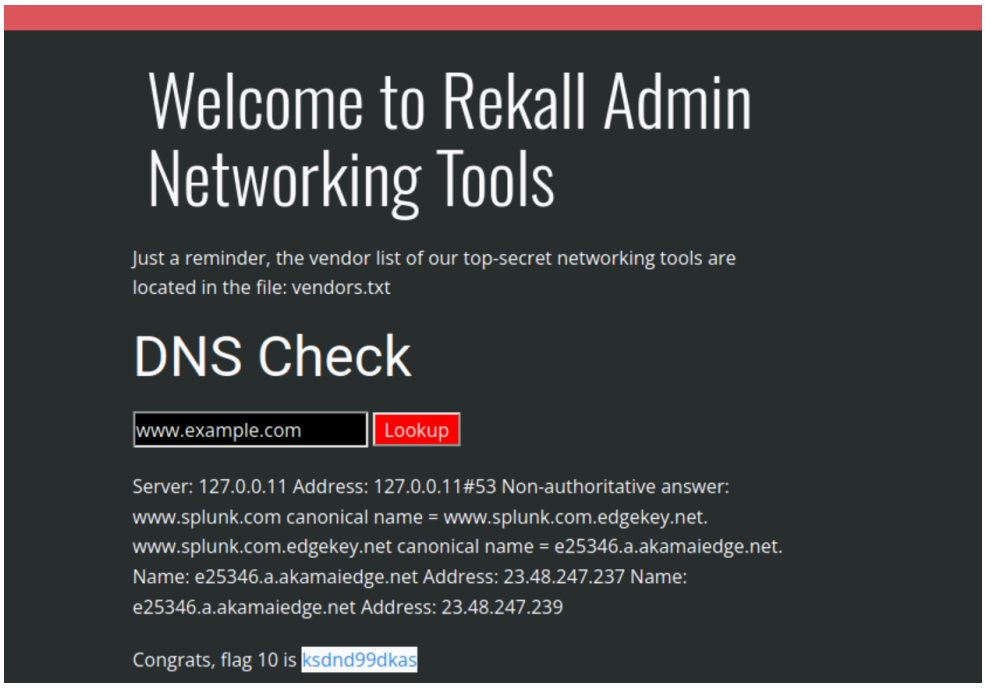
Vulnerability 2	**Findings**
Title	XSS Stored
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Medium
Description	When accessing the comment field, I entered <script>alert(“gimme the flag”)</script>

Images	 
Affected Hosts	192.168.14.35
Remediation	Implement XSS protection to disallow injection of any malicious script code.

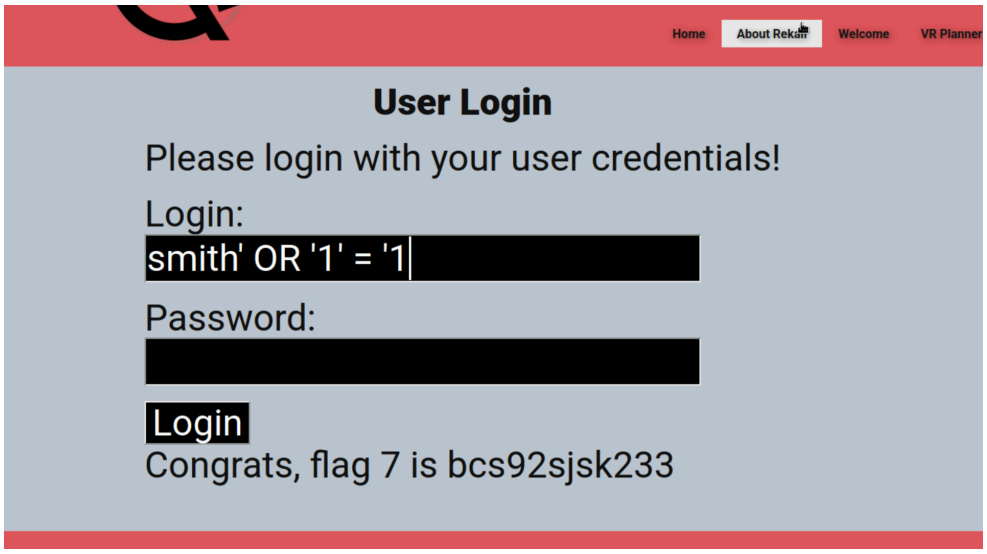
Vulnerability 3	Findings
Title	Local File Inclusion
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Critical
Description	Local file inclusion successfully executed, uploaded .php file onto the VR planner web page.

Images	 
Affected Hosts	192.168.14.35
Remediation	Prevent file paths from being able to be appended to directly.

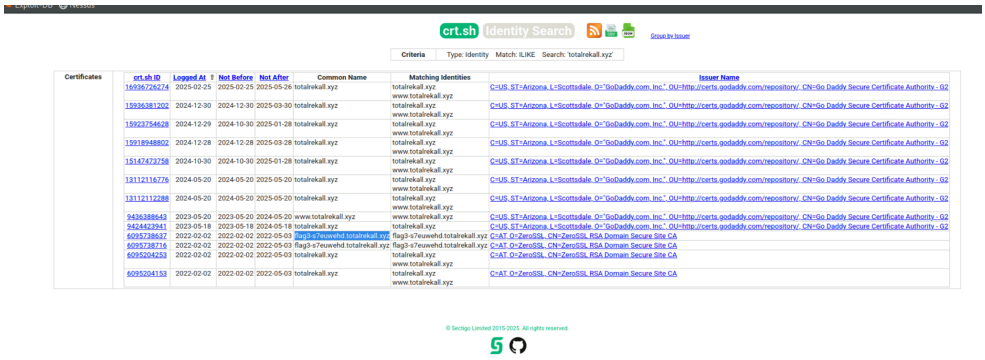
Vulnerability 4	Findings
Title	Command Injection
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Critical
Description	From /Networking.php, was able to navigate to disclaimer.php?page=vendors.txt After that I was able to input the phrase “splunk” in the field where it asks for a DNS check.

Images	 
Affected Hosts	192.168.14.35
Remediation	Input validation against misuse of input fields.

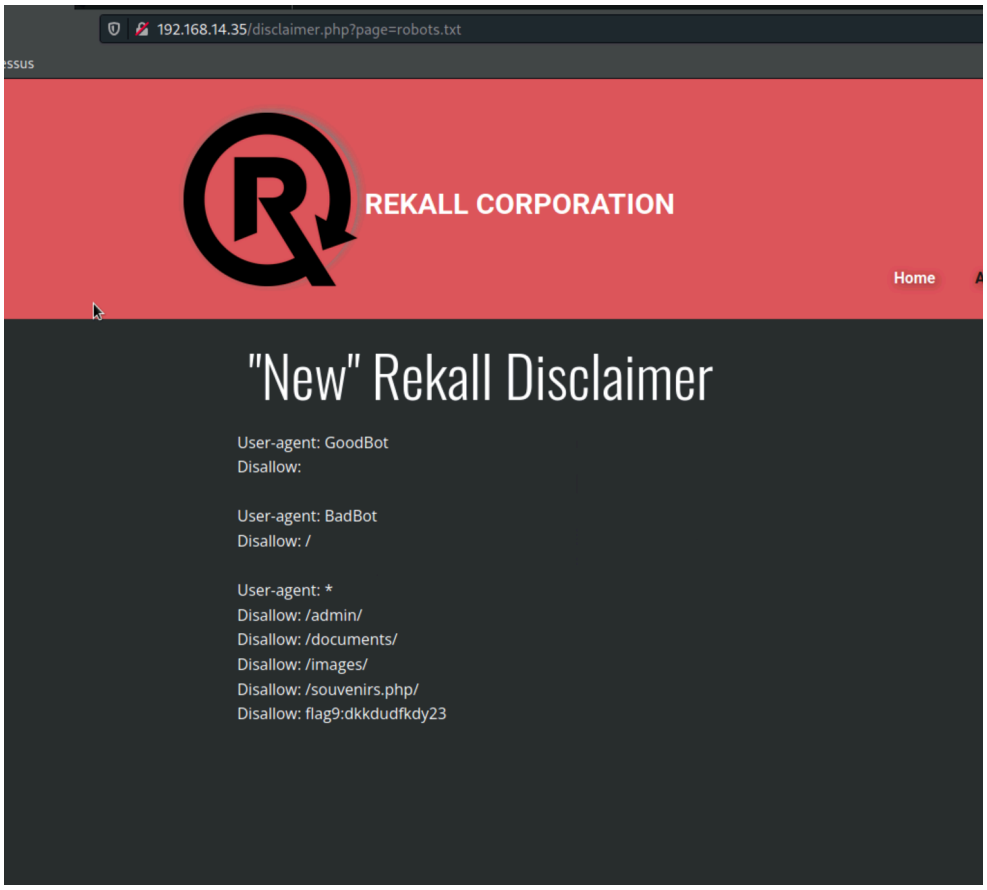
Vulnerability 5	**Findings**
Title	SQL Injection

Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Critical
Description	Was able to exploit the login field on the /login.php page by inputting (smith' OR '1'='1') payload into the password toolbar.
Images	
Affected Hosts	192.168.14.35
Remediation	Change the ability of the web page not using character escaping.

Vulnerability 6	**Findings**
Title	Certificate Searched on crt.sh
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Low
Description	On crt.sh did a search of totalrekall.xyz, leading to flag 3 on a stored certificate.

Images	
Affected Hosts	34.102.136.180
Remediation	Remedy the data you don't want shown publicly on crt.sh.

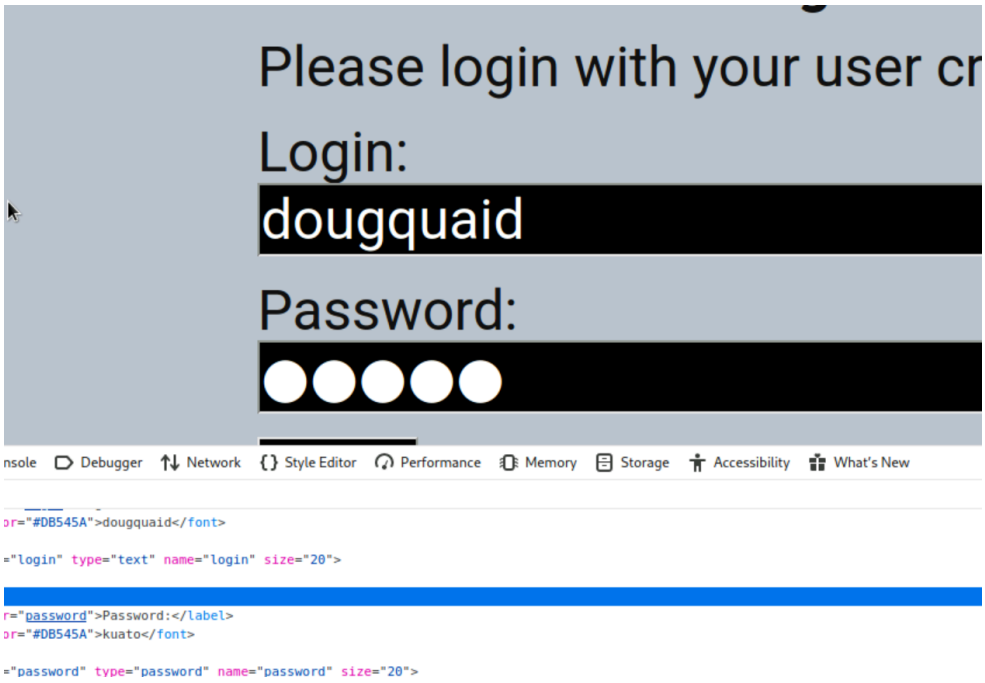
Vulnerability 7	Findings
Title	Robots.txt
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Low
Description	Added robots.txt to the end of the domain.

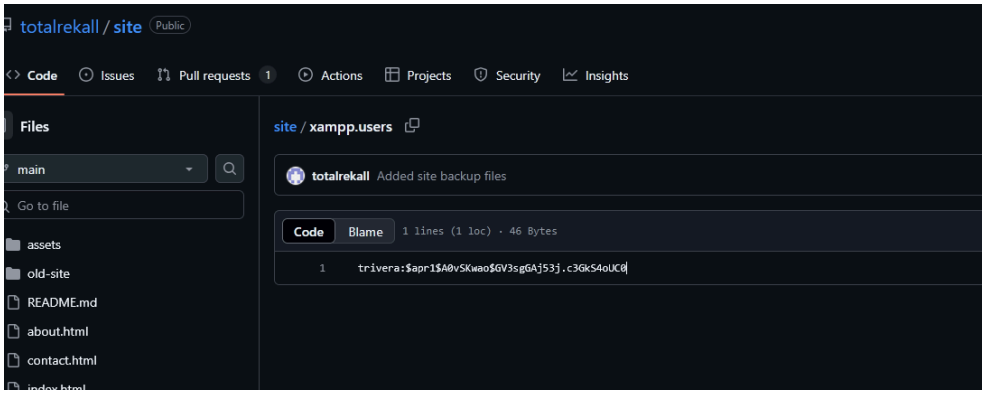
Images	
Affected Hosts	192.168.14.35
Remediation	Use noindex for pages that shouldn't be accessed by the public.

Vulnerability 8	Findings
Title	Open Source Exposed Data
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	High
Description	Viewed the who.is data for totalrekall.xyz

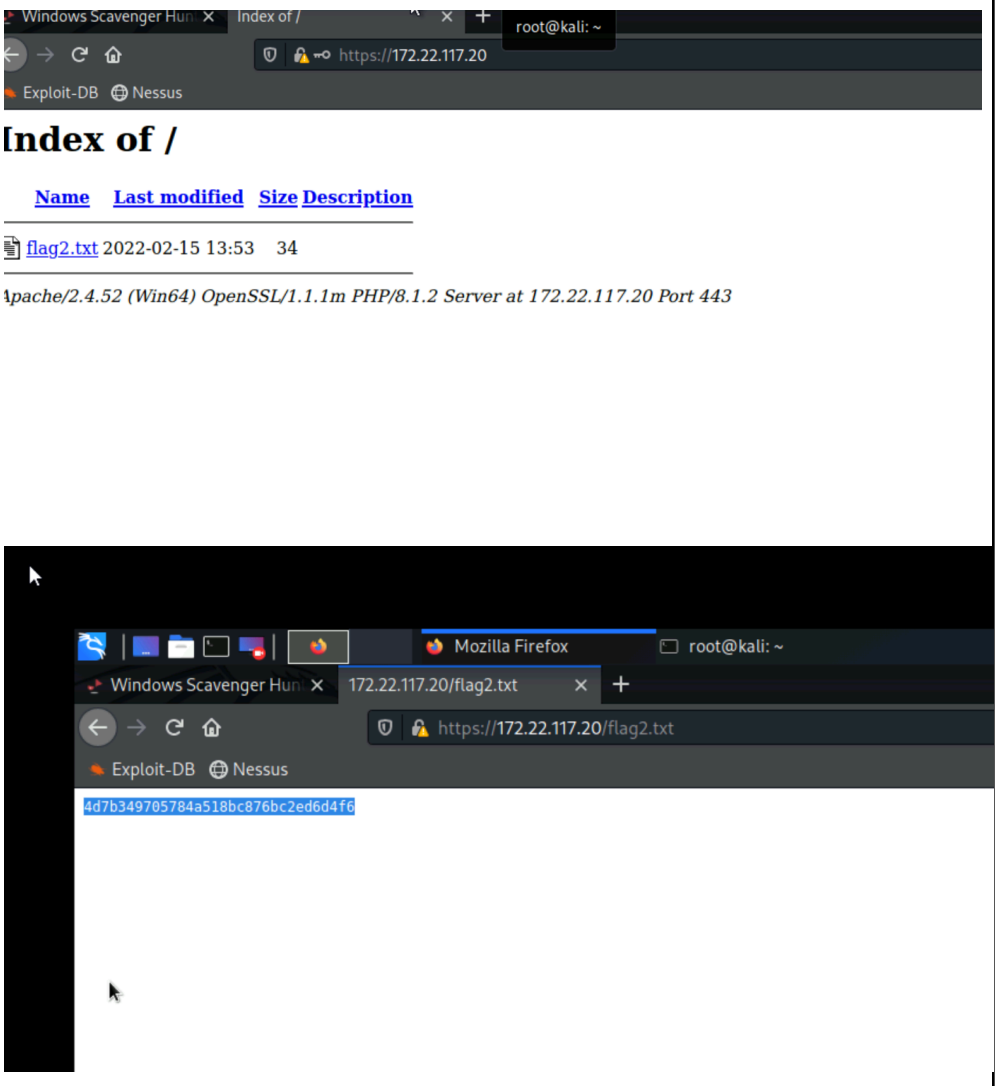
Images	Queried whois.godaddy.com with "totalrekall.xyz"... Domain Name: totalrekall.xyz Registry Domain ID: D273189417-CNIC Registrar WHOIS Server: whois.godaddy.com Registrar URL: https://www.godaddy.com Updated Date: 2025-02-03T15:00:39Z Creation Date: 2022-02-02T19:16:16Z Registrar Registration Expiration Date: 2026-02-02T23:59:59Z 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: jlow@2u.com Registry Tech ID: CR534509110 Tech Name: sshUser alice Tech Organization: Tech Street: h8s692hskasd Flag1 Tech City: Atlanta Tech State/Province: Georgia Tech Postal Code: 30309 Tech Country: US Tech Phone: +1.7702229999
Affected Hosts	N/A
Remediation	Just like the crt.sh page, do a cleanup of all publicly accessible data.

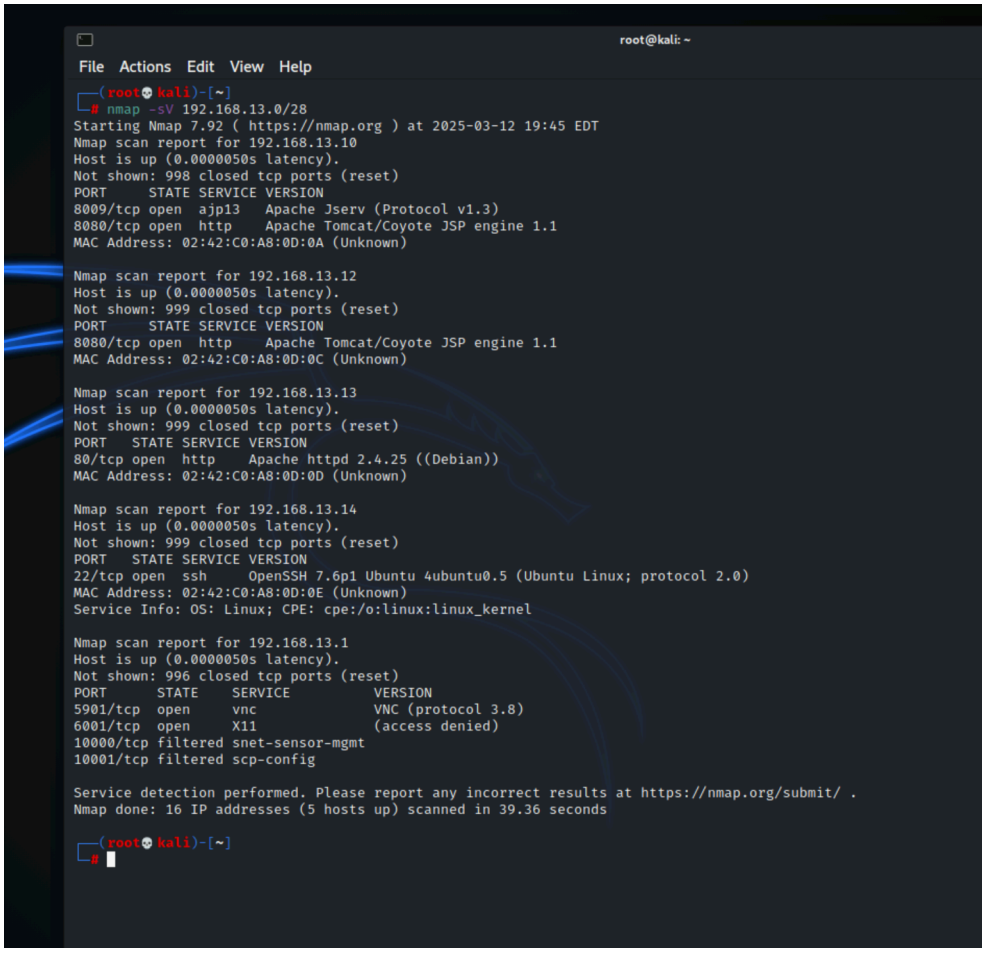
Vulnerability 9	Findings
Title	Admin Credentials Stored in HTML Source
Type (Web app / Linux OS / WIndows OS)	Web Page
Risk Rating	Critical
Description	With Developer tools, was able to gather admin credentials and login to totalrekall.xyz using easily found admin credentials.

Images	
Affected Hosts	192.168.14.35
Remediation	Do a full cleanup of the source code and do everything possible to eliminate the possibility of finding admin creds from a browser.

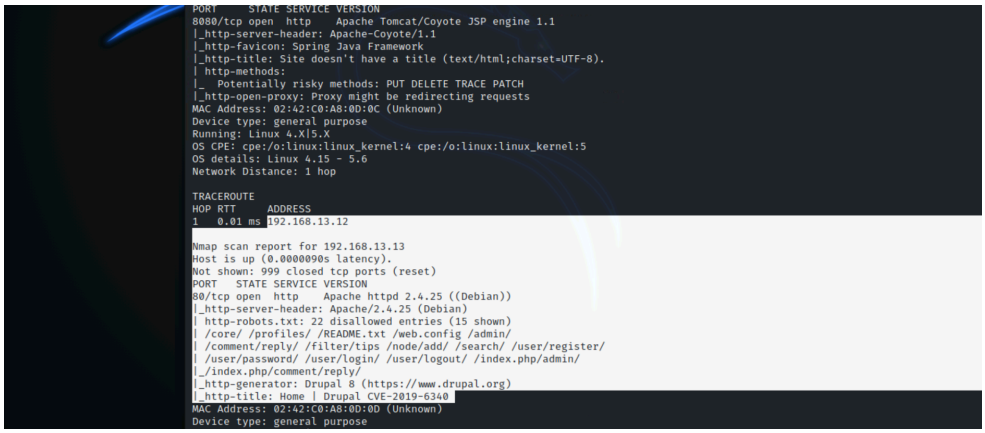
Vulnerability 10	**Findings**
Title	GitHub Username and Password Hash
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Critical
Description	Found a users credentials in the GitHub repo, was able to crack it using John in the Kali Box
Images	
Affected Hosts	NA

Remediation	Remove the repo off of the public web and GitHub.

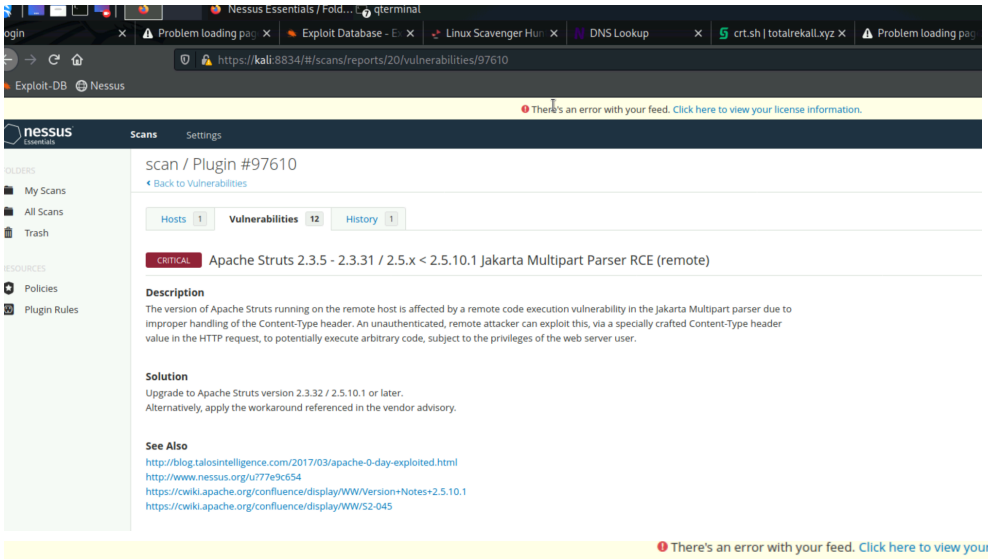
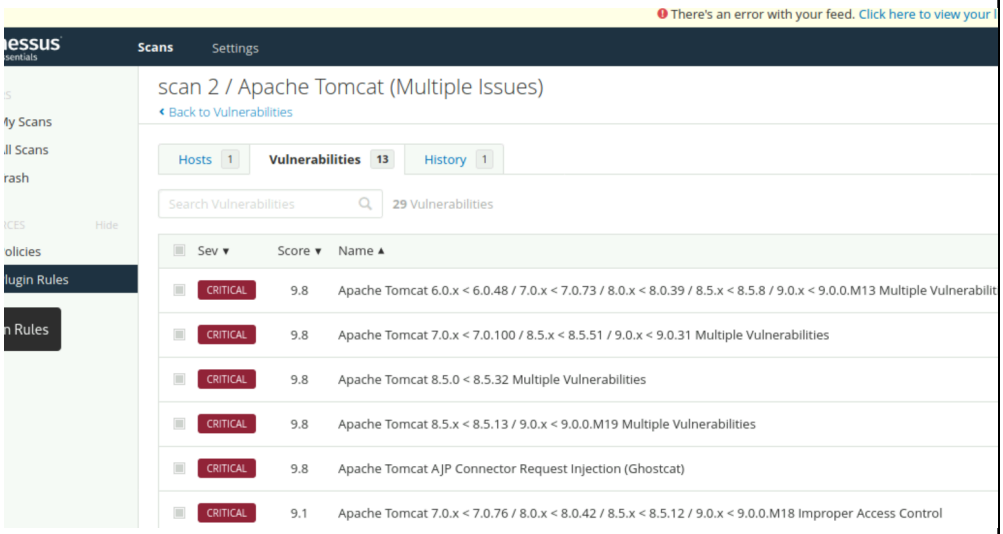
Vulnerability 11	Findings
Title	Nmap Scan
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Critical
Description	Using the cracked password hash from John the Ripper, was able to do a Nmap scan of 172.22.117.0/24. After this was able to find 117.22.117.20 had port 80 open, and was able to open the IP in a web browser, and log in with the (trivera:Tanya4Life) to log in, finding info.
Images	
Affected Hosts	172.22.117.20
Remediation	Same remediation as above, stronger password policies.

Vulnerability 12	Findings
Title	Nmap Scan finding visible IP's
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	After using "nmap -sV 192.168.13.0/28", discovered that there are 5 hosts visible with exposed IP addresses.
Images	
Affected Hosts	192.168.13.10 192.168.13.12 192.168.13.13 192.168.13.14 192.168.13.11
Remediation	Implement unauthorized users being able to scan IP's

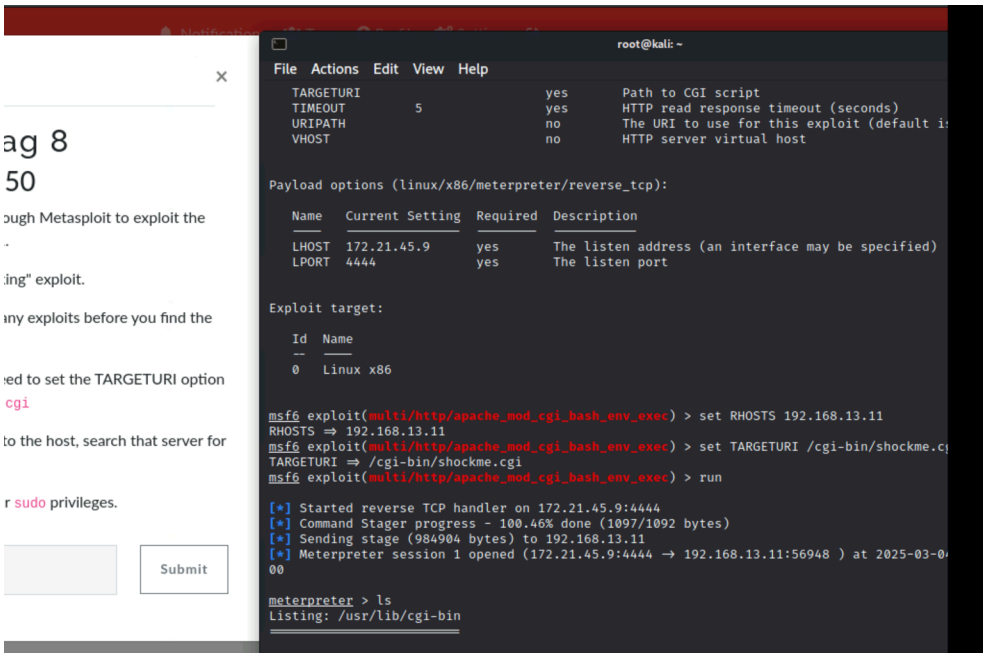
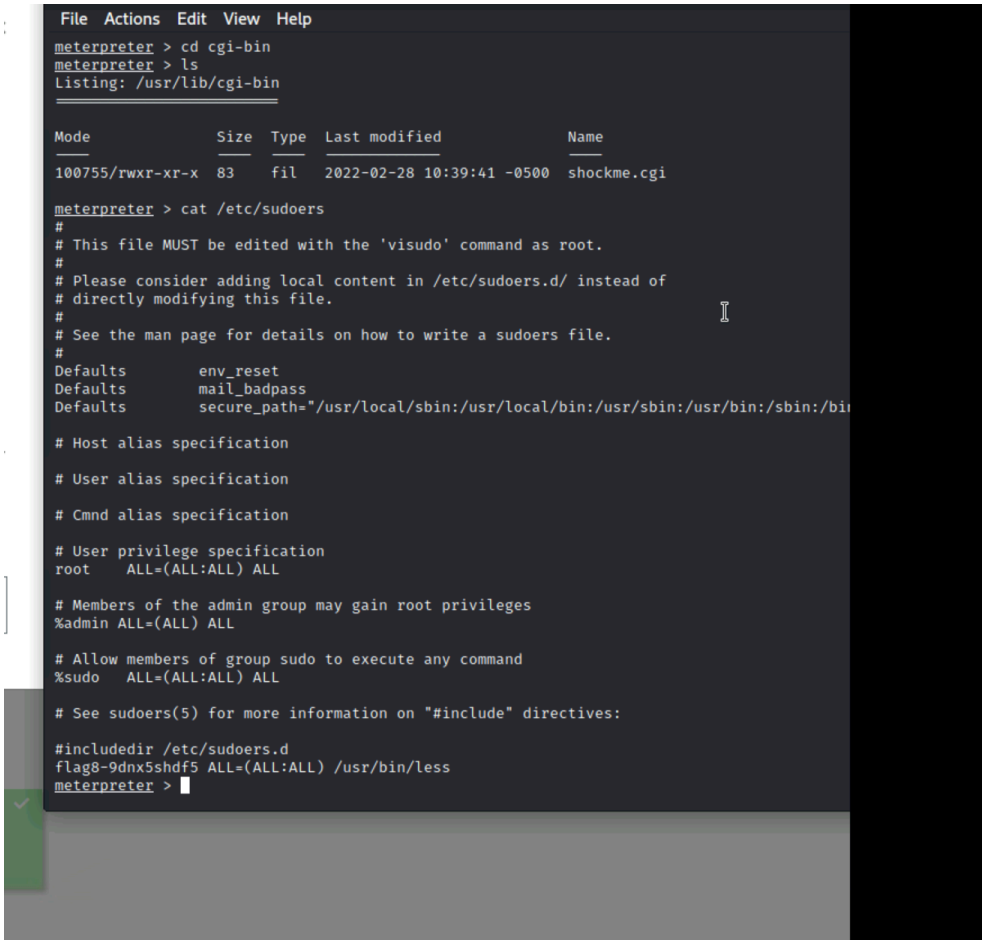
Vulnerability 13	Findings
Title	Aggressive Nmap Scan (Drupal)

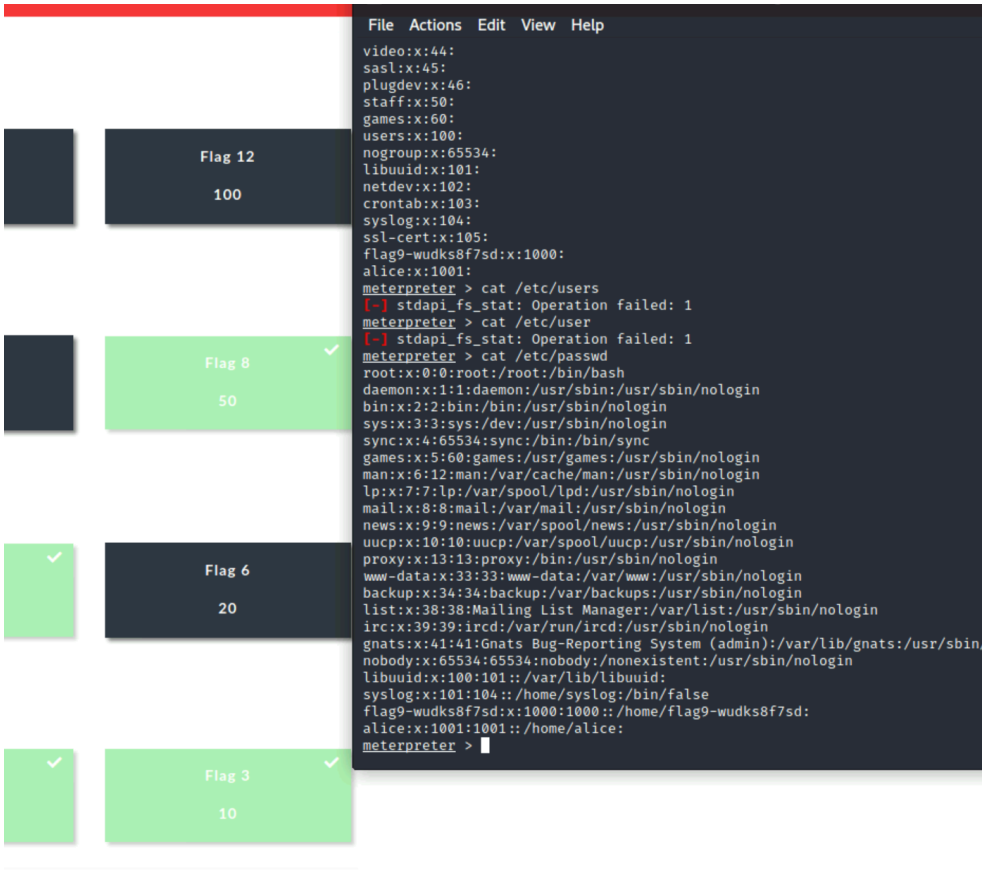
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	High
Description	After running “nmap -sV -A 192.168.13.0/28”, I discovered the host that was running Drupal.
Images	
Affected Hosts	192.178.13.12
Remediation	For aggressive Nmap scans, block the scan, implement a way to return misleading info if possible.

Vulnerability 14	Findings
Title	Apache Struts Discovery with Nessus
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	High
Description	After running a Nessus scan on the vulnerable 192.168.13.12 IP it revealed a critical Apache Struts vulnerability. Also found the info to exploit this in Metasploit.

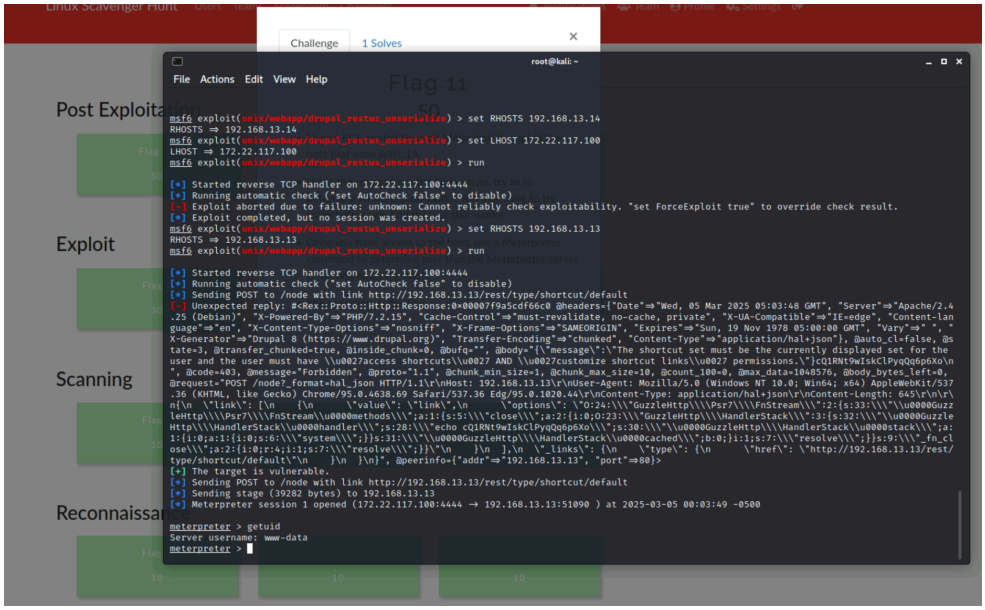
Images	 
Affected Hosts	192.168.13.12
Remediation	Update your Apache and conduct regular updates.

Vulnerability 15	Findings
Title	Shellshock on Web Server (Port 80)
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	Used the info I gained from the Nessus scan to use exploit/multi/http/apache_mod_cgi_bah_env_exec to gain access to the shell using Shellshock to find vulnerable info in the host.

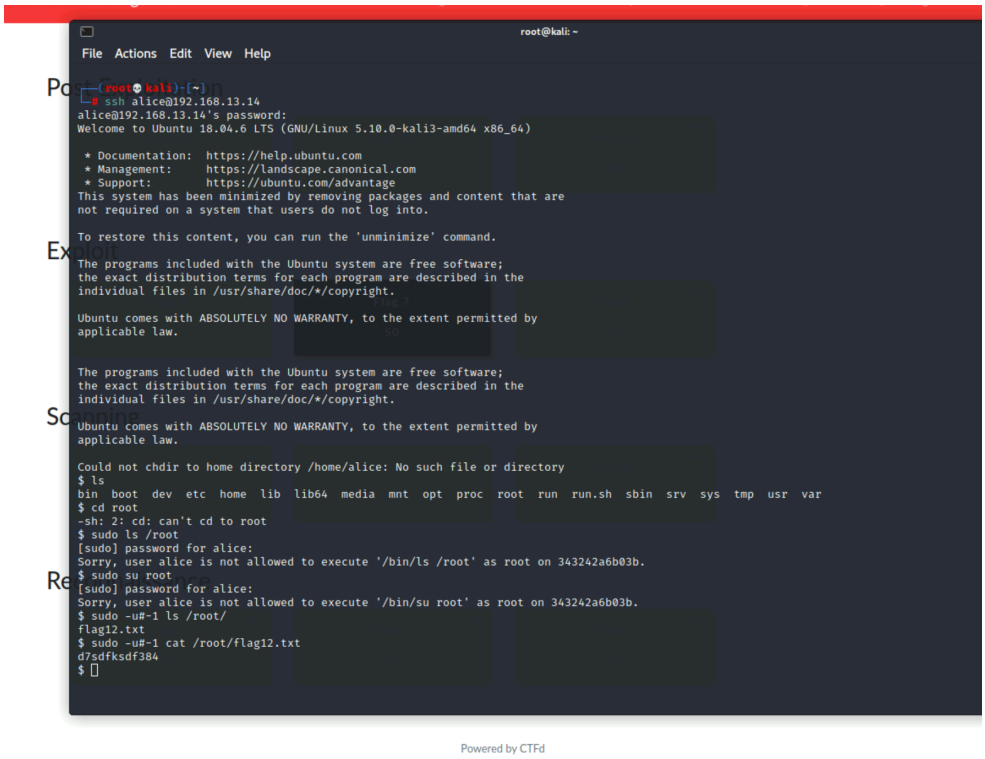
Images	 
Affected Hosts	192.168.13.11
Remediation	Eliminate the possibility of an attacker being able to use this Shellshock exploit to gain entrance into this host in Metasploit, or eliminate shockme.cgi altogether. Also edit the sudo privs for all accounts to limit ALL to just root user.

Vulnerability 16	Findings
Title	User Credential Exposure
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	After gaining access to the shell, snooped around in the /etc/ files going to /etc/passwd and seeing users and their info if I were to dig deeper, Alice info will be coming up later.
Images	
Affected Hosts	192.168.13.11
Remediation	Preventing shell access thus gaining the ability to look into the /etc/ files, again this goes back to remediating Apache and Shellshock.

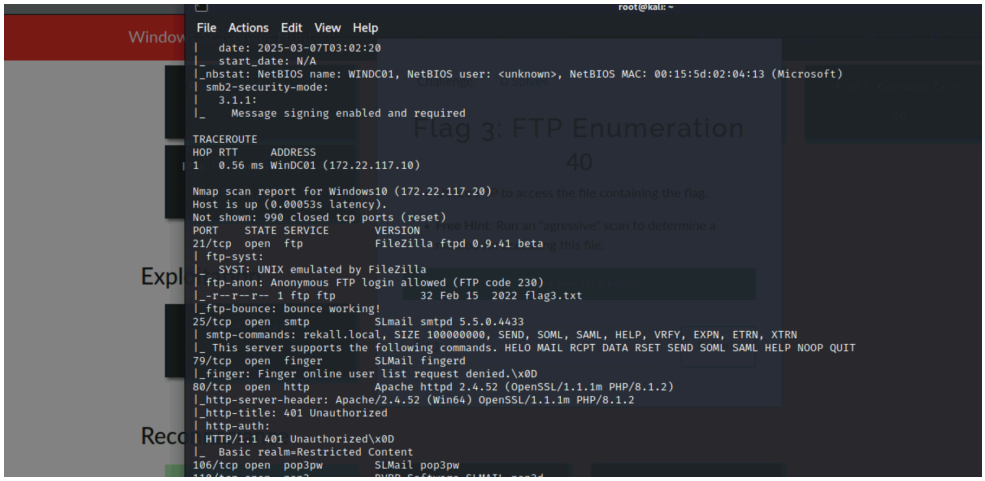
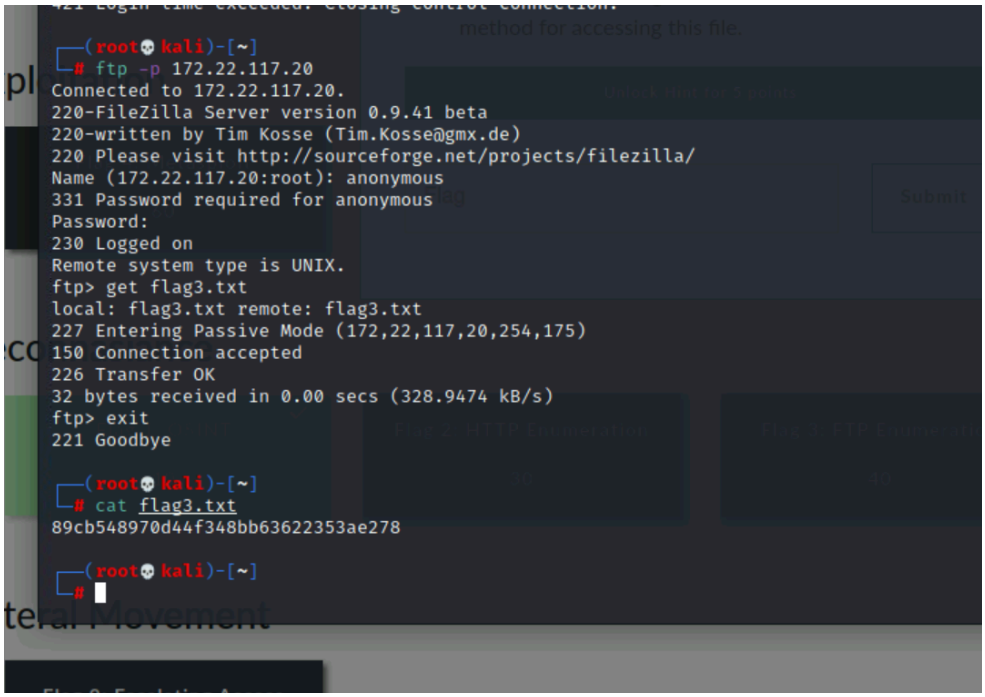
Vulnerability 17	Findings
Title	Drupal (CVE-2019-6340)
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical

Description	Used exploit/unix/webapp/drupal_restws_unserialize in Metasploit to gain access to the server hosting Drupal and find the server username using getuid once in the meterpreter shell.
Images	
Affected Hosts	192.168.13.13
Remediation	If Drupal is needed go back to giving fake info with an aggressive Nmap scan, if Drupal is not needed eliminate it from the system altogether.

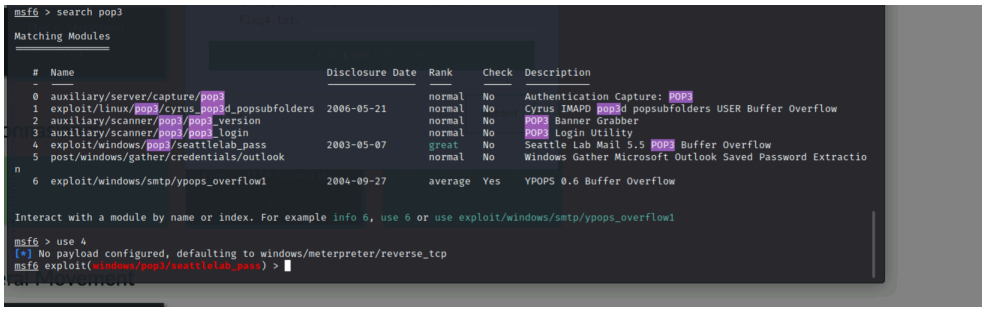
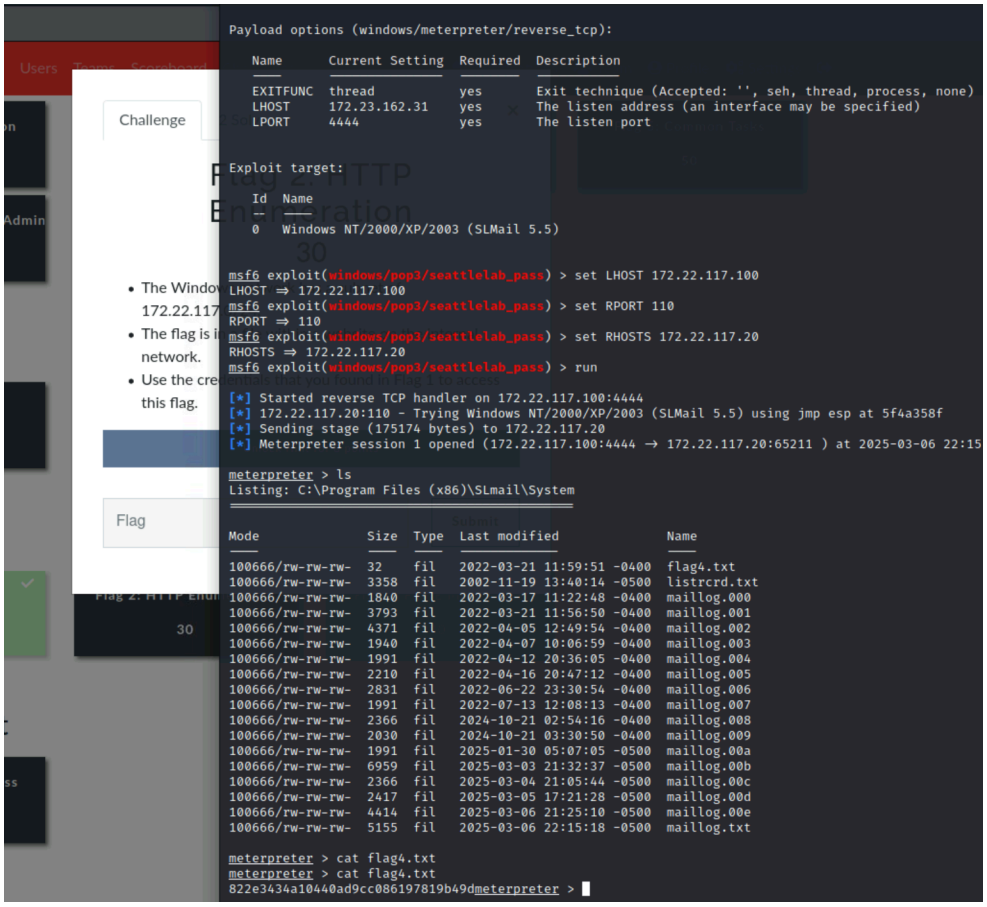
Vulnerability 18	Findings
Title	Privilege Escalation
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	From the credentials gained from a previou exploit from Alice, was able to escalate privileges using SSH and basic password guessing, the password being alice also.

Images	
Affected Hosts	192.168.13.14
Remediation	Enforce stronger password policies, force employees to use 2-factor authentication.

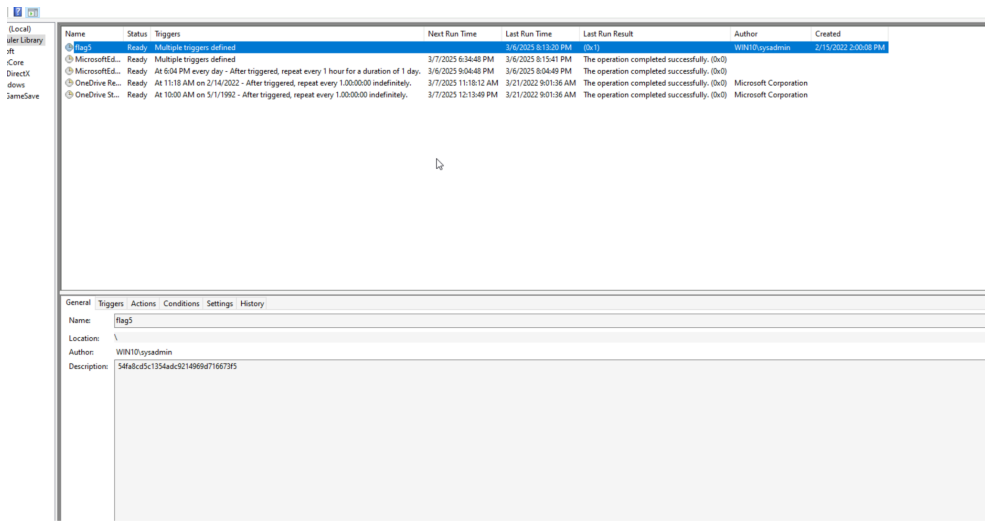
Vulnerability 19	Findings
Title	Port 21 FTP Open
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	High
Description	Through the Nmap scan was able to find Port 21 open, and was able to connect to it and find data

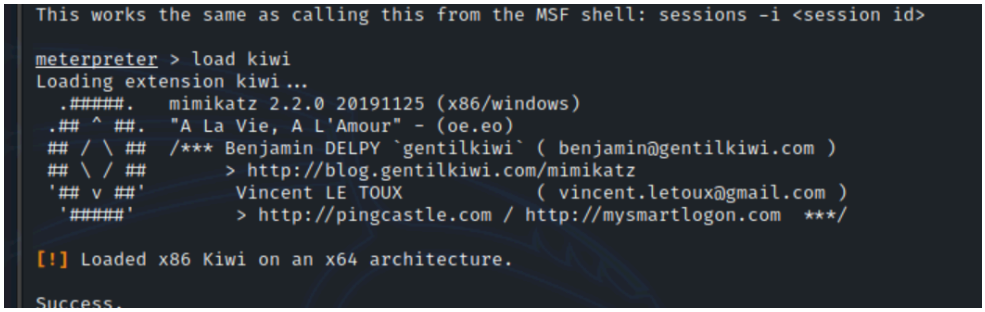
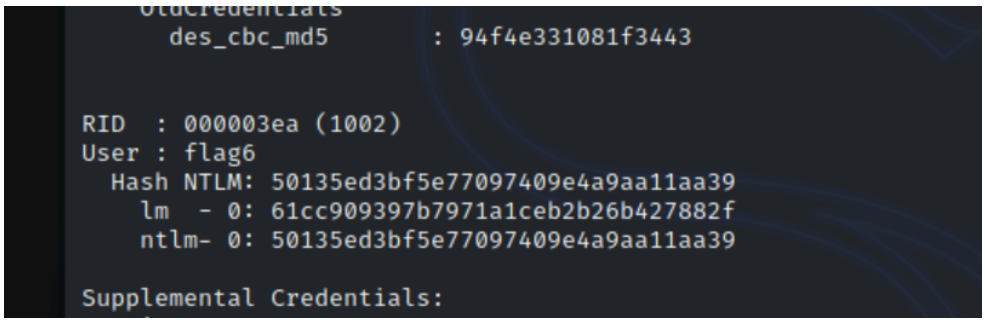
Images	 
Affected Hosts	172.22.117.20
Remediation	Close the FTP port for outsiders and allow a local FTP server only.

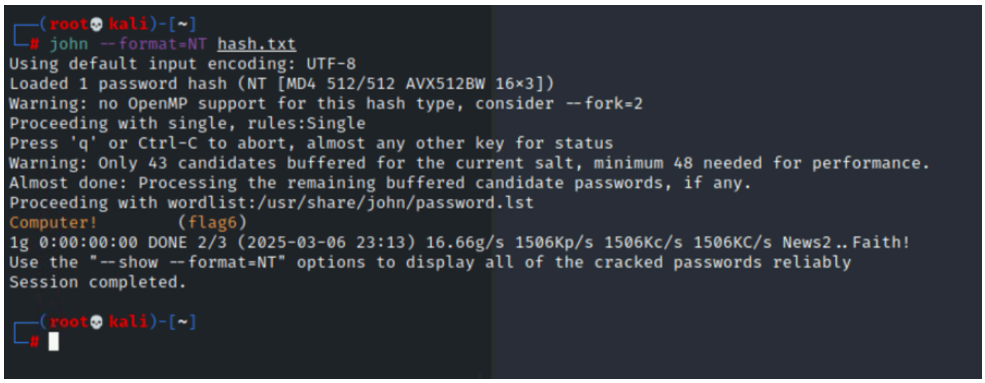
Vulnerability 20	Findings
Title	SLMail Port 110 Exploited with Metasploit (SeattleMail)
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Critical
Description	Using Nessus was able to determine that the 172.22.117.20 was vulnerable to exploit/windows/pop3/seattlelab_pass in Metasploit. Was able to connect using this exploit into the system gaining access to the shell and vulnerable info.

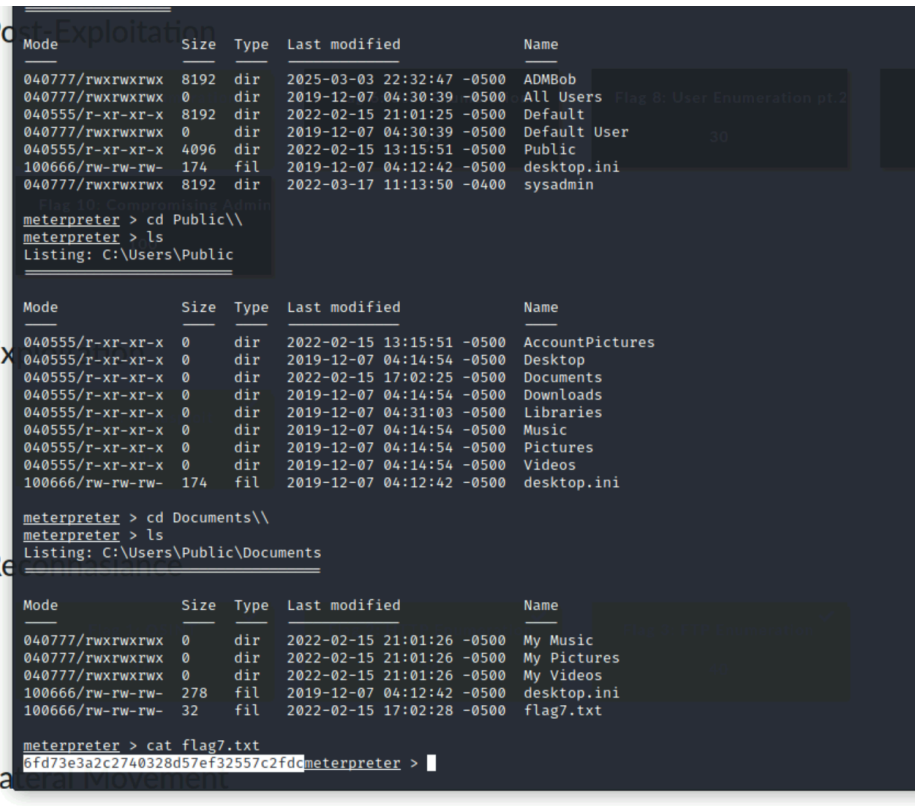
Images	 
Affected Hosts	172.22.117.20
Remediation	Update SLMail to prevent this breach or remove the service altogether, or simply close port 110.

Vulnerability 21	Findings
Title	Windows Task Scheduler
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	High
Description	After finding credentials using the SLMail exploit was able to log into the sysadmin account and find the scheduled tasks.

Images	
Affected Hosts	172.22.117.20
Remediation	Prevent unauthorized users from viewing scheduled tasks and avoid storing sysadmin credentials on any server susceptible to attacks.

Vulnerability 22	**Findings**
Title	Kiwi Password Hashes
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Critical
Description	Loaded kiwi within the meterpreter shell, used lsa_dump_sam to get all the password hashes, then cracked using john --format=NT hash.txt to get cracked hashes.
Images	 

	
Affected Hosts	172.22.117.20
Remediation	Don't store password hashes in unsecure areas of a system.

Vulnerability 23	Findings
Title	Sensitive Data Exposure in Public Data
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	High
Description	By navigating to Public/Documents was able to find vulnerable data
Images	
Affected Hosts	172.22.117.20

Remediation	Ensure easily accessible documents do not contain sensitive information.