​

**Millisec CTF**

**Report**

18.05.2025

**Amalya Aliyeva**

**Contents**

[1. Room Description 2](#_Toc198542861)

[2. Enumeration 2](#_Toc198542862)

[3. Initial Access 3](#_Toc198542863)

[4. Privilege Escalation 3](#_Toc198542864)

[5. Summary 4](#_Toc198542865)

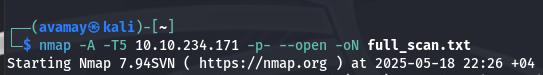
# **Room Description**

This is a mid-level Capture The Flag (CTF) challenge hosted on TryHackMe, titled “Millisec.” The objective was to perform enumeration, gain initial access, and escalate privileges to retrieve two key flags: user.txt and root.txt. The room also simulates real-world vulnerabilities, making it ideal for practicing practical penetration testing techniques.



# **Enumeration**

The assessment began with an **nmap** scan to identify open ports and services.



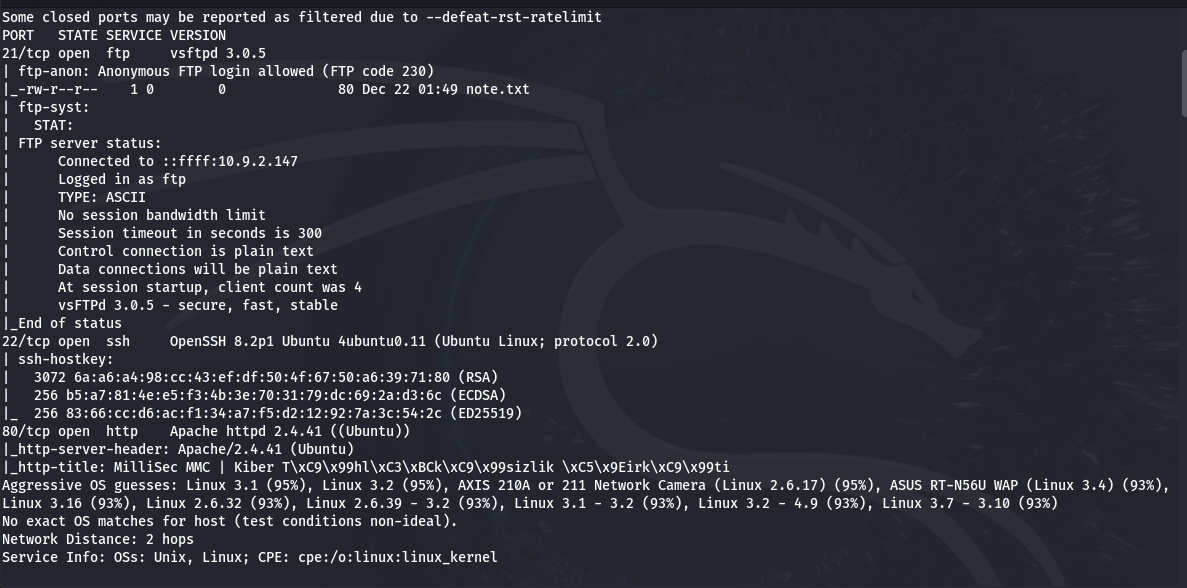
-A: Enables OS detection, version detection, script scanning, and traceroute

-T5: Sets the highest timing template for maximum speed

-p-: Scans all 65,535 ports

--open: Shows only open ports

-oN full\_scan.txt: Saves the output to a file



This revealed three open ports:

21 – FTP  (Anonymous login allowed)

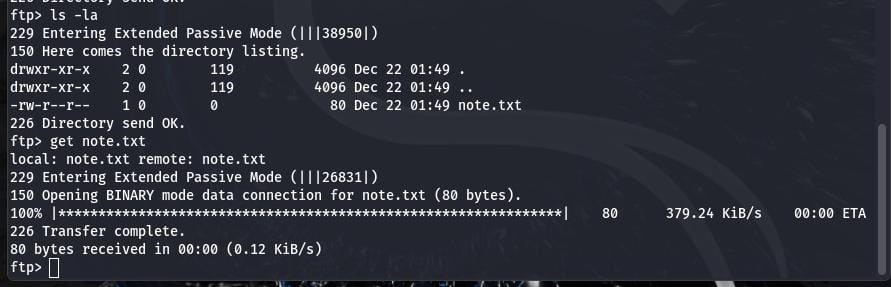
22 – SSH

80 – HTTP

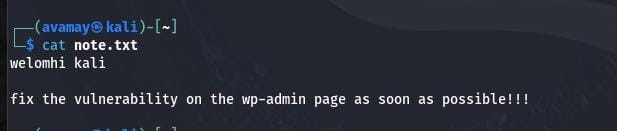
I logged into the FTP server using anonymous credentials.



Upon successful login, I listed the directory contents and downloaded the only file available, namely **note.txt**

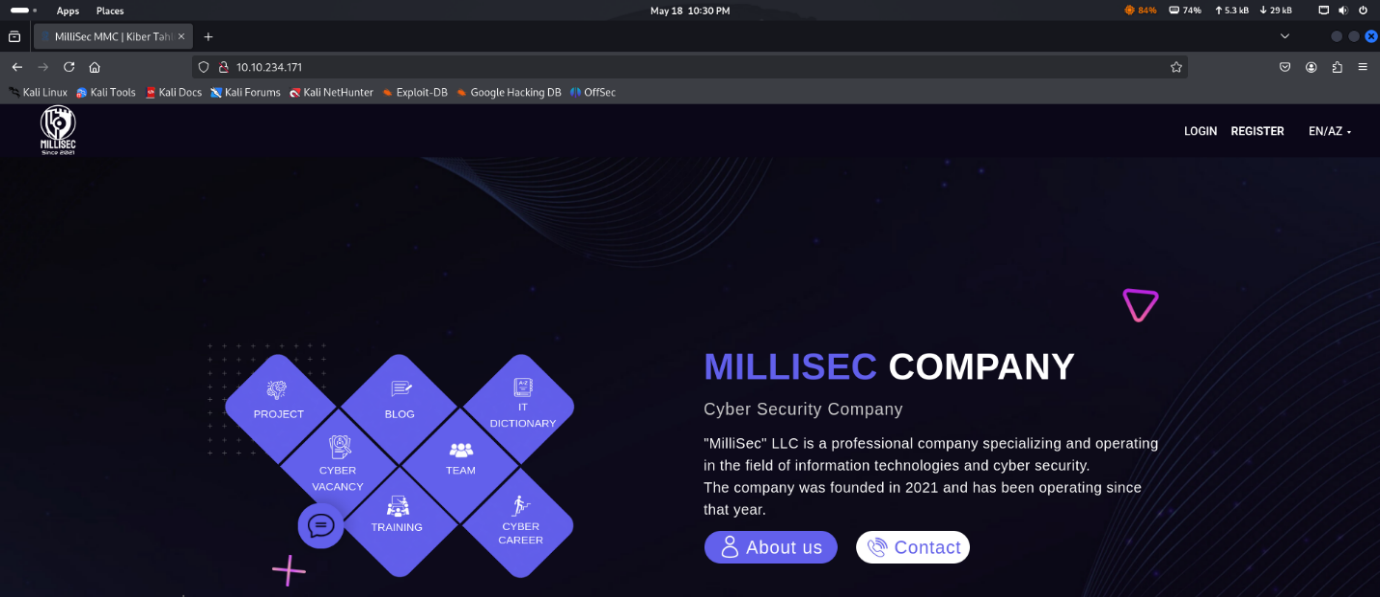
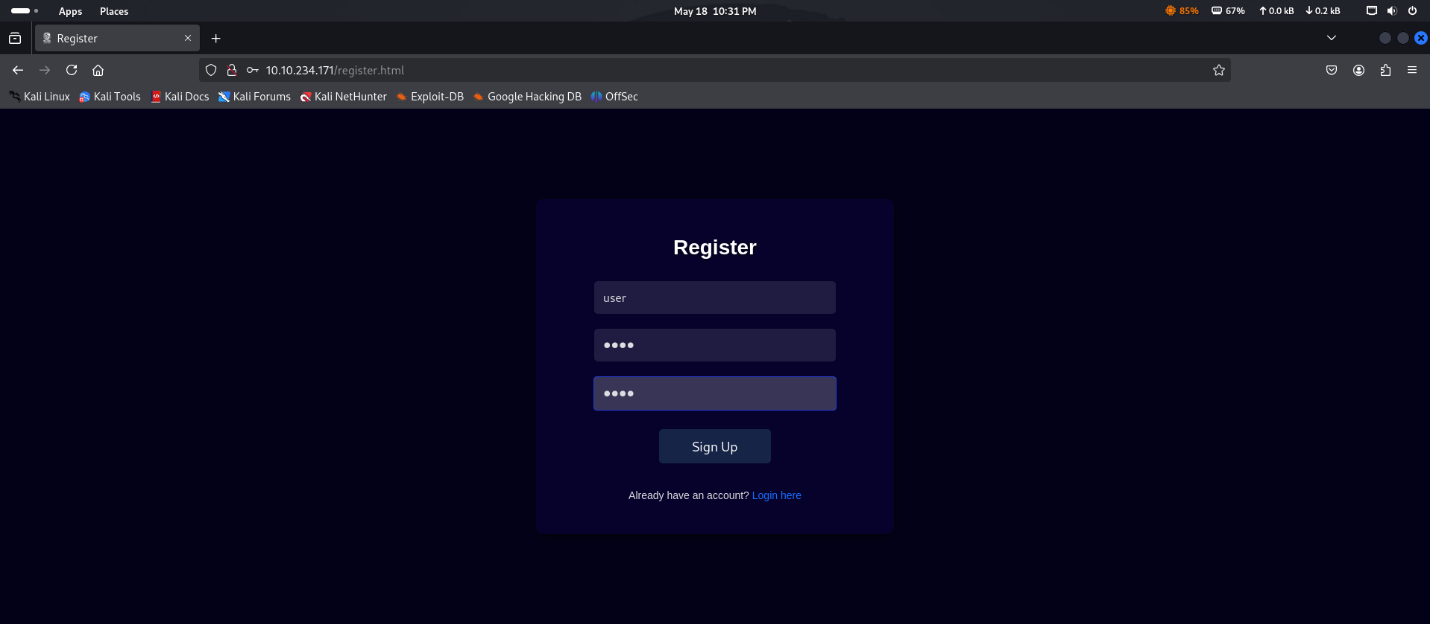


After downloading the file, I inspected its contents, using the **cat** command**.**



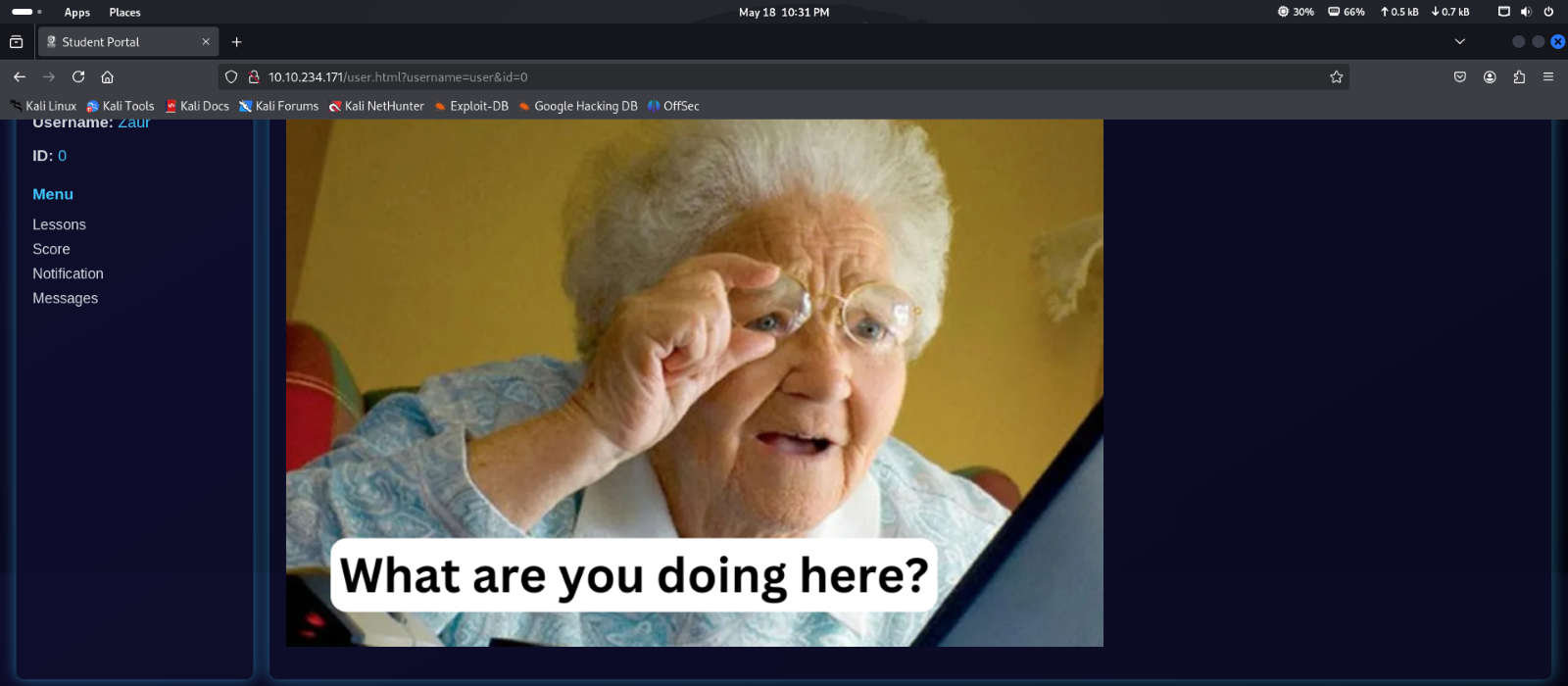
The note hinted that the target was running a WordPress site, likely accessible via the HTTP service on port 80. Based on this, I proceeded to investigate the web interface.

Navigating to the target’s IP in a browser revealed the homepage of the MilliSec company. To investigate further, I registered as a new user.

After registering, I noticed that the URL included a numeric user id. This raised the possibility of an IDOR vulnerability. IDOR – Insecure Direct Object Reference occurs when users can access unauthorized objects by modifying input values in the URL.

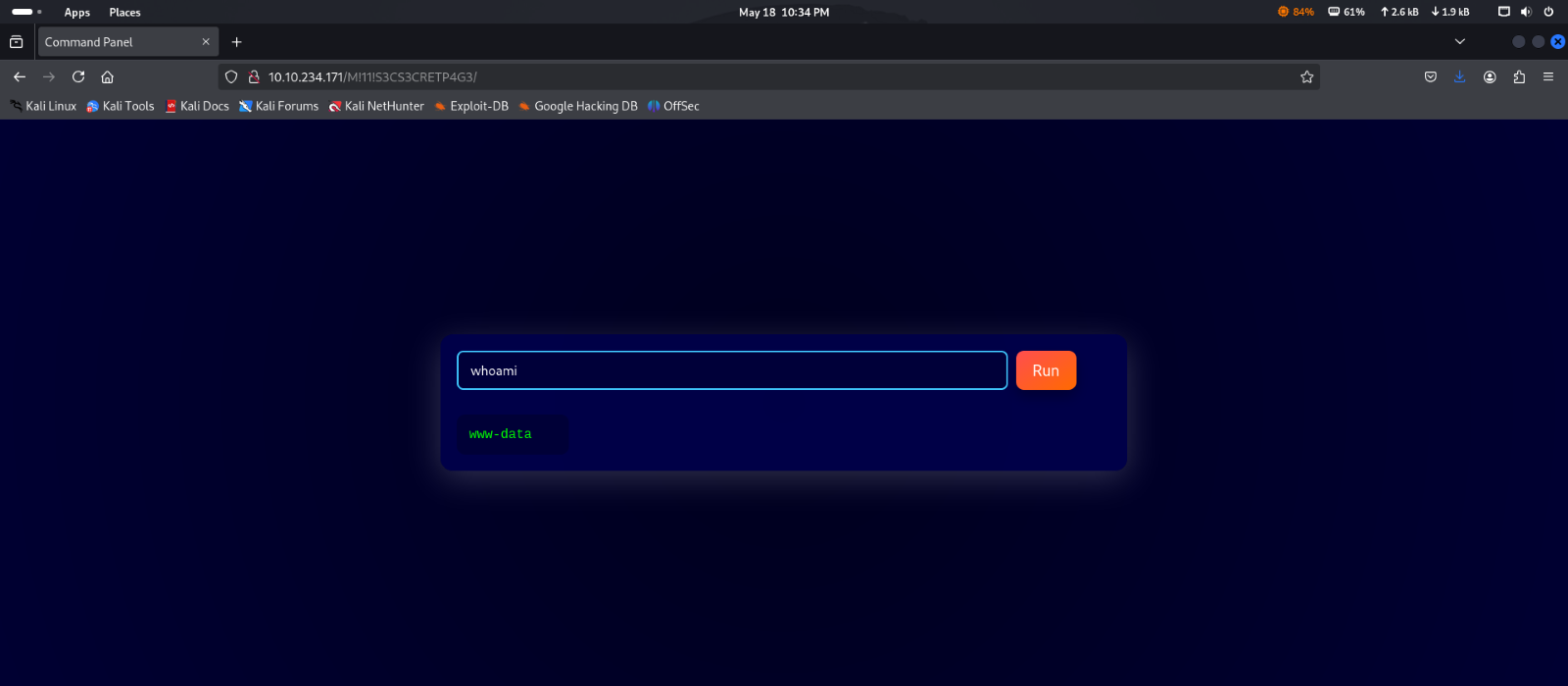
I manually changed the id to 0, which in my case redirected me to another user’s profile page featuring a user photo.



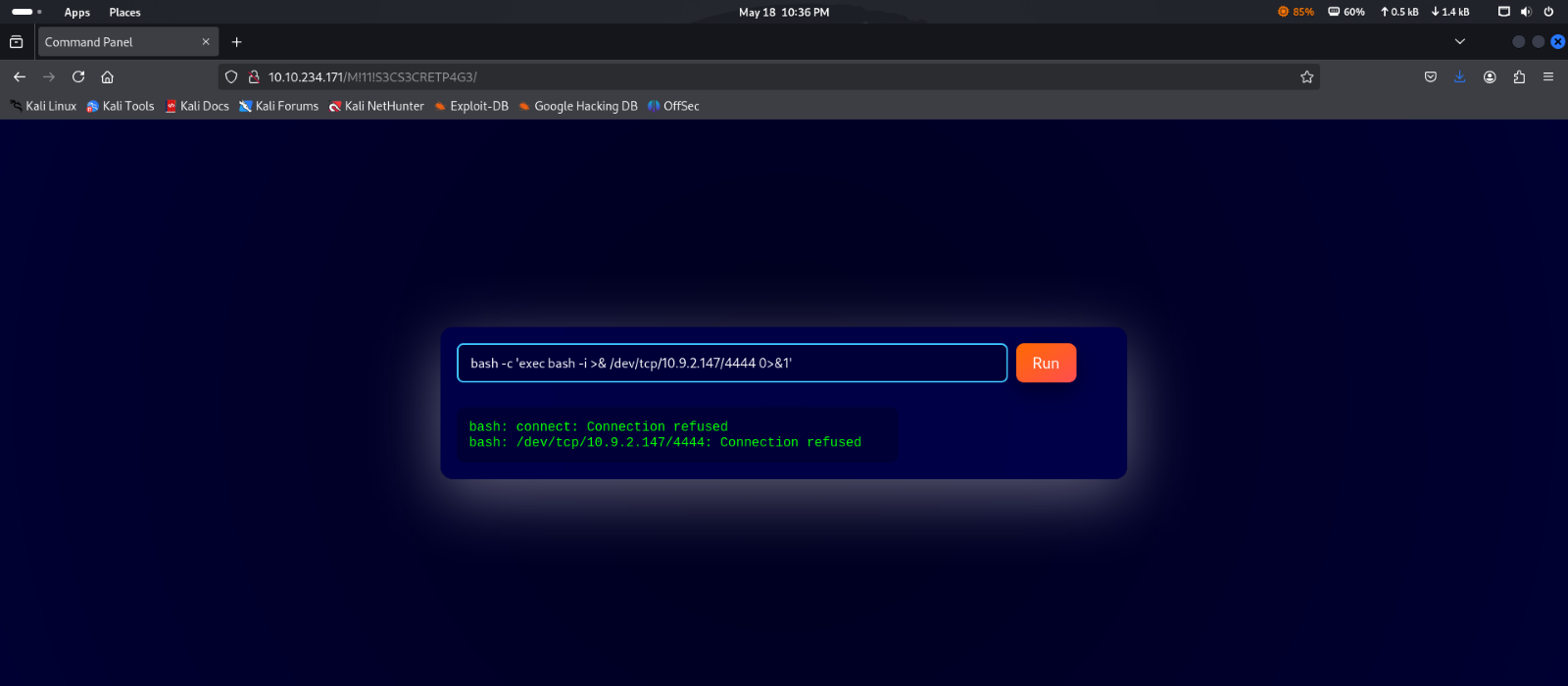
As the challenge hint suggested “metadata”, I used **exiftool** to analyze the user’s profile picture. This revealed a hidden secret key embedded in the image metadata.

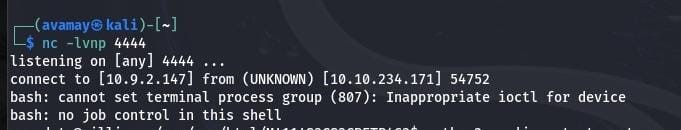
# **Initial Access**

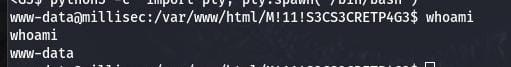
Using the key in a crafted URL, I discovered an RCE (Remote Code Execution) interface that allowed me to execute system commands on the server.



To make access more stable, I decided to establish a reverse shell for interactive use.

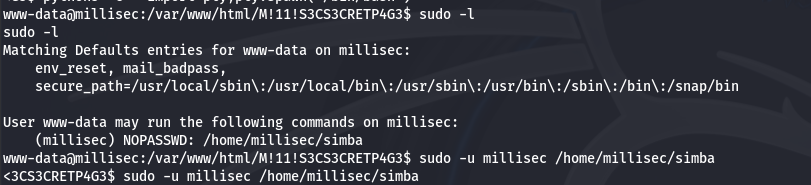






# **Privilege Escalation**

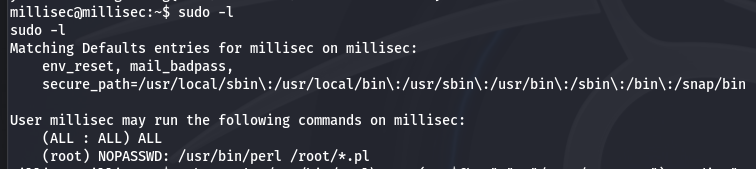
With a shell established, I checked sudo privileges. The output revealed that the user millisec could execute a specific file with no password required, which indicated a potential avenue for privilege escalation.



I executed the file with elevated privileges using **sudo -u**. To confirm the user, I ran **whoami**, which showed I was operating as millisec. Then, I navigated to the home directory, located the **user.txt** file, and read its contents, successfully capturing **the first flag**.



I ran **sudo -l** again to review available commands with root privileges, which revealed that I could execute Perl scripts in the root directory without a password. This presented аn opportunity for privilege escalation to root.



Ultimately, I used a single-line echo command to create a minimal Perl script in the /tmp directory, which was designed to read the contents of root.txt. I executed the script with root privileges, and successfully retrieved the second flag, completing the challenge.

*echo -e ‘**#!/usr/bin/perl\nopen(my $fh, “<”, “/root/root.txt”) or die “Cannot open /root/root.txt:* *$!\\n”; while (my $line = <$fh>)* *{ print $line**; } close($fh);’ > /tmp/script.pl*



# **Summary**

The CTF served as a valuable exercise in realistic exploitation. The IDOR vulnerability and metadata analysis emphasized the importance of thorough enumeration. The privilege escalation using ‘sudo’ and Perl scripting was a highlight, reinforcing post-exploitation skills.