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	PenTest Neidert LLC.
Contact Name	Carson Neidert
Contact Title	Head Penetration Tester

Document History

Version	Date	Author(s)	Comments
001	03-09-2025	Carson Neidert	Initial Version
002	03-10-2025	Carson Neidert	Version 2
003	03-13-2025	Carson Neidert	Version 3

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.

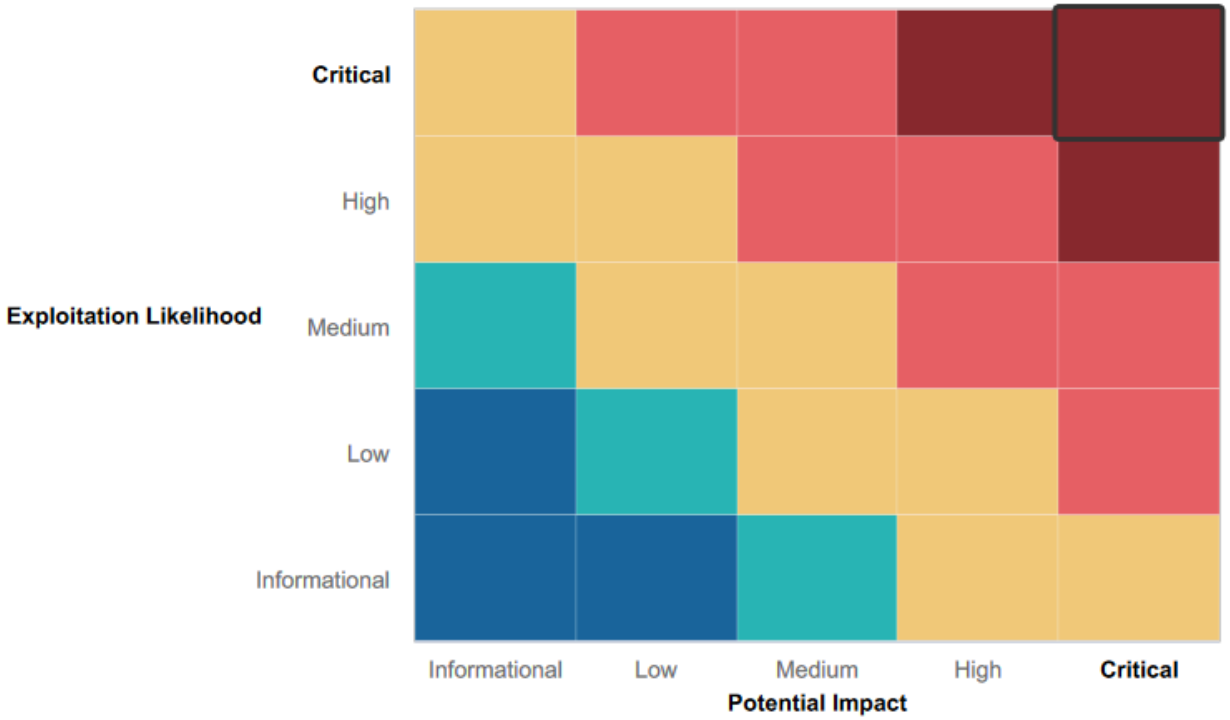
Executive Summary of Findings

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.

- Input Validation
- Authentication

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.

- SQL Injection
- XSS vulnerabilities
- Local File Inclusion
- Credentials stored in public repositories and embedded in website
- Password stored in hashes that were easy to crack
- Open ports
- Apache Struts
- SLMail
- Drupal
- SSH access
- Command Injection
- Shellshock

Executive Summary

[Provide a narrative summary of your steps and findings, including screenshots. It's fine to mention specifics (e.g., used Metasploit to exploit a vulnerable version of DistCC), but do not get too technical in these specifics. This should be an A–Z summary of your assessment.]

Web Applications

PenTest Neidert LLC. performed a security test on 192.168.14.35, which is Rekall's website. We performed exploitations by utilizing XSS by injecting <script>alert("hello")</script> for example, bypassing file uploading restrictions by using .php and .jpg.php files for uploading, as well as using SQL injections to gain unauthorized access. We then performed command injections in the DNS Check and MX Record Checker boxes in networking.php to view sensitive information that was left on the website. We also performed modifications to URLs to execute commands and reveal hidden directories, such as old_dislcaimers.

Linux Servers

PenTest Neidert LLC. then conducted security tests on the Linux Servers for Rekall. We started by doing reconnaissance on totalrekall.xyz and its network. We gathered domain information using Domain Dossier WHOIS, ping, crt.sh and then using that information to perform Zenmap and Nessus scans. Those scan revealed that 5 hosts were being affected, which were 192.168.13.10,192.168.13.11,192.168.13.12,192.168.13.13,192.168.13.14, which also revealed vulnerabilities on these hosts which were Drupal and Apache Struts issues. We then used Metasploit to create meterpreter sessions on these hosts, which allowed us to find flags on the systems. We were also able to get the hostname of the IP affected by Drupal as well as achieve root access by using SSH into a user by their credentials being on the system.

Windows Servers

PenTest Neidert LLC. finished off by conducting security tests on the Windows Servers for Rekall. We ran an Nmap scan to find two hosts 172.22.117.10 and 172.22.117.20 which were the Windows10 and WinDC01 machines. We did reconnaissance on Rekall's GitHub repository and received credentials from and used John the Ripper for password hashes. The Nmap scan revealed open ports such as HTTP, which allowed us to use those credentials. We performed an anonymous

FTP as the FTP port was open as well. We used Metasploit to create meterpreter sessions. One was against SLMail where we looked through directories, scheduled tasks, and used kiwi features to find a user and password to login into the WinDC01 machine. We created a new meterpreter session to get into the WinDC01 machine, and then performed searches of the users on the machine, searching through the directories, and using kiwi again to gain administrator access.

Summary Vulnerability Overview

Vulnerability	Severity
Web Applications	
Flag 1- XSS reflected	High
Flag 2- XSS reflected	High
Flag 3- XSS stored	High
Flag 4- Sensitive Data Exposure	Low
Flag 5- Local File Inclusion	High
Flag 6- Local File Inclusion	Medium
Flag 7- SQL Injection	Critical
Flag 8- Sensitive Data Exposure	Critical
Flag 9- Sensitive Data Exposure	High
Flag 10- Command Injection	Critical
Flag 11- Command Injection	Critical
Flag 12- Brute Force Attack (couldn't figure out)	NA
Flag 13- PHP Injection	Medium
Flag 14- Session Management (couldn't figure out)	NA
Flag 15- Directory Traversal	Critical
Linux Server	
Flag 1- Open Sourced Exposed Data	Low
Flag 2- Ping totalrekall.xyz	Low
Flag 3- Open Sourced Exposed Data	Low
Flag 4- Number of Hosts	Medium
Flag 5- Drupal Host	High
Flag 6- Nessus scan on 192.168.13.12	Critical
Flag 7- Apache Tomcat Remote Code Execution	Critical
Flag 8- Shellshock	High
Flag 9- Additional Vulnerabilities on affected Host - 192.168.13.11	Critical
Flag 10- Struts-CVE-2017-5638	High
Flag 11- Drupal-CVE-2019-6340	High
Flag 12- CVE-2019-14287	High
Windows Server	
Flag 1- totalrekall GitHub page	Low
Flag 2- Nmap Scan to see network hosts	Medium
Flag 3- FTP	Medium
Flag 4- SLMail/SMTP	Medium
Flag 5- Scheduled Tasks	Medium

Flag 6- SLMail Compromise	Critical
Flag 7- Lateral Movement	Critical
Flag 8- Attacking LSA	Critical
Flag 9- Navigating Exploit	Critical
Flag 10- Default Administrator Credentials	High

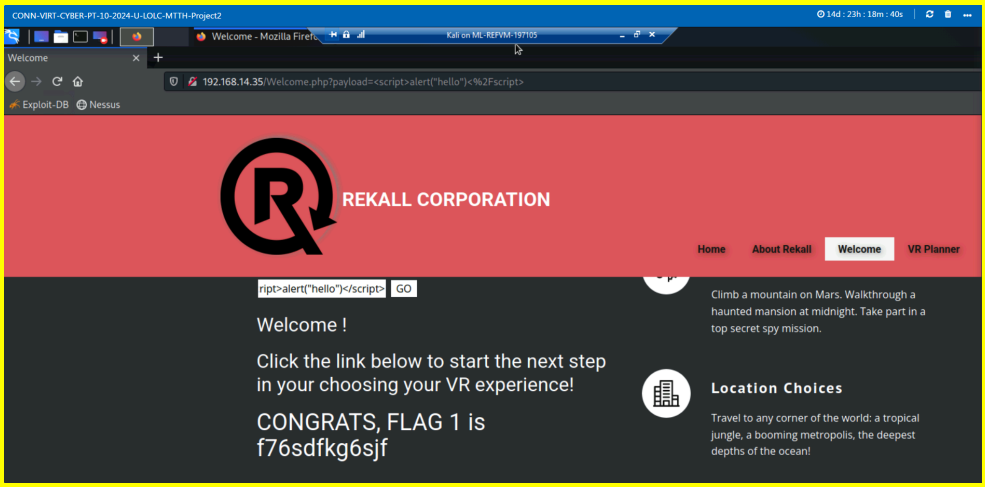
The following summary tables represent an overview of the assessment findings for this penetration test:

Scan Type	Total
Hosts	**Web Applications:** 192.168.14.35 **Linux Server:** 34.102.136.180 192.168.13.10 192.168.13.11 192.168.13.12 192.168.13.13 192.168.13.14 **Windows Server:** 172.22.117.10(WinDC01) 172.22.117.20(Windows10)
Ports	**Linux Server:** 22 80 8009 8080 **Windows Server:** WinDC01: 53 88 135 139 389 445 464 593 636 3268 3269 Windows10: 21 25 79 80 106 110 135 139 443 445

Exploitation Risk	Total
Critical	12
High	11
Medium	7
Low	5

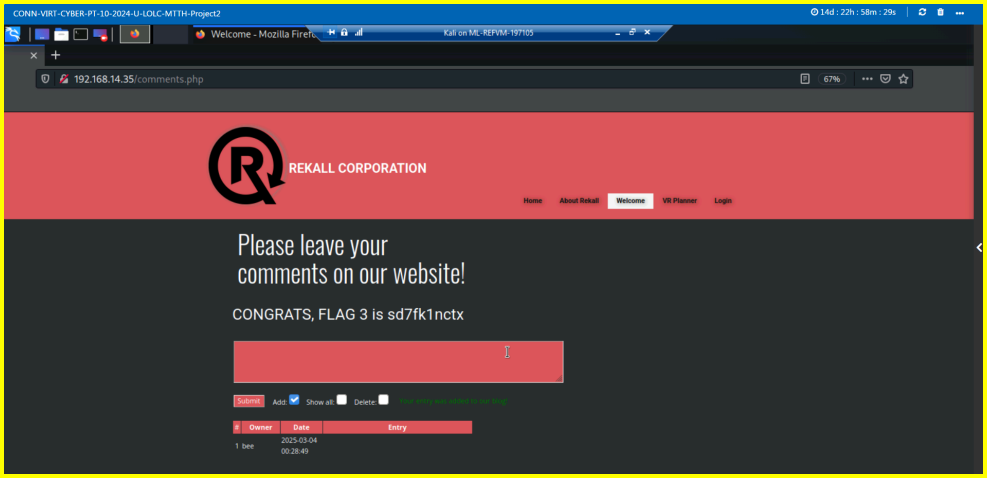
Vulnerability Findings

Web Applications

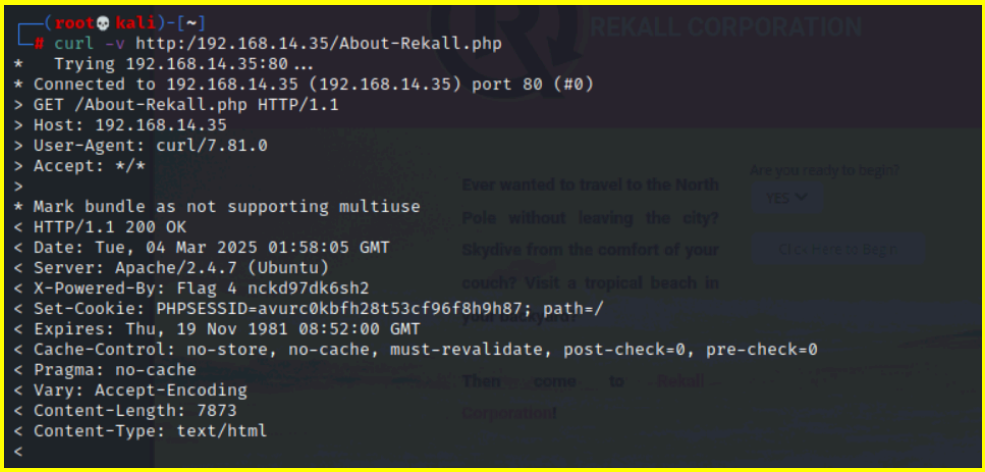
Vulnerability 1	Findings
Title	Flag 1- XSS reflected
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	High
Description	Used payload <script>alert(“hello”)</script> in Put Your Name box.
Images	
Affected Hosts	Welcome.php
Remediation	Input Validation and Sanitization,Output Encoding,Content Security Policy(CSP),Regular Security Audits

Vulnerability 2	Findings
Title	Flag 2- XSS reflected

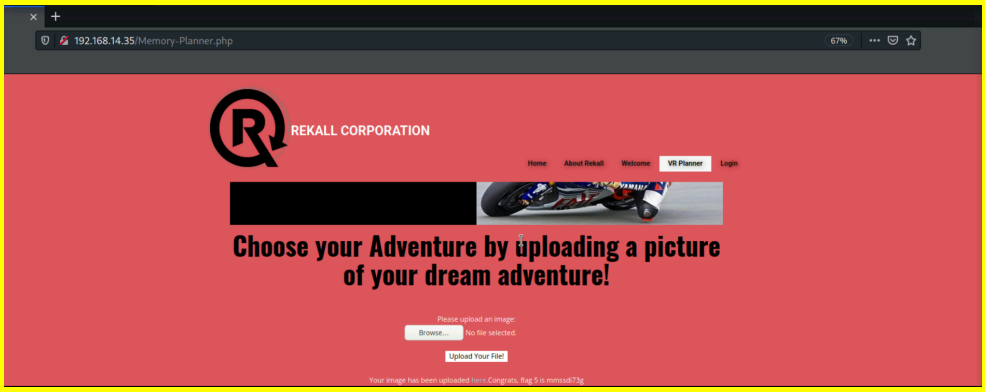
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	High
Description	Used payload <SCRIPscirptT>alert(“hello”)</SCRIPscripTt> in Choose your character box. This bypasses input validation of script.
Images	
Affected Hosts	Memory-Planner.php
Remediation	Input Validation and Sanitization,Output Encoding,Content Security Policy(CSP),Regular Security Audits

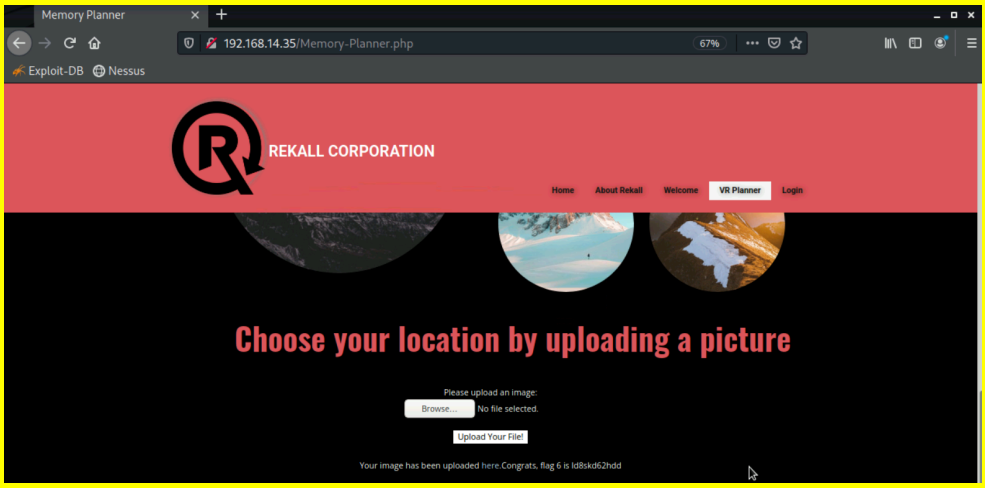
Vulnerability 3	Findings
Title	Flag 3- XSS stored
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	High
Description	Used payload <script>alert(“hello”)</script> in Comments box.
Images	

Affected Hosts	comments.php
Remediation	Secure handling of user input,Request blocking,Escaping,Choosing the right framework,Mitigating the damage of an XSS attack

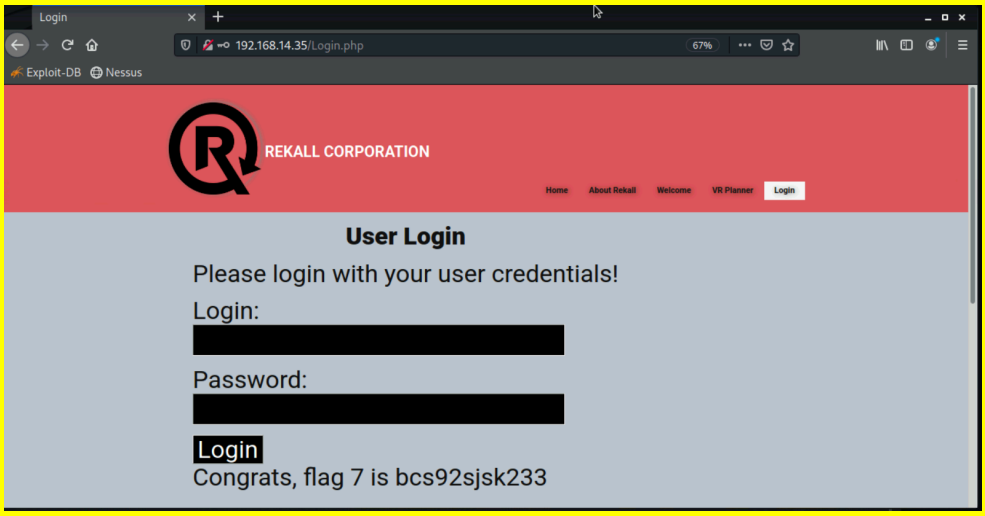
Vulnerability 4	Findings
Title	Flag 4- Sensitive Data Exposure
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	Low
Description	Used Curl command: curl -v http://192.168.14.35/About-Rekall.php
Images	
Affected Hosts	About-Recall.php
Remediation	Implement encryption, access controls, and regular security audits.

Vulnerability 5	Findings
Title	Flag 5- Local File Inclusion
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	High
Description	Created a .php file and uploaded into Browse… when choosing adventurer

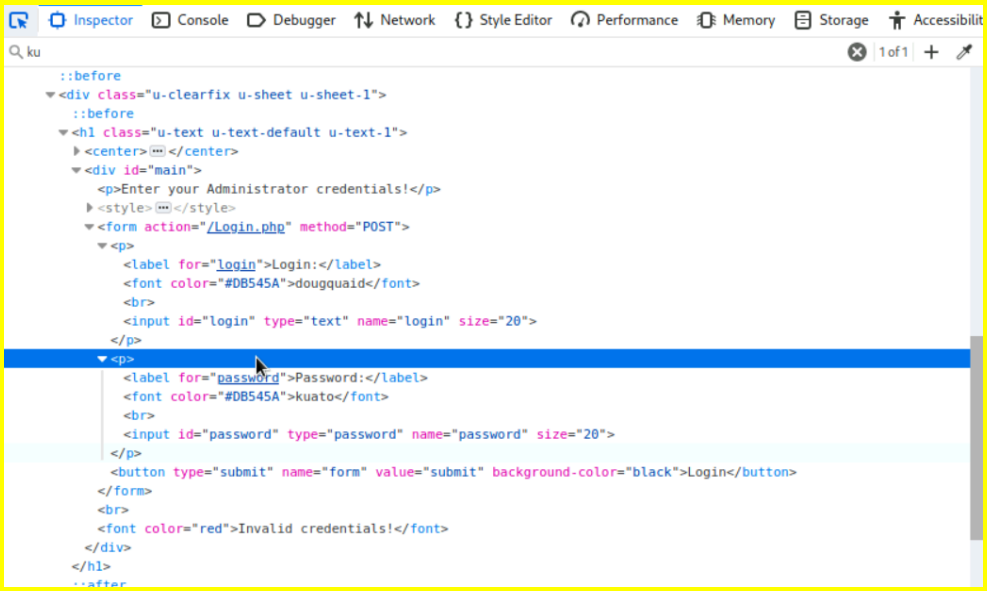
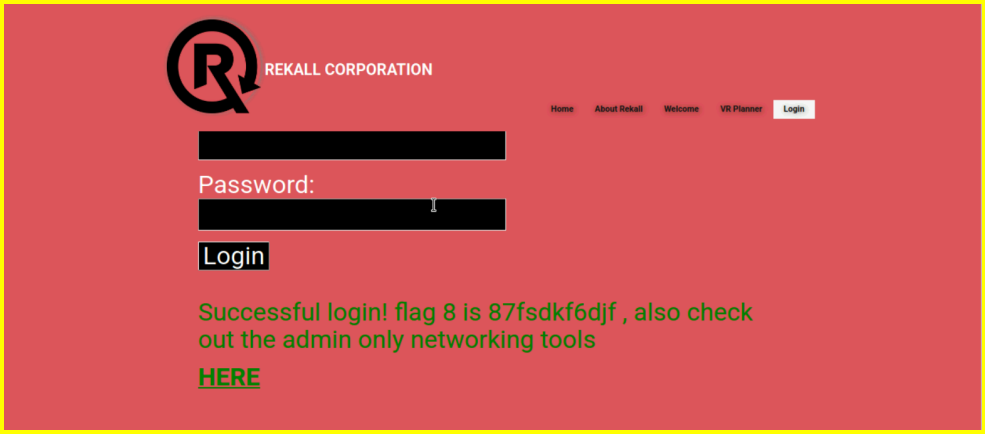
Images	
Affected Hosts	Memory-Planner.php
Remediation	ID assignation,Whitelisting,Use databases,Better server instructions

Vulnerability 6	**Findings**
Title	Flag 6- Local File Inclusion
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	Medium
Description	Created a .jpg.php to bypass input validation of .jpg in Browse… when choosing location
Images	
Affected Hosts	Memory-Planner.php
Remediation	ID assignation,Whitelisting,Use databases,Better server instructions

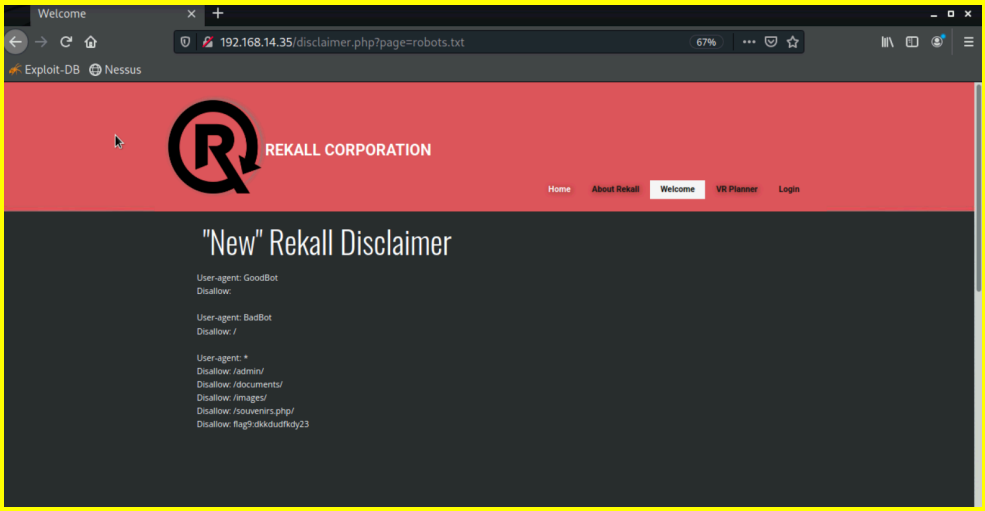
Vulnerability 7	**Findings**
Title	Flag 7- SQL Injection

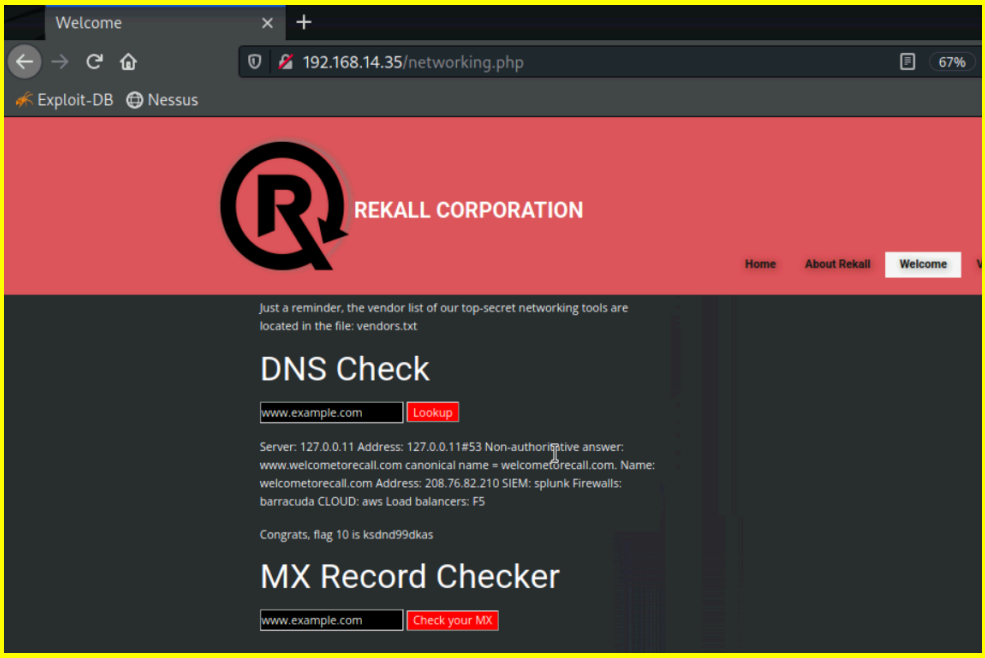
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	Critical
Description	Used SQL injection ‘ or ‘’=‘ for both the username and password in User Login section
Images	
Affected Hosts	Login.php
Remediation	OWASP recommends Use of Prepared Statements (with Parameterized Queries),Use of Properly Constructed Stored Procedures,Allow-list Input Validation as well as including Least Privilege

Vulnerability 8	Findings
Title	Flag 8- Sensitive Data Exposure
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	Critical
Description	Username and Password are in HTML. Used the credentials in the Admin Login

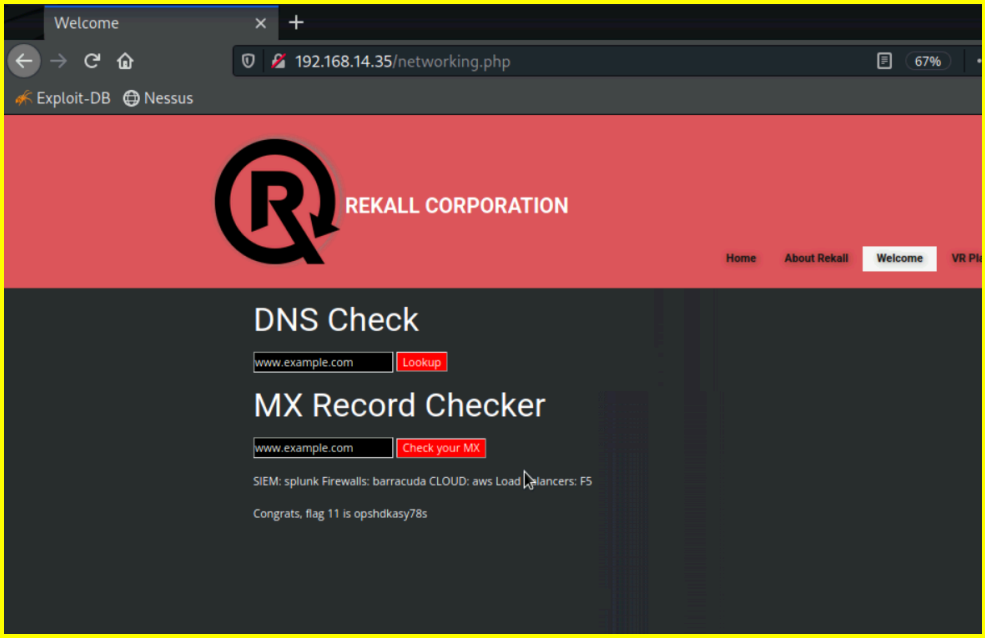
Images	 
Affected Hosts	Login.php
Remediation	Implement encryption, access controls, and regular security audits.

Vulnerability 9	Findings
Title	Flag 9- Sensitive Data Exposure
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	High
Description	set page=robots.txt

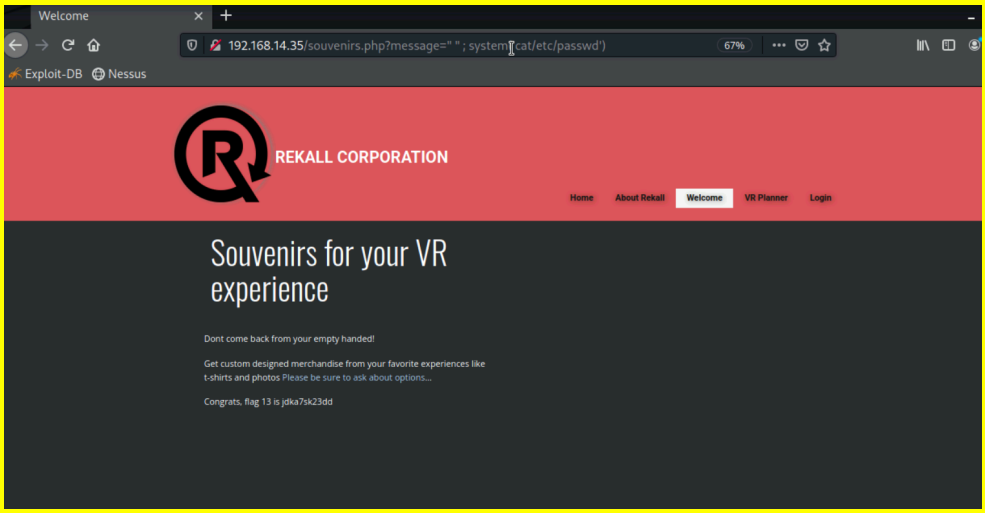
Images	
Affected Hosts	disclaimer.php & robots.txt
Remediation	Implement encryption, access controls, and regular security audits.

Vulnerability 10	**Findings**
Title	Flag 10- Command Injection
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	Critical
Description	In DNS Check: input www.welcometorecall.com && cat vendors.txt flag 10 appeared under sensitive information
Images	
Affected Hosts	networking.php

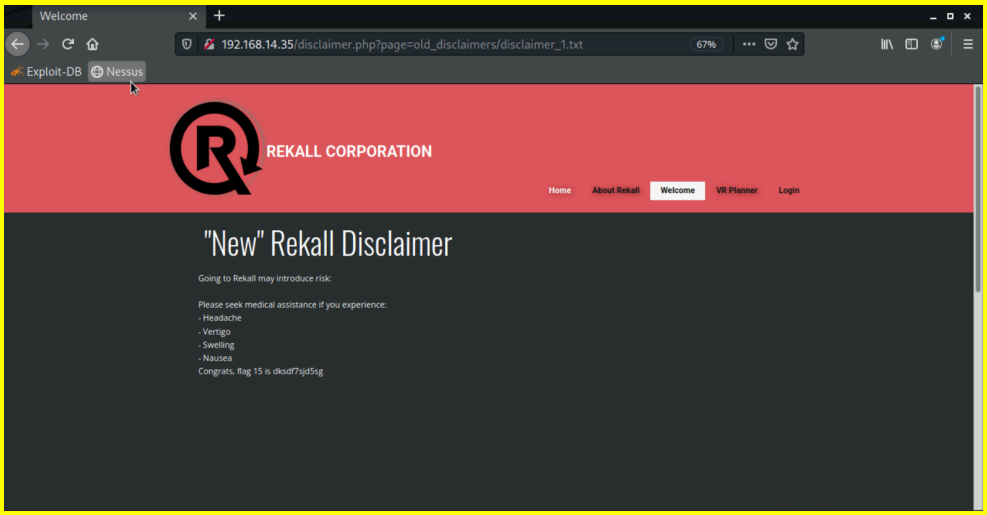
Remediation	OWASP recommends avoiding calling OS commands directly,Escape values added to OS commands specific to each OS,Parameterization in conjunction with Input Validation. Applications should run using the lowest privileges that are required to accomplish the necessary tasks, and If possible, create isolated accounts with limited privileges that are only used for a single task.

Vulnerability 11	Findings
Title	Flag 11- Command Injection
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	Critical
Description	In MX Record Checker: input www.welcometorecall.com | cat vendors.txt Cannot use “&” because of input validation flag 11 appeared under sensitive information
Images	
Affected Hosts	networking.php
Remediation	OWASP recommends avoiding calling OS commands directly,Escape values added to OS commands specific to each OS,Parameterization in conjunction with Input Validation. Applications should run using the lowest privileges that are required to accomplish the necessary tasks, and If possible, create isolated accounts with limited privileges that are only used for a single task.

Vulnerability 13	Findings
Title	Flag 13- PHP Injection

Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	Medium
Description	souvenirs.php was mentioned in flag 9. Changed the URL to : http://192.168.13.35/souvenirs.php?message=""; system('cat /etc/passwd')
Images	
Affected Hosts	souvenirs.php
Remediation	Avoid Using exec(), shell_exec(), system() or passthru(),Avoid Using Weak Sanitization Methods,Avoid Displaying Verbose Error Messages,Use a PHP Security Linter

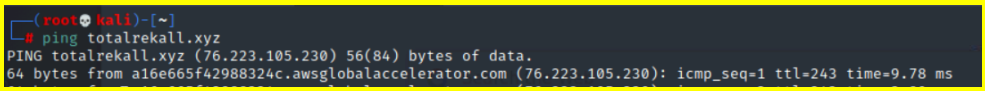
Vulnerability 15	**Findings**
Title	Flag 15- Directory Traversal
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	Critical
Description	The site says “New” Rekall Disclaimer providing a hint that there was an old one. Using the vulnerability from flag 10 and 11, we run an ls and see that there is a directory called old_disclaimers. We then changed the URL to : 192.168.14.35/disclaimer.php?page=old_disclaimers/disclaimer_1.txt.

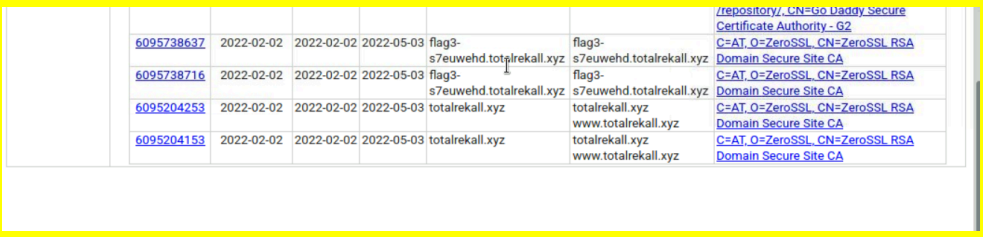
Images	
Affected Hosts	Disclaimer.php
Remediation	File system calls and user-supplied input can be dangerous together, so avoid it when possible ,When you are templating or using language files, you should use indexes instead of the actual sections of the file name,Prevent the user from supplying the whole path,Validate the user-supplied input by comparing it to a whitelist, Utilize chroot jails and access policies to control where files can be saved and retrieved ,If you must use user-supplied input in file operations, the input must be normalized before being used in files or APIs.

Linux Server

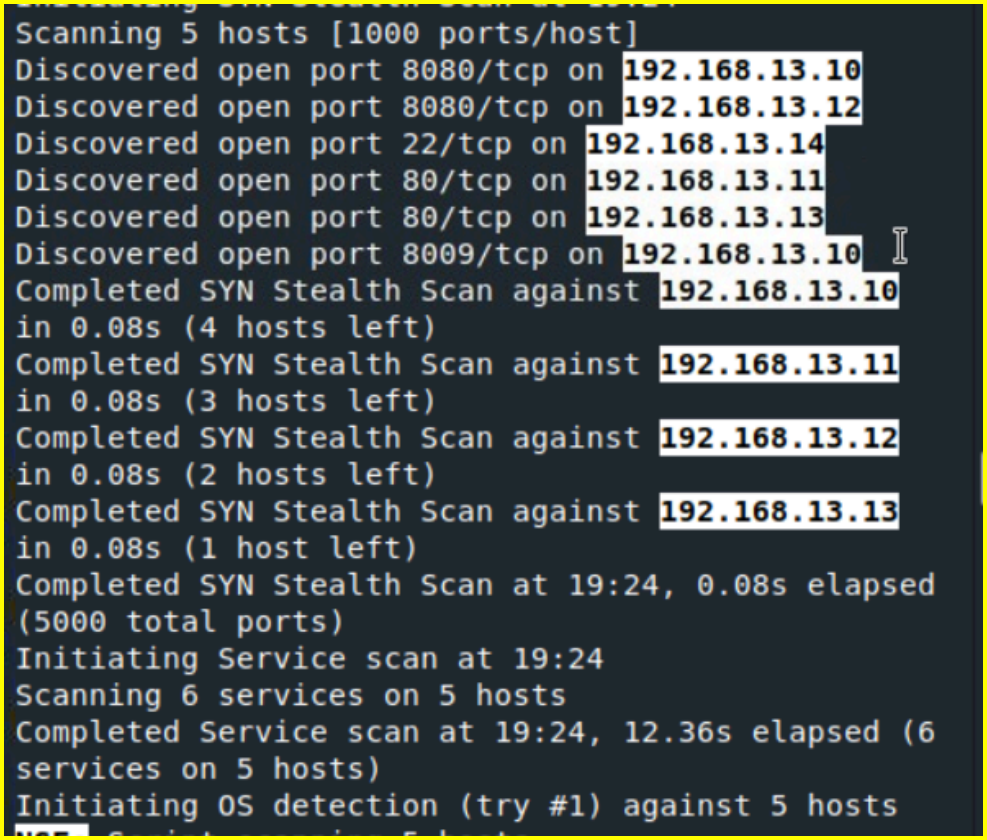
Vulnerability 1	Findings
Title	Flag 1- Open Sourced Exposed Data
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Low
Description	On the Domain Dossier page, viewing the WHOIS data for totalrekall.xyz
Images	Queried whois.godaddy.com with "totalrekall.xyz"... Domain Name: totalrekall.xyz Registry 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:
Affected Hosts	https://centralops.net/co/DomainDossier.aspx

Remediation	Adding services through the domain can help hide personal information.

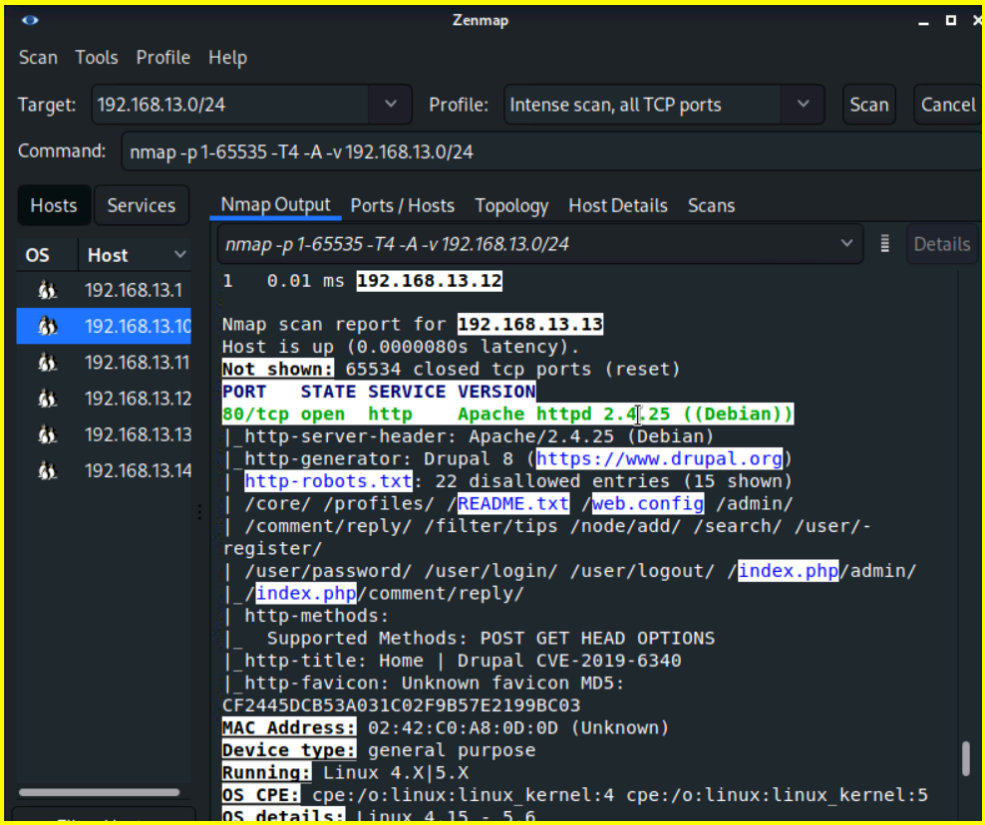
Vulnerability 2	**Findings**
Title	Flag 2- Ping totalrekall.xyz
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Low
Description	Ping the domain totalrekall.xyz
Images	 (note: issue giving wrong ip, instructor gave correct ip)
Affected Hosts	34.102.136.180
Remediation	It's difficult to hide your IP address

Vulnerability 3	**Findings**
Title	Flag 3- Open Sourced Exposed Data
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Low
Description	On crt.sh, searched up totalrekall.xyz
Images	
Affected Hosts	Certificates issued to company
Remediation	Adding services through the domain can help hide personal information.

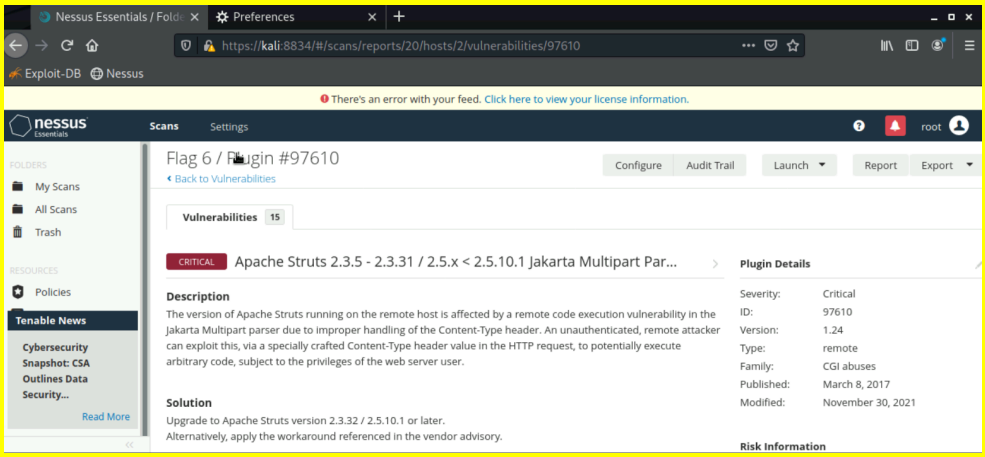
Vulnerability 4	**Findings**
Title	Flag 4- Number of Hosts
Type (Web app / Linux OS / WIndows OS)	Linux OS

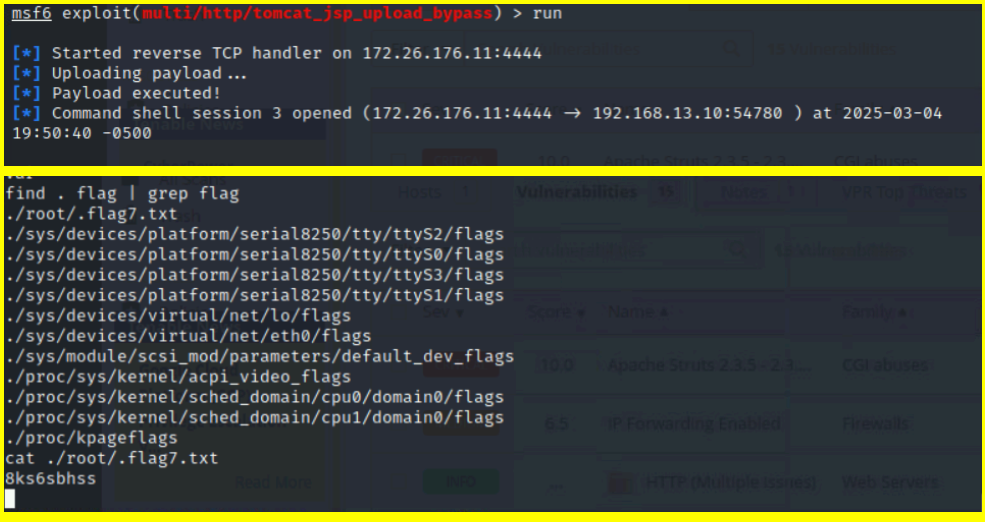
Risk Rating	Medium
Description	Zenmap scan found 5 hosts being affected
Images	
Affected Hosts	192.168.13.10,192.168.13.11,192.168.13.12,192.168.13.13,192.168.13.14
Remediation	The Nmap scan results provide valuable information about the open ports and running services on the target systems. By analyzing this data, you can identify potential security risks and vulnerabilities. For example, the presence of unnecessary open ports or outdated services with known vulnerabilities can indicate areas that require further investigation and remediation. (from labex.io)

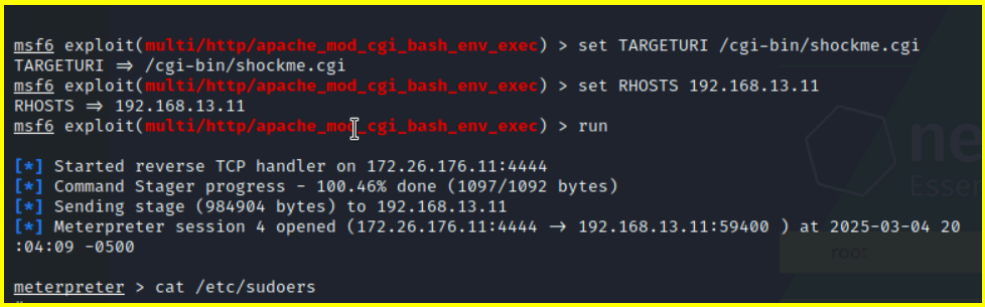
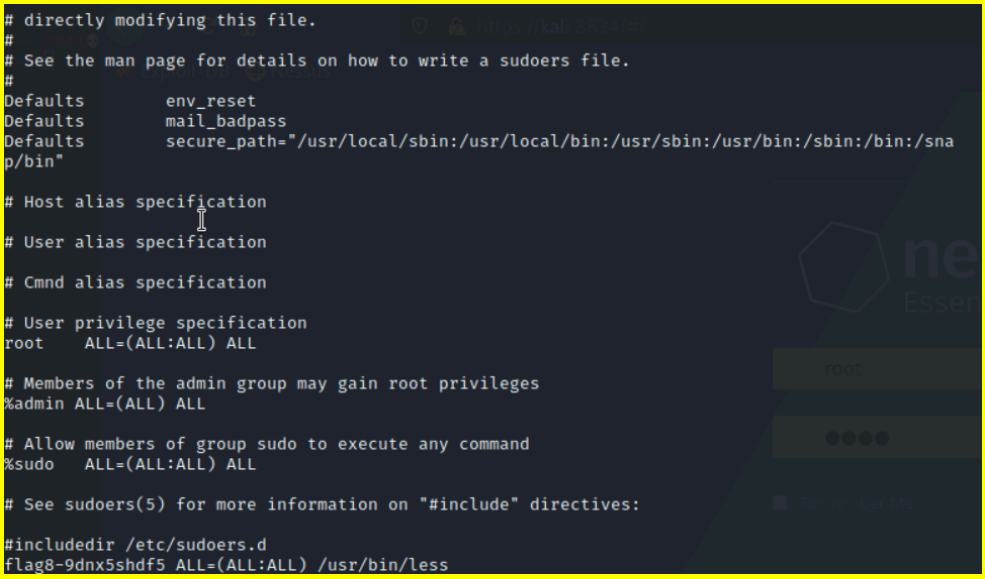
Vulnerability 5	Findings
Title	Flag 5- Drupal Host
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	High
Description	Ran a Zenmap scan to find the host running Drupal. Shows a vulnerability to CVE-2019-6430

Images	
Affected Hosts	192.168.13.13
Remediation	https://nvd.nist.gov/vuln/detail/CVE-2019-6340 make sure has latest security patch

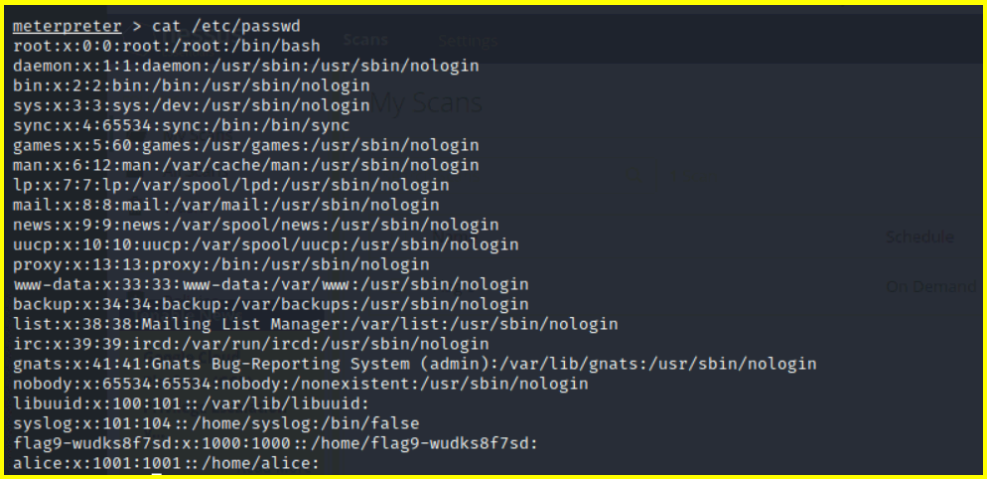
Vulnerability 6	Findings
Title	Flag 6- Nessus scan on 192.168.13.12
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	Ran a Nessus scan against 192.168.13.12. One critical vulnerability for Apache Struts(CVE-2017-5638). The ID# was the flag which was 97610

Images	
Affected Hosts	192.168.13.12
Remediation	https://nvd.nist.gov/vuln/detail/CVE-2017-5638 make sure has latest security patch

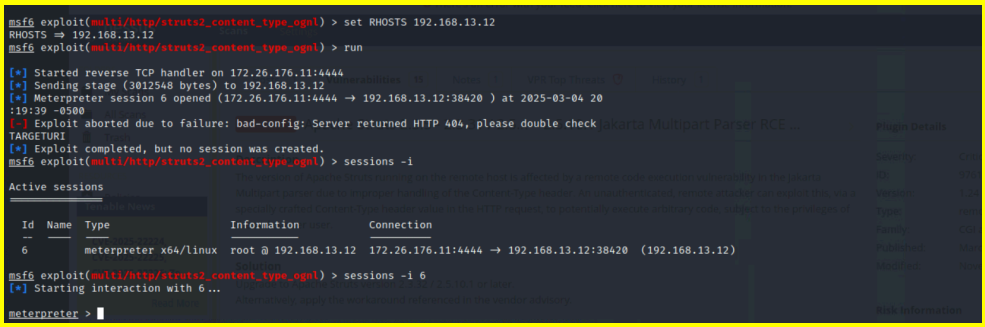
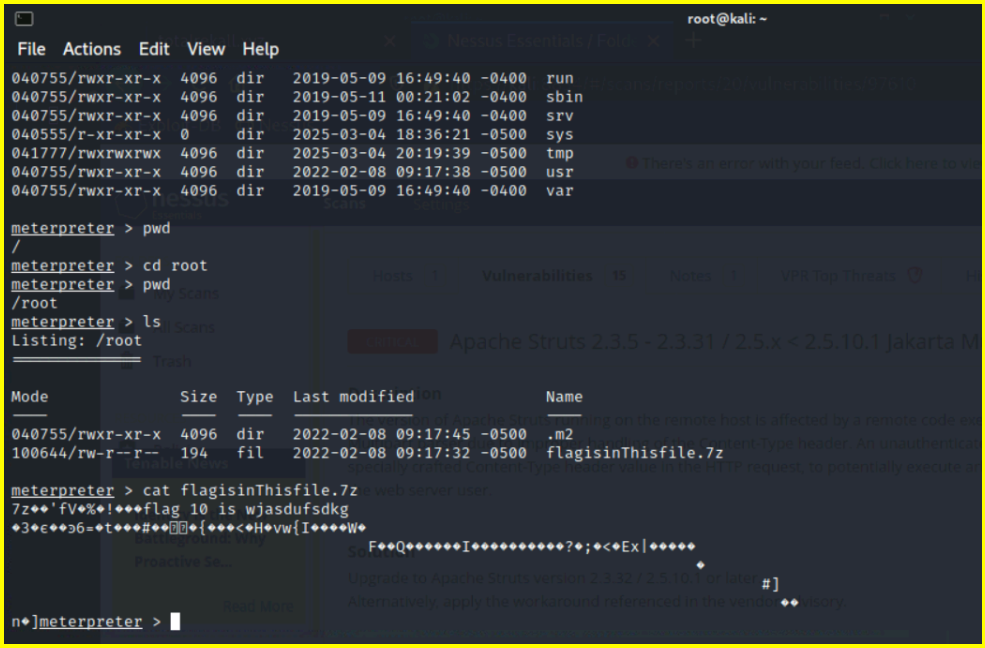
Vulnerability 7	Findings
Title	Flag 7- Apache Tomcat Remote Code Execution
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	Went into msfconsole. Used exploit(multi/http/tomcat_jsp_upload_bypass) to get into a meterpreter session. Set RHOSTS to 192.168.13.10. Used a find command to find the flag, then cat the file.
Images	
Affected Hosts	192.168.13.10
Remediation	Make sure Apache has the latest security patches

Vulnerability 8	Findings
Title	Flag 8- Shellshock
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	High
Description	Went into msfconsole. Used exploit(multi/http/apache_mod_cgi_bash_env_exec). Set the TARTURI to /cgi-bin/shockme.cgi and RHOSTS to 192.168.13.11. Then cat /etc/sudoers file and flag 8 was found scrolling through the sudoers file.
Images	 
Affected Hosts	192.168.13.11
Remediation	https://www.crowdstrike.com/en-us/blog/mitigating-bash-shellshock/ Shellshock type attacks can be avoided by not processing user data directly as variables in web/bash code,sanitizing user input and removing un-needed characters,Utilize the free CrowdStrike Shellshock Scanner,Monitor logs for evidence of attempted or successful command execution.(from crowdstrike)

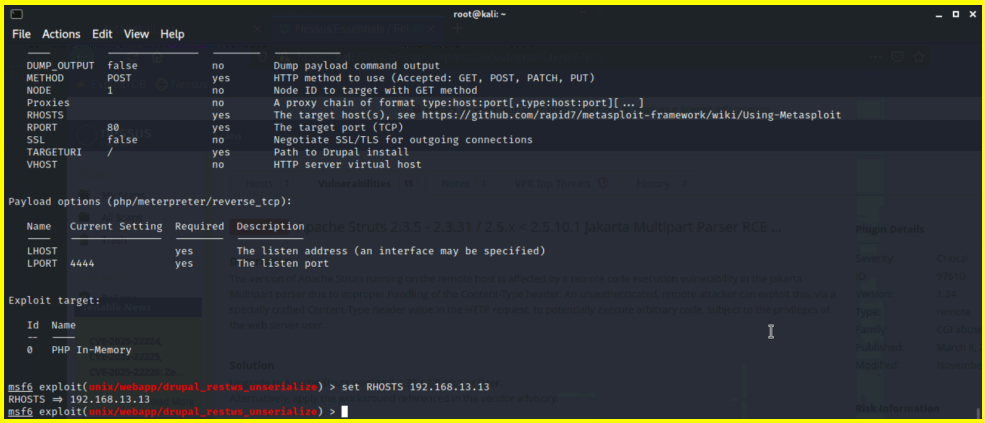
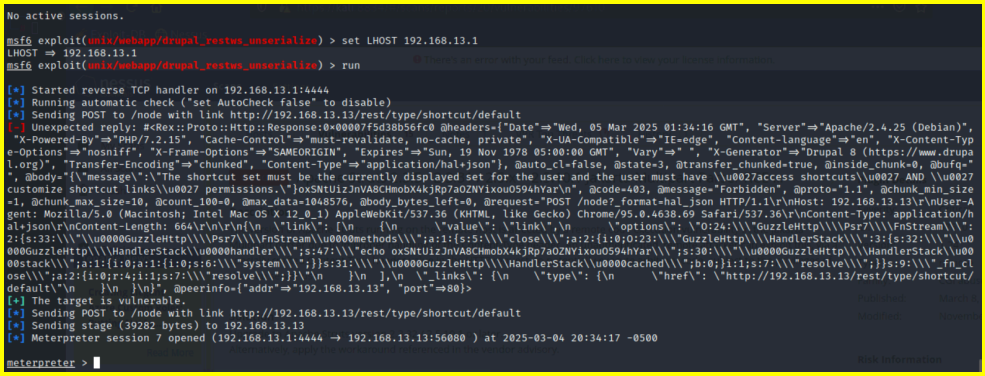
Vulnerability 9	Findings
Title	Flag 9- Additional Vulnerabilities on affected Host - 192.168.13.11

Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	Using the same meterpreter shell as flag 8, cat /etc/passwd revealed flag 9.
Images	
Affected Hosts	192.168.13.11
Remediation	https://www.crowdstrike.com/en-us/blog/mitigating-bash-shellshock/ Shellshock type attacks can be avoided by not processing user data directly as variables in web/bash code,sanitizing user input and removing un-needed characters,Utilize the free CrowdStrike Shellshock Scanner,Monitor logs for evidence of attempted or successful command execution.(from crowdstrike)

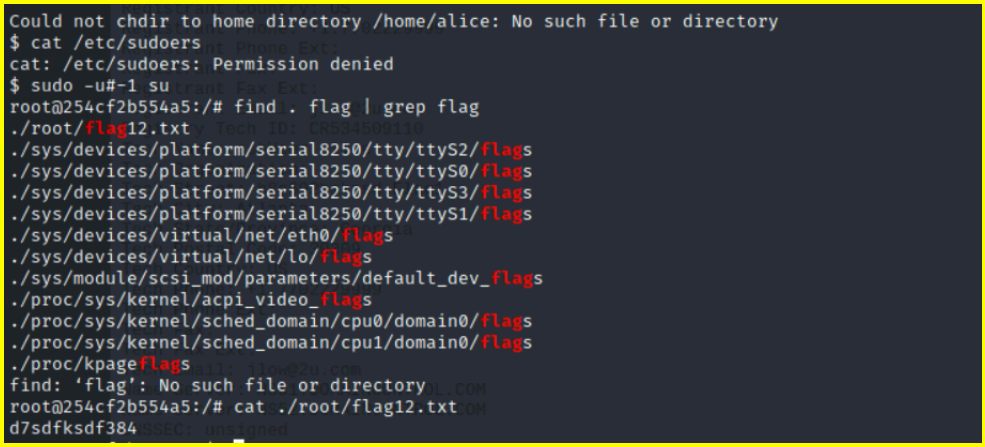
Vulnerability 10	Findings
Title	Flag 10- Struts-CVE-2017-5638
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	High
Description	Used msfconsole. Used exploit(multi/http/struts2_content_type_ognl). Set RHOSTS to 192.168.13.12. Initially it said that no meterpreter session was created but when putting sessions -i showed a session was active. Went into the session and ran ls to see the flag file which was flagisinThisfile.7z. cat that file and flag 10 appeared.

Images	 
Affected Hosts	192.168.13.12
Remediation	https://nvd.nist.gov/vuln/detail/CVE-2017-5638 make sure has latest security patch

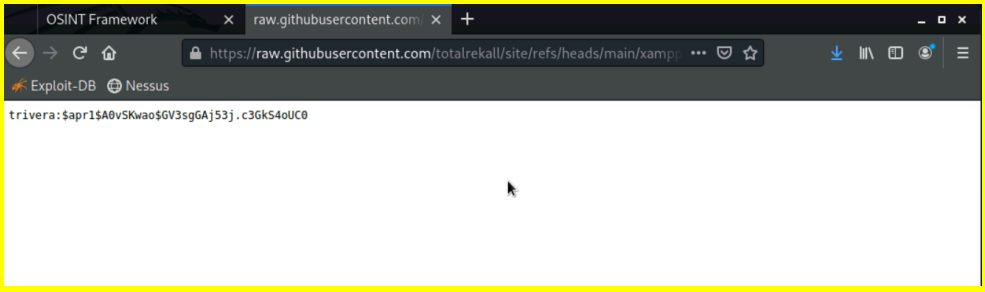
Vulnerability 11	Findings
Title	Flag 11- Drupal-CVE-2019-6340
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	High
Description	Using Drupal information from flag 5 we did an msfconsole. Used exploit(unix/webapp/drupal_restws_unserialize). Set RHOSTS to 192.168.13.13 and LHOST to 192.168.13.1. In meterpreter, ran getuid to find hostname,www-data, which was the flag

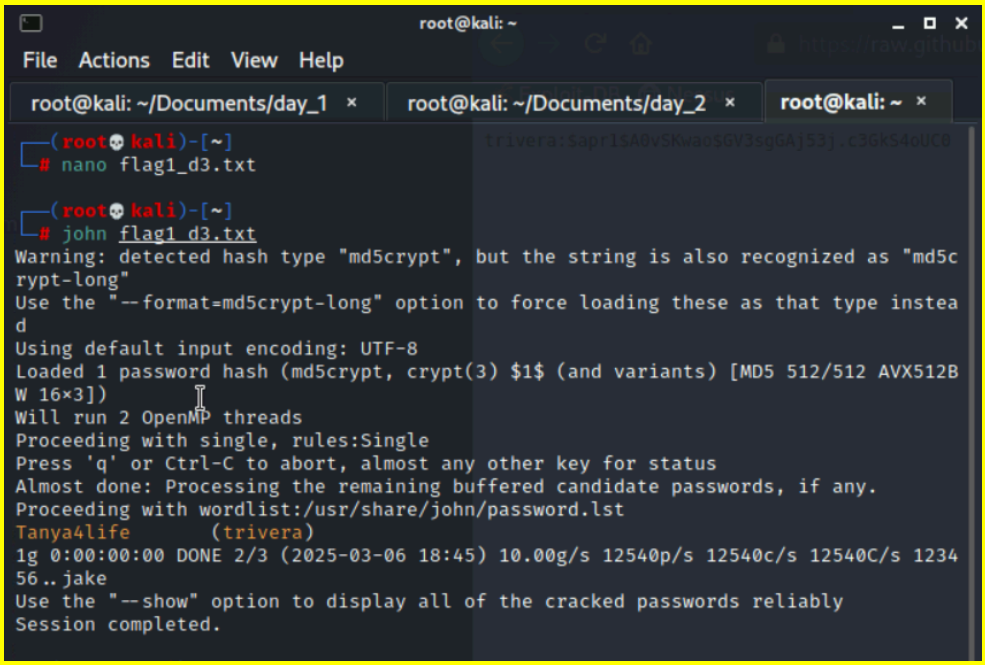
Images	 
Affected Hosts	192.168.13.13
Remediation	https://nvd.nist.gov/vuln/detail/CVE-2019-6340 make sure has latest security patch

Vulnerability 12	Findings
Title	Flag 12- CVE-2019-14287
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	High
Description	WHOIS data revealed a user sshuser Alice. sshd into Alice using ssh alice@192.168.13.14 and the password was alice. Alice had no sudo privileges so we needed to get into root. used command sudo -u#-1 su and got into root. Then used a find command to grab the flag then cat the path to the file to reveal the flag contents.

Images	
Affected Hosts	192.168.13.14
Remediation	https://nvd.nist.gov/vuln/detail/CVE-2019-14287 make sure has latest security patches

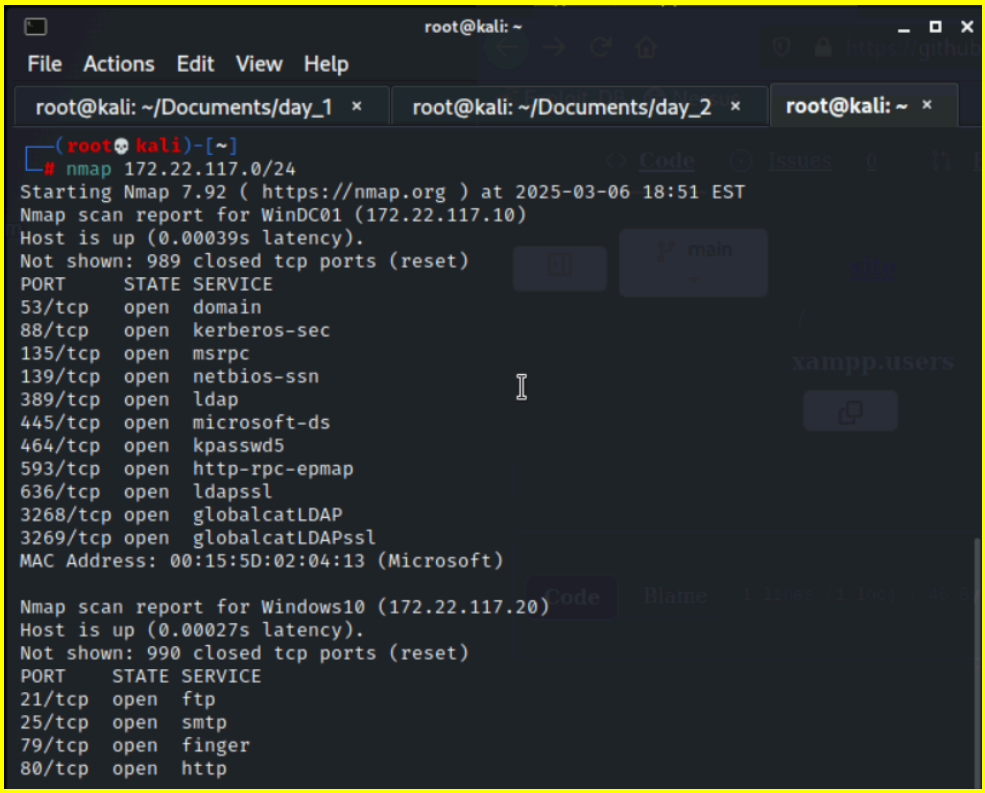
Windows Server

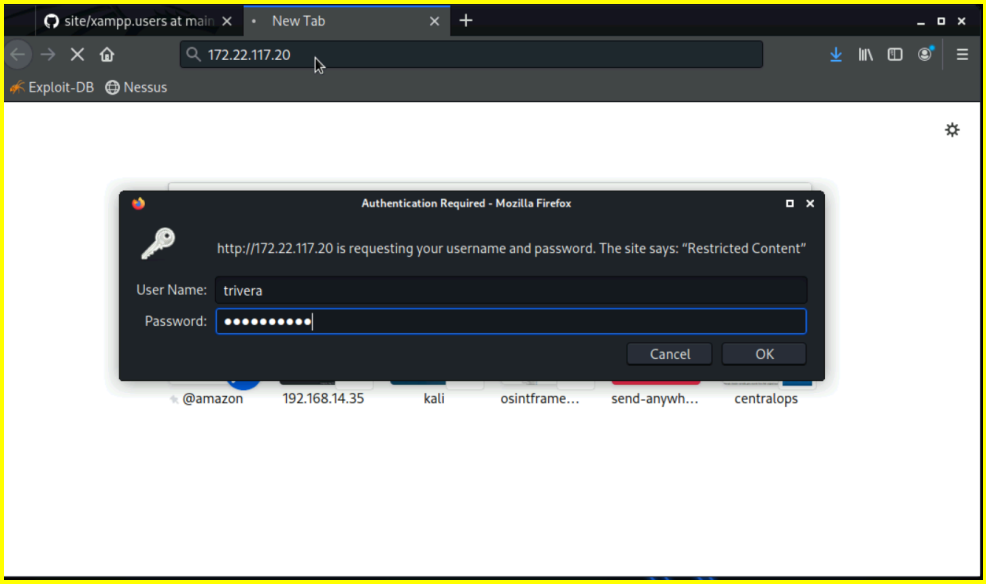
Vulnerability 1	Findings
Title	Flag 1- totalrekall GitHub page
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Low
Description	Searched GitHub for totalrekall repository. In the repository there is xampp.users and within contains credentials of trivera and the password hashes. Put the password hashes into a txt file and use John to solve the password. user: trivera password: Tanya4life
Images	

	
Affected Hosts	
Remediation	Don’t leave credentials and hashes on a public repository

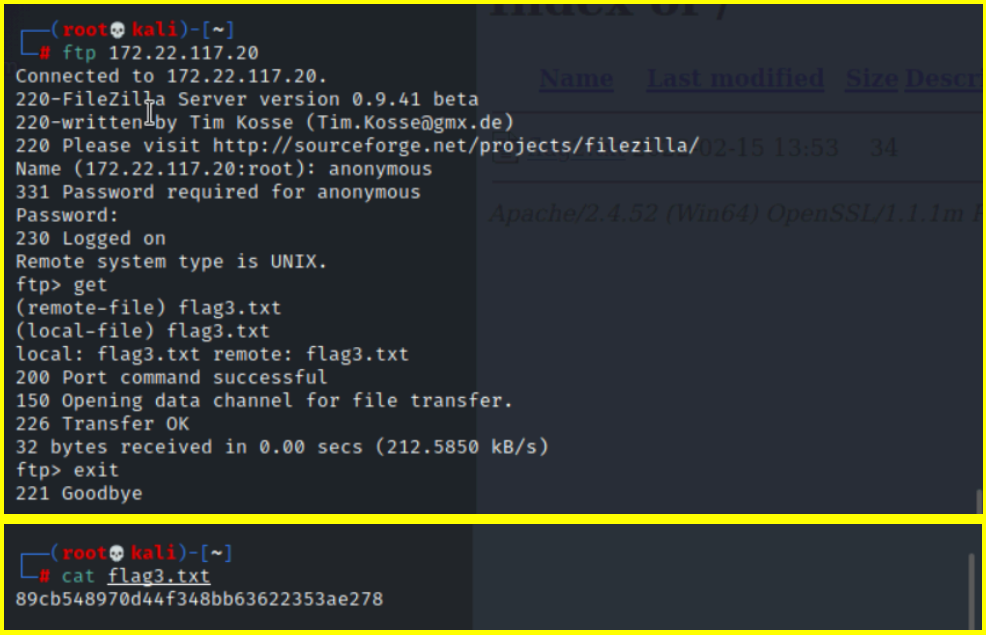
Vulnerability 2	Findings
Title	Flag 2- Nmap Scan to see network hosts
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Meidum
Description	Ran an Nmap scan on 172.22.117.0/24 revealed two IPs with open ports. HTTP was open on Windows10, so we entered 172.22.117.20 into a web browser and it prompted us with credentials. Using the credentials from flag 1 worked and revealed a text file with flag 2 inside.

Images

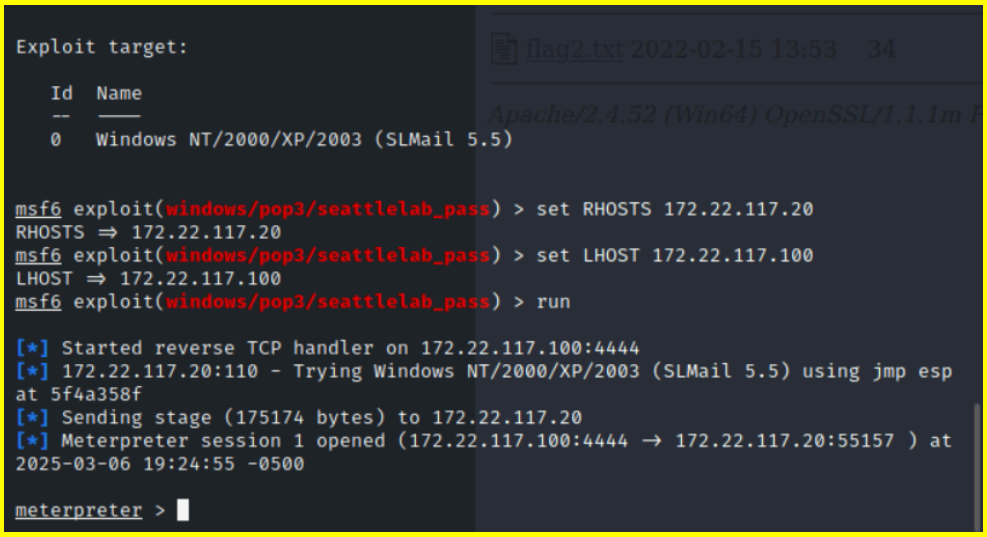
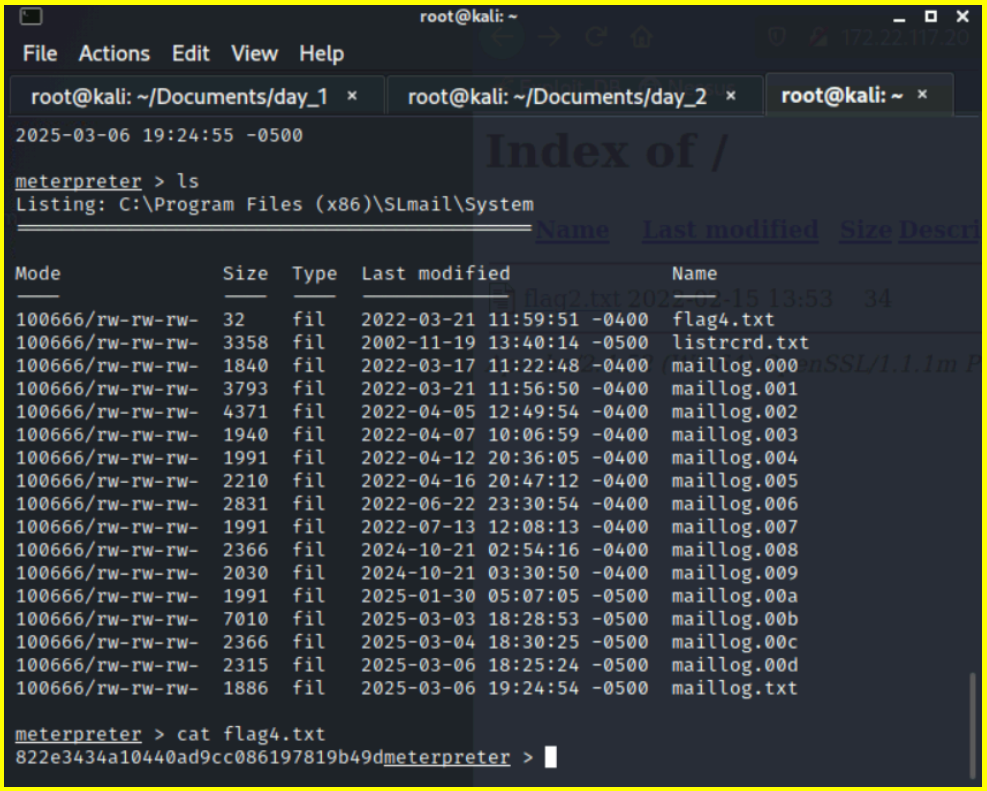


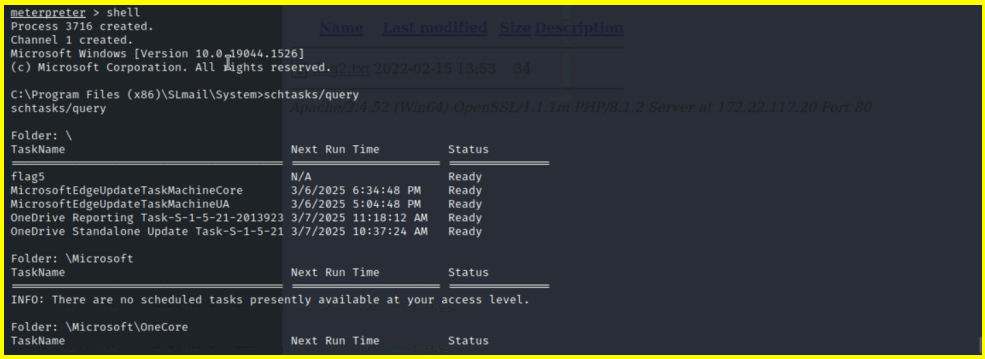


Affected Hosts	172.22.117.0/24
Remediation	The Nmap scan results provide valuable information about the open ports and running services on the target systems. By analyzing this data, you can identify potential security risks and vulnerabilities. For example, the presence of unnecessary open ports or outdated services with known vulnerabilities can indicate areas that require further investigation and remediation. (from labex.io)

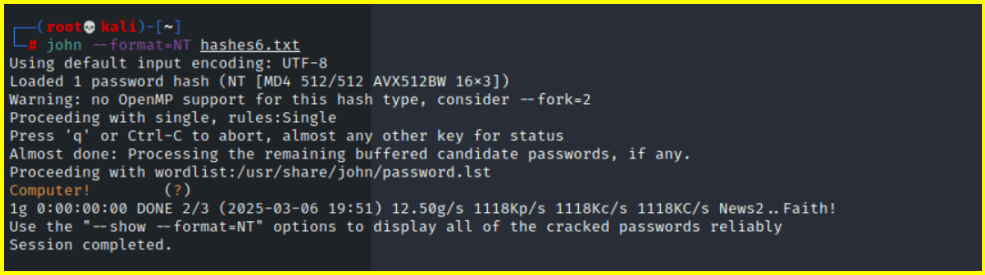
Vulnerability 3	Findings
Title	Flag 3- FTP
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Medium
Description	ftp port is open on the Windows10 machine, so we can ftp into the machine anonymously. Use anonymous for user and password to get in, then once in use get and flag3.txt to grab the flag. Once grabbed, you can exit and then in the command line, cat the txt file and flag 3 is revealed.
Images	
Affected Hosts	172.22.117.20
Remediation	Disable anonymous FTP access,Use strong authentication,Use encryption,Limit access to specific IP addresses,Use a firewall,Keep the FTP server software up to date

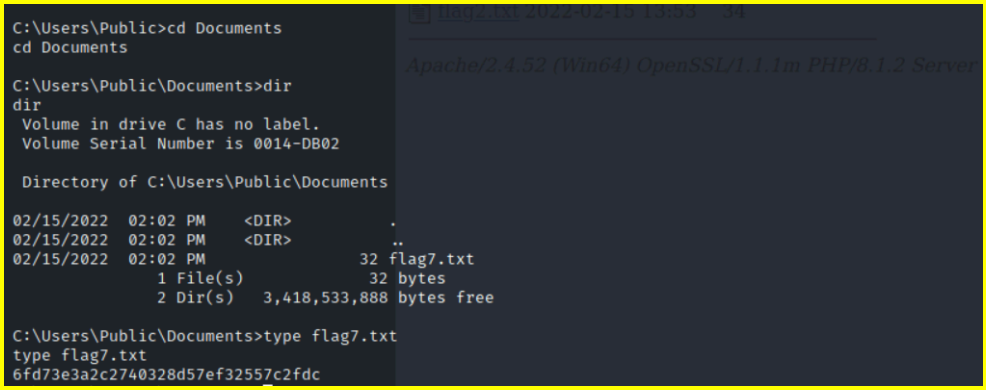
Vulnerability 4	Findings
Title	Flag 4- SLMail/SMTP

Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Medium
Description	SLMail was active on the Windows10 machine. Used exploit(windows/pop3/seattlelab_pass) in msfconsole. Set RHOSTS to 172.22.117.20 and LHOST to 172.22.117.100 and then created a meterpreter session. In the session ran ls and revealed flag4.txt, then cat the file to reveal contents.
Images	 
Affected Hosts	172.22.117.20
Remediation	Make sure system are running the latest security patches

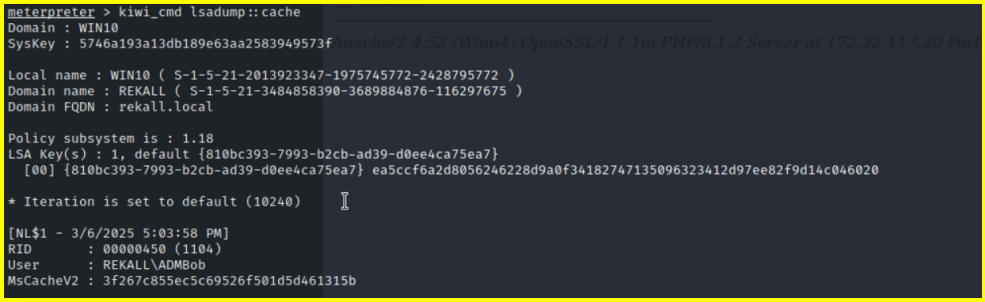
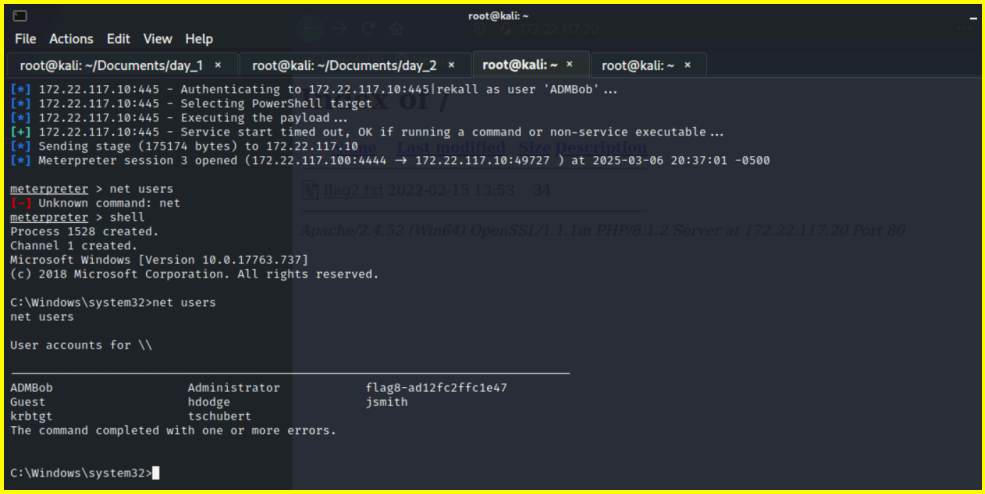
Vulnerability 5	Findings
Title	Flag 5- Scheduled Tasks
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Medium
Description	In the same meterpreter session, I created a shell. Run schtasks/query to see tasks and then run schtasks /query /tn flag5 /FO list to get contents of the task. The comment section is flag 5.
Images	
Affected Hosts	172.22.117.20
Remediation	Make sure system are running the latest security patches

Vulnerability 6	Findings
Title	Flag 6- SLMail Compromise
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Critical
Description	In the same meterpreter session, use load kiwi and then run lsa_dump_sam. This reveals a password hash that is then put into the file hashes6.txt. Use john –format=NT hashes6.txt to reveal the password which is Computer!
Images	

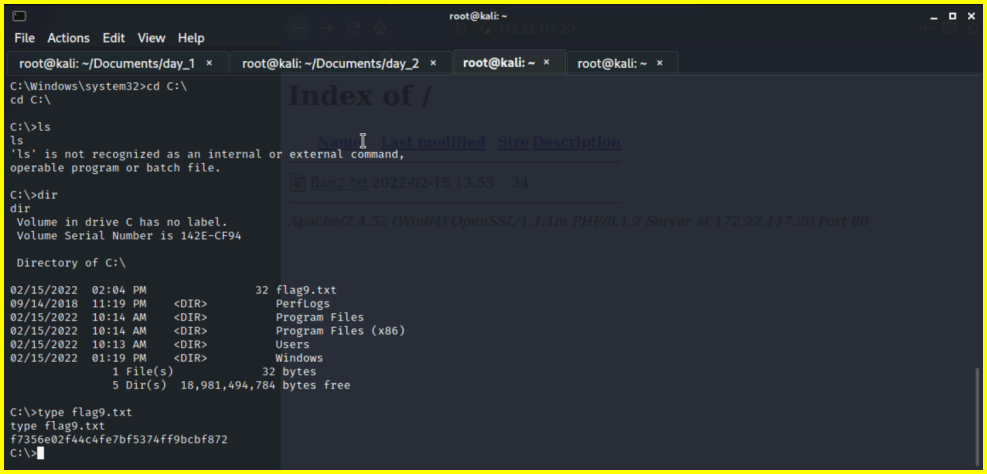
	
Affected Hosts	172.22.117.20
Remediation	Make sure system are running the latest security patches

Vulnerability 7	Findings
Title	Flag 7- Lateral Movement
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Critical
Description	Still in the meterpreter session on the Windows10 machine, I used a search command to find flag7.txt. Create a shell then move through the directories to get to the file and use type flag7.txt to reveal the contents.
Images	
Affected Hosts	172.22.117.20
Remediation	https://www.fortinet.com/resources/cyberglossary/lateral-movement Install software updates and system patches regularly,Update endpoint security solutions,Enforce the principle of least privilege (PoLP),Use multi-factor authentication (MFA),Implement network segmentation,Backup critical data,Implement zero-trust security.(from fortinet)

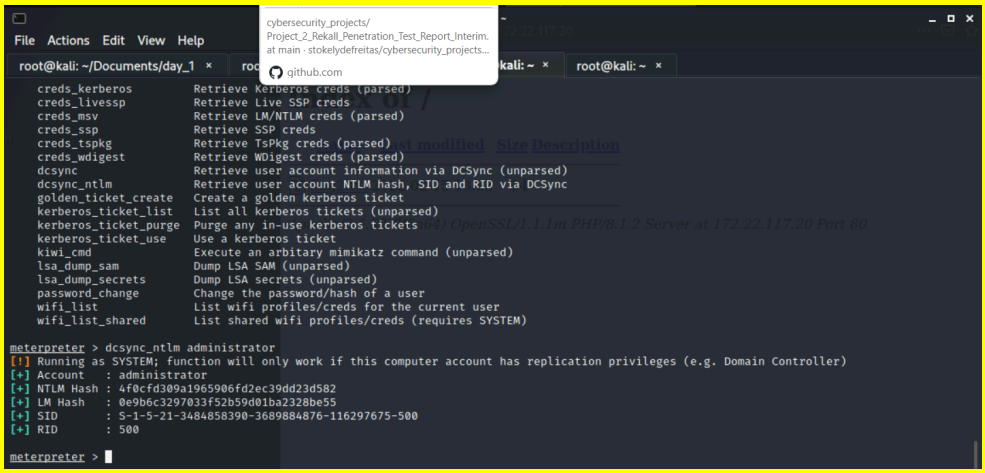
Vulnerability 8	Findings
Title	Flag 8- Attacking LSA

Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Critical
Description	In the same meterpreter session to get credentials for the WinDC01 machine, use kiwi_cmd lsadump::cache which reveals a user and password hashes. Put hashes into hash8.txt and run john hash8.txt –format=mscash2 to reveal the password Changeme! Then we use msfconsole to make a new meterpreter shell by using exploit(windows/smb/psexec) and set the necessary parameters. In the new meterpreter session we create a shell and run the command net users to see all the users on the WinDC01 machine. flag 8 and its contents are a user on the machine.
Images	 
Affected Hosts	172.22.117.20
Remediation	https://learn.microsoft.com/en-us/windows-server/security/credentials-protection-and-management/configuring-additional-lsa-protection The LSA, which includes the Local Security Authority Server Service (LSASS) process, validates users for local and remote sign-ins and enforces local security policies. Starting with Windows 8.1 and later, added protection for the LSA is provided to prevent reading memory and code injection by nonprotected processes. This feature provides added security for the credentials that LSA stores and manages(from microsoft)

Vulnerability 9	Findings
Title	Flag 9- Navigating Exploit

Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Critical
Description	In the same shell as flag 8, we can move all the way back to the C:\ directory and then use dir to list everything in this directory. Within this directory is flag9.txt and we use type flag9.txt to reveal the contents.
Images	
Affected Hosts	172.22.117.20
Remediation	https://learn.microsoft.com/en-us/windows-server/security/credentials-protection-and-management/configuring-additional-lsa-protection The LSA, which includes the Local Security Authority Server Service (LSASS) process, validates users for local and remote sign-ins and enforces local security policies. Starting with Windows 8.1 and later, added protection for the LSA is provided to prevent reading memory and code injection by nonprotected processes. This feature provides added security for the credentials that LSA stores and manages(from microsoft)

Vulnerability 10	Findings
Title	Flag 10- Default Administrator Credentials
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	High
Description	In the meterpreter session created in flag 8, we load kiwi. Run ? to see all options you can do using kiwi, and then use dsync_ntlm administrator. Once it runs, we are given account name and password hashes. Flag 10 is the NTLM Hash.

Images	
Affected Hosts	172.22.117.20
Remediation	https://learn.microsoft.com/en-us/windows-server/security/credentials-protection-and-management/configuring-additional-lsa-protection The LSA, which includes the Local Security Authority Server Service (LSASS) process, validates users for local and remote sign-ins and enforces local security policies. Starting with Windows 8.1 and later, added protection for the LSA is provided to prevent reading memory and code injection by nonprotected processes. This feature provides added security for the credentials that LSA stores and manages(from microsoft)