Cybersecurity

Penetration Test Report

Rekall Corporation

Penetration Test Report

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	**Rekall Corporation**.
Contact Name	Kateryna Broome
Contact Title	penetration tester

Document History

Version	Date	Author(s)	Comments
001	05/02/2022		

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.

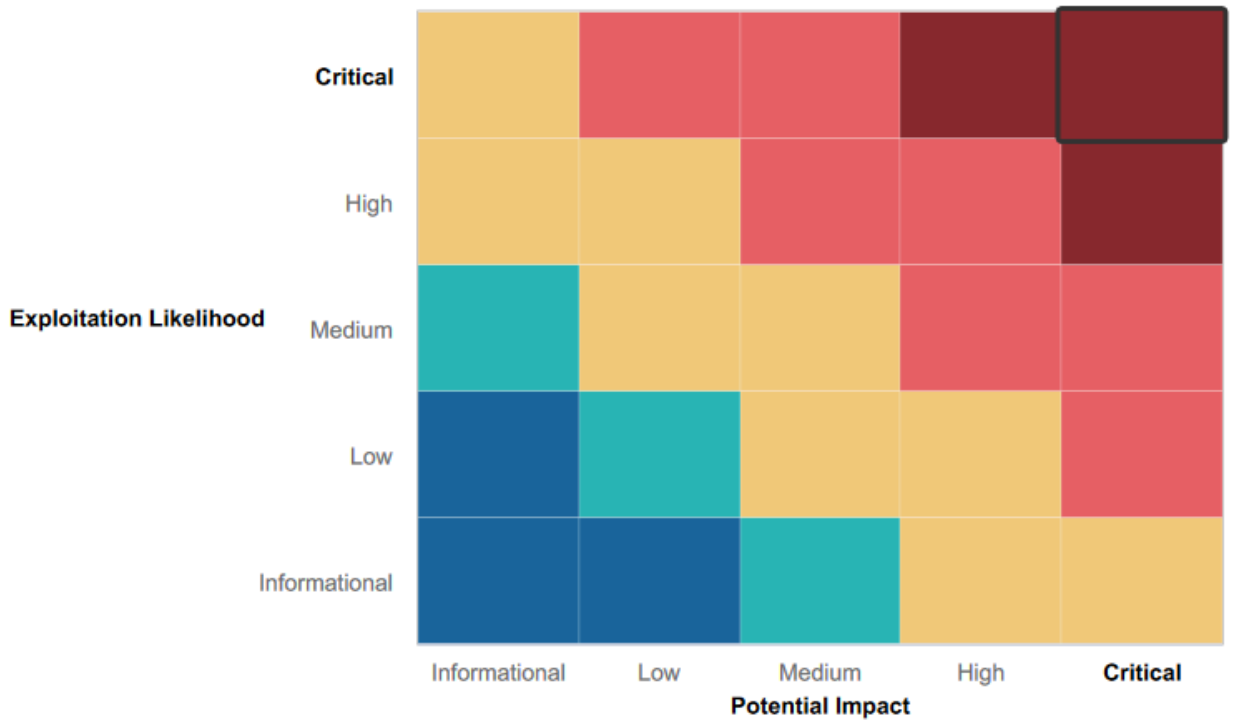
Executive Summary of Findings

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

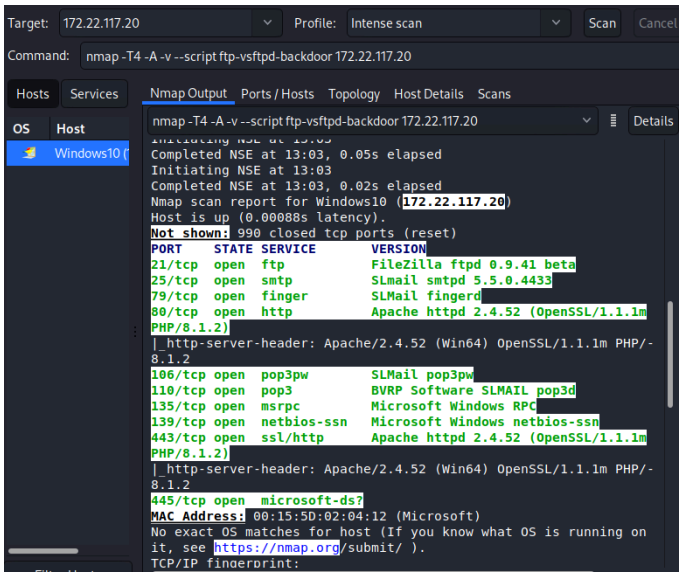
While the assessment team was successful in finding several vulnerabilities, the team also recognized several strengths within Rekall's environment. These positives highlight the effective countermeasures and defenses that successfully prevented, detected, or denied an attack technique or tactic from occurring.

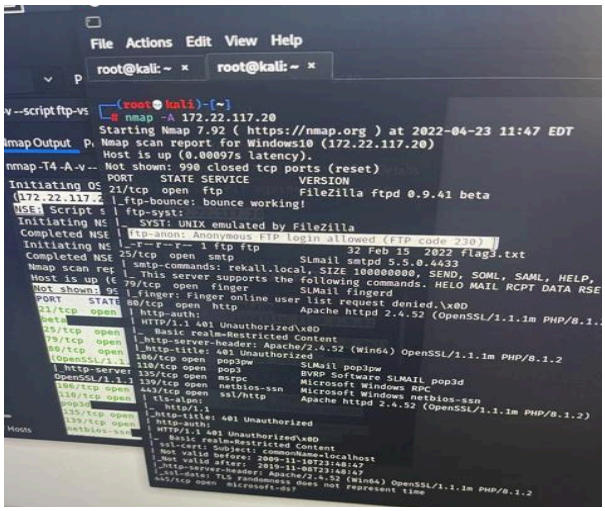
- Rekall Corporation has a strong organization web application
- Organization's Linux servers
- Organization's Windows servers

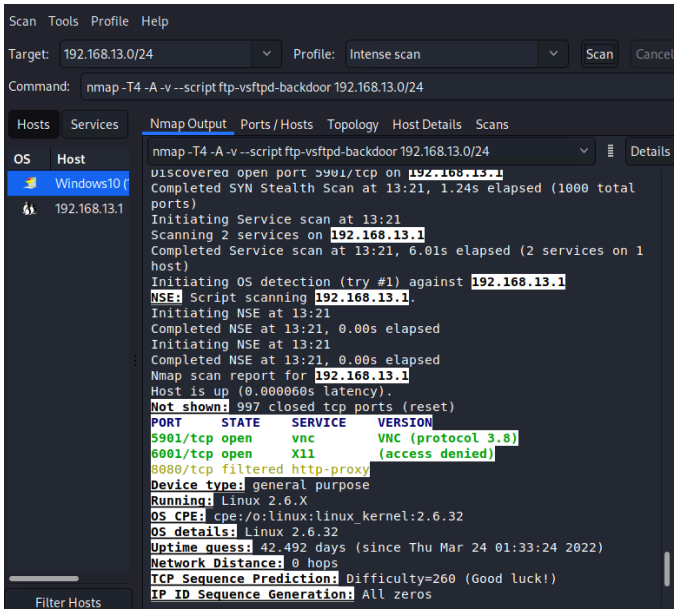
Summary of Weaknesses

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.

- Rekall corporation has a week password and login
- Rekall corporation has a Reflected cross-site scripting vulnerability
- Using port 21 FTP can expose sensitive information and network credentials to an attacker when transmitting data across the network or the Internet.
- By leaving port 25 unmonitored and open, web hosting providers are at risk of enabling spammers within their network to run wild with huge volumes of spam traffic.
- Attacks exploit vulnerability in website running on port 80/443 to get into system, HTTP protocol itself or HTTP application (apache, nginx etc.) vulnerability.
- Port 135 and port 139 pertaining to NetBios are vulnerable
- Linux vulnerability used Metasploit
- Windows vulnerability used Metasploit
- Apache http 2.4.52 has couple of vulnerabilities, tracked as CVE-2021-44790 and CVE-2021-44224 , that can lead to remote code execution attacks

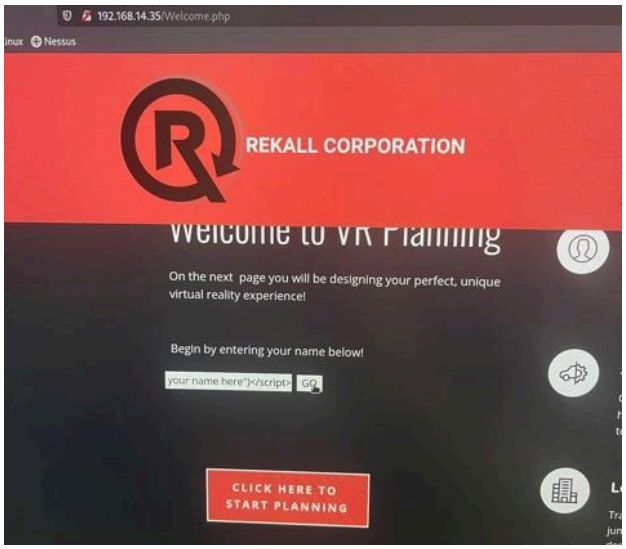


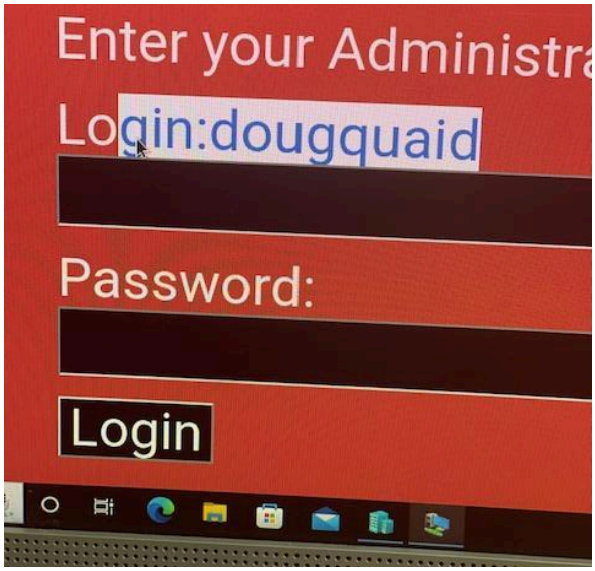


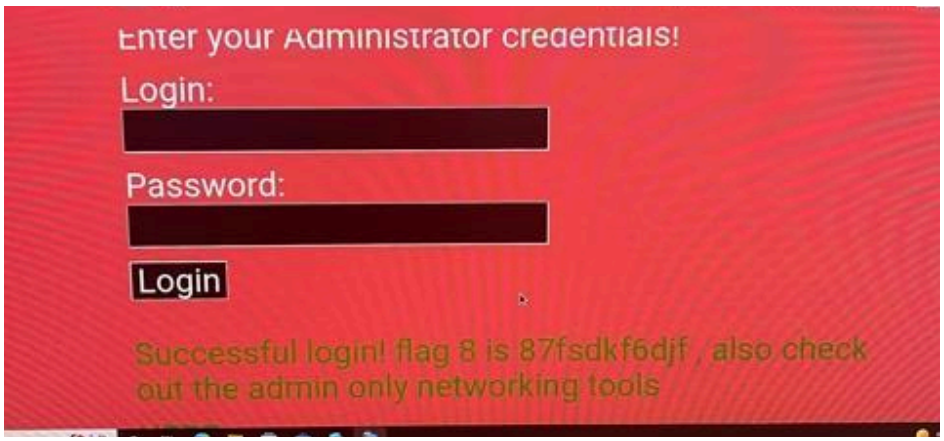


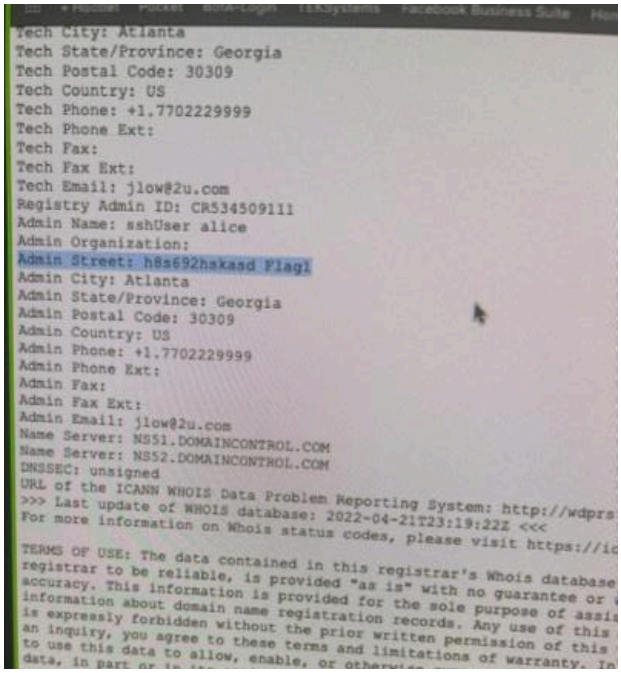
Executive Summary

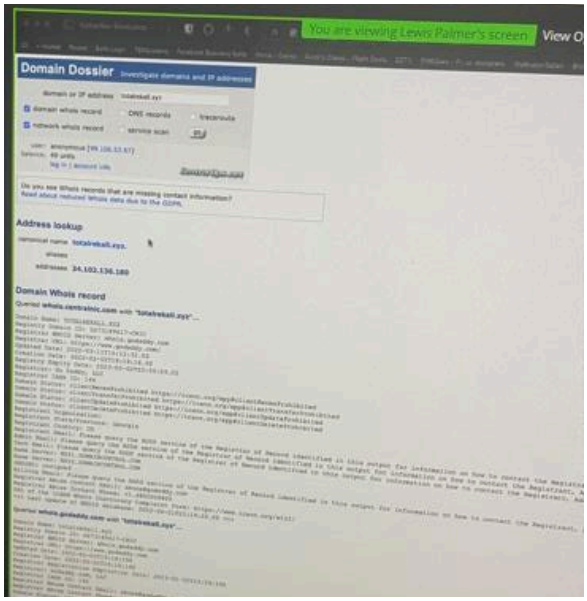
[Provide a narrative summary of your steps and findings, including screenshots. It's fine to mention specifics (e.g., used Metasploit to exploit a vulnerable version of DistCC), but do not get too technical in these specifics. This should be an A–Z summary of your assessment

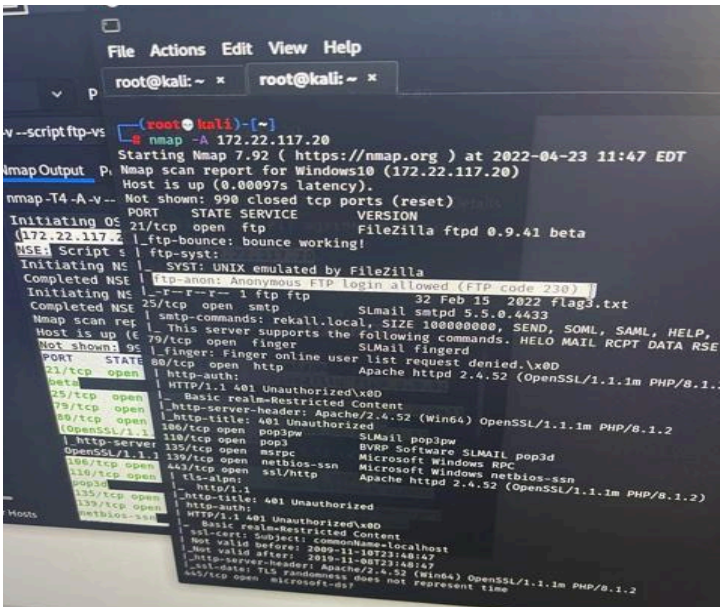


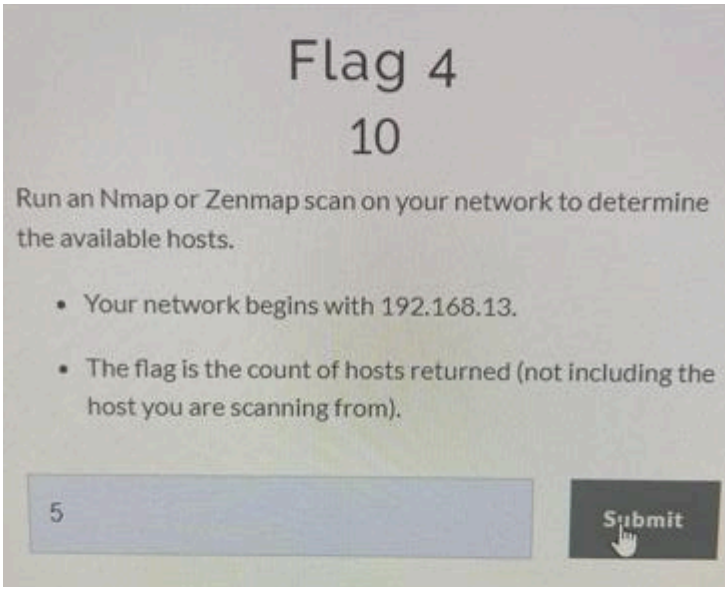


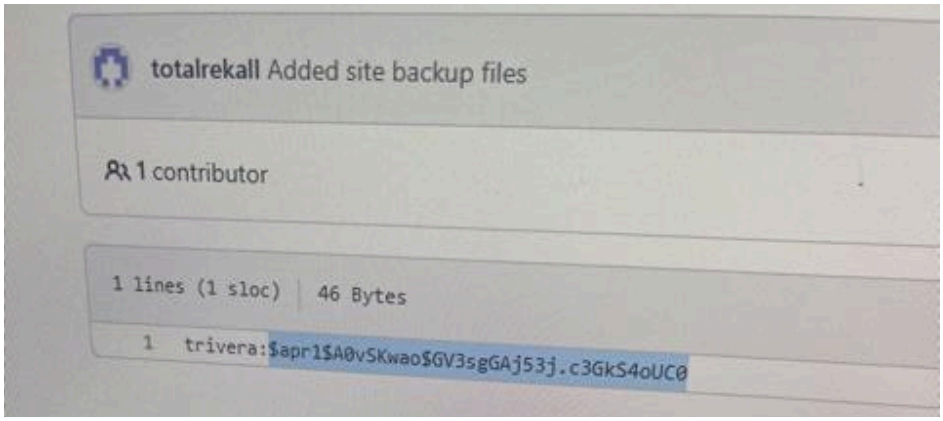


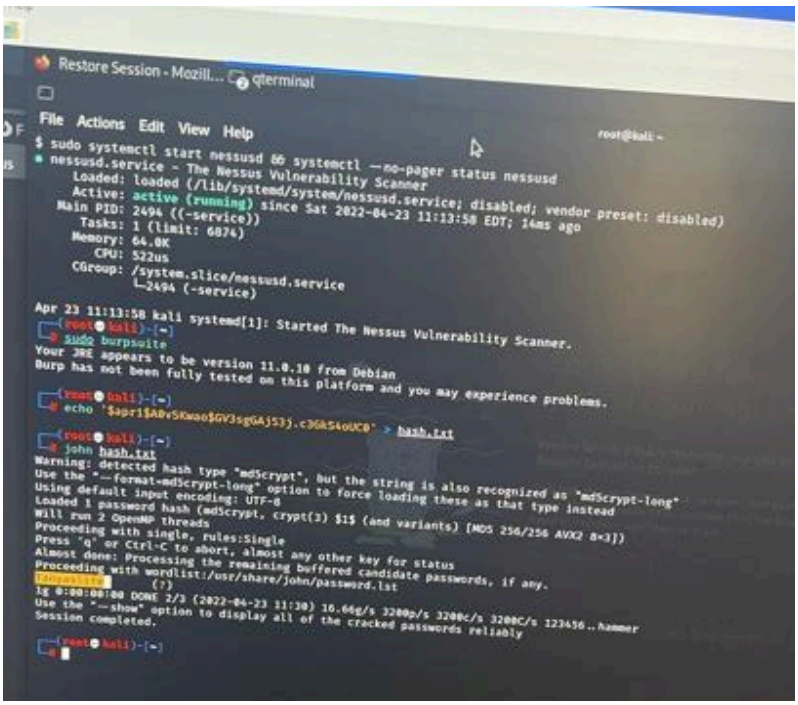


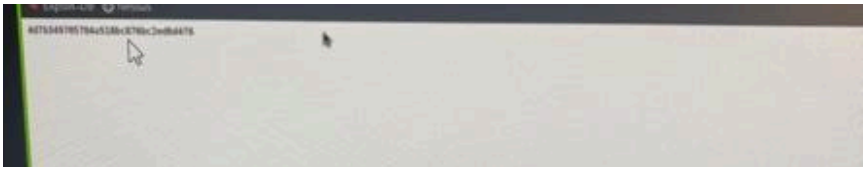


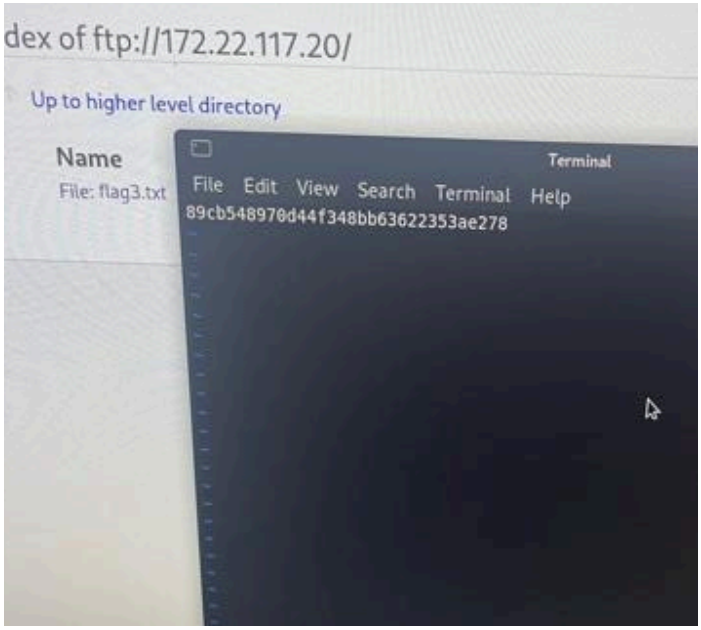


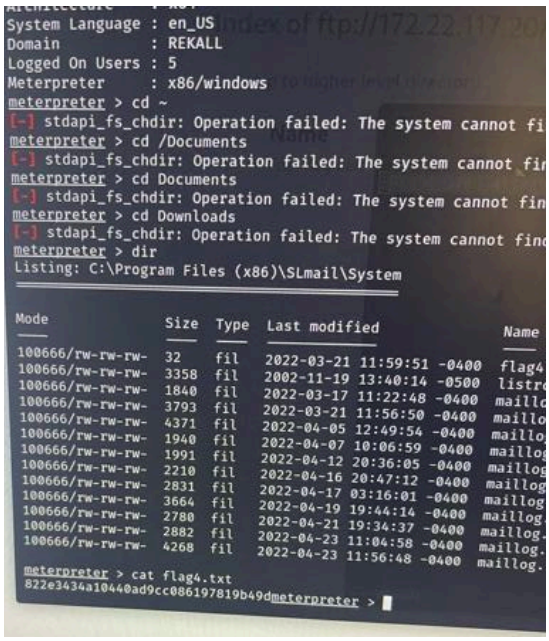


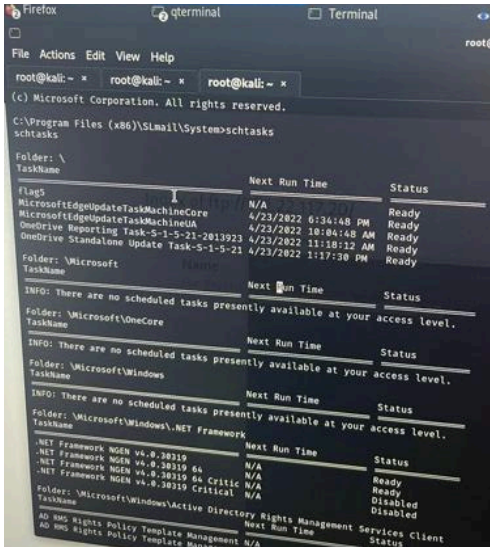


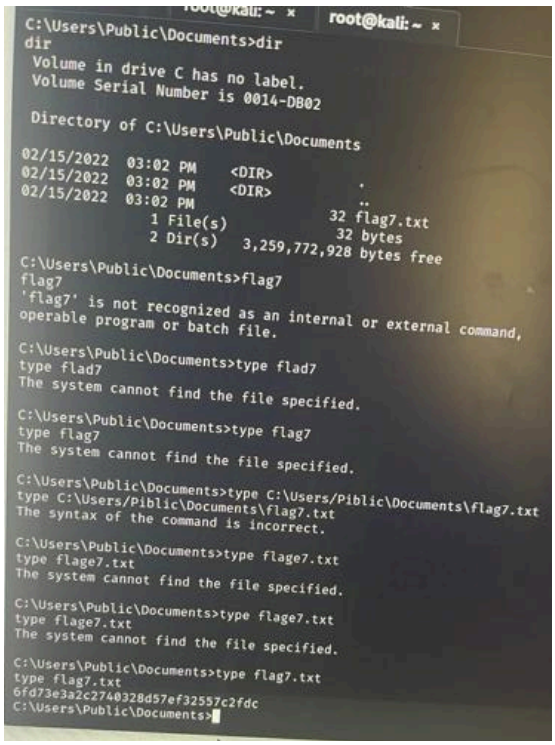




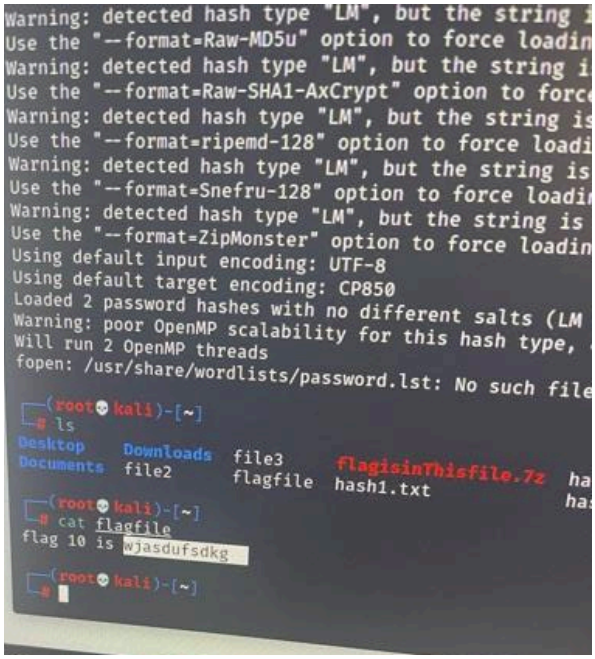








```
root@kali: ~ ×
C:\Users\Public\Documents>dir
 Volume in drive C has no label.
 Volume Serial Number is 0014-DB02

 Directory of C:\Users\Public\Documents

02/15/2022  03:02 PM    <DIR>          .
02/15/2022  03:02 PM    <DIR>          ..
02/15/2022  03:02 PM                32 flag7.txt
               1 File(s)             32 bytes
               2 Dir(s)   3,259,772,928 bytes free

C:\Users\Public\Documents>flag7
flag7
'flag7' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\Public\Documents>type flad7
type flad7
The system cannot find the file specified.

C:\Users\Public\Documents>type flag7
type flag7
The system cannot find the file specified.

C:\Users\Public\Documents>type C:\Users/Piblic\Documents\flag7.txt
type C:\Users/Piblic\Documents\flag7.txt
The syntax of the command is incorrect.

C:\Users\Public\Documents>type flage7.txt
type flage7.txt
The system cannot find the file specified.

C:\Users\Public\Documents>type flage7.txt
type flage7.txt
The system cannot find the file specified.

C:\Users\Public\Documents>type flag7.txt
type flag7.txt
6fd73e3a2c2740328d57ef32557c2fdc
C:\Users\Public\Documents>
```



```
Warning: detected hash type "LM", but the string i
Use the "--format=Raw-MD5u" option to force loadin
Warning: detected hash type "LM", but the string i
Use the "--format=Raw-SHA1-AxCrypt" option to forc
Warning: detected hash type "LM", but the string is
Use the "--format=ripemd-128" option to force loadi
Warning: detected hash type "LM", but the string is
Use the "--format=Snefru-128" option to force loadi
Warning: detected hash type "LM", but the string is
Use the "--format=ZipMonster" option to force loadin
Using default input encoding: UTF-8
Using default target encoding: CP850
Loaded 2 password hashes with no different salts (LM
Warning: poor OpenMP scalability for this hash type,
Will run 2 OpenMP threads
fopen: /usr/share/wordlists/password.lst: No such file

┌──(root💀 kali)-[~]
└─# ls
Desktop   Downloads  file3     flagisinThisfile.7z  ha
Documents file2      flagfile  hash1.txt            ha

┌──(root💀 kali)-[~]
└─# cat flagfile
flag 10 is wjasdufsdkg

┌──(root💀 kali)-[~]
└─#
```

Summary Vulnerability Overview

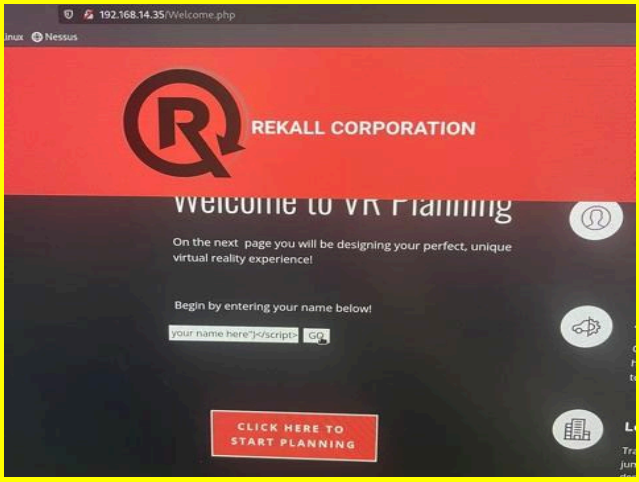
Vulnerability	Severity
Website is vulnerable to XSS	hight
Users password can be determined through the passive monitoring of an SSHv1 session	critical
Port 80 open	low
Port 21 open	low
Port 25 open	medium
Port 135/139 open	medium
Port 443 open /Apache	low
Port 79 open Finger	critical
Windows and Linux vulnerabilities using Metasploit	medium
Port 445 open	critical
Port 8080 open	high
SLMail service	high

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

Scan Type	Total
Hosts	1 (172.22.117.20) 2 (192.168.13.1)
Ports	10 ports open 3 ports open

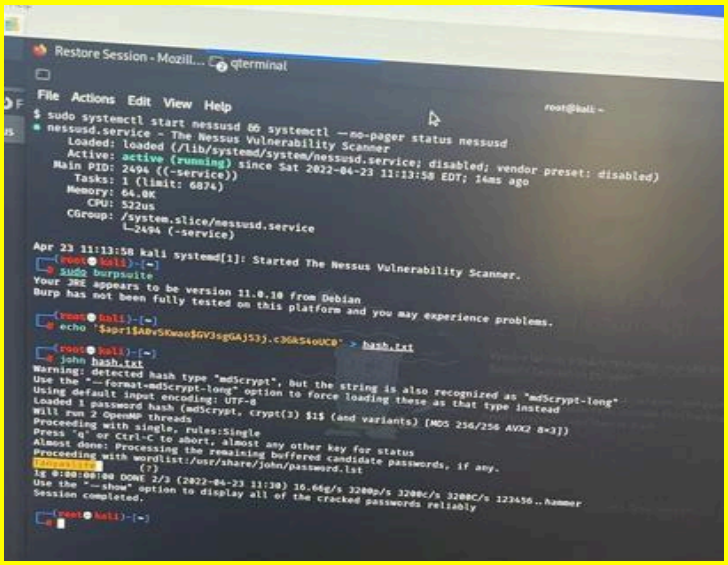
Exploitation Risk	Total
Critical	5
High	4
Medium	0
Low	2

Vulnerability Findings

Vulnerability 1	Findings
Title	Website is vulnerable to XSS
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	high
Description	Cross-site scripting (XSS) is a type of computer security vulnerability typically found in web applications which allow code injection by malicious web users into the web pages viewed by other users.
Images	

Affected Hosts	172.22.117.20
Remediation	• Filter input on arrival. At the point where user input is received, filter as strictly as possible based on what is expected or valid input. • Encode data on output. ... • Use appropriate response headers. ... • Content Security Policy.

Vulnerability 2	Findings
Title	Users password can be determined through the passive monitoring
Type (Web app / Linux OS / WIndows OS)	Web app and Windows
Risk Rating	critical
Description	Attacker can gain an access to the system using stollen credentials of users
Images	

	
Affected Hosts	
Remediation	As long as strong passwords are used, a successful attack through the normal SSH authentication mechanism is unlikely. Upgrade to the latest version of SSH and ensure that proper logging is taking place and that logs are monitored on a regular basis.

Vulnerability 3	Findings
Title	Port 80 open
Type (Web app / Linux OS / WIndows OS)	Linux and Windows
Risk Rating	Low
Description	TCP port 80: HTTP Web header: Apache 2.4.52 Apache/2.2.52: This version of Apache is vulnerable to an information leakage bug that would allow an attacker to retrieve a directory listing and obtain pathnames. This information could be leveraged for other attacks, but is considered a low-risk vulnerability

Images	
Affected Hosts	172.22.117.20
Remediation	The administration tools are protected by password authorization, so as long as strong passwords are used, the risk is minimal. For best results, apply access control mechanisms to prevent directory access of /admin in the first place. An attacker could still attempt to run a brute force attack on passwords

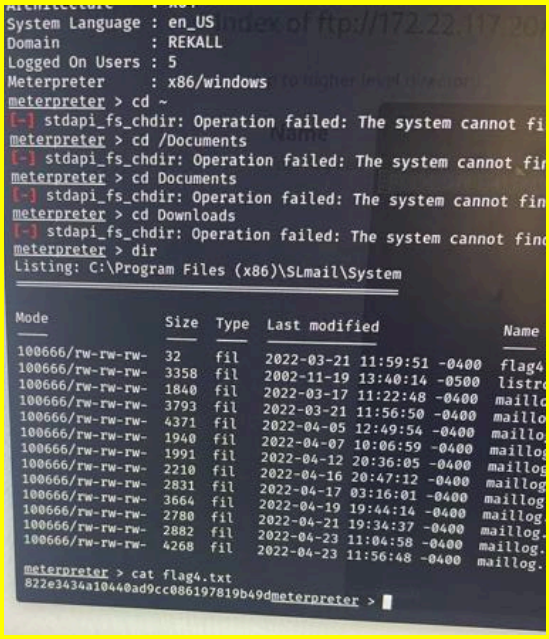
Vulnerability 4	Findings
Title	Port 8080 open
Type (Web app / Linux OS / WIndows OS)	Linux Windows
Risk Rating	high
Description	Leaving port 8080 open to the global Internet allows a potential attacker to retrieve various data about the servers operating environment
Images	
Affected Hosts	192.168.13.1
Remediation	Close port 8080, or disable the service if it's not needed, since crackers scanning for proxy servers will find this port, drawing unnecessary attention to your site.

Vulnerability 5	Findings
Title	Port 21 open
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	low
Description	TCP port 21 connects FTP servers to the internet. **FTP servers carry numerous vulnerabilities such as anonymous authentication capabilities, directory traversals, and cross-site scripting**, making port 21 an ideal target.

Images	
Affected Hosts	172.22.117.20
Remediation	1. Access ports using a secure virtual private network (VPN). If a business needed something like RDP, ITS would use an encrypted VPN connection to access RDP instead of leaving it open to the internet. ... 2. Use multi-factor authentication. ... 3. Implement network segmentation. ... 4. Scan network ports regularly.

Vulnerability 6	Findings
Title	Port 79 open
Type (Web app / Linux OS / WIndows OS)	Linux
Risk Rating	high
Description	**Finger** is a program you can use to find information about computer users. It usually lists the login name, the full name, and possibly other details about the user you are fingering. These details may include the office location and phone number (if known), login time, idle time, time mail was last read, and the user's plan and project files.
Images	
Affected Hosts	172.22.117.20
Remediation	Disable on all host unless finger service is stubbed to only provide scripted data response (eg: system admin contact info - etc.).

Vulnerability 7	Findings
Title	SLMail service using a port 110
Type (Web app / Linux OS / WIndows OS)	Windows App
Risk Rating	high
Description	Number one **vulnerability** database documenting and explaining security **vulnerabilities**, threats, and exploits

Images	 System Language : en_US Domain : REKALL Logged On Users : 5 Meterpreter : x86/windows meterpreter > cd ~ [-] stdapi_fs_chdir: Operation failed: The system cannot fi meterpreter > cd /Documents [-] stdapi_fs_chdir: Operation failed: The system cannot fi meterpreter > cd Documents [-] stdapi_fs_chdir: Operation failed: The system cannot fin meterpreter > cd Downloads [-] stdapi_fs_chdir: Operation failed: The system cannot fin meterpreter > dir Listing: C:\Program Files (x86)\SLmail\System Mode Size Type Last modified Name 100666/rw-rw-rw- 32 fil 2022-03-21 11:59:51 -0400 flag4 100666/rw-rw-rw- 3358 fil 2002-11-19 13:40:14 -0500 listr 100666/rw-rw-rw- 1840 fil 2022-03-17 11:22:48 -0400 maillo 100666/rw-rw-rw- 3793 fil 2022-03-21 11:56:50 -0400 maillo 100666/rw-rw-rw- 4371 fil 2022-04-05 12:49:54 -0400 maillo 100666/rw-rw-rw- 1940 fil 2022-04-07 10:06:59 -0400 maillo 100666/rw-rw-rw- 1991 fil 2022-04-12 20:36:05 -0400 maillog 100666/rw-rw-rw- 2210 fil 2022-04-16 20:47:12 -0400 maillog 100666/rw-rw-rw- 2831 fil 2022-04-17 03:16:01 -0400 maillog 100666/rw-rw-rw- 3664 fil 2022-04-19 19:44:14 -0400 maillog. 100666/rw-rw-rw- 2780 fil 2022-04-21 19:34:37 -0400 maillog. 100666/rw-rw-rw- 2882 fil 2022-04-23 11:04:58 -0400 maillog. 100666/rw-rw-rw- 4268 fil 2022-04-23 11:56:48 -0400 maillog. meterpreter > cat flag4.txt 822e3434a10440ad9cc086197819b49dmeterpreter >
Affected Hosts	172.22.117.20
Remediation	Use strong password and credentials