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** | Zacks Cyber Security |
| **Contact Name** | Zackary Tullar |
| **Contact Title** | Ethical hacker |

# Document History

| Version | Date | Author(s) | Comments |
|---|---|---|---|
| 001 | 10/25/22 | ZackaryTullar | |

# 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.

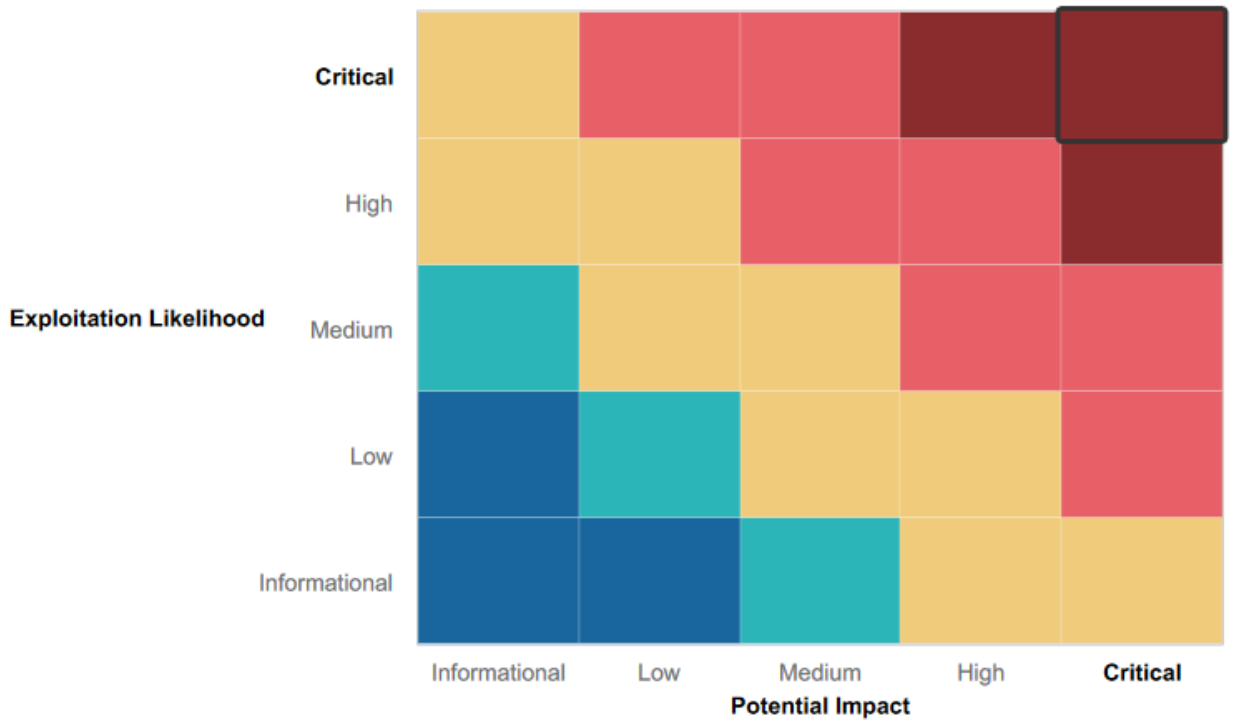
# Executive Summary of Findings

## 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.

- High-level summary of strengths here
-

## 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.

- High-level summary of weaknesses here
- Several open ports.
- Several ways to implement XSS
- Alot of vulnerable information with several different scans
- Easy access into the network
- Easy lateral movement inside the network
- Several ways to access the server from exploits

# Executive Summary

We Started with the website and found several way to implement cross site scripting to allow popups that should not be allowed. After that we were able to find sensitive data using a simple curl command that gave us flag 4. We used a Ping request to find the ip address of totalrekall.xyz. using that ip address we were able to run multiple scans using nmap and nessus. the nmap scan gave us the information on the hosts connected to the network and the nessus scan gave us a list of vulnerabilities. one of the vulnerabilities listed let us know to use a struts2 exploit to access the server. using that exploit were able to access it and navigate to the directory which contained the flag we needed. on the windows server we were able to locate a github repository giving us the credentials of a user. we were then able to use FTP anonymous to access ftp and navigate to find flag3.txt. we then were able to access the mail servers using a pop3 exploit that gave us more access and control on the server. using that access we were able to execute several things.the first was using scheduled tasks in order to find flag5.txt. using the same access we were able to perform lateral movement to find flag7 in the directory

# Summary Vulnerability Overview

| Vulnerability | Severity |
|---|---|
| Cross Site Scripting | Critical |
| Cross Site Scripting | Critical |
| Sensitive data | High |
| Ping request | Medium |
| Nmap Network enumeration | Critical |
| nessus scan | Critical |
| vulnerability in struts | High |
| OSINT | Critical |
| FTP access | Critical |
| Port 110 access | Critical |
| schtasks | Critical |
| Lateral movement | Critical |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |

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

| Scan Type | Total |
|---|---|
| Hosts | 192.168.14.35<br>totalrekall.xyz<br>192.168.13.0/24<br>172.22.117.0/24<br>172.22.117.10 |

| | |
|---|---|
| | 172.22.117.20 |
| Ports | 21,25,79,106,109,135,145,335,443 |

| Exploitation Risk | Total |
|---|---|
| Critical | 9 |
| High | 2 |
| Medium | 1 |
| Low | 0 |

# Vulnerability Findings

| Vulnerability 1 | Findings |
|---|---|
| Title | Cross site scripting |
| Type (Web app / Linux OS / WIndows OS) | Web app |
| Risk Rating | Critical |
| Description | we were able to put in a script to make a pop up appear on the welcome page. which could be used to access sensitive data by injecting harmful code. |
| Images | |
| Affected Hosts | 192.168.14.35 |
| Remediation | a WAF or firewall could help prevent this. |

| Vulnerability 2 | Findings |
|---|---|
| Title | Cross site scripting |
| Type (Web app / Linux OS / WIndows OS) | Web app |
| Risk Rating | Critical |
| Description | We were able to input a script into the comments page to make a pop up appear which could be used to inject harmful code that would allow them to access sensitive data. |
| Images | |

| | |
|---|---|
| **Affected Hosts** | 192.168.14.35 |
| **Remediation** | implementing a WAF or firewall could help prevent this. |

| Vulnerability 3 | Findings |
|---|---|
| **Title** | Sensitive data exposure |
| **Type (Web app / Linux OS / WIndows OS)** | Web app |
| **Risk Rating** | High |
| **Description** | We were able to do a curl command to the about page to find flag 4 |
| **Images** | |
| **Affected Hosts** | 192.168.14.35 |
| **Remediation** | they should encrypt the data to make it not as accessible |

| Vulnerability 4 | Findings |
|---|---|
| **Title** | Ping request |
| **Type (Web app / Linux OS / WIndows OS)** | Linux OS |
| **Risk Rating** | Medium |
| **Description** | We were able to ping the host to find the ip address |
| **Images** | |
| **Affected Hosts** | totalrekall.xyz |
| **Remediation** | They should implement a firewall to block ping request |

| Vulnerability 5 | Findings |
|---|---|
| **Title** | Nmap scan |
| **Type (Web app / Linux OS / WIndows OS)** | Linux OS |
| **Risk Rating** | Critical |
| **Description** | We were able to run an Nmap scan to view the ip addresses for all of their servers |
| **Images** | |

| | |
|---|---|
| **Affected Hosts** | Totalrekall.xyz |
| **Remediation** | Blocking the ping request would prevent being able to do this in general but adding a firewall would be the best option |

| Vulnerability 6 | Findings |
|---|---|
| **Title** | Nessus scan |
| **Type (Web app / Linux OS / WIndows OS)** | Linux OSw |
| **Risk Rating** | Critical |
| **Description** | We were able to run a scan through nessus which was able to identify all of the vulnerabilities in the server |
| **Images** | |
| **Affected Hosts** | 192.168.13.12 |
| **Remediation** | they need a monitor on their network to notify them when it has been scanned to prevent damage |

| Vulnerability 7 | Findings |
|---|---|
| **Title** | Vulnerability in struts |
| **Type (Web app / Linux OS / WIndows OS)** | Linux OS |
| **Risk Rating** | Critical |
| **Description** | We were able to use metasploit to run an exploit on struts to which gave us access to the host which led to us escalating privilege and finding the flag inside the root folder and we were able to view it running a cat command |
| **Images** | |
| **Affected Hosts** | 192.168.13.12 |
| **Remediation** | They need to update their systems to patch their struts to prevent access to with this exploit and keep their systems and servers upto date |

Add any additional vulnerabilities below.

Vulnerability 8, OSINT
OS TYPE:Windows OS
Risk:Critical

Description:We were able to find inside a github repository the Login credentials of a user with the login and a hashed password that we were able to crack using john.

```
┌──(root💀 kali)-[~]
└─# john hashes.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 512/512 AVX512BW 16×3])
Will run 2 OpenMP threads
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
Tanya4life       (trivera)
1g 0:00:00:00 DONE 2/3 (2022-10-31 19:26) 4.761g/s 5971p/s 5971c/s 5971C/s 123456..jake
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

┌──(root💀 kali)-[~]
└─# nmap 172.22.117.10
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-31 19:29 EDT
Nmap scan report for WinDC01 (172.22.117.10)
Host is up (0.00068s latency).
Not shown: 989 closed tcp ports (reset)
PORT     STATE SERVICE
53/tcp   open  domain
88/tcp   open  kerberos-sec
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
389/tcp  open  ldap
445/tcp  open  microsoft-ds
464/tcp  open  kpasswd5
593/tcp  open  http-rpc-epmap
636/tcp  open  ldapssl
3268/tcp open  globalcatLDAP
3269/tcp open  globalcatLDAPssl
MAC Address: 00:15:5D:02:04:13 (Microsoft)

Nmap done: 1 IP address (1 host up) scanned in 19.06 seconds
```

Affected Hosts: 172.22.117.20
Remediation: Change the credentials asap and any others that may be exposed online.

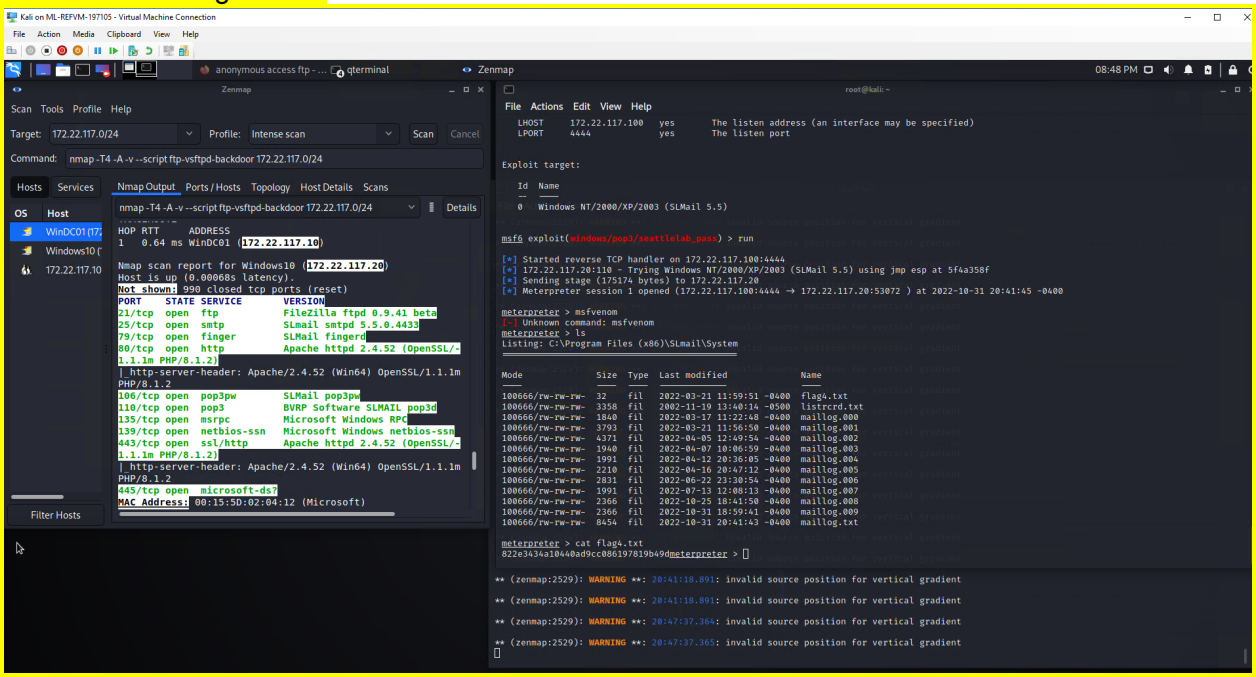
Vulnerability 9: FTP access
OS TYPE: Windows OS
Risk: Critical
Description: We were able to access the host using FTP and were able to find the flag3.txt file. we were able to download the file onto our machine which let us view the file finding the flag.

```
┌──(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:
230 Logged on
Remote system type is UNIX.
ftp> get flag3.txt
local: flag3.txt remote: flag3.txt
200 Port command successful
150 Opening data channel for file transfer.
226 Transfer OK
32 bytes received in 0.00 secs (82.2368 kB/s)
ftp> !
┌──(root💀 kali)-[~]
└─# ls downloads
ls: cannot access 'downloads': No such file or directory

┌──(root💀 kali)-[~]
└─# ls
Desktop  Documents  Downloads  file2  file3  flag3.txt  flagisinThisfile.7z  hashes.txt  LinEnum.sh  Music  Pictures  Public  Scripts  Templates  Videos

┌──(root💀 kali)-[~]
└─# cd Downloads

┌──(root💀 kali)-[~/Downloads]
└─# ls

┌──(root💀 kali)-[~/Downloads]
└─# cd ..

┌──(root💀 kali)-[~]
└─# cat flag3.txt
89cb548970d44f348bb63622353ae278

┌──(root💀 kali)-[~]
└─#
```

Affected hosts: 172.22.117.20
Remediation:Close port 21 and require credentials to access the host

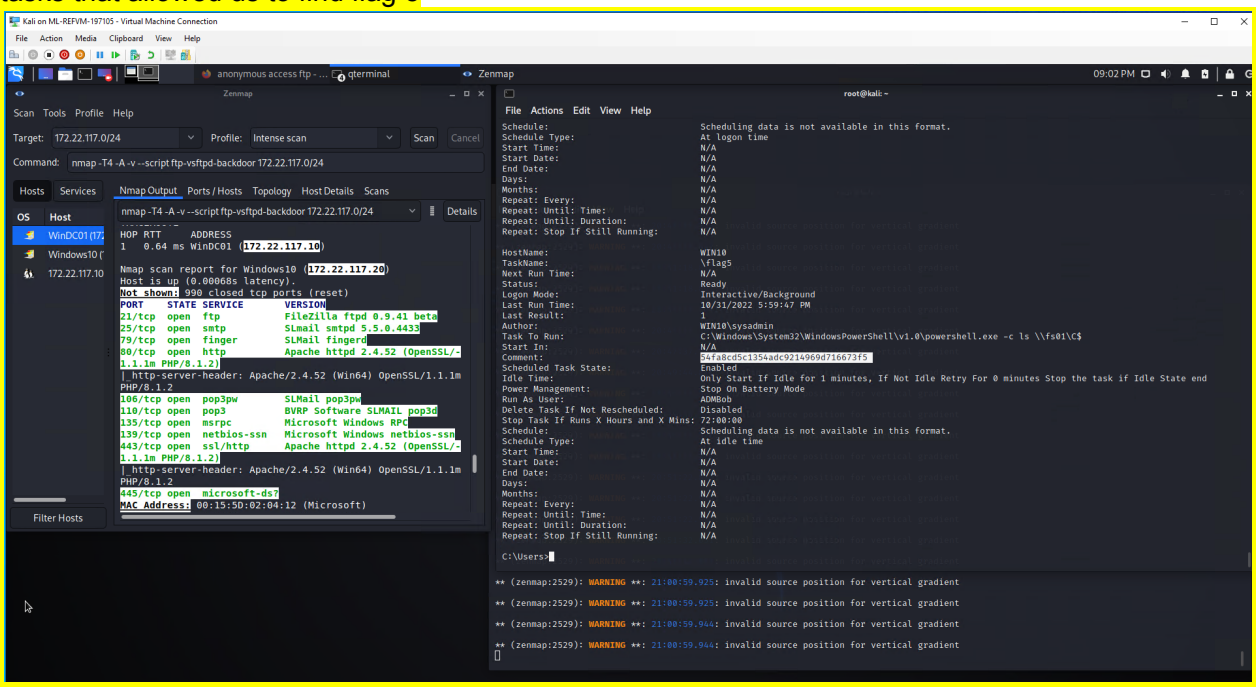
Vulnerability 10: Port 110 access
OS TYPE: Windows OS
Risk critical

Description: We were able to use SLpass exploit through metasploit to access port 110 running ls -a let us view the flag4.txt file




Affected hosts: 172.22.117.20
Remediation: Rekall needs to patch their mail servers and close port 110

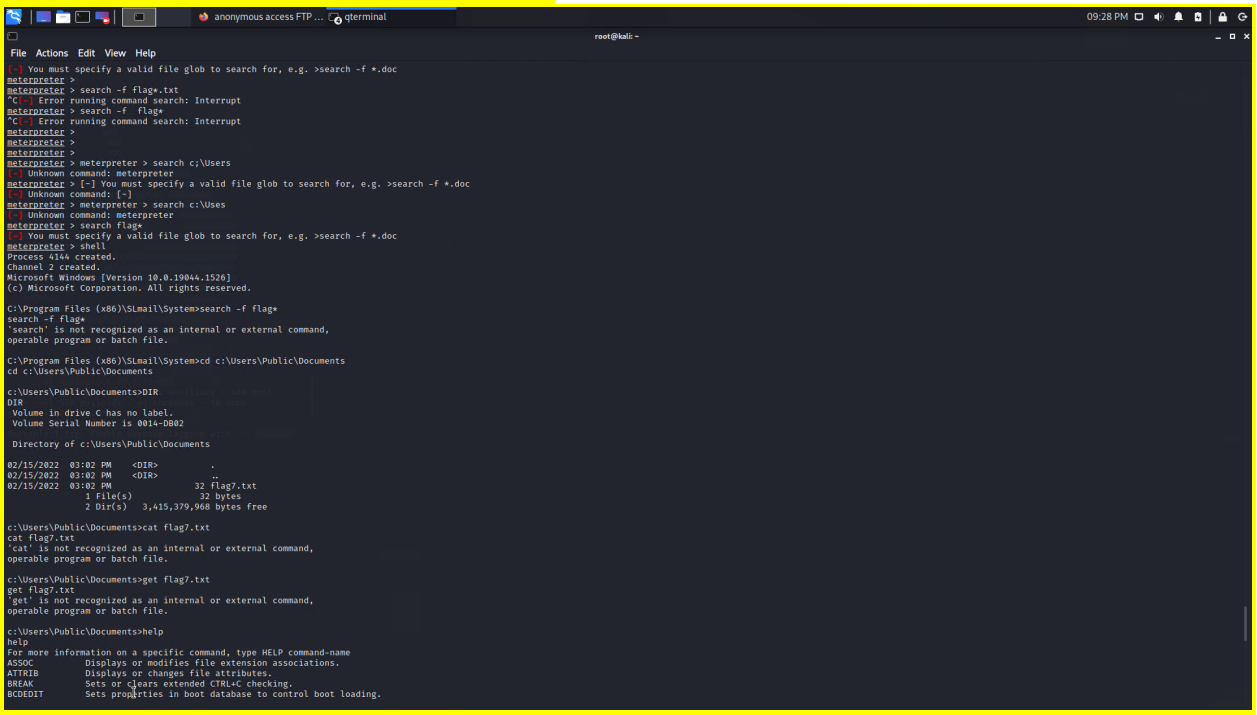
Vulnerability 11: schtasks
OS TYPE: Windows 10
Risk: Critical
Description: using the access we gained through port 110 we were able to navigate to the scheduled tasks that allowed us to find flag 5




Affected hosts: 172.22.117.20
Remediation: having the updated mail servers would prevent access altogether better security infrastructure would be the only prevention with them having access

Vulnerability 12: lateral movement
OS TYPE: Windows 10

Risk: Critical
Description: Using the meterpreter session we created into the mail servers we were able to perform lateral movement into the c:\Users\Public\Documents directory in order to find Flag7.txt although we could not read the file we were able to find it.




Affected hosts: 172.22.117.20
Remediation: Better infrastructure, Preventing access to the server in general is the best and only way to prevent this.