Cybersecurity

Penetration Test Report

Rekall Corporation

Penetration Test Report

Student Note: Complete all sections highlighted in yellow.

Confidentiality Statement

This document contains confidential and privileged information from Rekall Inc. (henceforth known as Rekall). The information contained in this document is confidential and may constitute inside or non-public information under international, federal, or state laws. Unauthorized forwarding, printing, copying, distribution, or use of such information is strictly prohibited and may be unlawful. If you are not the intended recipient, be aware that any disclosure, copying, or distribution of this document or its parts is prohibited.

Table of Contents

Contact Information

Company Name	CyberLux
Contact Name	leeroy samudio
Contact Title	PenTester

Document History

Version	Date	Author(s)	Comments
001	01/13/2023	leeroy samudio	

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.

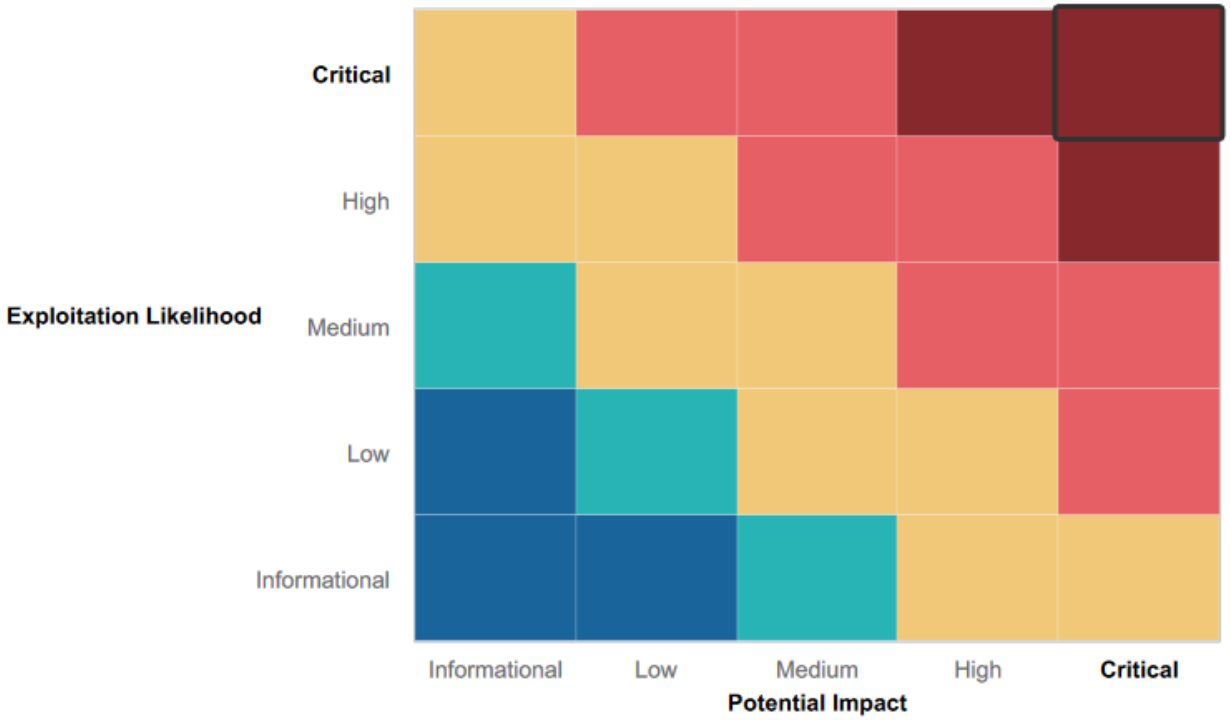
Executive Summary of Findings

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.

- To ensure network availability, a DDOS attack mitigation plan is in place.
- Due to the mapping network architecture, there is no open source data compromise
- Metasploit, Hashcat, and Nmap are used to prevent illegal access.
- A proactive defensive and attacking approach
- Current and ongoing penetration testing to uncover and mitigate vulnerabilities

Summary of Weaknesses

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

- Web Application is vulnerable to SQL injection and XSS
- Credentials are saved within HTML source code
- The Apache web server is obsolete and susceptible to several attacks.
- The SLMail server is susceptible to exploits that give shell access
- Unauthorized access to password hashes permits password cracking and elevation of privileges
- The physical address of Rekall's server is publicly disclosed.
- When performing an IP lookup, credentials are shown.
- IP addresses within Rekall's IP range are indicative of opportunity.
- Scans reveal vulnerabilities (open ports, IP addresses, etc.)
- Open ports permit file scanning and unwanted access.

Executive Summary

The purpose of this penetration testing (pentest) report is to provide Totalrekall with a comprehensive assessment of the security posture of its [systems/networks/applications] and to identify vulnerabilities and weaknesses that could be exploited by an attacker. The scope of the pentest included 192.168.13.1, 192.168.13.10, 192.168.13.13, 192.168.13.12, 192.168.13.14.

Key Findings:

19 high severity vulnerabilities were identified. These vulnerabilities could potentially be exploited by an attacker to gain unauthorized access to sensitive data or systems, or to compromise the availability of Totalrekall's services.

10 medium severity vulnerabilities were identified. While these vulnerabilities may not pose as great a risk as the high severity vulnerabilities, they should still be addressed in a timely manner to reduce the overall risk to Totalrekall.

5 low severity vulnerabilities were identified. These vulnerabilities represent a lower risk to Totalrekall, but should still be addressed as part of a comprehensive vulnerability management program.

Recommendations:

Totalrekall should prioritize the remediation of the high severity vulnerabilities, as these represent the greatest risk to the organization.

The medium severity vulnerabilities should also be addressed in a timely manner, as they could potentially be exploited in combination with other vulnerabilities to increase the risk to the organization.

The low severity vulnerabilities should be addressed as part of Totalrekall's ongoing vulnerability management program.

Conclusion:

Overall, the pentest identified a number of vulnerabilities and weaknesses in TotalRekall's [systems/networks/applications] that could be exploited by an attacker. By implementing the recommended remediation measures, Totalrekall can significantly reduce the risk of a successful cyber attack and improve its overall security posture."

Summary Vulnerability Overview

Vulnerability	Severity
SQL injection	critical
Sensitive data exposure	Medium
Apache struts 2.3.5 - 2.3.31 / 2.5x < 2.5.10.1 Jakarta Multipart Parser RCE (remote)	Critical
BVRP Software slmail pop3d exploit	Critical
SLmail system schtasks exploit	Medium
Drupal - CVE-2019-6340	Medium
Lsa_dump_sam Exploit	Critical

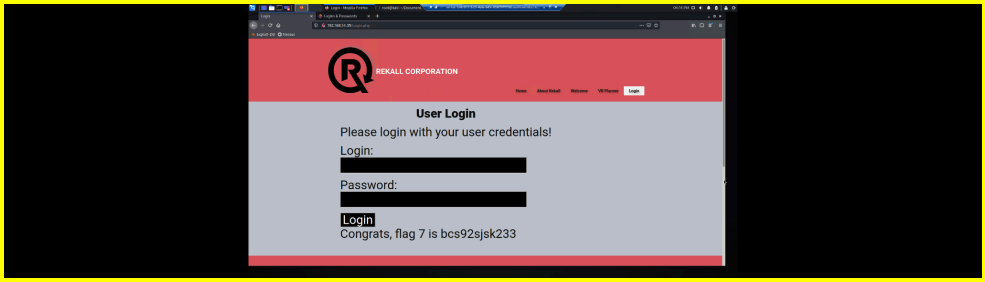
The following summary tables represent an overview of the assessment findings for this penetration test:

Scan Type	Total
Hosts	192.168.13.1, 192.168.13.10, 192.168.13.13, 192.168.13.12, 192.168.13.14 [5]
Ports	22, 5901, 6001 80, 8009, 8080, 10000, 10001 [8]

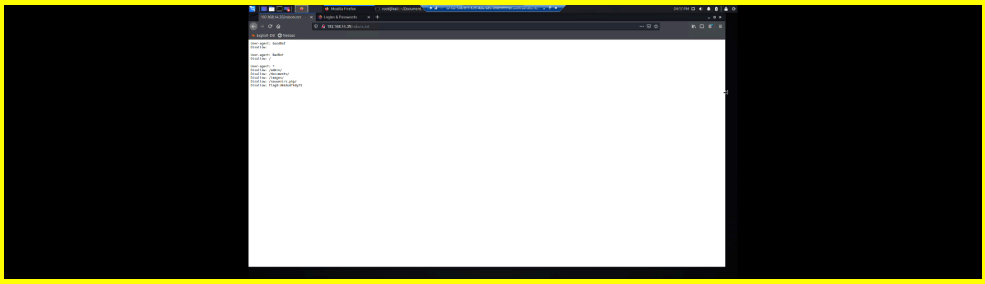
Exploitation Risk	Total
Critical	11

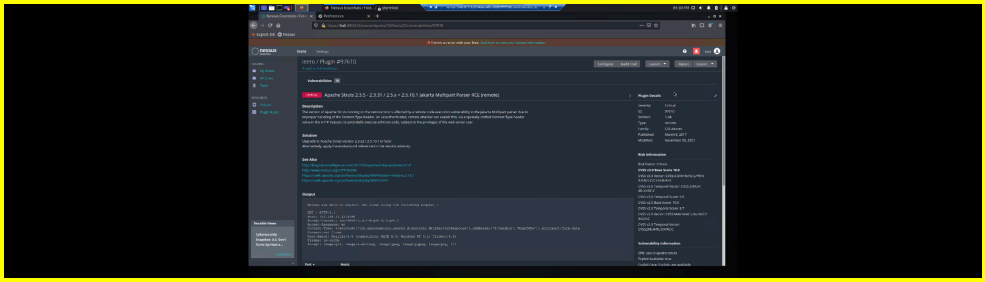
High	19
Medium	10
Low	5

Vulnerability Findings

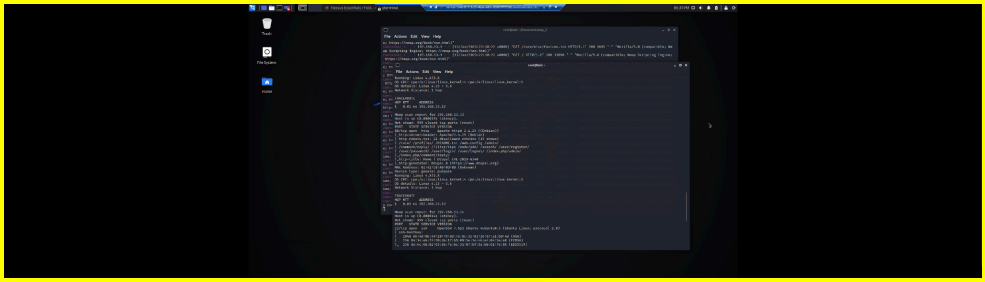
Vulnerability 1	Findings
Title	SQL injection
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	Critical
Description	In the password field, used the following payload: cat' or 1=1–
Images	
Affected Hosts	totalrekall.com
Remediation	Implement input validation: Ensure that all user input is validated and sanitized to remove any malicious code.

Vulnerability 2	Findings
Title	Sensitive data exposure
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Medium
Description	Was Able to access hidden text file on the web page url

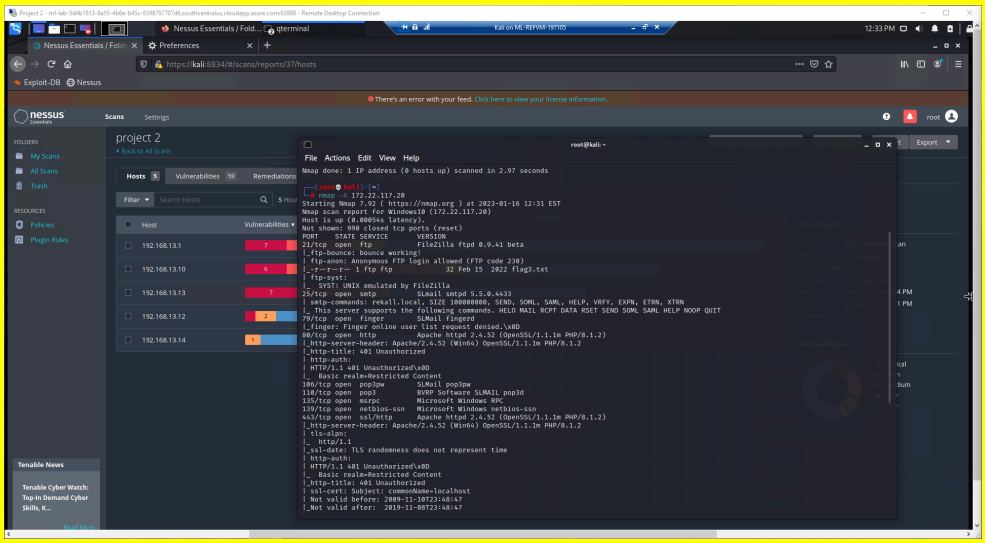
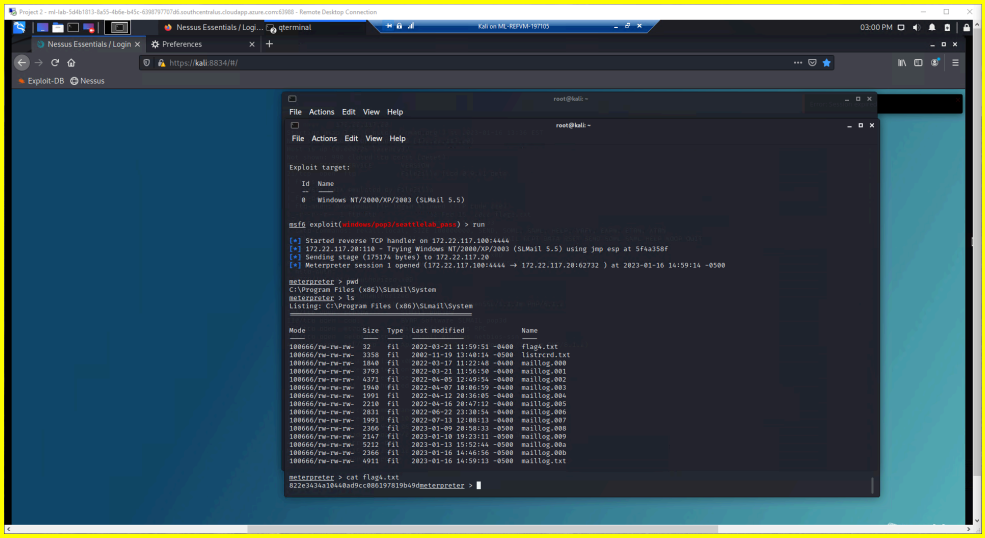
Images	
Affected Hosts	Totallrekall.com
Remediation	• Store sensitive data in secure locations and restrict access to only those who require it. • Encrypt sensitive data while it is both at rest and in transit to prevent unauthorized access.

Vulnerability 3	Findings
Title	Apache struts 2.3.5 - 2.3.31 / 2.5x < 2.5.10.1 Jakarta Multipart Parser RCE (remote)
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	This vulnerability allows an attacker to gain unauthorized access to sensitive data, execute arbitrary code on the vulnerable system, and take control of the web application. This vulnerability is especially dangerous because it can be exploited remotely.
Images	
Affected Hosts	192.168.13.12
Remediation	Upgrade to a version of Apache Struts that is not vulnerable to this issue. This vulnerability's official fix is version 2.3.32 or 2.5.10.1.

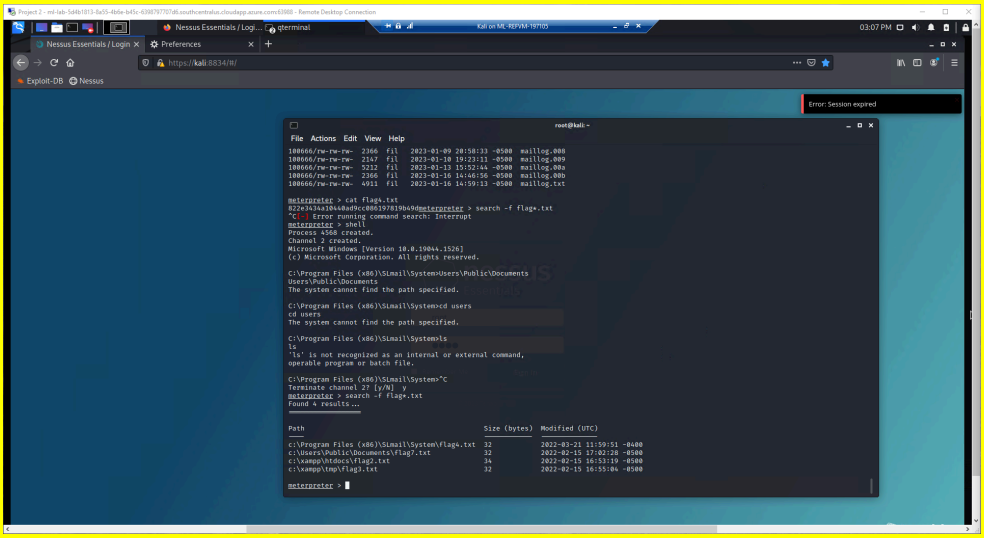
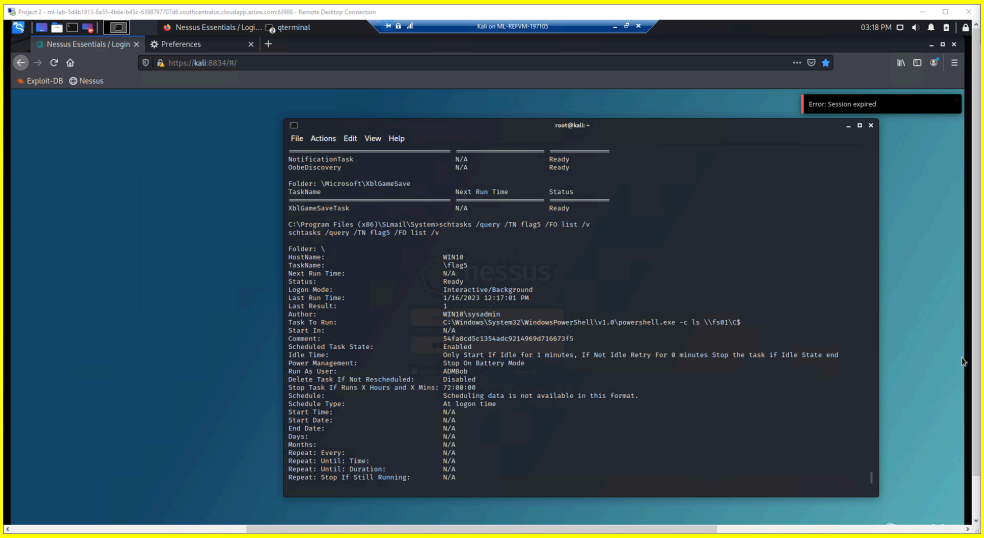
Vulnerability 4	Findings
Title	Drupal - CVE-2019-6340

Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Medium
Description	The vulnerability allows an attacker to execute arbitrary code with the permissions of the web server by sending a specially crafted HTTP request to a Drupal website. This could allow an attacker to gain complete control of the affected website and access sensitive data.
Images	
Affected Hosts	192.168.13.13
Remediation	• Update your Drupal installation to version 8.6.9 or later in order to eliminate the vulnerability. • Ensure that any contributed modules utilized by your website are also updated, as some of them may not be compatible with the latest version of Drupal.

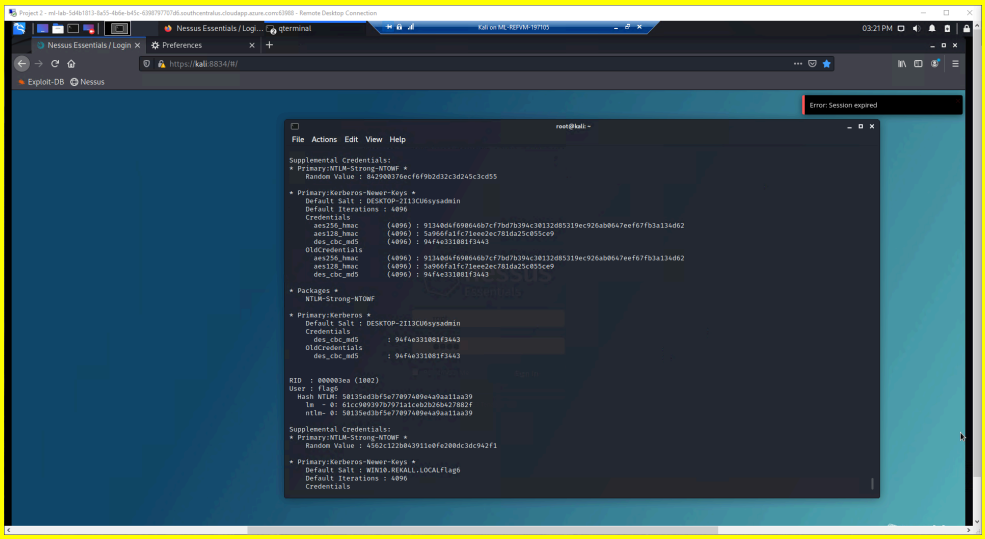
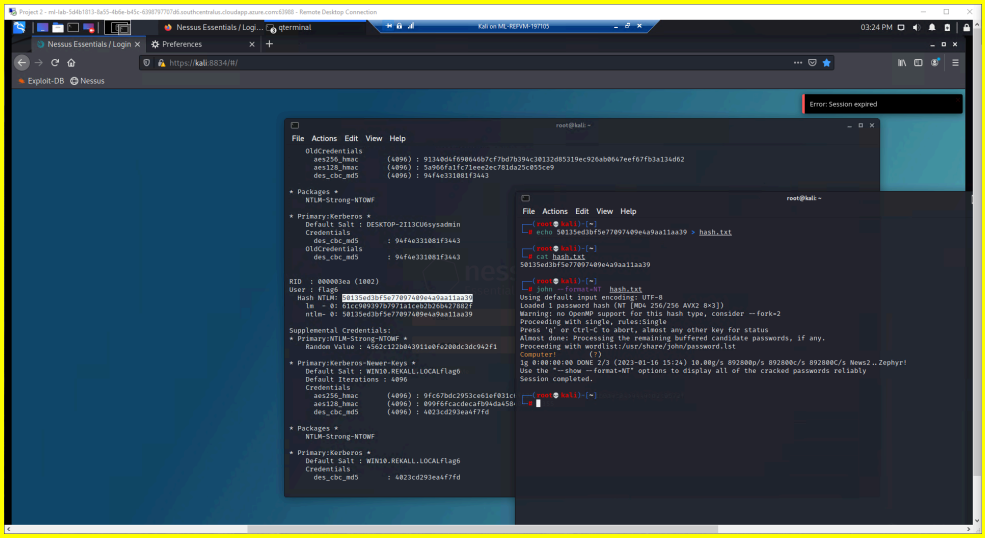
Vulnerability 5	**Findings**
Title	BVRP Software slmail pop3d exploit
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Critical
Description	This remote exploitable flaw could allow an attacker to execute arbitrary code with the privileges of the slmail service on a vulnerable system. This could enable the attacker to seize control of the compromised system, access sensitive data, and potentially infect other systems with malware.

Images	 
Affected Hosts	172.22.117.20 port 110
Remediation	• As this software is no longer being updated by the vendor, it is advised to switch to a more secure and actively maintained email server. • Applying the patch: To address the buffer overflow vulnerability in the software, apply the patch provided by BVRP Software.

Vulnerability 6	Findings
Title	SLmail system schtasks exploit
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Medium
Description	The exploit exploits the manner in which SLmail processes certain POP3 commands, specifically the "USER" command. An attacker can execute arbitrary code with the privileges of the SLmail service by sending a specially crafted "USER" command that triggers a buffer overflow in the SLmail server.

	After executing code on the system, an attacker can use the Windows Task Scheduler to schedule the execution of a malicious payload at a later time. This enables the attacker to maintain persistence on the system and potentially gain access to sensitive data or spread malware.
Images	 
Affected Hosts	172.22.117.20 port 110
Remediation	• Limit the privileges of the user or application that interacts with the email server to the bare minimum required for the task. • Monitoring and logging: Monitor and log all email server activity to detect and respond to any suspicious behavior.

Vulnerability 7	Findings
Title	Lsa_dump_sam Exploit
Type (Web app / Linux OS / WIndows OS)	Windows OS

Risk Rating	Critical
Description	The method involves loading the LsaDumpSAM function of the Lsadump2 tool, which is then used to extract password hashes from the SAM database. The attacker then employs specialized software to offline decrypt the password hashes and reveal the plaintext passwords. This may allow the attacker to access other systems on the network or steal sensitive data.
Images	 
Affected Hosts	172.22.117.20 port 110
Remediation	• Use of security tools: To protect the email server, employ security tools such as firewalls, intrusion detection and prevention systems, and encryption. • Regularly conduct penetration testing to identify and address vulnerabilities in the email server.

Add any additional vulnerabilities below.