| 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](#_30j0zll)

[Contact Information 4](#_1fob9te)

[Document History 4](#_3znysh7)

[Introduction 5](#_2et92p0)

[Assessment Objective 5](#_3dy6vkm)

[Penetration Testing Methodology 6](#_2s8eyo1)

[Reconnaissance 6](#_17dp8vu)

[Identification of Vulnerabilities and Services 6](#_3rdcrjn)

[Vulnerability Exploitation 6](#_26in1rg)

[Reporting 6](#_lnxbz9)

[Scope 7](#_35nkun2)

[Executive Summary of Findings 8](#_44sinio)

[Grading Methodology 8](#_z337ya)

[Summary of Strengths 9](#_3j2qqm3)

[Summary of Weaknesses 9](#_1y810tw)

[Executive Summary Narrative](#_4i7ojhp) 10

[Summary Vulnerability Overview 1](#_2xcytpi)3

Vulnerability Findings [1](#_1ci93xb)4

# 

## Contact Information

| **Company Name** | Guardian IT Security |
| --- | --- |
| **Contact Name** | Kelly Kilpatrick |
| **Contact Title** | Chief Security Officer |

## 

## Document History

| **Version** | **Date** | **Author(s)** | **Comments** |
| --- | --- | --- | --- |
| 001 | 4/23/2023 | Kelly Kilpatrick |  |

# 

## 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:

Chart

Description automatically generated with medium confidence

### 

### 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.

* Conducting ongoing penetration testing to detect and address vulnerabilities.
* Employing proactive defensive and offensive strategies.
* Utilizing tools such as Metasploit and Nmap to safeguard against unauthorized access.
* Ensuring no vulnerability from open-source data through effective network architecture mapping.
* Implementing a mitigation strategy to counter DDOS attacks and maintain network availability.

### Summary of Weaknesses

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

* The Apache web server is outdated, exposing it to various exploits.
* Unauthorized access to password hashes can lead to password cracking and privilege escalation.
* Credentials are revealed during an IP lookup.
* Open ports enable file enumeration and unauthorized access.
* The web application is susceptible to XSS and SQL injection attacks.
* The Apache web server is outdated, exposing it to various exploits.
* Unauthorized access to password hashes can lead to password cracking and privilege escalation.
* Credentials are revealed during an IP lookup.
* Scanning IP addresses within Rekall’s range shows potential vulnerabilities, such as open ports.

## Executive Summary

During the penetration testing of Rekall’s IT assets, Guardian IT Security identified several vulnerabilities, including critical ones that could severely impact Rekall's revenue or reputation. Guardian IT Security successfully infiltrated Rekall's systems, exfiltrated sensitive data, and escalated privileges, as detailed below.

Guardian IT Security first assessed Rekall’s web application and found it vulnerable to XSS Reflected attacks, allowing malicious scripts to run on the home page. The application also has a Local File Inclusion vulnerability, permitting file uploads from the VR Planner web page. An XSS Stored vulnerability was detected on the Comments page, enabling script execution, and SQL Injection attacks were possible on the Login.php toolbar. Additionally, the Networking.php page was susceptible to Command Injection attacks.

Open-source data was exposed and accessible through OSINT, with crt.sh searches revealing a stored certificate. Alarmingly, user login credentials were stored in plain view within the HTML source code of the Login.php page and were visible by simply highlighting the page in a web browser. The file robots.txt was also exposed and accessible. Further research uncovered user credentials in a Github repository, leading to unauthorized access to the web host's files and directories. The Apache server was outdated and had a Struts vulnerability.

In the Windows OS environment, Guardian IT Security found that FTP Port 21 and Port 110 (used for SLMail service) were open and vulnerable. Using Metasploit, they discovered a password hash file, cracked it, and created a reverse shell. Scheduled tasks were visible within the Windows 10 Task Scheduler, and Metepreter was used to display directories on public Windows directories.

In the Linux environment, Guardian IT Security uncovered five publicly exposed IP addresses, with one host running Drupal. Stolen credentials allowed access to a host and privilege escalation to root. A known shell RCE execution vulnerability was discovered using Meterpreter. Additionally, the sudoers file was accessible via a Shellshock exploit in Metasploit.

In summary, these vulnerabilities could be maliciously exploited, causing significant damage to Rekall’s assets and overall business functionality. Guardian IT Security has provided detailed recommendations for mitigating each vulnerability to prevent potential harm and loss.

## 

## 

## 

## 

## Summary Vulnerability Overview

| **Vulnerability** | **Severity** |
| --- | --- |
| Local File Inclusion | **Critical** |
| Access System and Run lsa\_dump\_sam via Kiwi Shows Password Hashes | **Critical** |
| Sensitive Data Exposure | **Critical** |
| Admin Server Credentials Dumped via Kiwi | **Critical** |
| Drupal (CVE-2019-6340) | **Critical** |
| Shellshock on Web Server (Port 80) | **Critical** |
| Apache Struts (CVE-2017-5638) | **Critical** |
| Linux Privilege Escalation | **Critical** |
| SLMail Port 110 Exploited via Metasploit (SeattleMail) | **Critical** |
| SQL Injection | **Critical** |
| User Credentials Exposure | **Critical** |
| System Shell Executed with Dumped Admin Server Credentials | **Critical** |
| IPs visible with Nmap | **Critical** |
| Command Injection | **Critical** |
| Open Source Exposed Data | **High** |
| Apache Tomcat Remote Code Execution Vulnerability (CVE-2017-12617) | **High** |
| Run as ALL Sudoer (CVE-2019-14287) | **High** |
| Open FTP Port 21 | **High** |
| Sensitive Information Stored in Public/Documents Folder | **High** |
| XSS Reflected | **Medium** |
| XSS Stored | **Medium** |
| 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** | 5 |
| **Medium** | 3 |
| **Low** | 0 |

## Vulnerability Findings

| **Vulnerability 1** | **Findings** |
| --- | --- |
| **Title** | XSS Reflected |
| **Type (Web app / Linux OS / WIndows OS)** | Web App |
| **Risk Rating** | Medium |
| **Description** | Malicious script successfully reflected on host home page  <script>alert(“Julie was Here”)<script> |
| **Images** |  |
| **Affected Hosts** | 192.168.14.35 |
| **Remediation** | Input Validation |

| **Vulnerability 2** | **Findings** |
| --- | --- |
| **Title** | Local File Inclusion |
| **Type (Web app / Linux OS / WIndows OS)** | Web App |
| **Risk Rating** | Critical |
| **Description** | On the Memory-Planner.php page, we entered the following script in the “Choose Your Character” field to make a pop-up.  <sscriptcript>alert(“Julie was Here”)</scsriptript> |
| **Images** |  |
| **Affected Hosts** | 192.168.14.35 |
| **Remediation** | Ensure that all inputs are validated and sanitized before processing. This can be done both on the client-side (for immediate feedback) and server-side (to ensure security). |

| **Vulnerability 3** | **Findings** |
| --- | --- |
| **Title** | XSS Stored |
| **Type (Web app / Linux OS / WIndows OS)** | Web App |
| **Risk Rating** | Critical |
| **Description** | While accessing /Comments page, entered <script>alert(“Julie was Here”)<script> to reveal Flag 3 |
| **Images** |  |
| **Affected Hosts** | 192.168.14.35 |
| **Remediation** | Implement XSS protection to disallow injection of script code |

| **Vulnerability 4** | **Findings** |
| --- | --- |
| **Title** | Sensitive Data Exposure |
| **Type (Web app / Linux OS / WIndows OS)** | Web App |
| **Risk Rating** | Medium |
| **Description** | Inspecting elements from comments.php page, under network tab using php. Clicking on Memory-Planner.php shows sensitive information |
| **Images** |  |
| **Affected Hosts** | 192.168.14.35 |
| **Remediation** | Sanitize input data to remove any potential XSS vectors. Use a library or built-in functions to escape special characters. |

| **Vulnerability 5** | **Findings** |
| --- | --- |
| **Title** | Local File Inclusion |
| **Type (Web app / Linux OS / WIndows OS)** | Web App |
| **Risk Rating** | Critical |
| **Description** | LFI successfully executed, uploaded .php file from the toolbar located on  the VR Planner page |
| **Images** |  |
| **Affected Hosts** | 192.168.14.35 |
| **Remediation** | Disallow web app to accept direct input and/or implement character  escaping |

| **Vulnerability 6** | **Findings** |
| --- | --- |
| **Title** | LFI Exploit with File Name Manipulation |
| **Type (Web app / Linux OS / WIndows OS)** | Web App |
| **Risk Rating** | Critical |
| **Description** | Exploiting the LFI vulnerability on the 'Memory-Planner' page, the sixth flag was discovered by renaming a .jpg file to .php and uploading it. |
| **Images** |  |
| **Affected Hosts** | 192.168.14.35 |
| **Remediation** | Implement input validation unintended access |

| **Vulnerability 7** | **Findings** |
| --- | --- |
| **Title** | SQL Injection |
| **Type (Web app / Linux OS / WIndows OS)** | Windows OS |
| **Risk Rating** | Critical |
| **Description** | While accessing /Login.php page, payload (JSMITH or ‘1’=’1) was entered in  toolbar intended for password successfully resulting in exploit |
| **Images** |  |
| **Affected Hosts** | 172.22.117.20 |
| **Remediation** | Restrict access to Port 21 |

| **Vulnerability 8** | **Findings** |
| --- | --- |
| **Title** | User Credentials Exposure |
| **Type (Web app / Linux OS / WIndows OS)** | Web App |
| **Risk Rating** | Critical |
| **Description** | User credentials are visible within HTML of the Login.php and when  highlighting page in a web browser. also viewable in the inspect elements html. |
| **Images** |  |
| **Affected Hosts** | 192.168.14.35 |
| **Remediation** | Delete this information from the HTML, implement 2-factor authentication  for enhanced security. |

| **Vulnerability 9** | **Findings** |
| --- | --- |
| **Title** | Sensitive Data Exposure |
| **Type (Web app / Linux OS / WIndows OS)** | Web App |
| **Risk Rating** | Medium |
| **Description** | Unrestricted access to robots.txt page |
| **Images** |  |
| **Affected Hosts** | 192.168.14.35 |
| **Remediation** | Restrict access to robots.txt to authorized users |

| **Vulnerability 10** | **Findings** |
| --- | --- |
| **Title** | Command Injection |
| **Type (Web app / Linux OS / WIndows OS)** | Web App |
| **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** | https://centralops.net/co/DomainDossier.aspx |
| **Remediation** | Implement input validation unintended access |

| **Vulnerability 11** | **Findings** |
| --- | --- |
| **Title** | Advanced Command Injection |
| **Type (Web app / Linux OS / WIndows OS)** | Web App |
| **Risk Rating** | Medium |
| **Description** | Using an advanced command injection payload www.example.com | cat vendors.txt on the 'Networking' page, the eleventh flag was secured. |
| **Images** |  |
| **Affected Hosts** | 34.102.136.180 |
| **Remediation** | Use functions or APIs that do not require constructing command strings with user input. |

| **Vulnerability 12** | **Findings** |
| --- | --- |
| **Title** | Brute Force Attack on 'Login' Page |
| **Type (Web app / Linux OS / WIndows OS)** | Linux OS |
| **Risk Rating** | Critical |
| **Description** | A brute force attack was performed on the 'Login' page using simple password payloads in burp intruder and found the password for melina:melina ,uncovering the twelfth flag. |
| **Images** |  |
| **Affected Hosts** | 192.168.14.35 |
| **Remediation** | Account lockout policies temporarily disable an account after a certain number of failed login attempts, deterring brute force attacks. |

| **Vulnerability 13** | **Findings** |
| --- | --- |
| **Title** | PHP Injection |
| **Type (Web app / Linux OS / WIndows OS)** | Linux OS |
| **Risk Rating** | Critical |
| **Description** | Exploiting a PHP injection vulnerability on the 'Souvenirs' page using the payload ;system(‘cat/etc/passwd’) revealed the thirteenth flag. |
| **Images** |  |
| **Affected Hosts** | 192.178.13.12 |
| **Remediation** | When interacting with databases, always use prepared statements to prevent SQL injection, which can lead to PHP injection in some scenarios. |

| **Vulnerability 14** | **Findings** |
| --- | --- |
| **Title** | Session Management Vulnerability |
| **Type (Web app / Linux OS / WIndows OS)** | Web App |
| **Risk Rating** | Critical |
| **Description** | Exploiting a session management vulnerability on the 'admin\_legal\_data.php' page using the Burp Intruder tool to brute force session IDs, the fourteenth flag was captured. |
| **Images** |  |
| **Affected Hosts** | 192.168.14.35 |
| **Remediation** | Ensure that the entire session, including the login process and subsequent data exchange, is encrypted using HTTPS. |

| **Vulnerability 15** | **Findings** |
| --- | --- |
| **Title** | Directory Traversal |
| **Type (Web app / Linux OS / WIndows OS)** | Web App |
| **Risk Rating** | Medium |
| **Description** | The fifteenth flag was obtained by exploiting a directory traversal vulnerability present on the 'disclaimer.php' page. Through the exploitation of a common injection exploit, an attacker was able to navigate through the directory structure, ultimately resulting in the discovery of the fifteenth and final flag. |
| **Images** |  |
| **Affected Hosts** | 192.168.14.35 |
| **Remediation** | Instead of allowing arbitrary file paths to be accessed, create a whitelist of permitted directories or files that can be accessed through the 'disclaimer.php' page. Only allow access to these whitelisted paths. |

| **Vulnerability 16** | **Findings** |
| --- | --- |
| **Title** | Open source exposed data |
| **Type (Web app / Linux OS / WIndows OS)** | Web App |
| **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** | 192.168.13.12 |
| **Remediation** | Perform regular updates on Apache |

| **Vulnerability 17** | **Findings** |
| --- | --- |
| **Title** | NPrivilege Escalation |
| **Type (Web app / Linux OS / WIndows OS)** | Linux OS |
| **Risk Rating** | Critical |
| **Description** | looking up the records of totalrekall.xyz showed a txt record of flag 2 |
| **Images** |  |
| **Affected Hosts** | 192.168.13.14 |
| **Remediation** | Periodically review all TXT records associated with your domain to ensure they contain only essential and up-to-date information. |

| **Vulnerability 18** | **Findings** |
| --- | --- |
| **Title** | Certificate Search via crt.sh |
| **Type (Web app / Linux OS / WIndows OS)** | Linux OS |
| **Risk Rating** | Critical |
| **Description** | Searched for totalrekall.xyz on crt.sh, found stored certificate |
| **Images** |  |
| **Affected Hosts** | 192.168.13.12 |
| **Remediation** | Regularly monitor Certificate Transparency logs for new certificates issued for your domain. |

| **Vulnerability 19** | **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’ |
| **Images** |  |
| **Affected Hosts** | 192.168.13.14 |
| **Remediation** | Implement network segmentation to isolate critical assets and restrict lateral movement within the network. |

| **Vulnerability 20** | **Findings** |
| --- | --- |
| **Title** | Aggressive Nmap Scan |
| **Type (Web app / Linux OS / WIndows OS)** | Windows OS |
| **Risk Rating** | Critical |
| **Description** | Ran aggressive Nmap scan (Nmap -A 192.168.13.0/28) to discover host  running Drupal |
| **Images** |  |
| **Affected Hosts** | 172.22.117.20 |
| **Remediation** | Block probes, restrict information returned, slow down the aggressive Nmap scan, and/or return misleading information |

| **Vulnerability 21** | **Findings** |
| --- | --- |
| **Title** | Nessus scan |
| **Type (Web app / Linux OS / WIndows OS)** | Web App |
| **Risk Rating** | Medium |
| **Description** | Nessus scan revealed Apache Struts vulnerability |
| **Images** |  |
| **Affected Hosts** | 172.22.117.20 |
| **Remediation** | Continuously monitor your network for security threats and anomalies. |

| **Vulnerability 22** | **Findings** |
| --- | --- |
| **Title** | Meterpreter shell RCE execution (CVE 2017-5638)Drupal (CVE-2019-6340) |
| **Type (Web app / Linux OS / WIndows OS)** | Linux OS |
| **Risk Rating** | Critical |
| **Description** | With Meterpreter, used multi/http/struts2\_content\_type\_ognl exploit with  PAYLOAD= linux/x86/shell\_reverse\_tcp |
| **Images** |  |
| **Affected Hosts** | 192.168.13.12 |
| **Remediation** | Apply updates per vendor instructions |

| **Vulnerability 23** | **Findings** |
| --- | --- |
| **Title** | Shellshock on Web Server (Port 80) |
| **Type (Web app / Linux OS / WIndows OS)** | Windows 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 |
| **Images** |  |
| **Affected Hosts** | 172.22.117.20 |
| **Remediation** | Edit the sudoers file to limit access for all sudo accounts, limit the orarom  user from running commands (enabled for patching from Oracle platinum  support), except for sudo su to root  orarom ALL = ALL, !/bin/s |

| **Vulnerability 24** | **Findings** |
| --- | --- |
| **Title** | Run as ALL Sudoer (CVE-2019-14287) |
| **Type (Web app / Linux OS / WIndows OS)** | Windows OS |
| **Risk Rating** | High |
| **Description** | user to run commands as the root user even if they are restricted from doing so. This vulnerability is critical because it can allow unauthorized users to escalate their privileges, potentially gaining full control of the system. |
| **Images** |  |
| **Affected Hosts** | 192.168.13.14 |
| **Remediation** | Consider using tools like auditd to track usage of sudo commands. |

| **Vulnerability 25** | **Findings** |
| --- | --- |
| **Title** | Username and Password Hash in Rep |
| **Type (Web app / Linux OS / WIndows OS)** | Web App |
| **Risk Rating** | Critical |
| **Description** | Using credentials found in Github repo, was able to crack password and gain  access using john the ripper. |
| **Images** |  |
| **Affected Hosts** | Total Rekall web server |
| **Remediation** | Restrict access and remove credentials from Github |

| **Vulnerability 26** | **Findings** |
| --- | --- |
| **Title** | Port Scan of Subnet |
| **Type (Web app / Linux OS / WIndows OS)** | Web App |
| **Risk Rating** | Critical |
| **Description** | Using credentials gained from Github repo 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 |
| **Images** |  |
| **Affected Hosts** | 172.22.117.20 |
| **Remediation** | Require stronger credentials and or 2-factor authentication |

| **Vulnerability 27** | **Findings** |
| --- | --- |
| **Title** | FTP Enumeration |
| **Type (Web app / Linux OS / WIndows OS)** | Windows OS |
| **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 |

| **Vulnerability 28** | **Findings** |
| --- | --- |
| **Title** | SLMail Exploit |
| **Type (Web app / Linux OS / WIndows OS)** | Windows OS |
| **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, disuse SLMail service and replace |

| **Vulnerability 29** | **Findings** |
| --- | --- |
| **Title** | Windows 10 Machine Task Scheduler |
| **Type (Web app / Linux OS / WIndows OS)** | Windows OS |
| **Risk Rating** | Medium |
| **Description** | Within the Windows 10 machine, able to view details of scheduled tasks |
| **Images** |  |
| **Affected Hosts** | 172.22.117.20 |
| **Remediation** | Change permissions of accounts to restrict unauthorized access |

| **Vulnerability 30** | **Findings** |
| --- | --- |
| **Title** | Access System and Run lsa\_dump\_sam via Kiwi Shows Password Hashes |
| **Type (Web app / Linux OS / WIndows OS)** | Windows OS |
| **Risk Rating** | Critical |
| **Description** | Using Kiwi, I was able to lsa\_dump\_sam to find User Flag 6 with NTLM Hash. Using john was able to crack the password |
| **Images** |  |
| **Affected Hosts** | 172.22.117.20 |
| **Remediation** | Investigate the lsa\_dump\_sam output to identify which user accounts' hashes have been dumped. |

| **Vulnerability 31** | **Findings** |
| --- | --- |
| **Title** | Public Directory Search |
| **Type (Web app / Linux OS / WIndows OS)** | Windows OS |
| **Risk Rating** | Medium |
| **Description** | Navigating to the Users\Public\Documents directory, used the ls command in  Meterpreter to display files |
| **Images** |  |
| **Affected Hosts** | 172.22.117.20 |
| **Remediation** | Move sensitive files to more secure areas and/or restrict unauthorized access |

| **Vulnerability 32** | **Findings** |
| --- | --- |
| **Title** | Admin Server Credentials Dumped via Kiwi |
| **Type (Web app / Linux OS / WIndows OS)** | Windows OS |
| **Risk Rating** | Critical |
| **Description** | Using kiwi on the WIN10 domain to use the command kiwi\_cmd lsadump::cache to reveal User ADMBob and the MsCacheV2 hash to crack with john the ripper. With the cracked credentials ADMBOB:Changeme! we then used exploit /windows/smb/psexec which would allow the ability to remotely execute commands. With an open session we were able to list all users on the machine. |
| **Images** |  |
| **Affected Hosts** | 172.22.117.20 |
| **Remediation** | Force a password reset for all administrative accounts immediately. Consider all administrative accounts compromised if hashes were dumped. Ensure new passwords are strong and unique. |

| **Vulnerability 33** | **Findings** |
| --- | --- |
| **Title** | Escalating Access |
| **Type (Web app / Linux OS / WIndows OS)** | Windows OS |
| **Risk Rating** | Critical |
| **Description** | searching in the “heart” of the machine, we searched the C:/ drive and used ls to find flag9.txt |
| **Images** |  |
| **Affected Hosts** | 172.22.117.20 |
| **Remediation** | Immediately disconnect the affected machine from the network to prevent further malicious activity and lateral movement by the attacker. |

| **Vulnerability 34** | **Findings** |
| --- | --- |
| **Title** | Administrator credential Access in kiwi performing dcsync\_ntlm |
| **Type (Web app / Linux OS / WIndows OS)** | Windows OS |
| **Risk Rating** | Critical |
| **Description** | Using SYSTEM access on the meterpreter, we loaded kiwi and used dcsync\_ntlm administrator to receive password hash for administrator |
| **Images** |  |
| **Affected Hosts** | 172.22.117.20 |
| **Remediation** | Identify and terminate any malicious processes, such as Mimikatz or Kiwi, running on compromised systems using tools like Task Manager, Process Explorer, or PowerShell. |