Cybersecurity

Penetration Test Report

Rekall Corporation

Penetration Test Report

Assessed by Ezra Shore on behalf of SusCorp Unlmtd.
March 9, 2023

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	SusCorp. Unlmtd
Contact Name	Ezra Shore
Contact Title	Penetration Tester

Document History

Version	Date	Author(s)	Comments
001	March 9, 2023	Ezra Shore	Final Report

Introduction

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

For the testing, we focused on the following:

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

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

Assessment Objective

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

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

Rekall has outlined the following objectives:

Table 1: Defined Objectives

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

Penetration Testing Methodology

Reconnaissance

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

Identification of Vulnerabilities and Services

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

Vulnerability Exploitation

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

Reporting

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

Scope

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

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

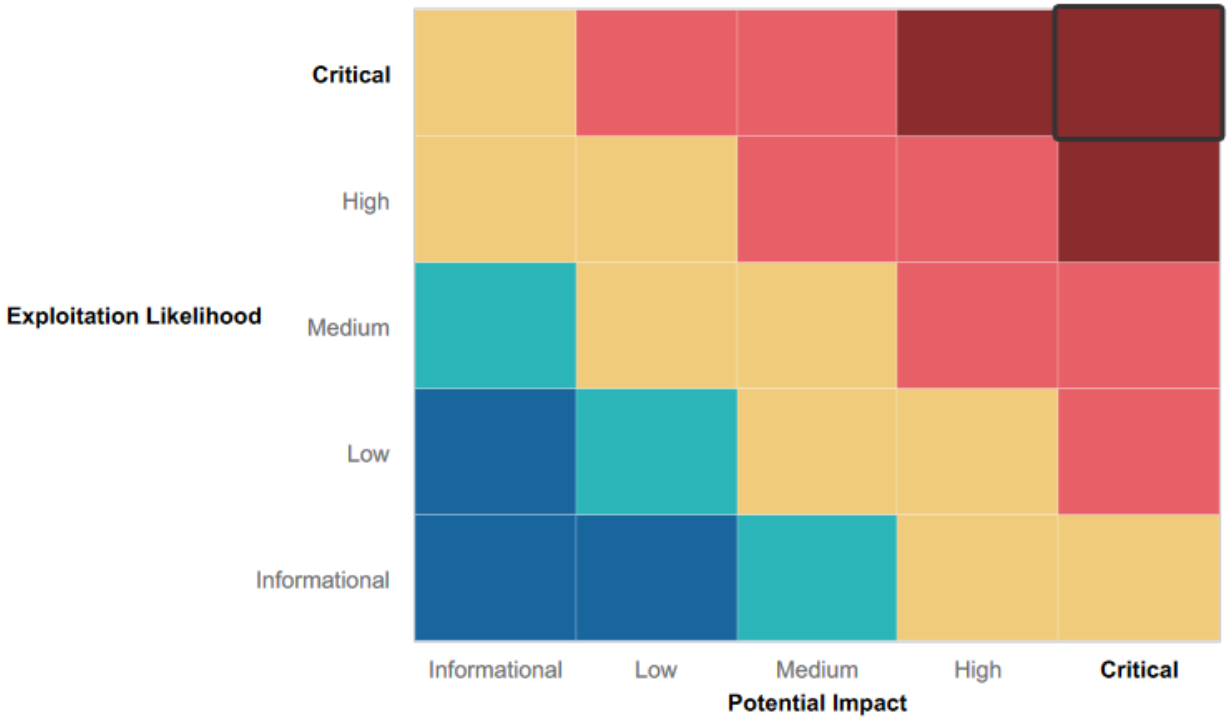
Executive Summary of Findings

Grading Methodology

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

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

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



Summary of Strengths

While SusCorp 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.

- Mitigation strategy in place for denial of DDOS Attacks to ensure network availability
- Solid Physical Security in place including Armed Guards, Man Traps, Surveillance and Physical Badging
- Current Vulnerability Scanning and continuing penetration testing(Red Teaming) to identify vulnerabilities for mitigation

Summary of Weaknesses

SusCorp 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 Application is vulnerable to XSS and SQL payload injection
- Credentials are being stored in HTML source code
- Apache web server 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
- Rekall's server physical address is publicly available
- Credentials are displayed when doing a IP lookup
- IP addresses within Rekall's IP range display potential vulnerabilities (open ports, IP addresses, etc.) when scanned
- Open ports allow for file enumeration and unauthorized access

Executive Summary

SusCorp Unltd was able to identify multiple vulnerabilities during the Penetration Testing of Rekall's IT assets, including a number of Critical vulnerabilities that could have a potentially catastrophic impact on Rekall's revenue or reputation. SusCorp Unltd was able to compromise Rekall's assets, steal sensitive data, and escalate privileges within systems, as shown below.

SusCorp Unltd was the first to test Rekall's Web Application. Because malicious script can be run on the home page, we determined that it is vulnerable to an XSS Reflected attack. Because files can be uploaded from the VR Planner web page, the Web App is also vulnerable to Local File Inclusion. On the Comments page, an XSS Stored vulnerability was discovered, which allows scripting code to be executed. SQL Injection attacks on the Login.php toolbar are also possible, and the Networking.php page is vulnerable to Command Injection attacks.

Using OSINT, open source data was determined to be exposed and viewable, and searching crt.sh revealed a stored certificate. Furthermore, user login credentials were stored plainly in the HTML source code of the Login.php page and could be viewed by simply highlighting the page in a web browser. The file robots.txt was also discovered to be exposed and easily accessible.

SusCorp Unltd then tested the Windows OS environment, and discovered that FTP Port 21 was open and vulnerable, as was Port 110, which is used for SLMail service. Metasploit was used to find this vulnerability and gain access to a password hash file, which was then cracked to reveal a high-profile username and password, which was then used to create a reverse shell. Additionally, scheduled tasks were easily visible within the Windows 10 Machine Task Scheduler, and Metepreter could be used to display directories on public Windows directories.

SusCorp Unltd was able to reveal 5 publicly exposed and vulnerable IP addresses within the Linux environment. Stolen credentials were used to gain access to a single host and elevate privileges to root. Meterpreter was used to discover another common known shell RCE execution vulnerability. The sudoers file was also accessible via Metasploit's Shellshock exploit.

In summary, these vulnerabilities could be maliciously exploited to cause catastrophic damage to the assets and the overall functionality of the business. SusCorp Unlimited has provided detailed recommendations for mitigating each of these vulnerabilities in order to avoid potential harm and loss.

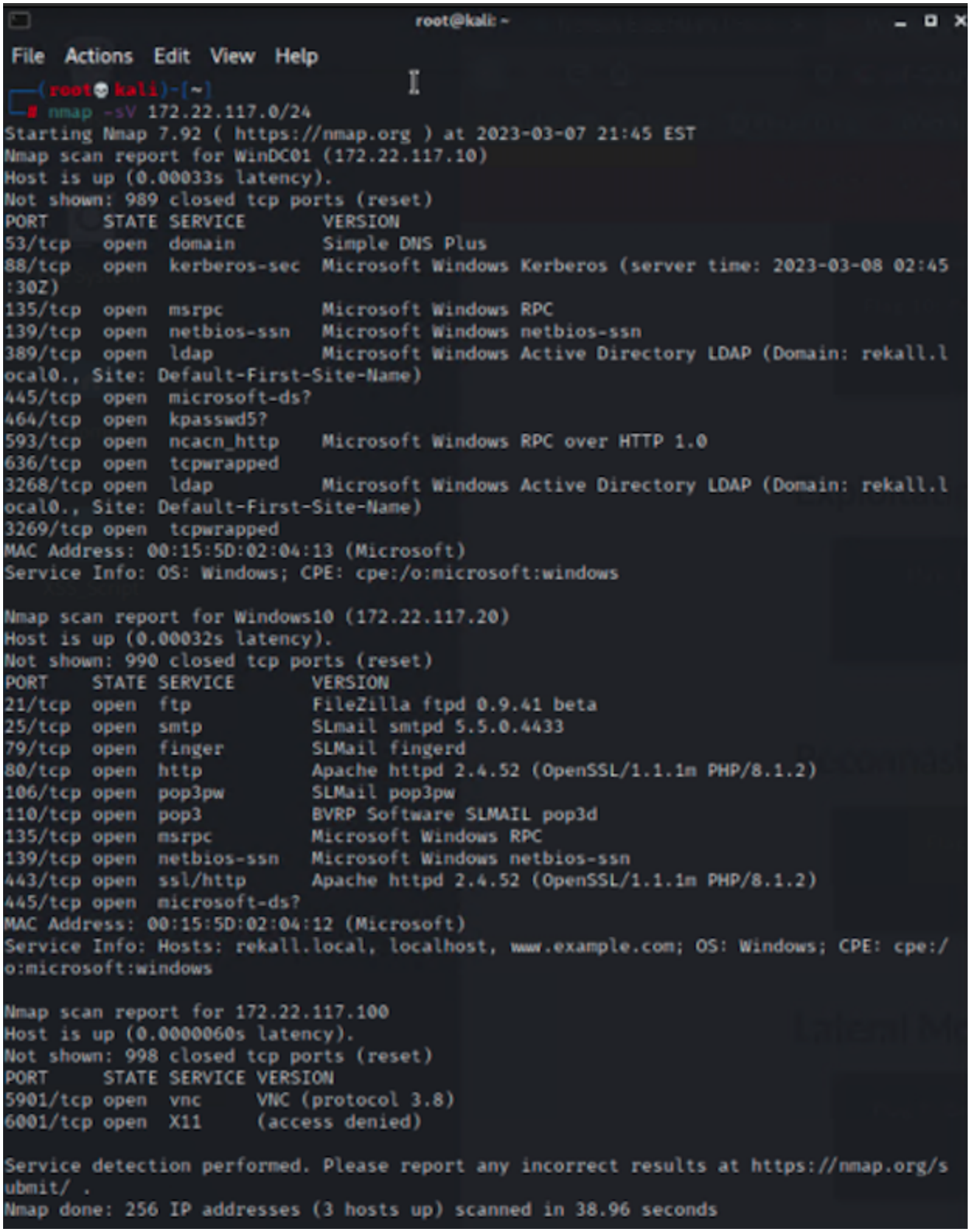
Summary Vulnerability Overview

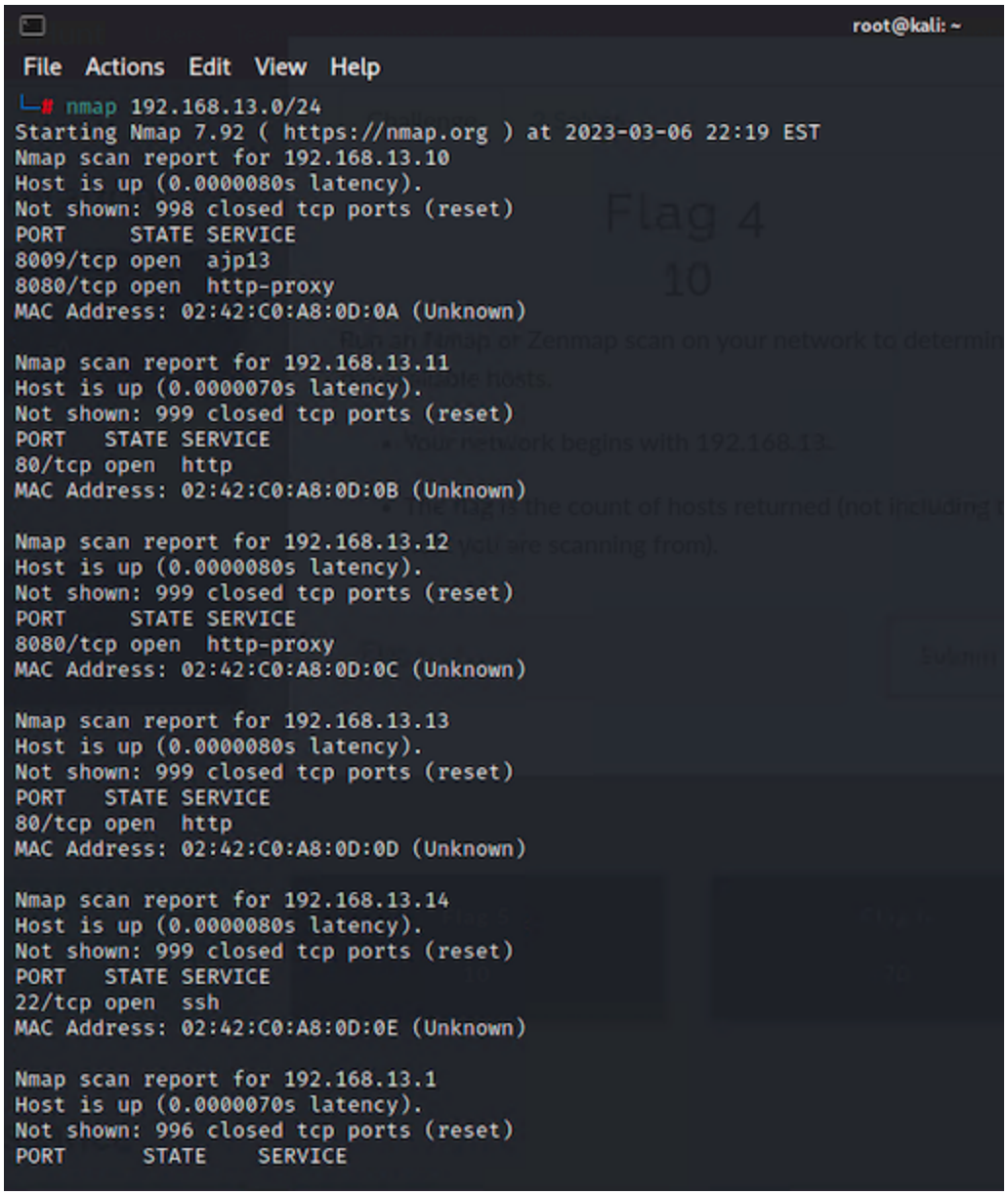
Vulnerability	Severity
Local File Inclusion	Critical
Persistent Xss(Cross Site Scripting)	Critical
SQL Injection	Critical
Command Injection	Critical
FTP Enumeration	Critical
SLMail Exploit	Critical
Sensitive Data/Cred Dump	Critical
Aggressive NMAP Scan	Critical
User Credential Exposure	Critical
Privilege Escalation	Critical
Metrerpreter shell RSE Execution	Critical
Port Scan of Subnet	Critical
NMAP Scan	High
Reflected XSS(Cross Site Scripting)	Medium
Open Source Exposed Data	Medium
Certificate Search using Crt.sh	Medium
Nessus Scan	Medium
Public Directory Search	Low

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

Scan Type	Total
Hosts	Windows 172.22.117.10 172.22.117.20 Linux 192.168.13.10 192.168.13.11 192.168.13.12 192.168.13.13 192.168.13.14
Ports	21 - FTP 22 - SSH 80 - HTTP 106 - SLMail 110 - SLMAIL

	135 - Microsoft RPC 443 - HTTPS/SSL 445 - Microsoft DS





Exploitation Risk	Total
Critical	13
High	2
Medium	4
Low	1

Vulnerability Findings

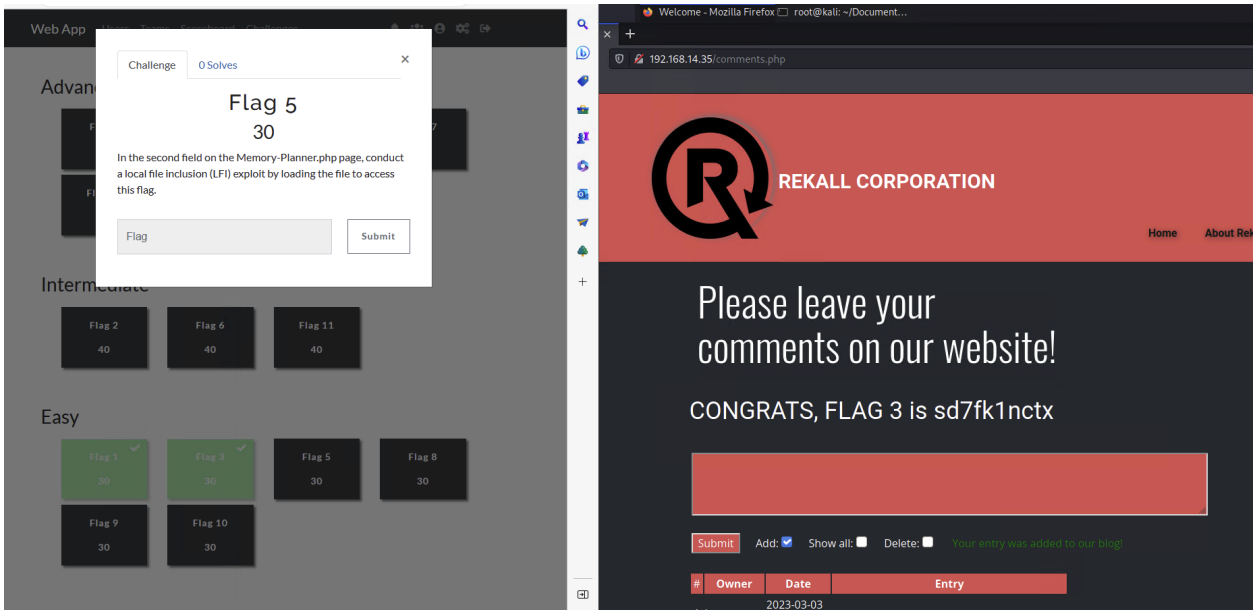
Local File Inclusion

Risk Rating: Critical

Description:
LFI successfully executed, uploaded .php file from the tool bar located on the VR Planner page.

Affected Hosts: 192.168.14.35

Remediation: Prevent file paths from being appended directly; if possible, limit API inclusion to a directory and the directories below it.



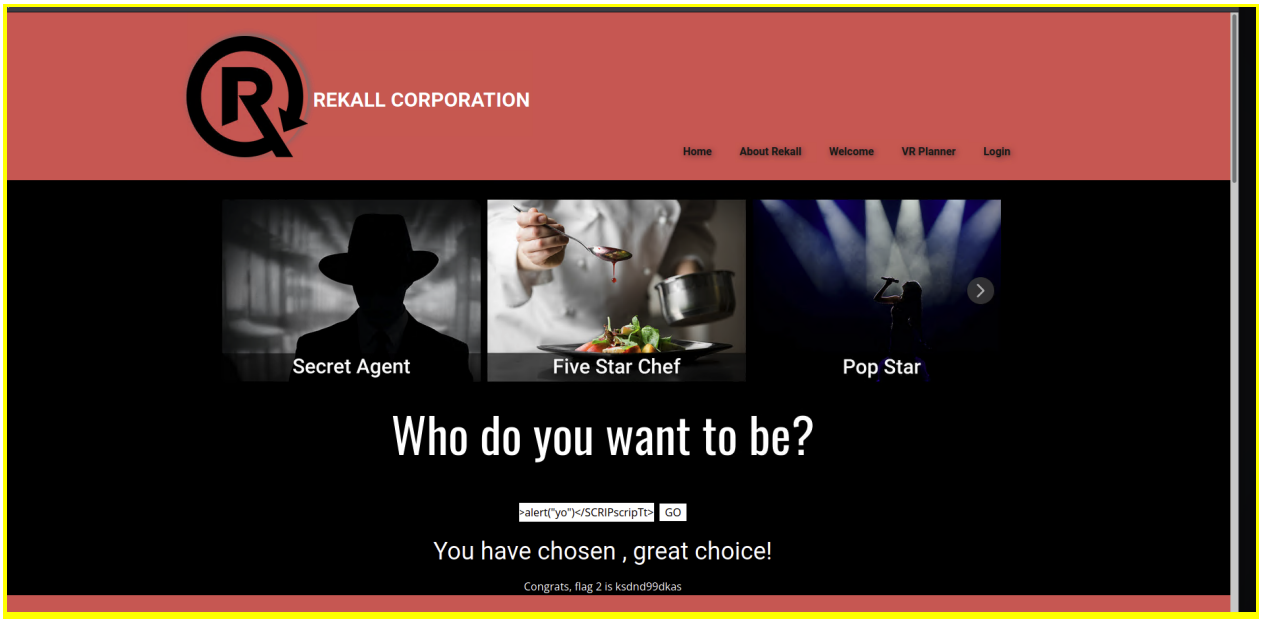
Persistent Cross Site Scripting

Risk Rating: Critical

Description:
While accessing /Comments page, enter <script>alert(“Yo”)</script> to reveal Flag 3.

Affected Hosts: 192.168.14.35

Remediation: Prevent file paths from being appended directly; if possible, limit API inclusion to a directory and the directories below it.



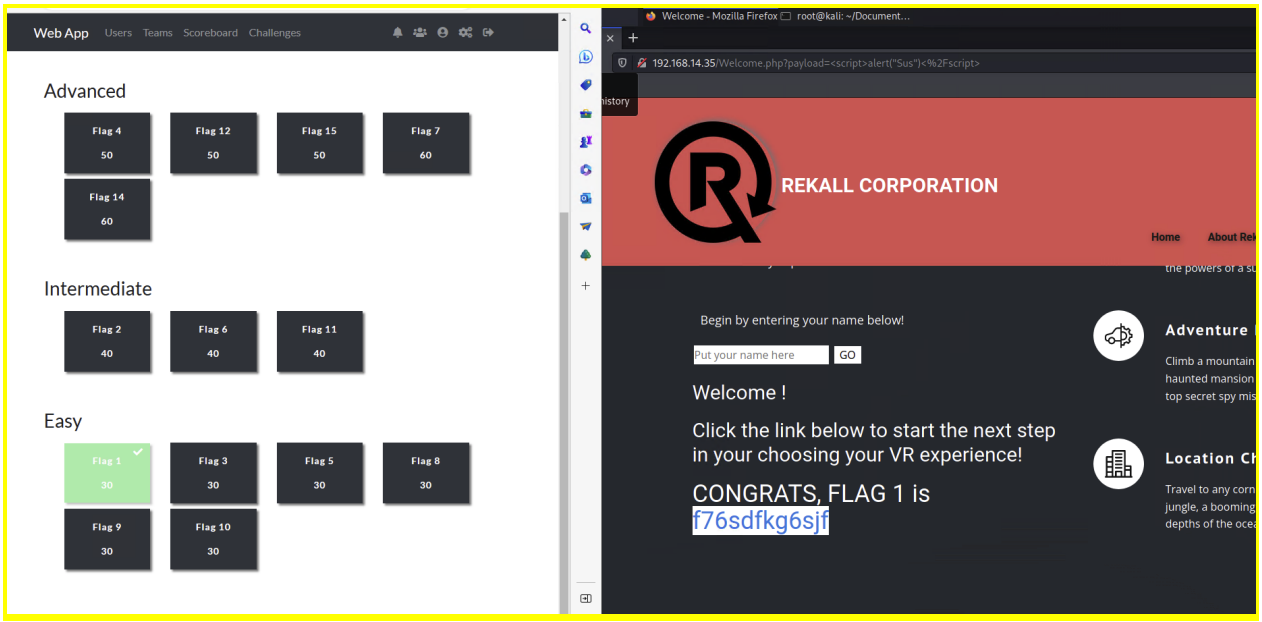
SQL Injection

Risk Rating: Critical

Description:
While accessing the /Login.php page, the payload (Name or "1=1") was successfully entered in the toolbar intended for password, resulting in the exploit Image Affected Hosts 192.168.14.35 Remediation Disallow the web app to accept direct input and/or use character escaping.

Affected Hosts: 192.168.14.35

Remediation: Prevent file paths from being appended directly; if possible, limit API inclusion to a directory and the directories below it.



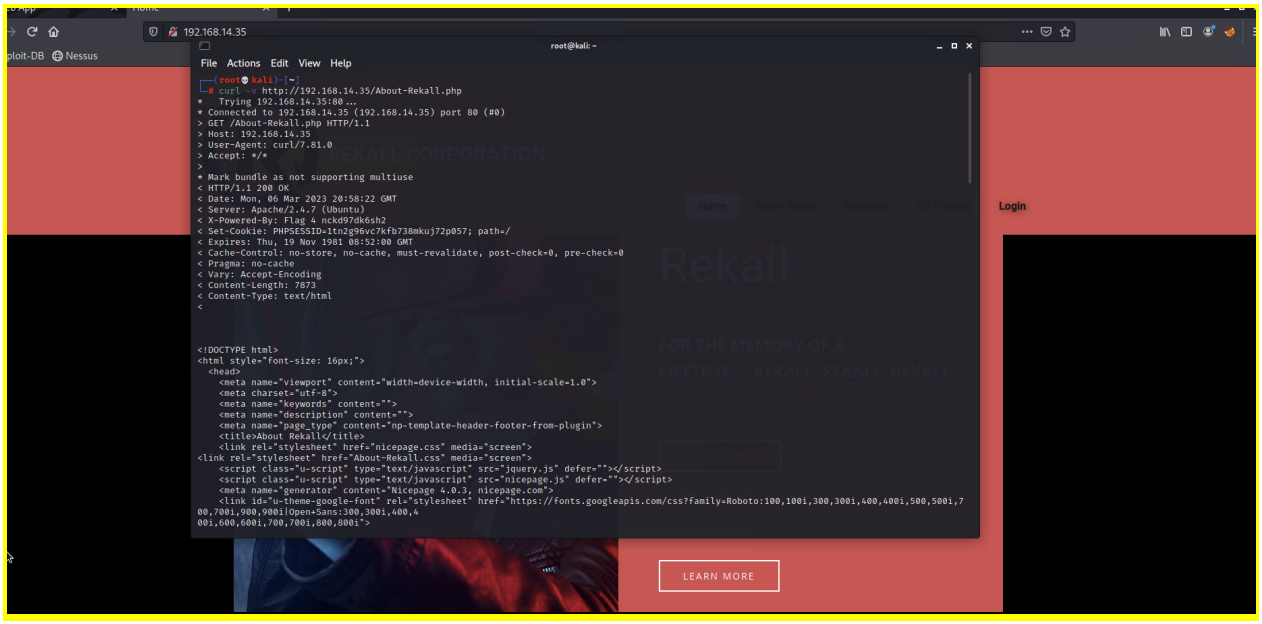
Command Injection

Risk Rating: Critical

Description:
Navigation allowed from /Networking.php to 192.168.14.35/disclaimer.php?page=vendors.txt via 192.168.14.35/networking.php Able to input “splunk” inside of toolbar intended for DNS Check Images

Affected Hosts: 192.168.14.35

Remediation: Implement input validation to prevent unauthorized access.



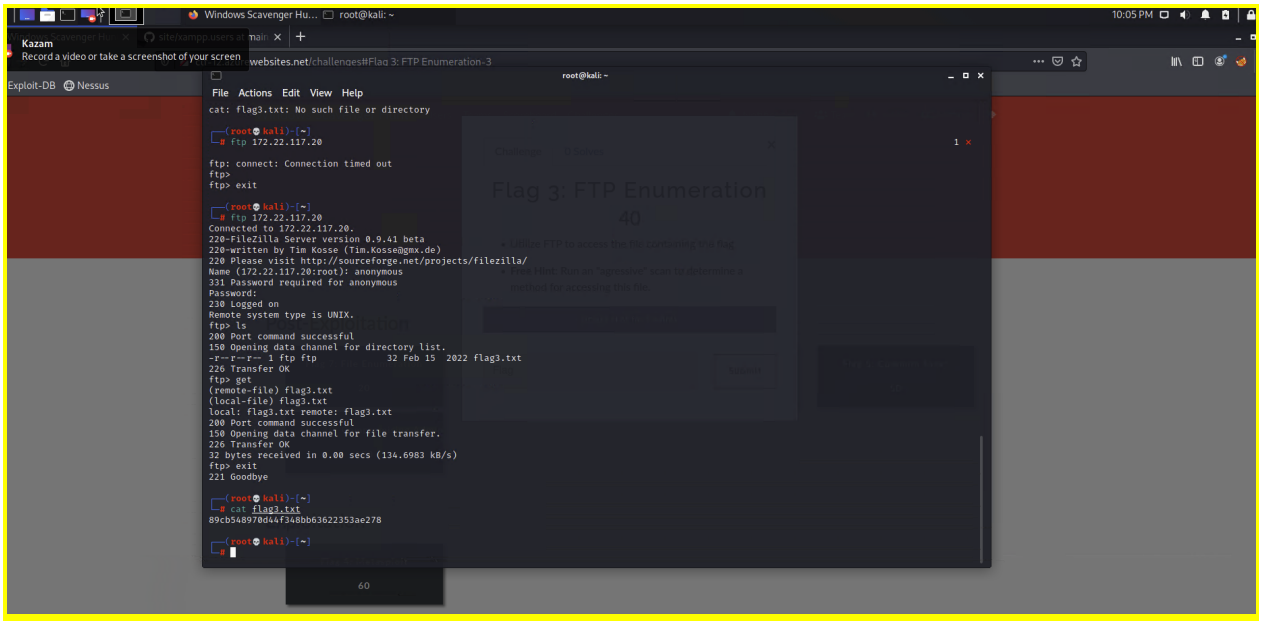
FTP Enumeration

Risk Rating: Critical

Description: Open Port 21 allows for FTP enumeration through FTP connection on host IP which resulted in successful transfer and access/download of vulnerable files Images

Affected Hosts: 172.22.117.20

Remediation: Restrict Access to Port 21



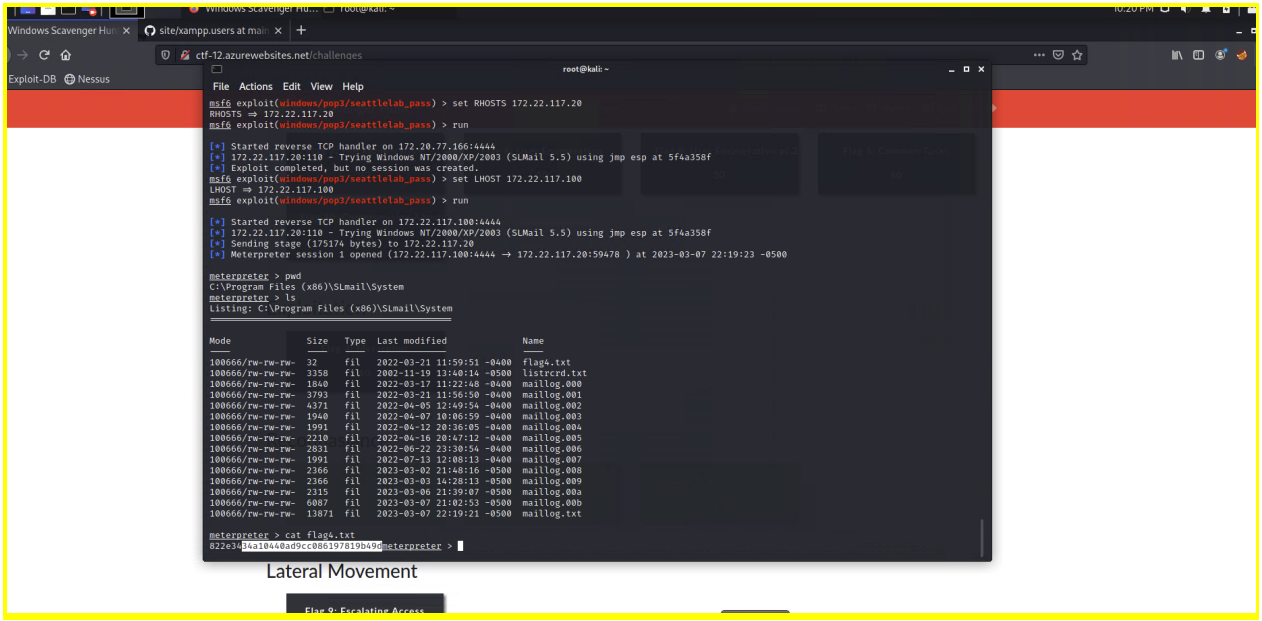
SLMail Exploit

Risk Rating: Critical

Description: Vulnerability in SLMail due to open port 110 was successfully exploited through use of windows/pop3/seattlelab_pass exploit within Metasploit which resulted in successful Meterpreter session Images

Affected Hosts: 172.22.117.20

Remediation: Restrict access to Port 110 and steer away from using SLMail service.



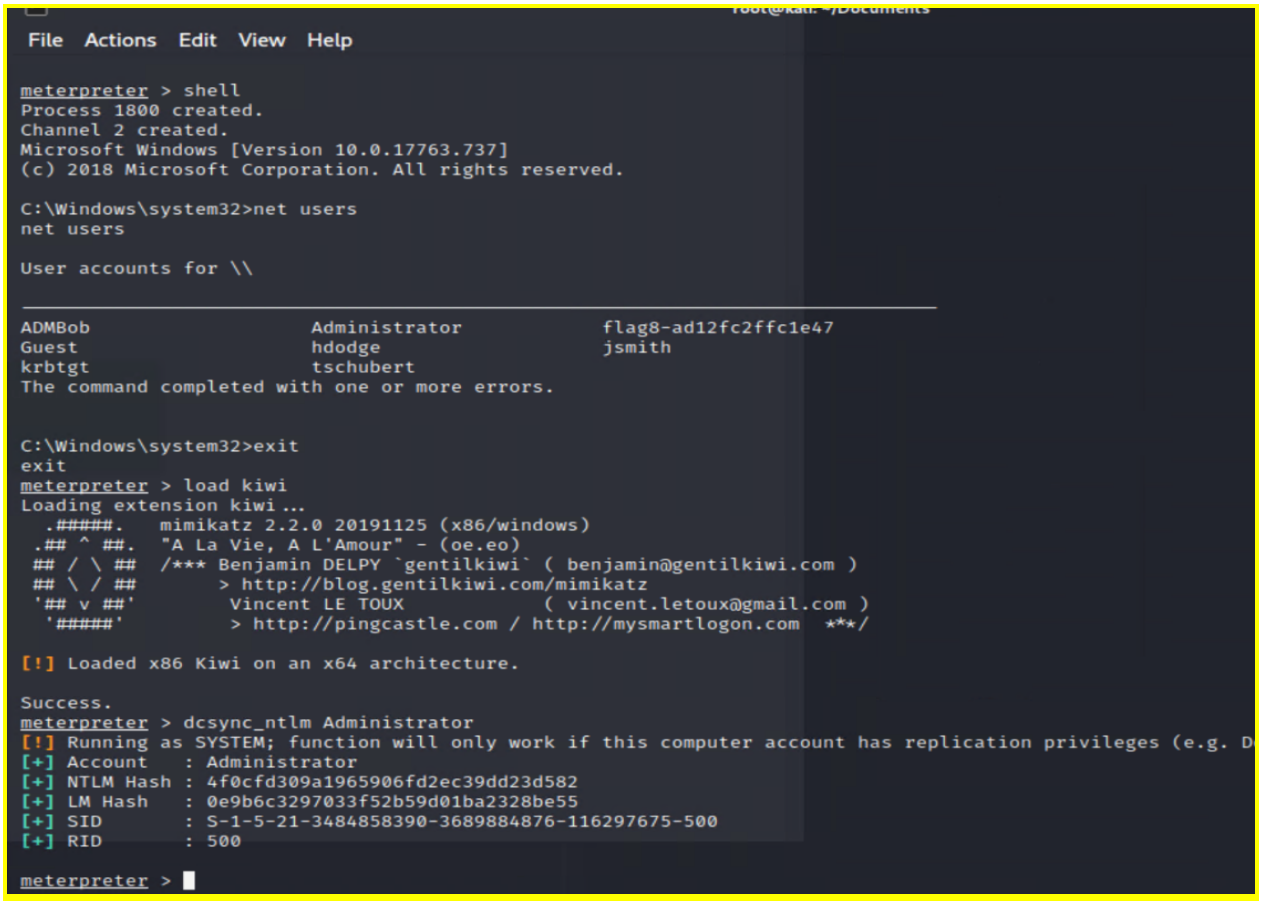
Sensitive Data/Cred Dump

Risk Rating: Critical

Description: Continued use of a previously successful exploit via a Metasploit/Meterpreter session; use Kiwi to access vulnerable passwords; file obtained. Then, within post/windows/gather/hashdump, a successful hash dump. Passwords were cracked using john, resulting in successful access to credentials and the creation of a reverse shell.

Affected Hosts: 172.22.117.20

Remediation: Restrict access to vulnerable files by updating permissions on files and user permissions; move files to an non-public domain



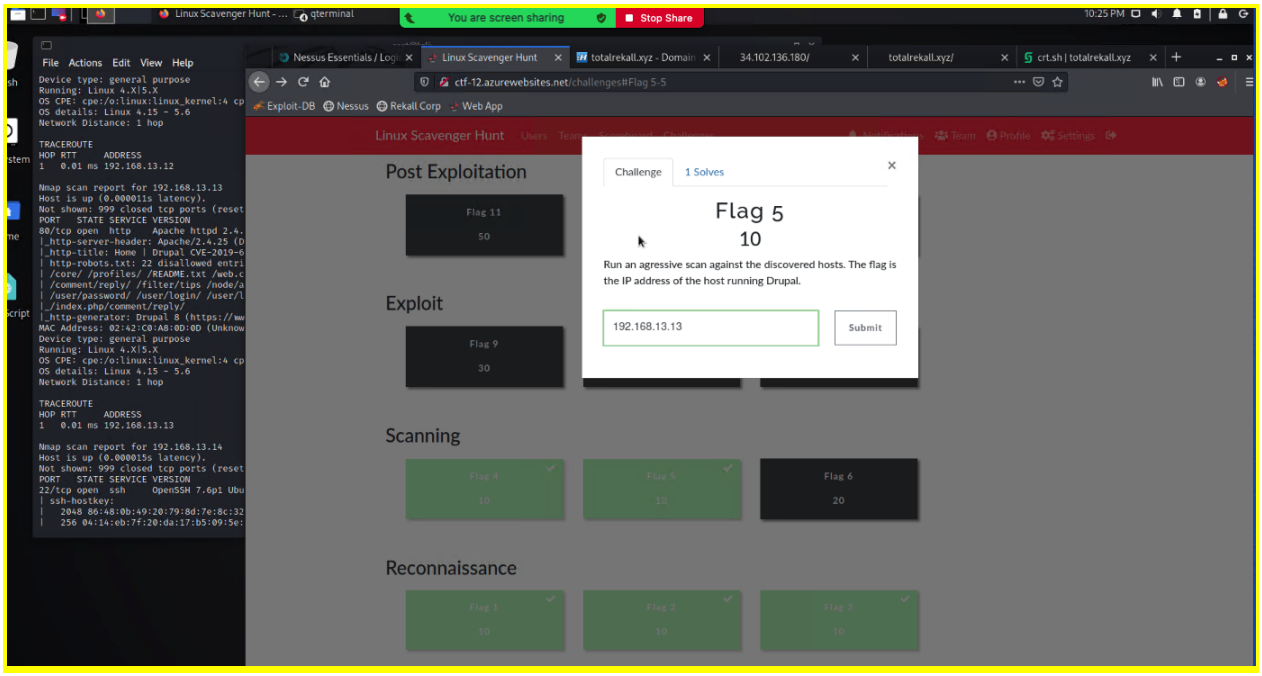
Aggressive NMAP Scan

Risk Rating: Critical

Description: Run aggressive Nmap scan (Nmap -A 192.168.13.0/28) to discover host.

Affected Hosts: 192.178.13.13

Remediation: Block probes, restrict information returned, slow down the aggressive Nmap scan, and/or return misleading information



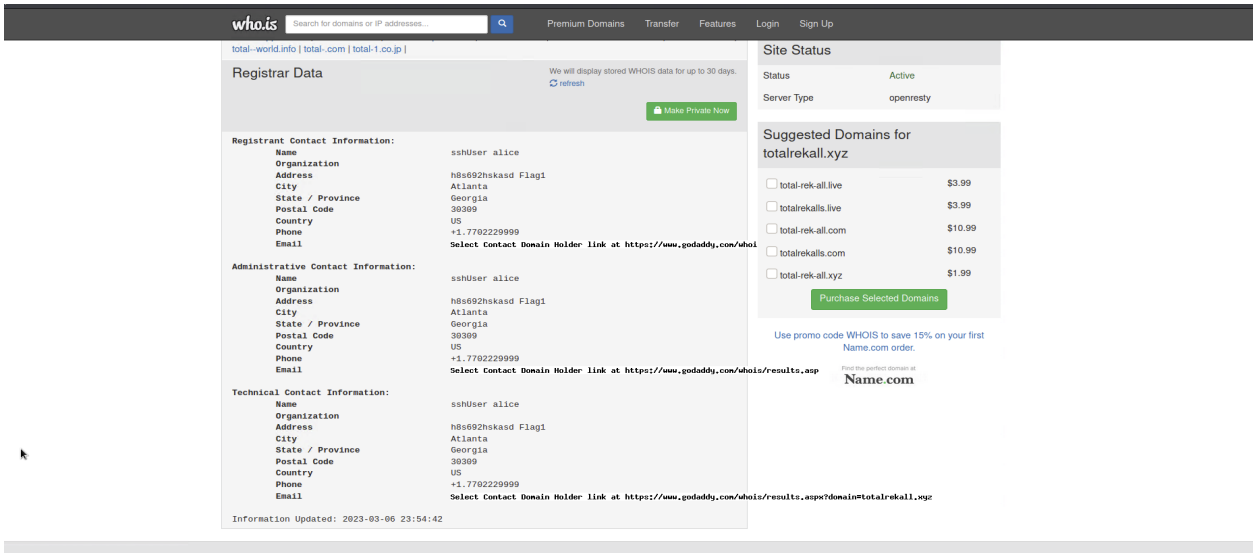
User Credential Exposure

Risk Rating: Critical

Description: User credentials are visible within HTML of the Login.php and when highlighting a page in a web browser Images.

Affected Hosts: 192.168.14.35

Remediation: Restrict access to vulnerable files by updating permissions on files and user permissions; move files to an non-public domain



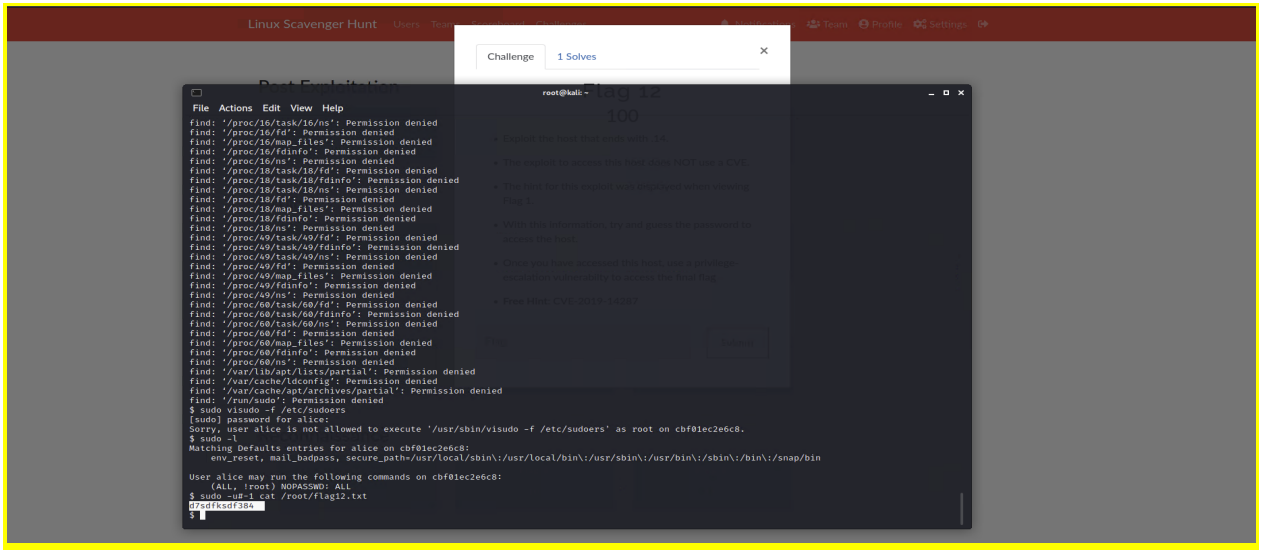
Privilege Escalation

Risk Rating: Critical

Description: Able to escalate privileges via SSH from stolen credentials.

Affected Hosts: 192.168.13.14

Remediation: Close port 22, enforce stronger credentials, and/or implement 2-factor authentication.



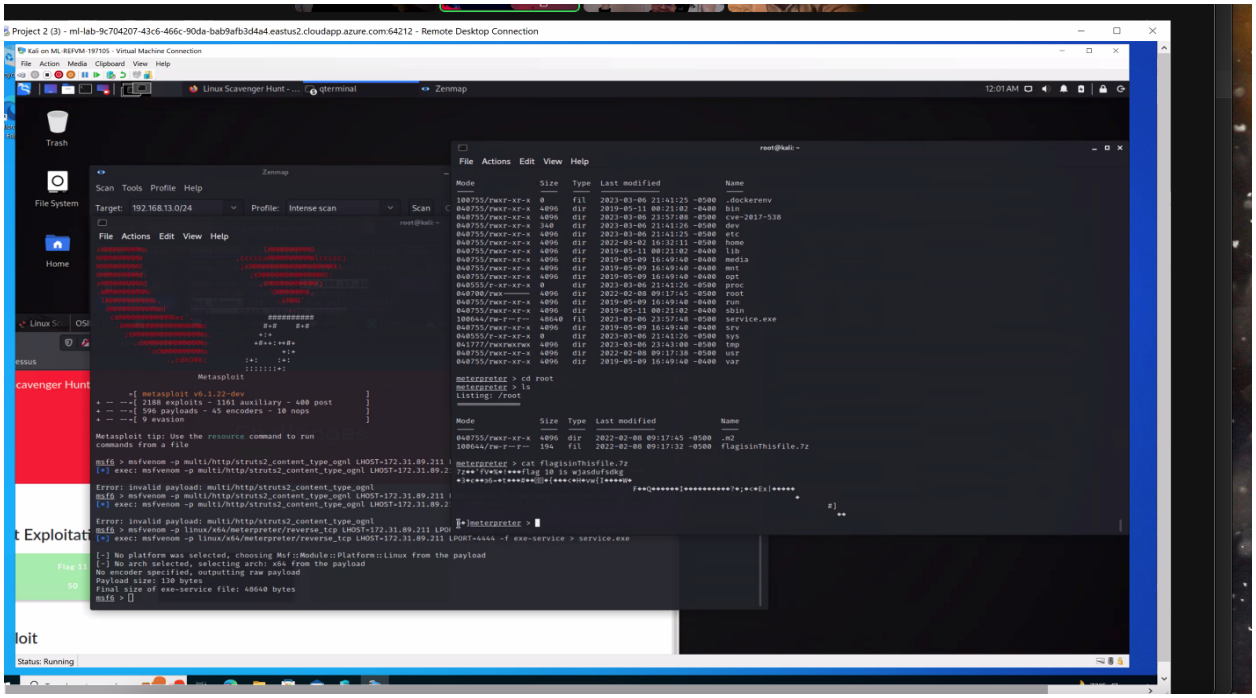
Metrerpreter shell RSE Execution

Risk Rating: **Critical**

Description: With MSFVenom, used multi/http/struts2_content_type_ognl exploit with PAYLOAD= linux/x86/shell_reverse_tcp Images

Affected Hosts: 192.168.13.12

Remediation: Apply Patches and Updates.



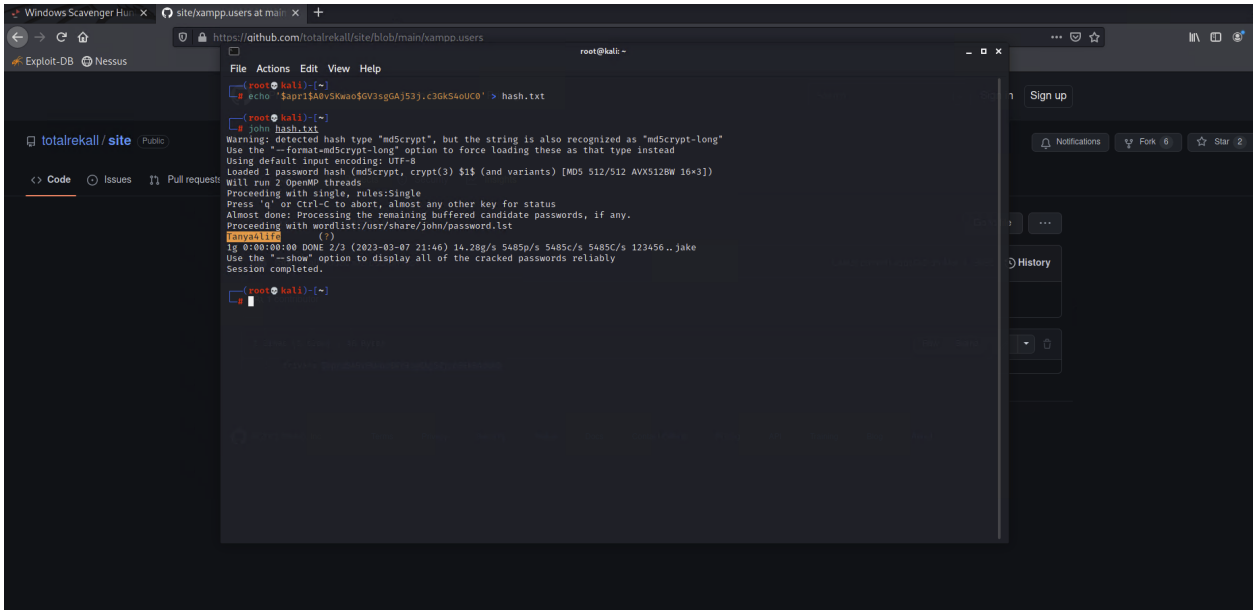
Port Scan of Subnet

Risk Rating: Critical

Description: Using credentials gained from Online to login, there was a single file there named flag2.txt containing the flag Method/Payload to Exploit:
• Nmap 172.22.117.0/24 • 172.22.117.20 has port 80 open • Opened 172.22.117.20 in a web browser • Provide credentials from Flag 1 (trivera Tanya4life) to log in • File flag2.txt is located in root directory Image

Affected Hosts: 172.22.117.20

Remediation: Use Stronger credentials and 2-factor authentication



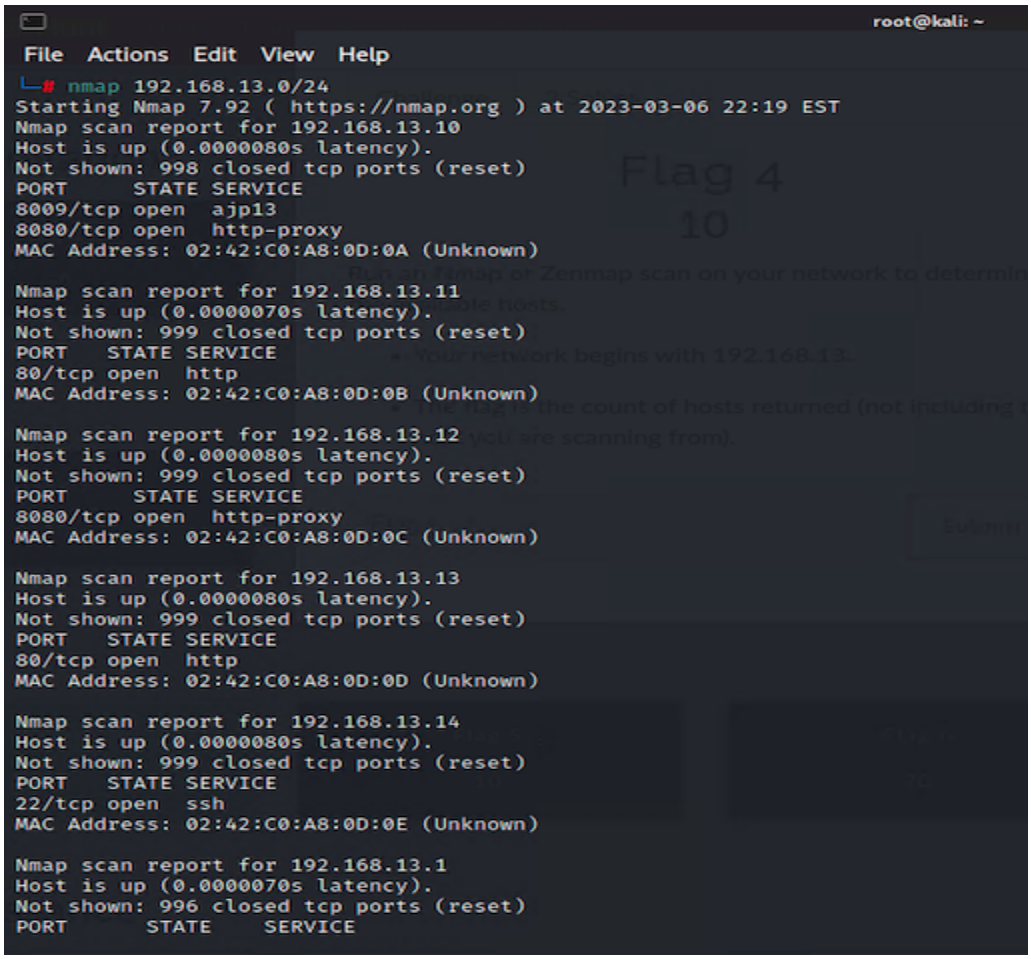
NMAp Scan

Risk Rating: High

Description:
Nmap scan on 192.168.13.0/24 revealed 5 hosts are visible with exposed IP's Image Affected Hosts 192.168.13.10 192.168.13.11 192.168.13.12 192.168.13.13 192.168.13.14.

Affected Hosts: 192.168.0/24

Remediation: Use IP Blocking for Unauthorized Users



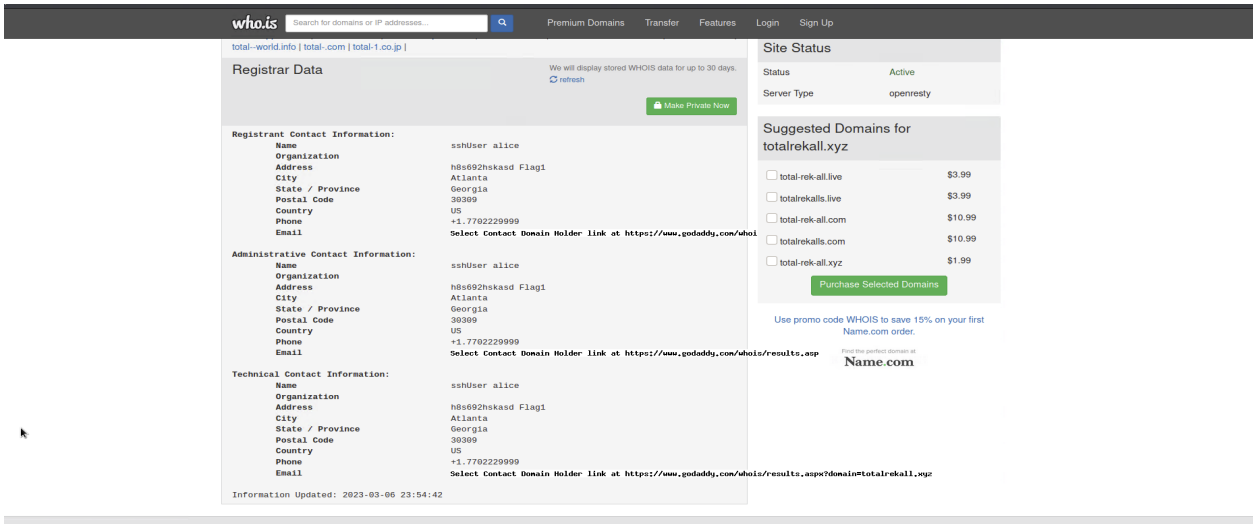
Open Source Exposure of Data

Risk Rating: **Medium**

Description: On the Domain Dossier webpage, viewed the WHOIS data with OSINT for Total rekall.xyz to access sensitive information Images

Affected Hosts: https://centralops.net/co/DomainDossier.aspx

Remediation: Ensure no sensitive data is being shared publicly, clean up WHOIS records



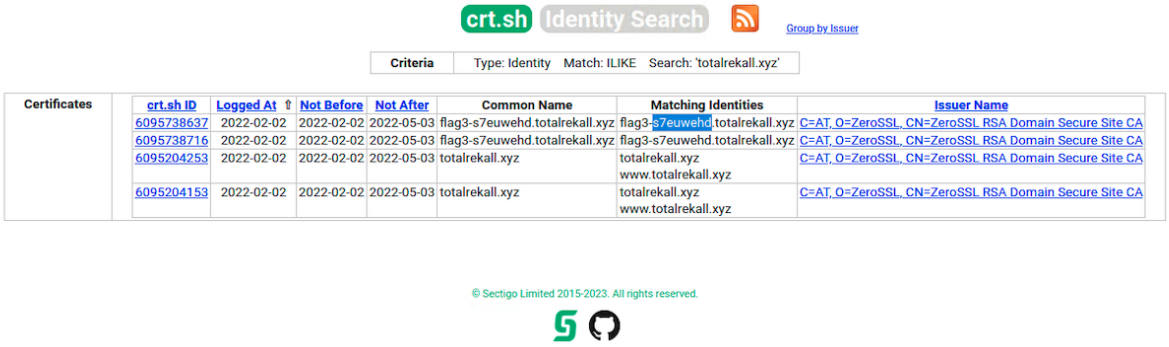
Certificate Search using CRT.sh

Risk Rating: Medium

Description: Searched for totalrekall.xyz on crt.sh, found stored certificate Image.

Affected Hosts: 34.102.136.180

Remediation:Clean up the information being exposed by the crt.sh site



Nessus Scan

Risk Rating: Medium

Description: Nessus scan revealed Apache Struts vulnerability Image

Affected Hosts: 192.168.13.12

Remediation: Update Apache Regularly