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	Lonestar,LLC
Contact Name	Oscar Benavidez
Contact Title	Penetration Tester

Document History

Version	Date	Author(s)	Comments
001	01/28/23	Oscar Benavidez	

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.

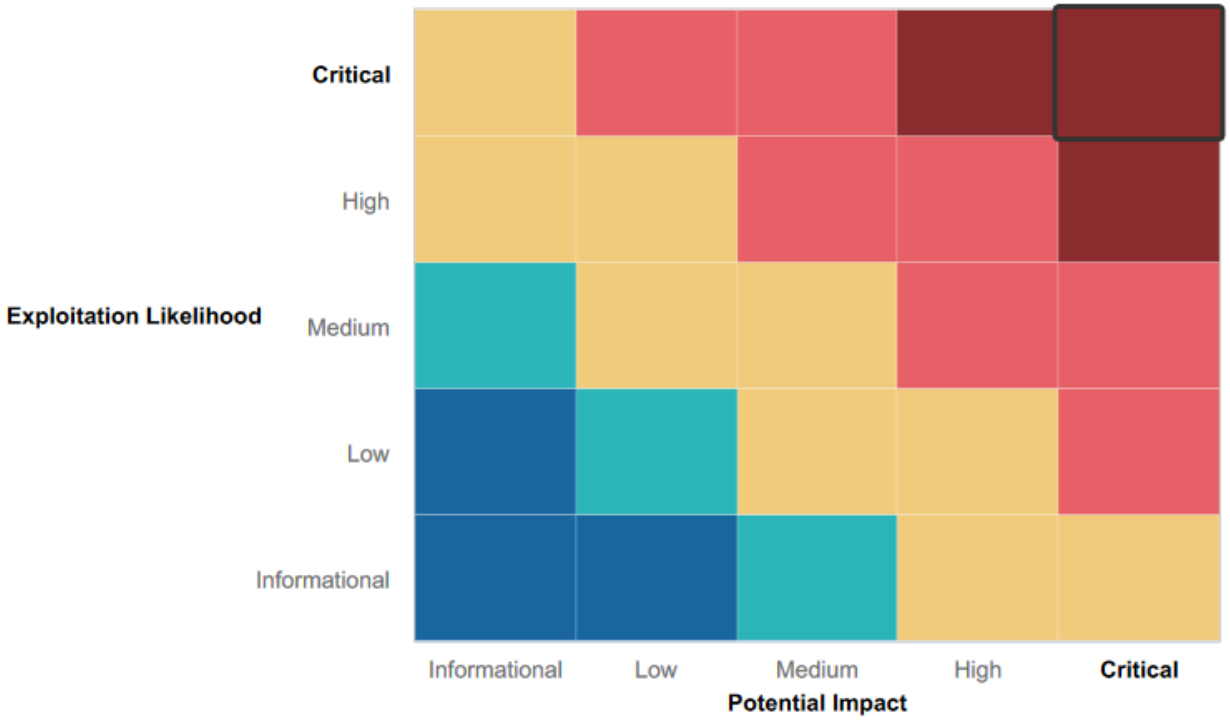
Executive Summary of Findings

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.

- Most services were not active on host machines.
- Getting a third party to Pentest your security 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.

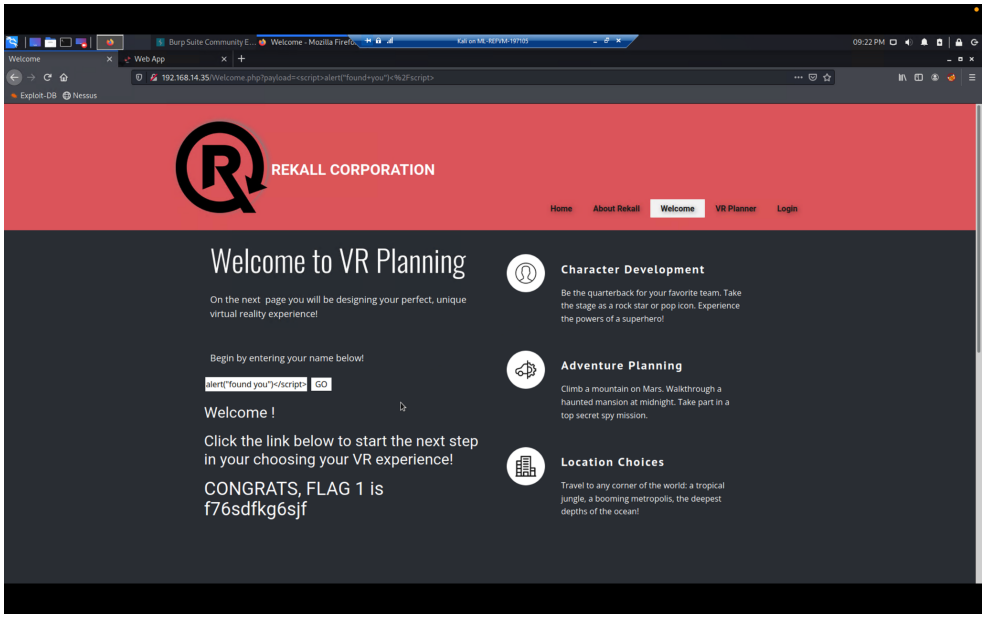
- Websites are vulnerable to XSS and SQL payloads
- Credentials (user:hash) were available to the public on the totalrekall GitHub allowing access to client webpage.
- Credentials have been stored as html files that are available to the public on totalrekall sever webpage.
- The open port 21 allows for an ftp exploit. The port also allows anonymous login which bypasses the need to obtain user credentials to access the machine.
- Port 110 has a SLMail vulnerability that allowed access to a meterpreter shell.

Executive Summary

[Provide a narrative summary of your steps and findings, including screenshots. It's fine to mention specifics (e.g., used Metasploit to exploit a vulnerable version of DistCC), but do not get too technical in these specifics. This should be an A–Z summary of your assessment.]

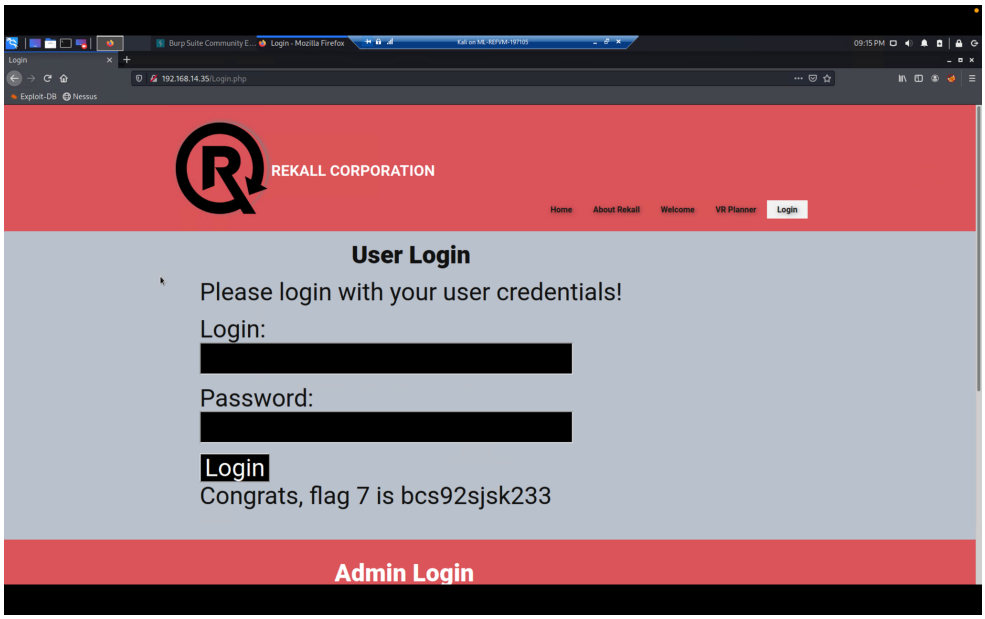
Vulnerability 1

The IP Address 192.168.14.35 was utilized to navigate to the VR Rekall Corp page. On the enter your name section of the page a script (<script>alert("Found You")</script>) was entered. This script allowed for inadvertent access to the VR experience without a proper username.



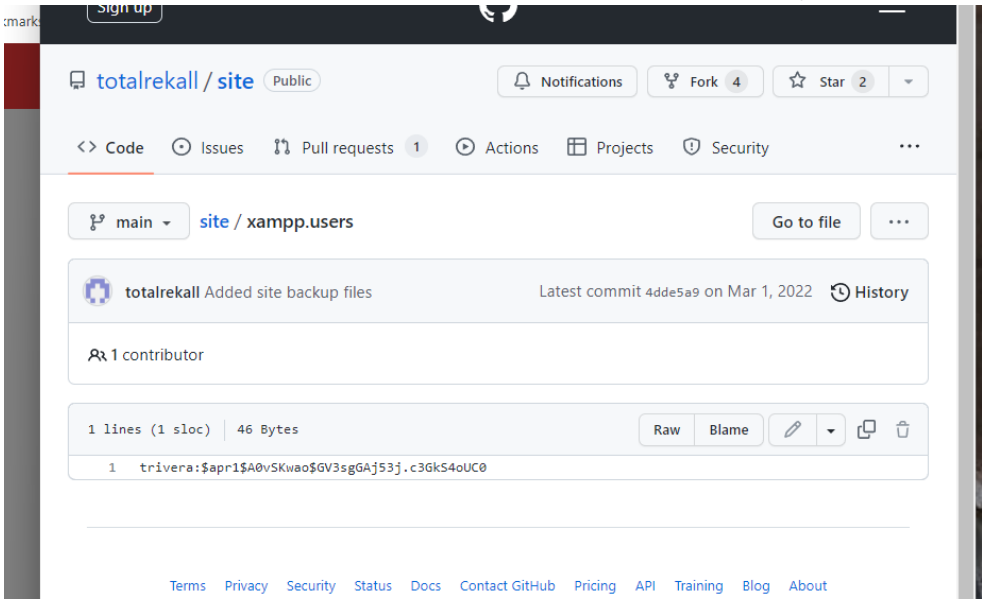
Vulnerability 2

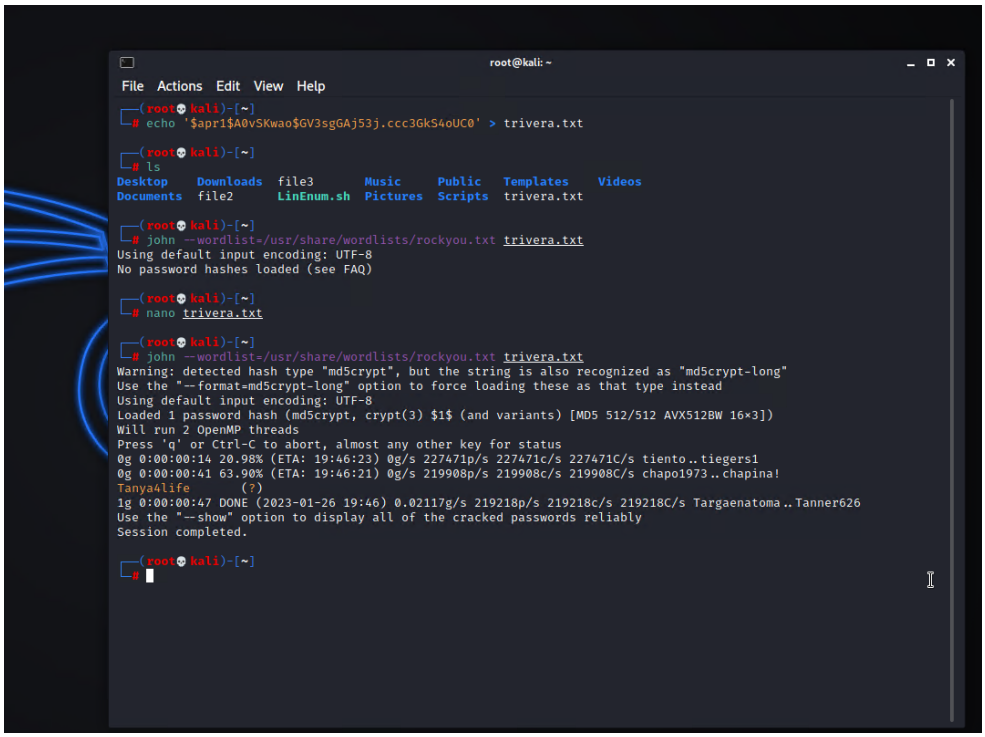
Vulnerability was performed on the Rekall Corp login page. On the login section SQL injection techniques were deployed. The injection (1' OR '1' = '1) was input in place of actual credentials and resulted in access as a user without valid credentials.



Vulnerability 3

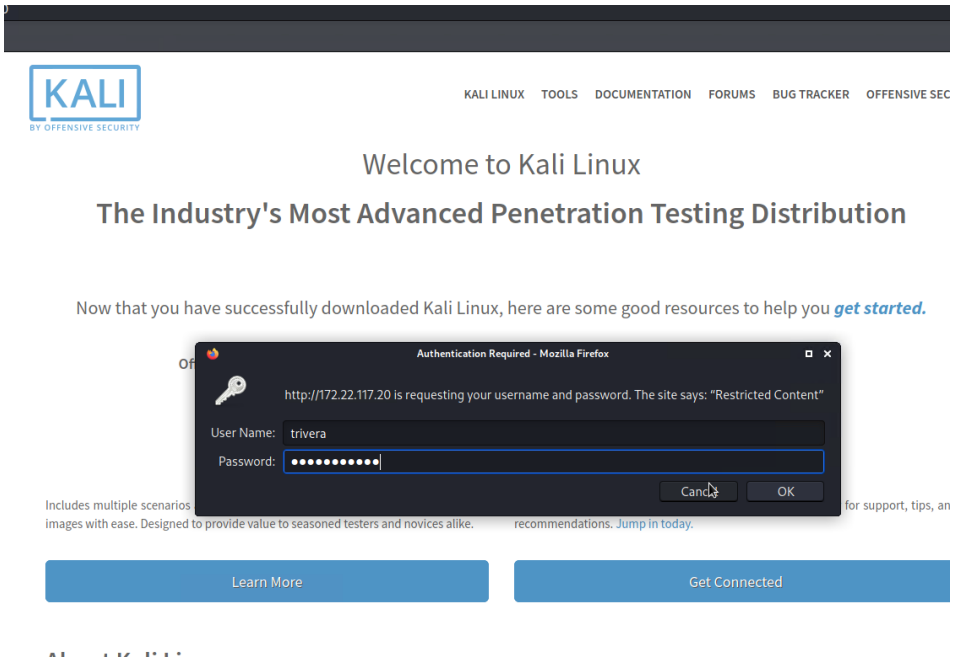
Started with a search for totalrekall GitHub page to find the site repository that allowed access to xampp.users page. This page contained trivera:$apr1$A0cSKwao$GV3sgGAj53j.c3GkS4oUC0 credentials. The credentials were cracked and the password Tanya4life was discovered.

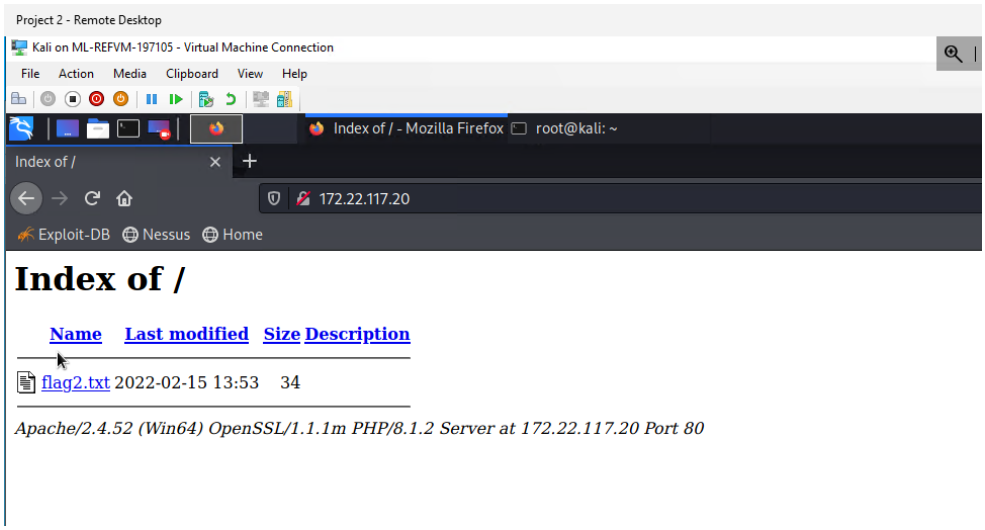




Vulnerability 4

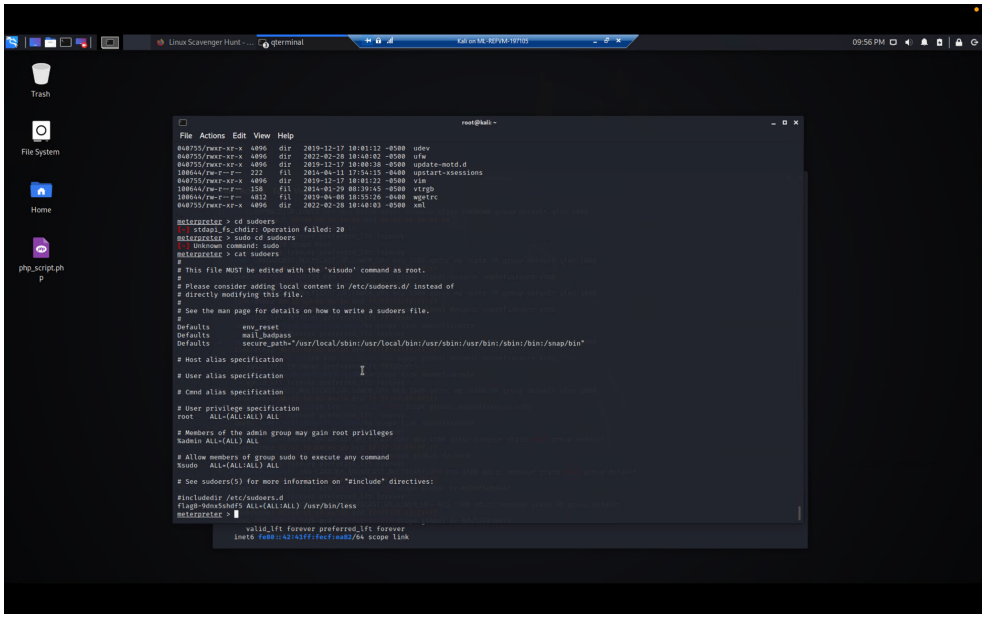
A port scan for 172.22.117.0/24 was done revealing two machines (Win10@172.22.117.20 & Server2019@172.22.117.10). The Win10 machine was exploited due to finding an http port 80 open. The IP Address 172.22.117.20 was used to reach the required webpage and the credentials found in vulnerability 3 were used to login providing access to client sensitive information.





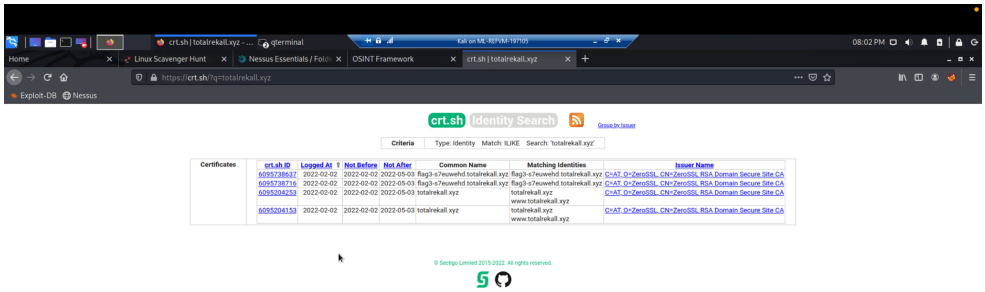
Vulnerability 5

The exploit Shell Shock was done on IP Address 192.168.13.11 the module exploit(/multi/http/apache_mod_cgi_bash_env_exec) was run. This provided access to the 172.22.117.11 machine where I navigated to the sudoers file.



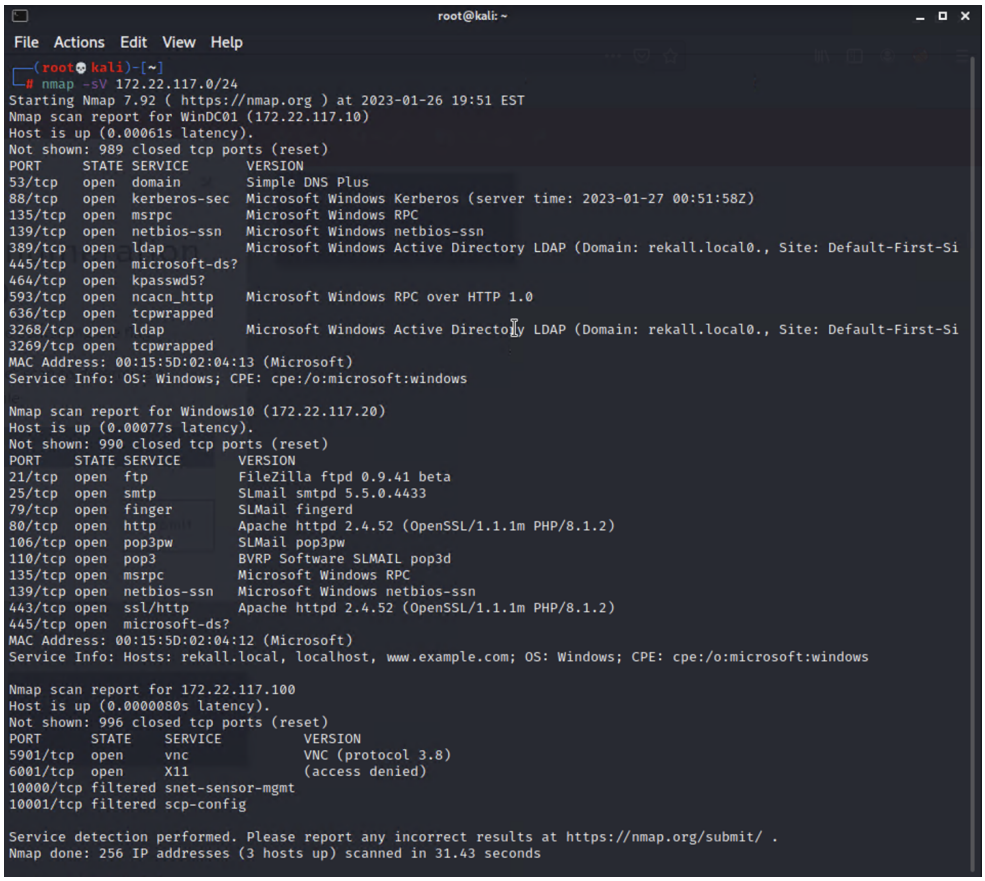
Vulnerability 6

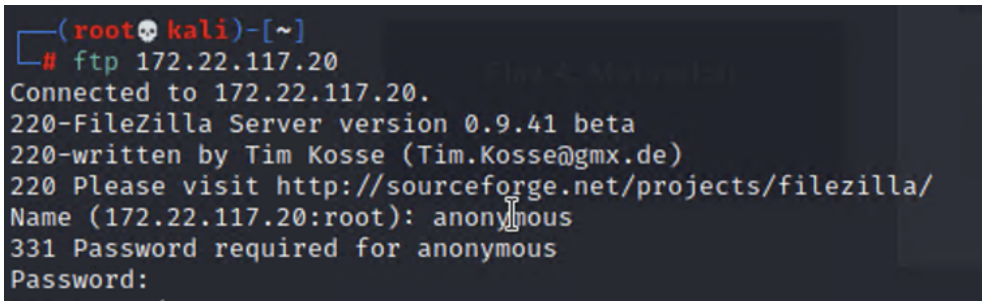
A stored certificate on the crt.sh/totalrekall.xyz page was found. Under the common name section the required data was collected.

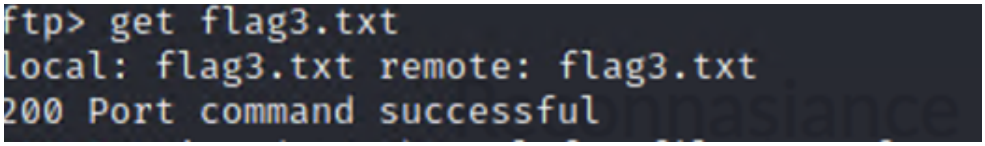


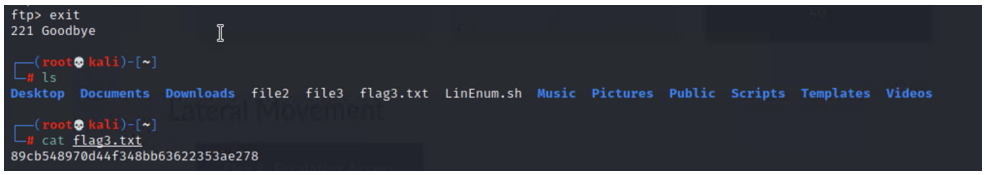
Vulnerability 7

Nmap scan was run for 172.22.117.0/24 subnet, an ftp exploit on IP Address 172.22.117.20 was discovered. No credentials were yet discovered for access to the ftp exploit however, login was achieved through anonymous login. File flag3 was copied from target machine to local machine and viewed with [cat] command.



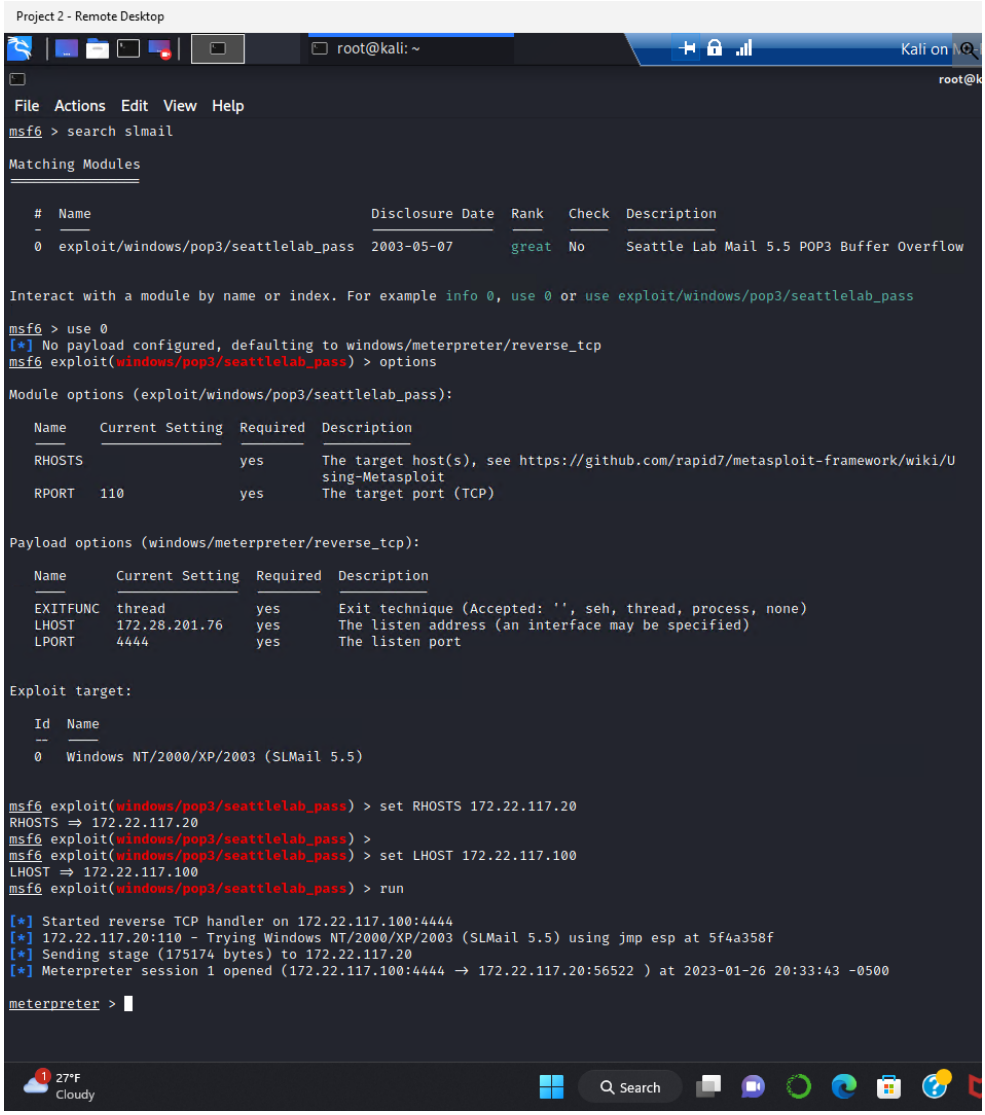


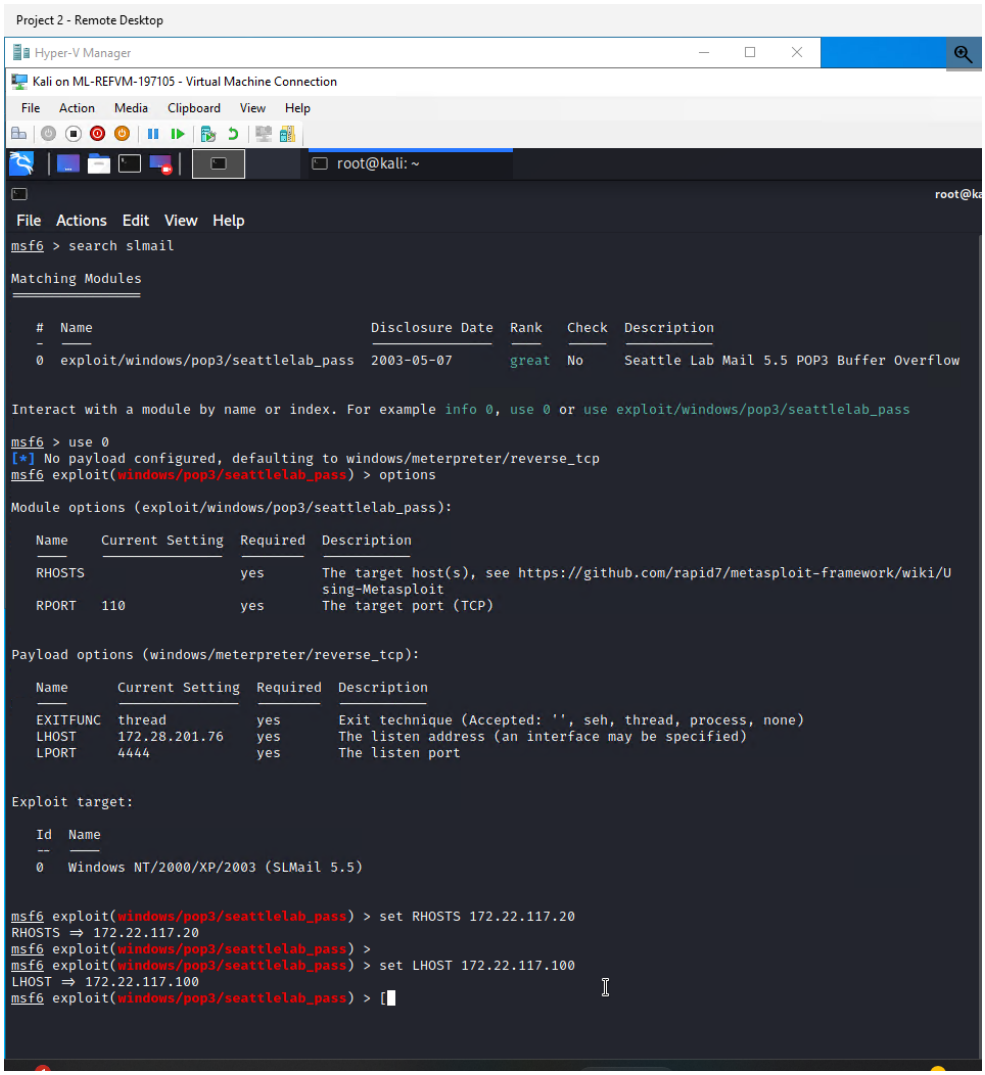


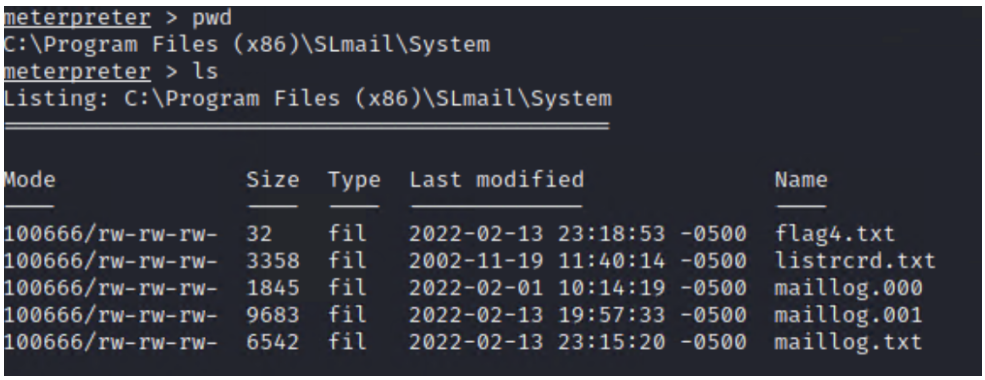


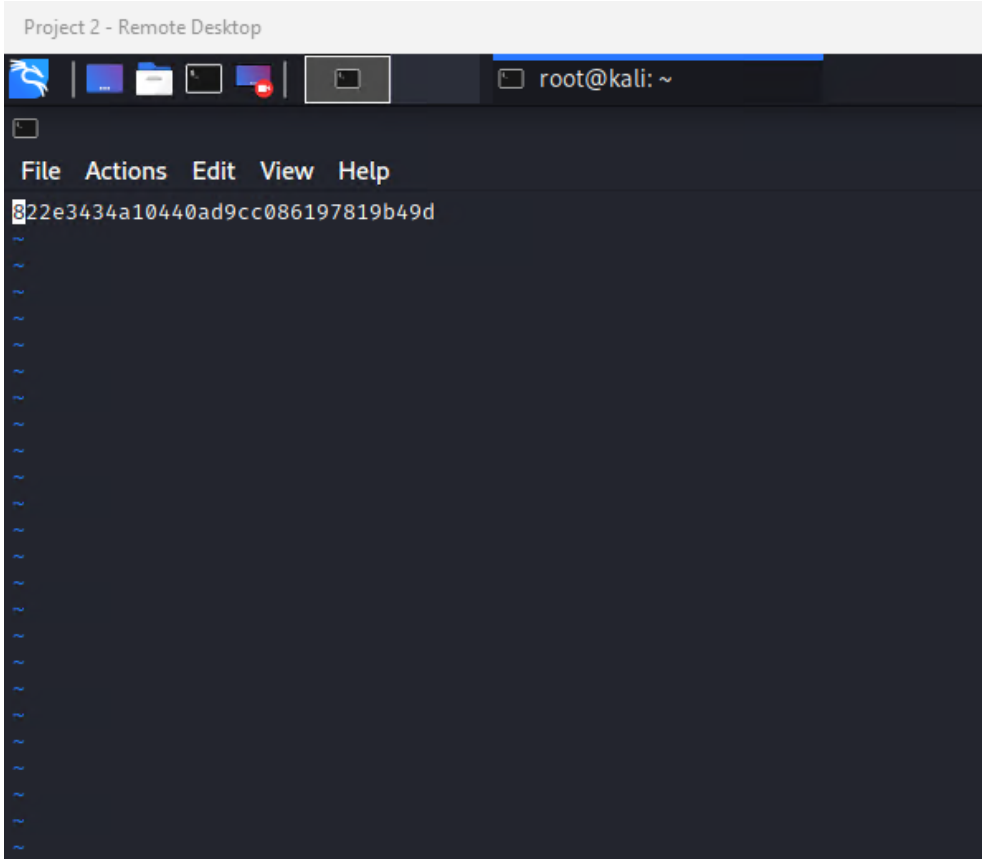
Vulnerability 8

The port scan results gathered previously for 172.22.117.20 also provided a list of other open ports and services. In this case the SLMail service on POP3 port 110 was the focus of attack. Searchsploit was used to find the correct version required to gain access. Metasploit was loaded and the exploit /windows/pop3/seattlelab_pass was used. Once correct options were set the exploit was run, allowing access into a meterpreter shell.



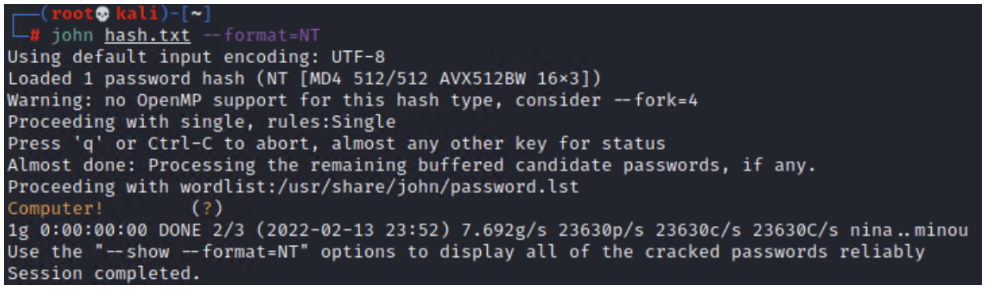






Vulnerability 9

In a meterpreter for IP Address 172.22.117.20 the kiwi extentison was loaded. In kiwi the command [lsa_dump_sam} was run displaying user:flag6 & Hash NTLM: 50135ed3bf5e77097409e4a9aa11aa39. The hash was copied to a local machine and john the ripper was used to crack the hash by running command [john hash.txt --format=NT]. The password Computer! was discovered.



Summary Vulnerability Overview

Vulnerability	Severity
Reflected XSS	Medium
SQL Injection	Critical
Finding user credentials on Github total rekall GitHub	Critical
Port Scan	Critical
Shell Shock on Web Server	Critical
Search via crt.sh	Medium
FTP enumeration, anonymous user access	Critical
SLMMail Port 110 Vulnerability	Critical
Credential Dump	Critical

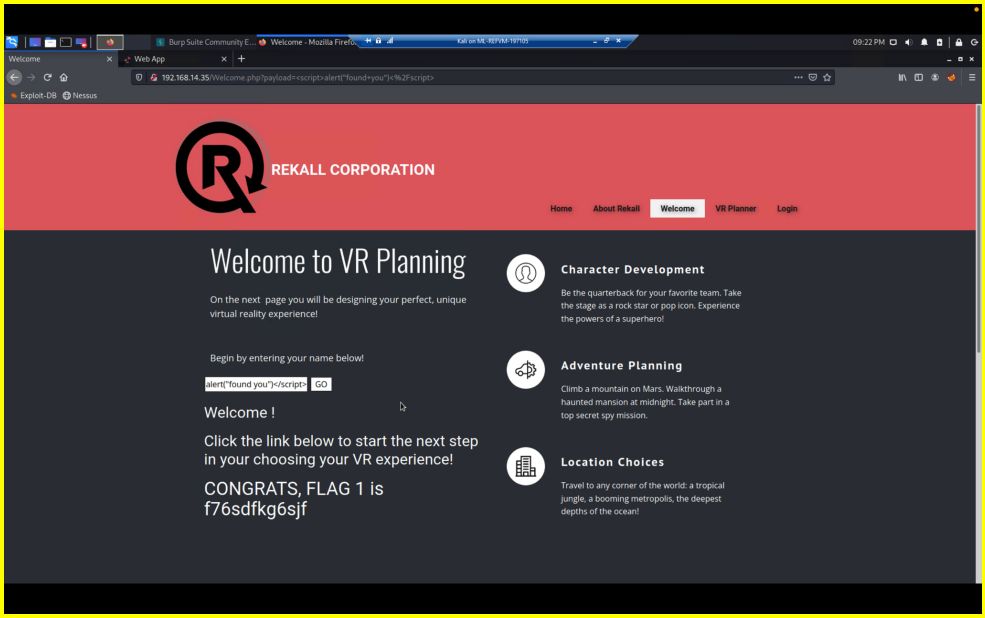
The following summary tables represent an overview of the assessment findings for this penetration test:

Scan Type	Total
Hosts	192.168.14.35, 192.168.13.10, 192.168.13.11, 192.168.13.12, 192.168.13.13, 192.168.13.14, 34.102.136.180, 172.22.117.20, 172.22.117.10
Ports	21, 22, 80, 110, 8080, 8009

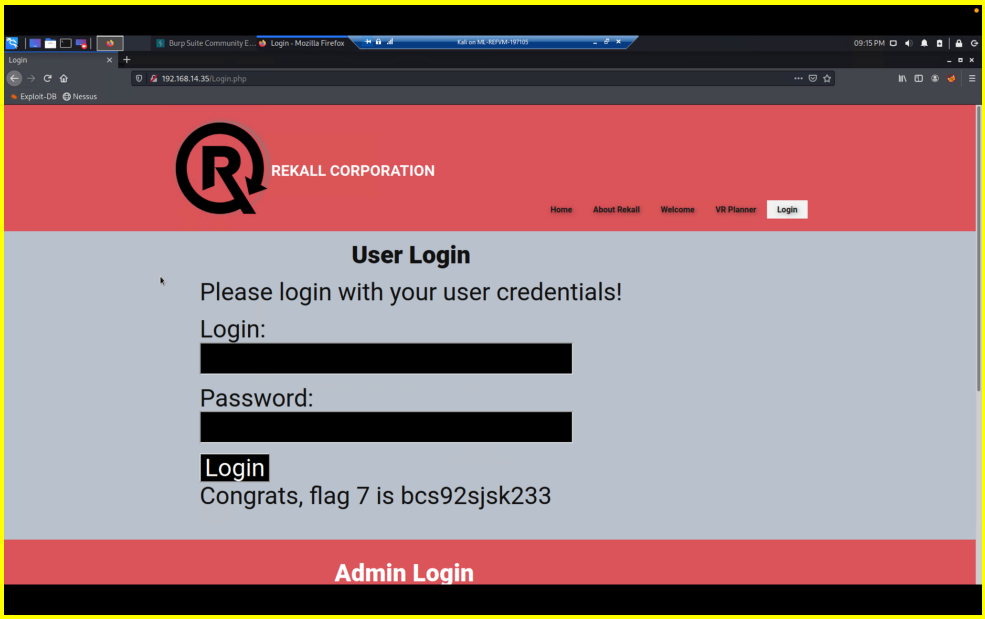
Exploitation Risk	Total
Critical	7
High	0
Medium	2

Low	0

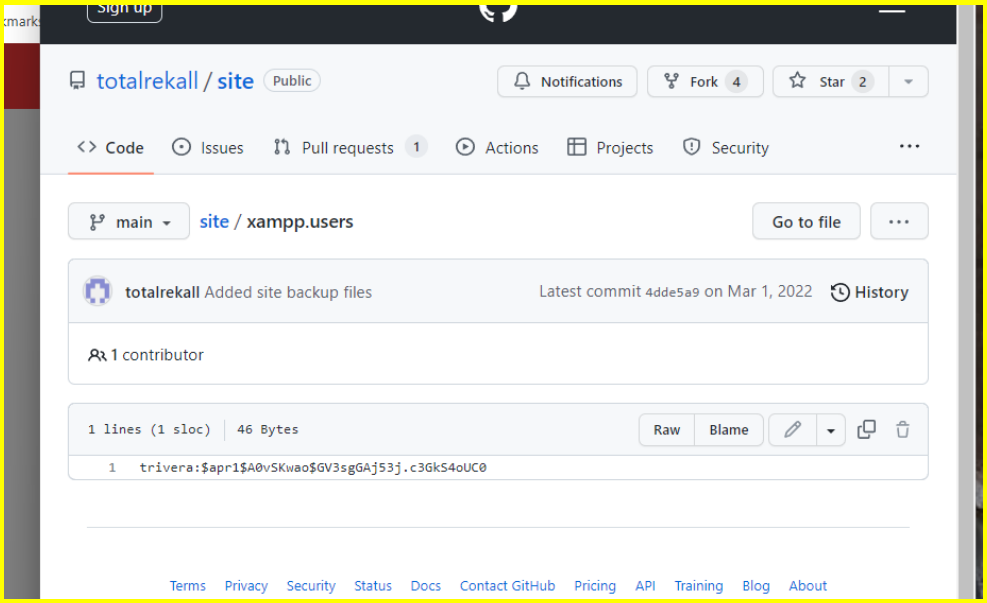
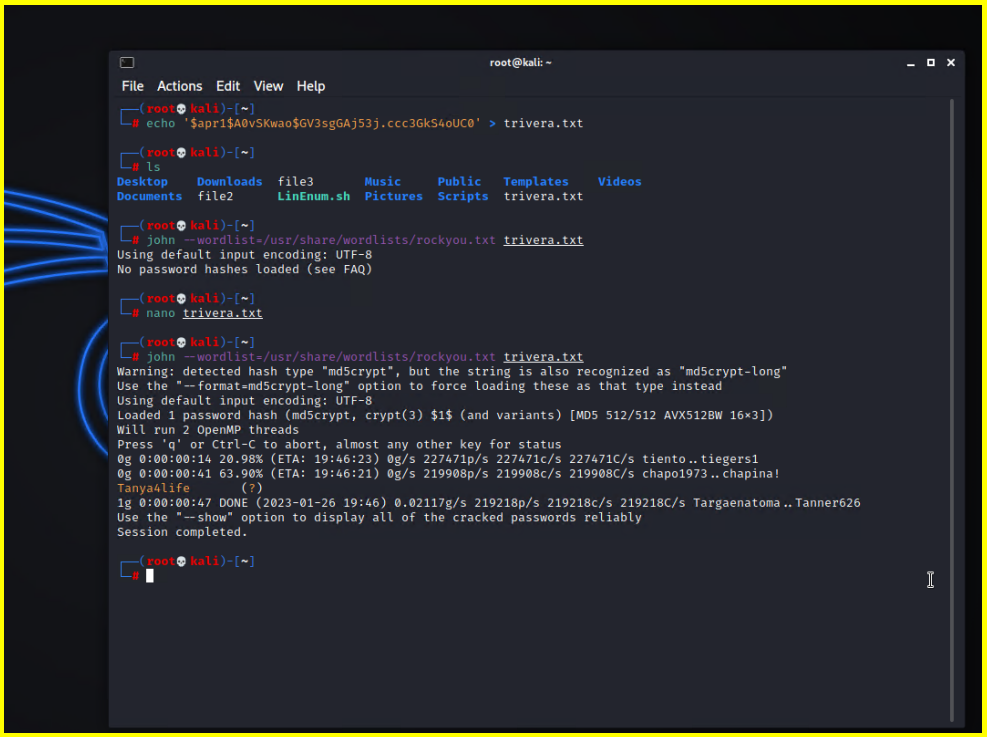
Vulnerability Findings

Vulnerability 1	Findings
Title	Reflected XSS
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Medium
Description	Exploit was performed by inputting <script>alert(“Found You”)</script>.
Images	
Affected Hosts	192.168.14.35
Remediation	Implement Input Validation

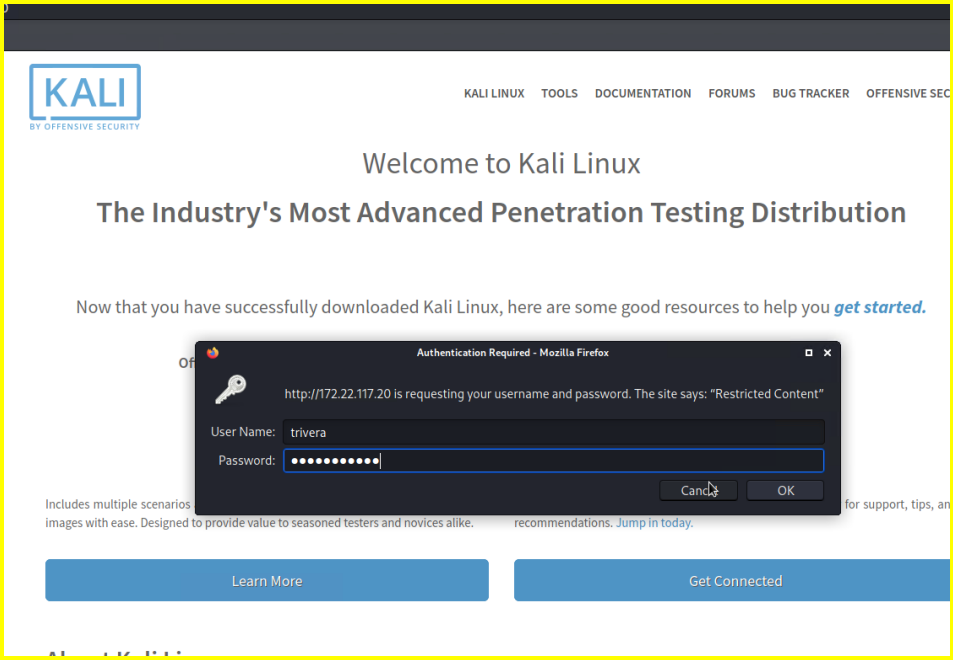
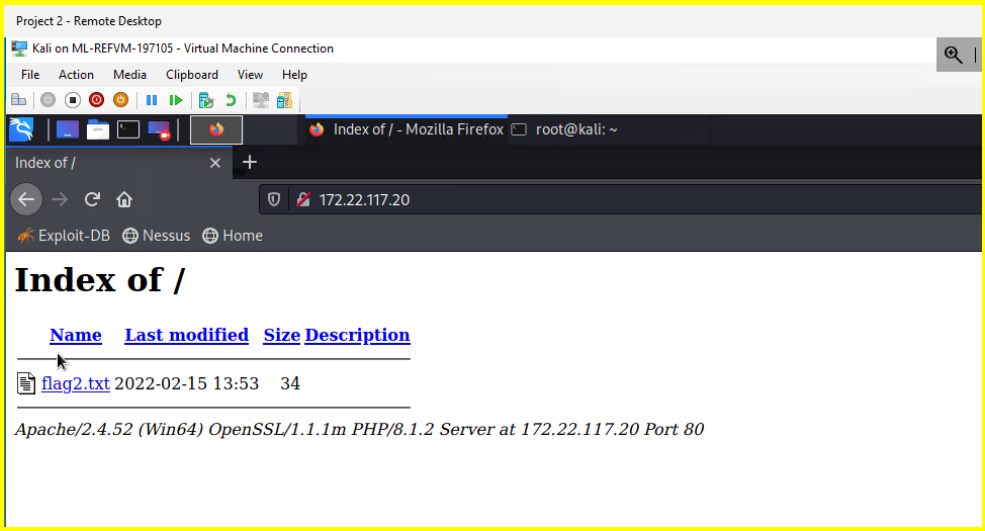
Vulnerability 2	Findings
Title	SQL Injection
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Critical

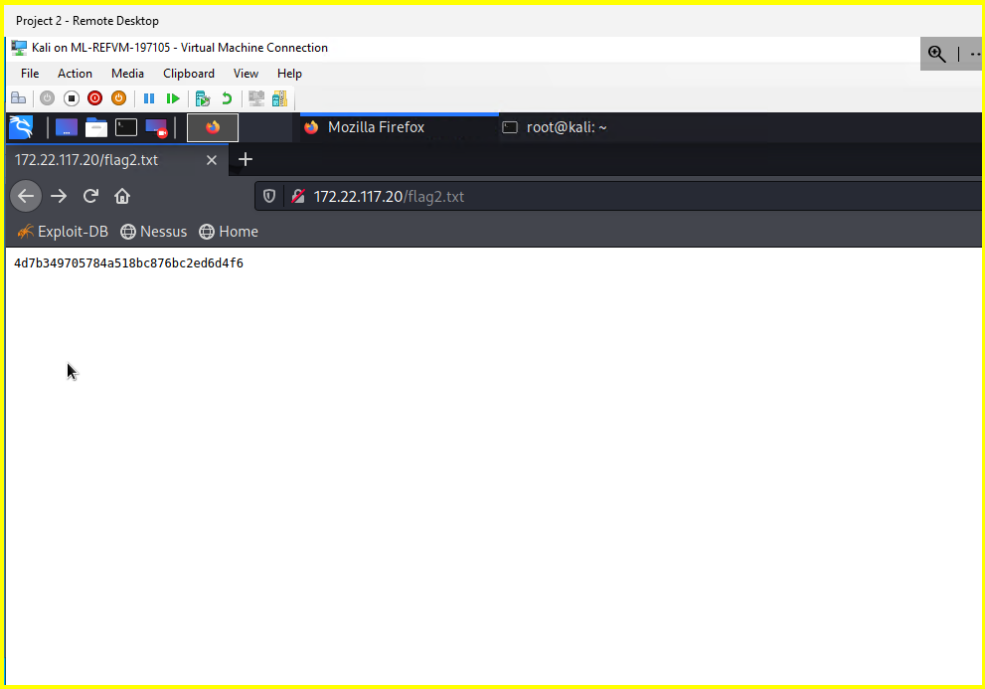
Description	In the login.php page, (1' OR '1' = '1) was used to bypass the need for correct credentials.
Images	
Affected Hosts	192.168.14.35
Remediation	Configure web app to block the use of direct inputs.

Vulnerability 3	Findings
Title	Finding user credentials on Github TotalRekall GitHub
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Critical
Description	Found user:hash credentials on Github, cracked hash which provided the password tanya4life. The password is flag 1.

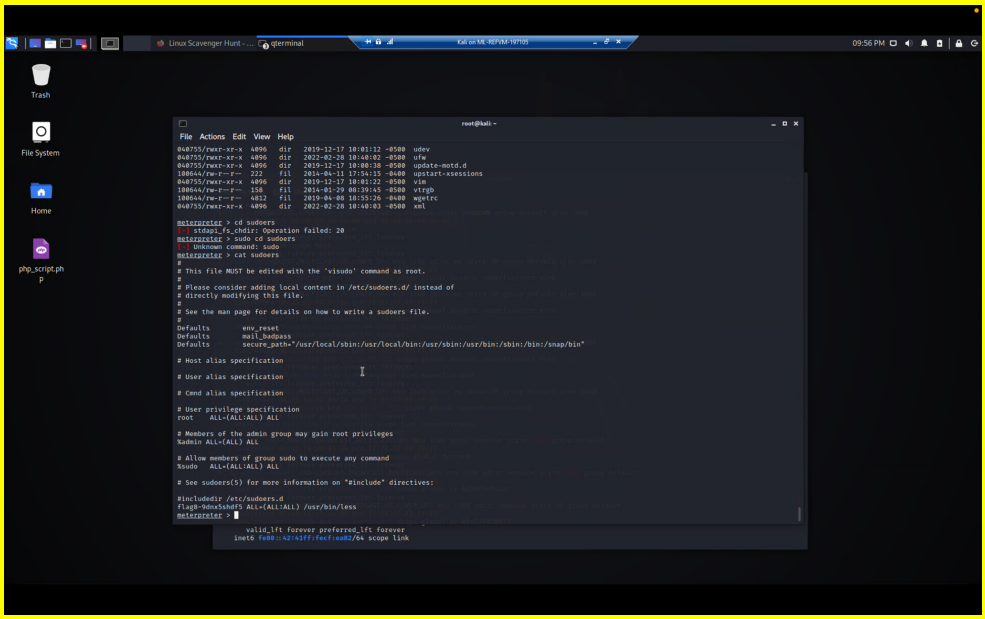
Images	 
Affected Hosts	Total Rekall Web Server (172.22.117.20)
Remediation	Remove credentials from the website and don't allow public access to sensitive data.

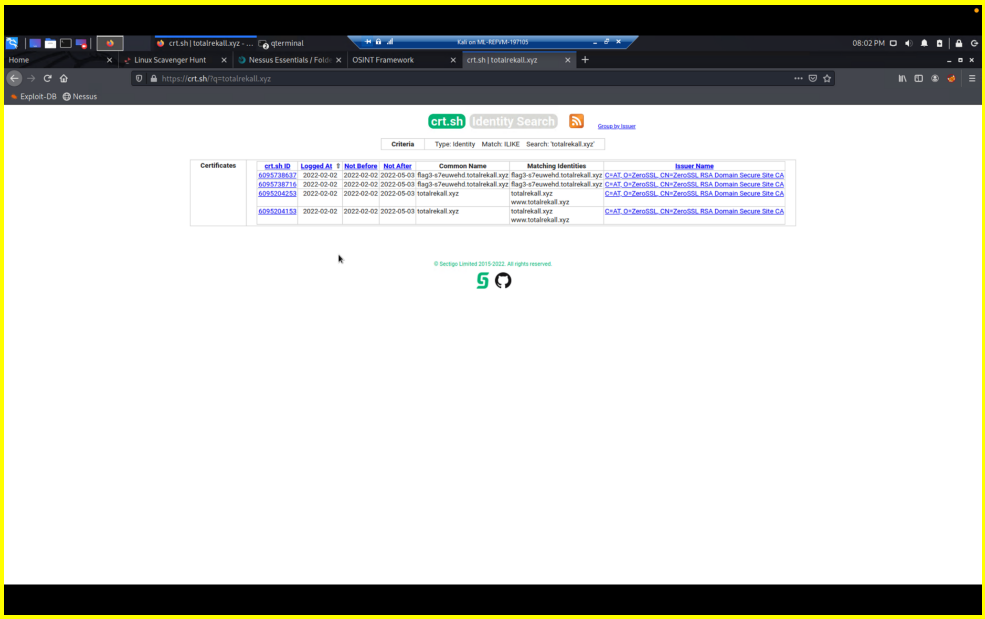
Vulnerability 4	Findings
Title	Port Scan
Type (Web app / Linux OS / WIndows OS)	Web App

Risk Rating	Critical
Description	Once the login info for flag1 is found. Use the credentials to login into the website 172.22.117.20. This will display flag2 as a file.
Images	 

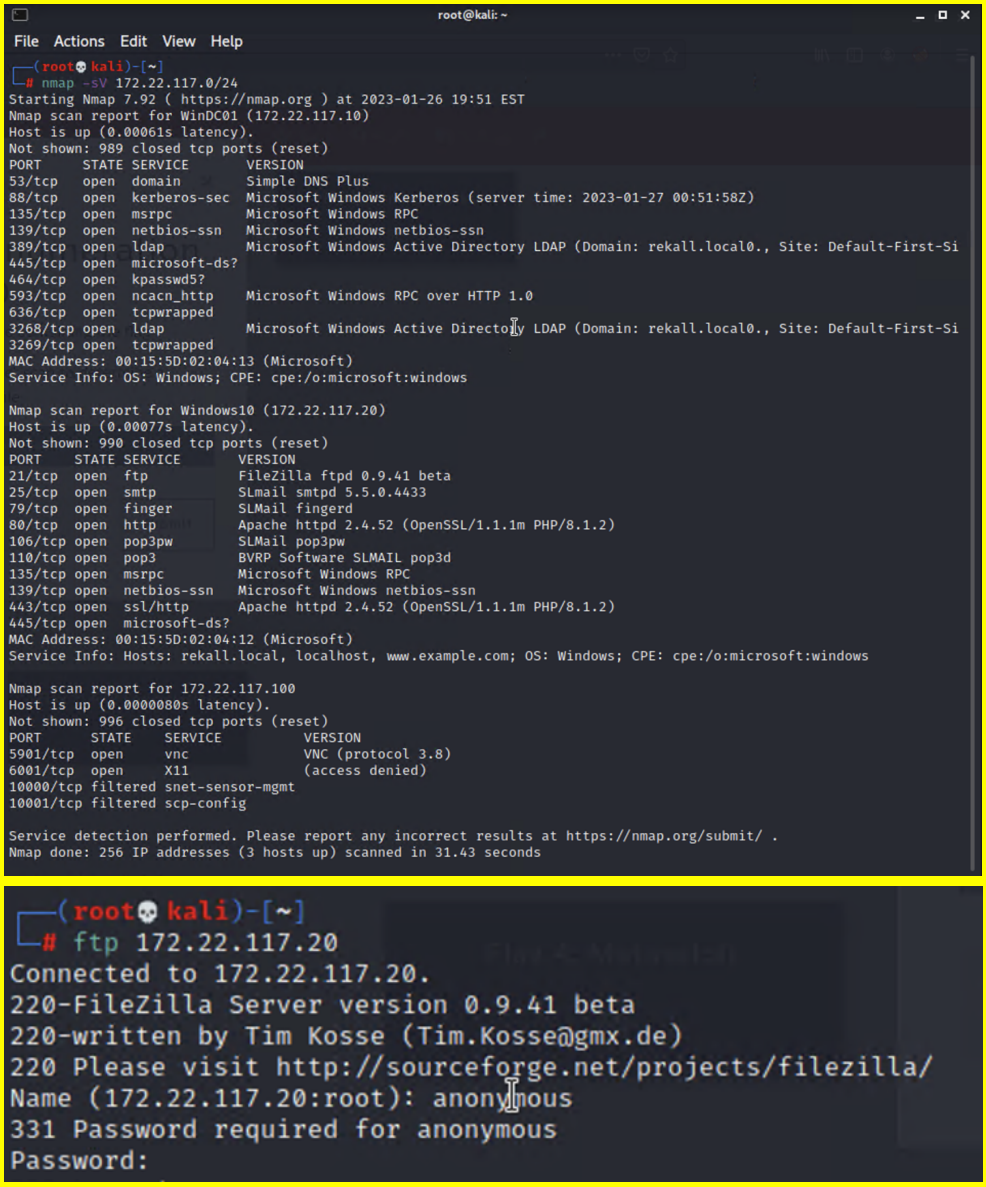
	
Affected Hosts	172.22.117.20
Remediation	Use two factor authentication. Stop storing sensitive data on websites that can be used for exploits.

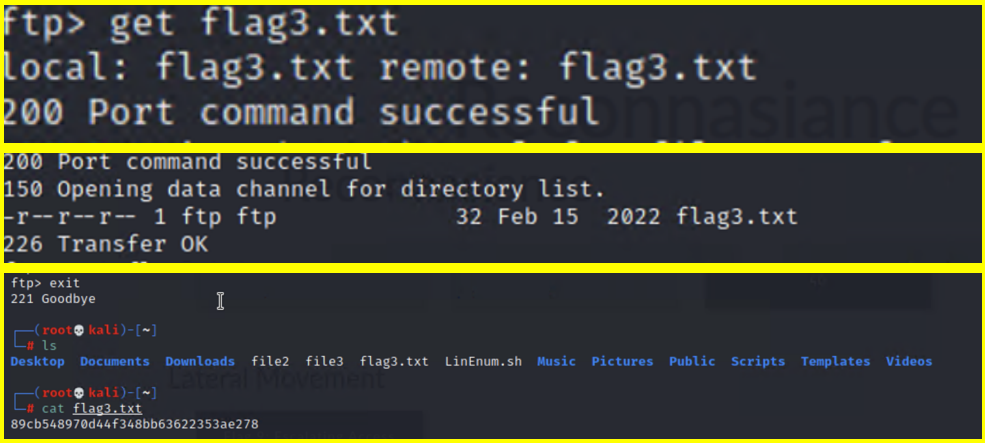
Vulnerability 5	Findings
Title	Shell Shock on Web Server
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	Using the metasploit exploit(/multi/http/apache_mod_cgi_bash_env_exec)

Images	
Affected Hosts	192.168.13.11
Remediation	Limit access to the sudoers file and accounts.

Vulnerability 6	**Findings**
Title	Search via crt.sh
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Medium
Description	Found the stored certificate for the totalrekall.xyz on the crt.sh site.
Images	

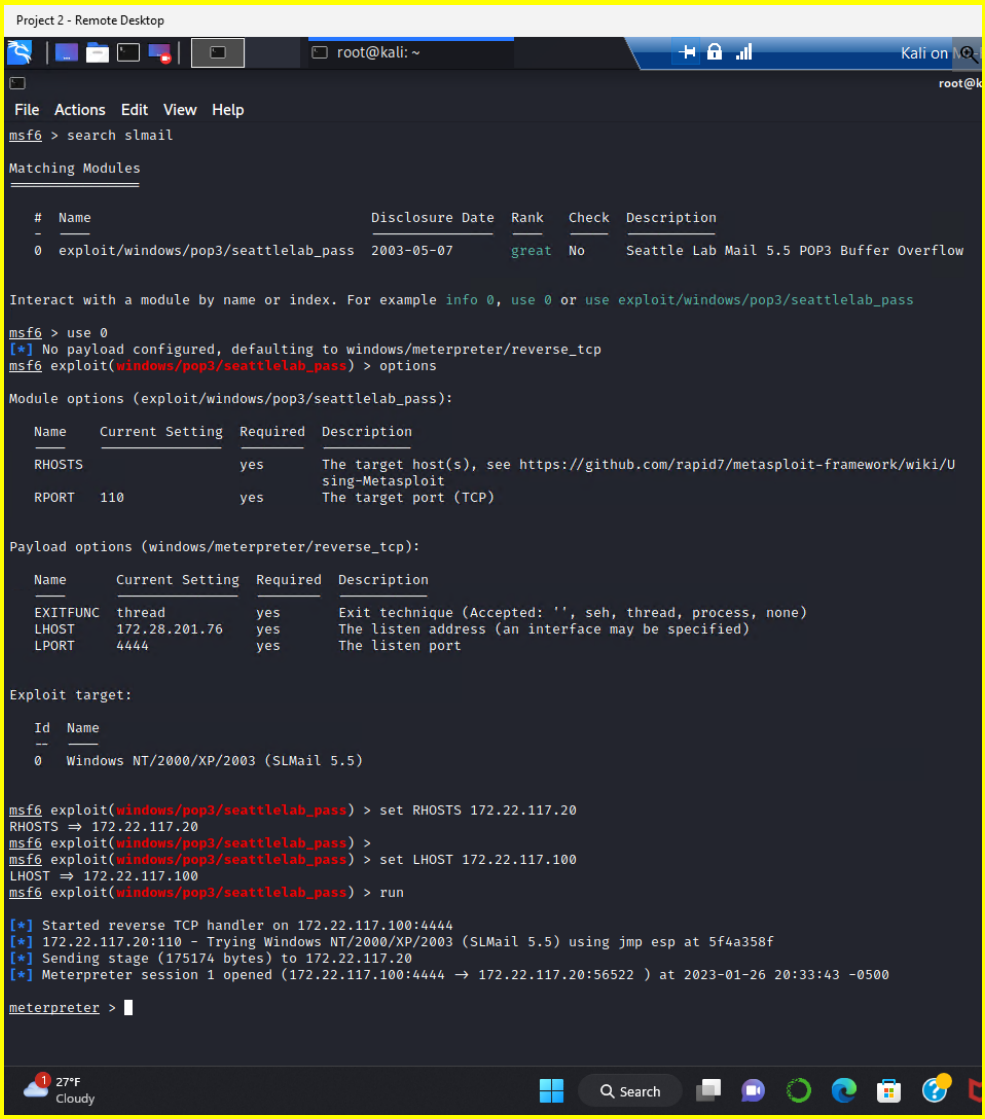
Affected Hosts	34.102.136.180
Remediation	Don't make sensitive information available to the public, such as on websites like crt.sh. Eliminate access to sensitive data.

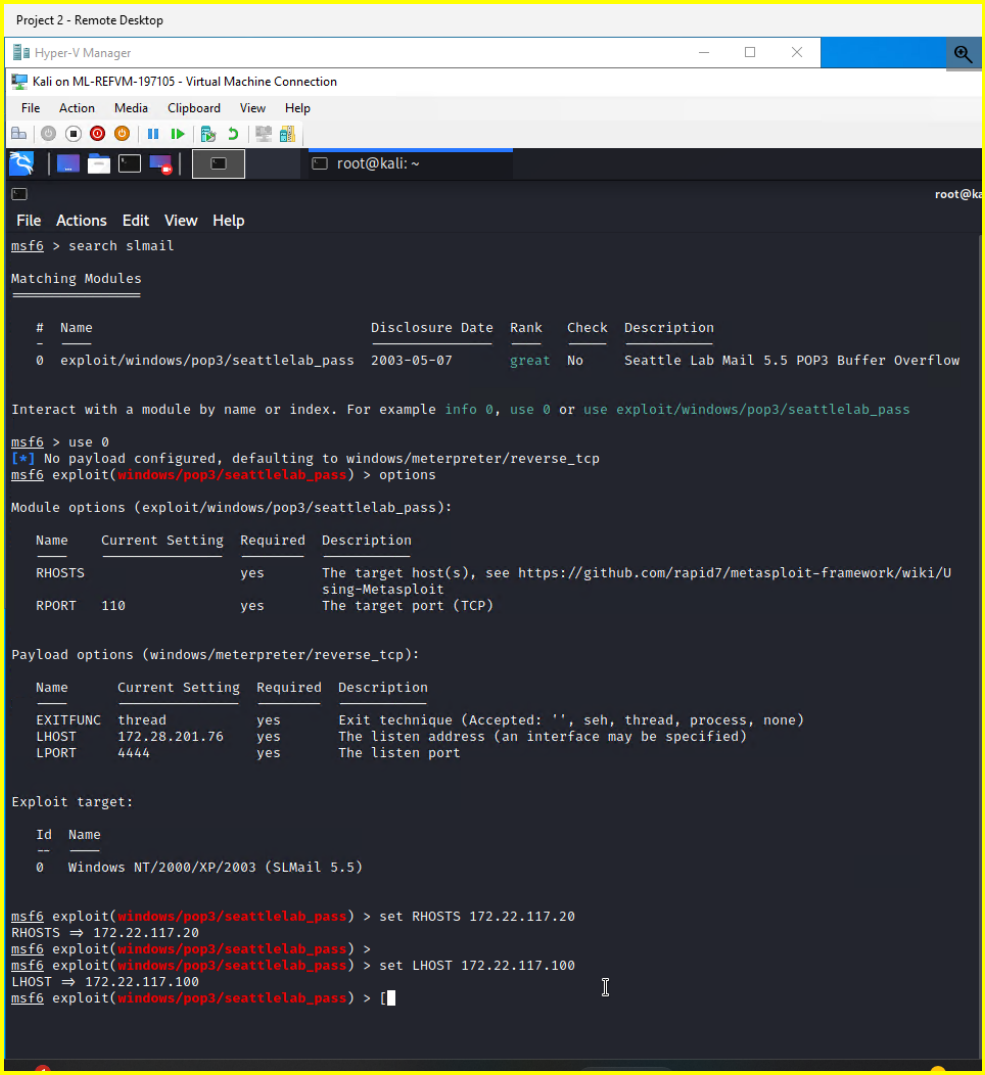
Vulnerability 7	**Findings**
Title	FTP enumeration, anonymous user access
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Critical
Description	Nmap scan showed port 21 ftp login. Access was gained using anonymous login technique.
Images	

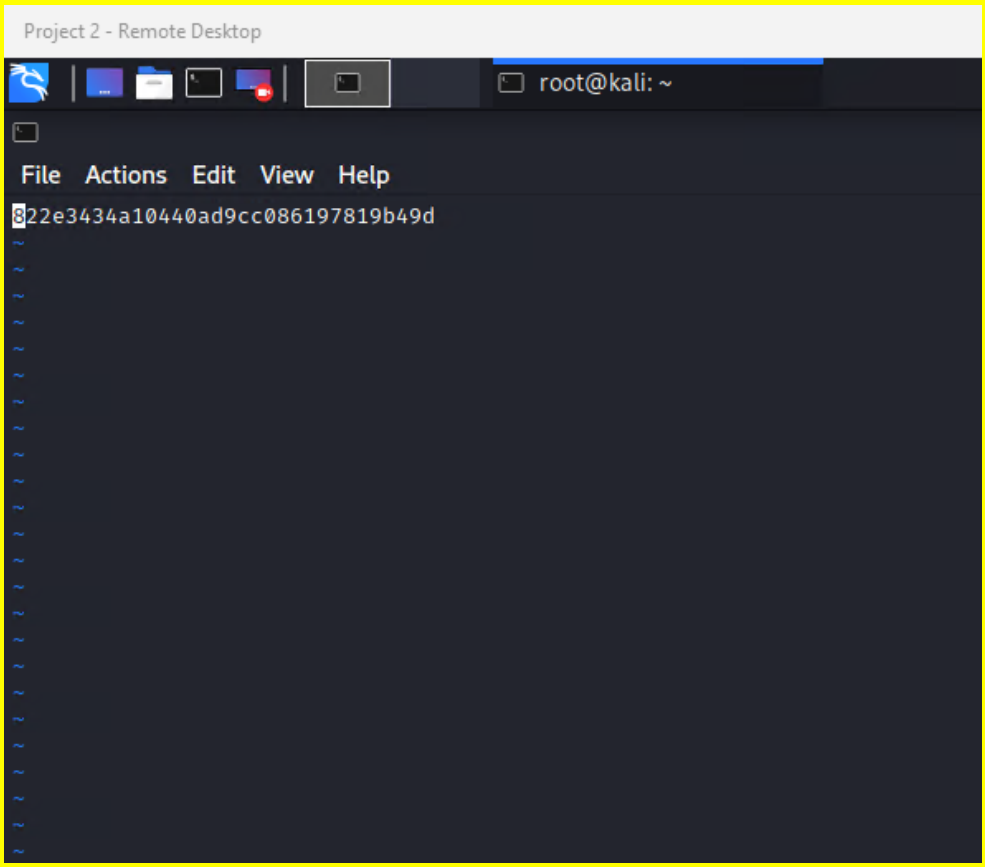
	
Affected Hosts	172.22.117.20
Remediation	Block anonymous login ability. Block access through port 21.

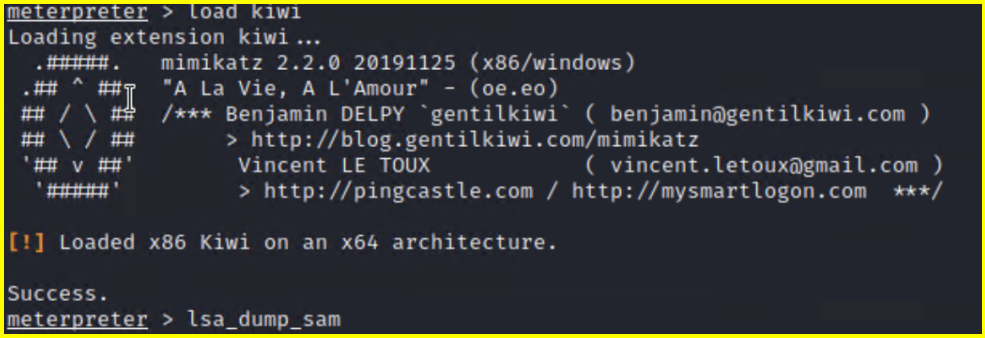
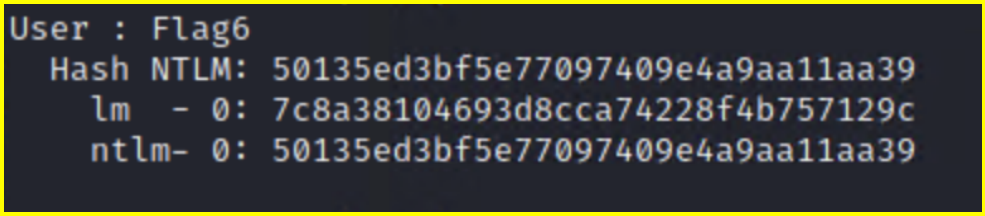
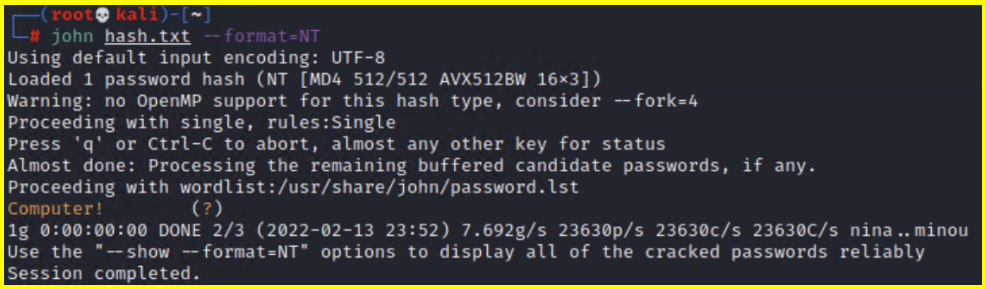
Vulnerability 8	Findings
Title	SLMMail Port 110 Vulnerability
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Critical
Description	Found that Port 110 was open, used Metasploit and ran exploit(windows/pop3/seattlelab_pass)

Images





	
Affected Hosts	172.22.117.20
Remediation	Block access to port 110. Use a different Mail service or keep up with updates to eliminate vulnerabilities.

Vulnerability 9	Findings
Title	Credential Dump
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Critical
Description	Used the meterpreter shell, loaded kiwi extension and ran the lsa_dump_sam command. Copied the hashes and cracked with john the ripper.
Images	  
Affected Hosts	172.22.117.20
Remediation	Update user permissions to better protect from non admin users gaining access to sensitive data.