Cyber Security Club, Uttara University

Name : Md. Rana Islam

Batch : 64

Section : A

Id : 2252081025

Username : PhantomSolver

CTF Night 0x2 Writeups

Find the hacker

Category: OSINT

Flag format: CSCUU{shisir_sir}

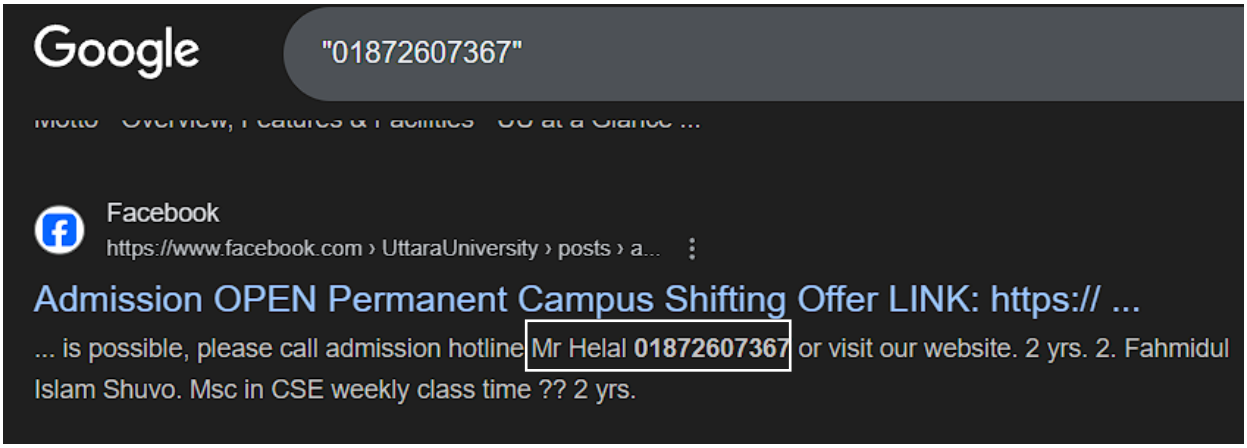
Description:

You've been given a phone number: **01872607367**.
Your goal is to find a Name that's linked to this number — maybe through social media, a data leak, or some other public source.
This is an OSINT challenge, so you'll need to use your searching skills, tools, and creativity to track it down.

⚠️ **Please don't call or message the number.**
This challenge is about research, not contacting people. If you call or interact with the number, whatever happens is your responsibility.

Approach:

I opened an internet browser then I just simply tried to google dork. Then I got many search results among them in the second result I noticed (Mr Helal **01872607367)** was mentioned then I just simply arranged helal in the mentioned flag format and I submitted the flag. And it was a right guess.



Flag: CSCUU{helal_sir}

News

Category: OSINT

Flag format: CSCUU{X} (digits only)

Description:

Summary: The number of people in certain areas around the city are tracked, recorded and available for public view. These are sensors provided by the City of Melbourne.

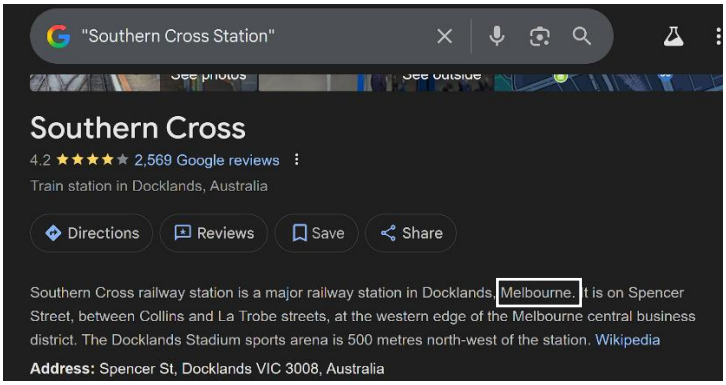
Description: We've just received a report of The Daily News publishing an article that is causing a lot of concern and fear in the public. Given its wording and theme, we are sure its fake news generated by the Roomba. However, TDN will not disclose their source. Here's the article, we need you to find the exact number of people that went through Southern Cross Station at the exact time referenced so we can determine if the article is fake. SX Station has released a statement saying that all footage of that night has been deleted so we can't rely on visuals.

Article text: "Wild scenes as 40 people confirmed to be infected with COVID-19 ran through Southern Cross Station at 4:00am on Friday, the 28th of February 2020. The frightening witness account has caused panic buying at stores around the country as people prepare to stay indoors. Our source confirms they were the only witness and that this infectious routine could be happening at other major transport venues through the country without the public's knowledge."

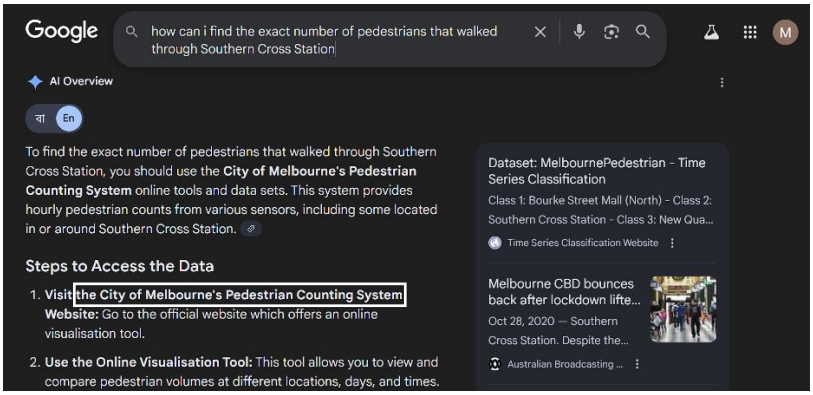
Find the exact number of pedestrians that walked through Southern Cross Station that morning at 4am, on Friday, the 28th of February.

Approach:

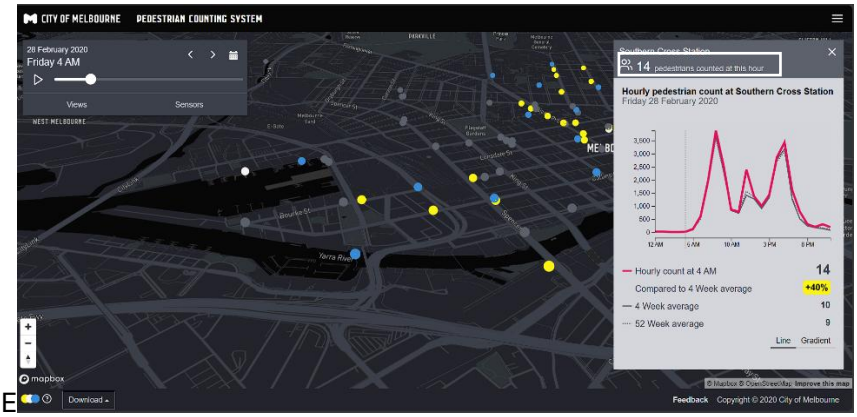
After reading the problem description carefully I first think where is this "Southern Cross Station". So, I opened an internet browser then I use google dork method and I found the station in Melbourne, Australia.



Then, I searched: how can I find the exact number of pedestrians that walked through Southern Cross Station. In the search result I learned that if I go to The City of Melbourne's Pedestrian Counting System, I can get the public records.



Then, I went to that website and I filtered the mention timeline in the website and I got the pedestrian count. Then I just put the number in the mentioned flag format.



E

Flag: CSCUU{14}

Disss

Category: OSINT

Flag format: CSCUU{.....}

Description:

Do you know about discord bot?

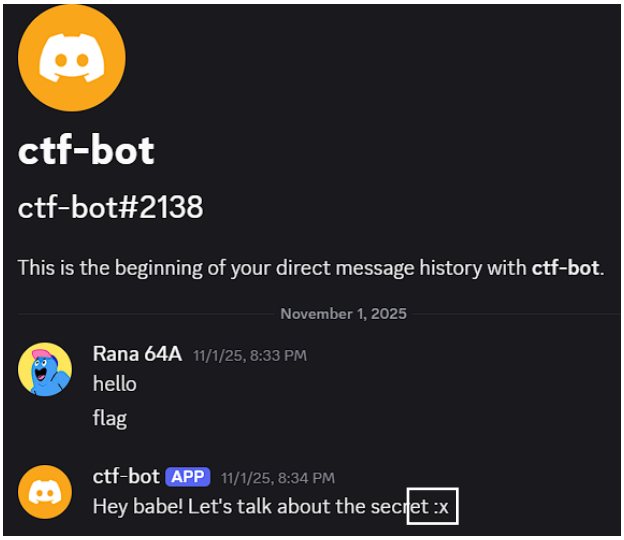
https://discord.gg/TfnSxp8S

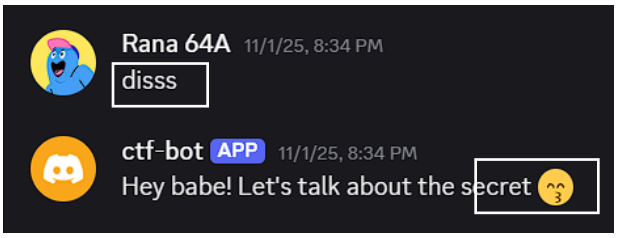
Hint:

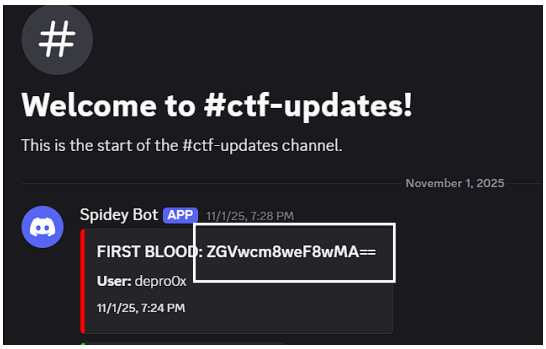
@ctf-bot isn't a fan of public chatter. Send her a private message 🐓

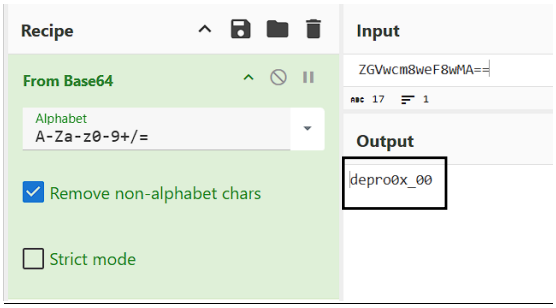
Approach:

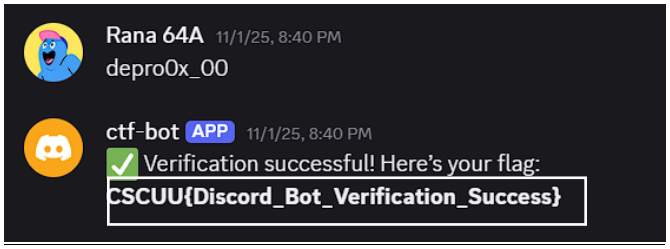
At first, I tried to solve this problem without any hint but I failed then I used hint option. At the hint it was mentioned that @ctf-bot isn't a fan of public chatter. So, I started a private conversation. First, I said Hello Flag. Then it replies me that I have to tell some secrets to the bot. Then I send some text but the wasn't the main secret then I noticed in the last part of the bot's reply there was a (X) then I thought why not try the problem name. Then I reply (disss) then the (x) turn into an emoji. Then again I reply many things but that wasn't bot's correct prompt. Then I remembered in the ctf updates room depro0x mention a encrypted text. So, I went there and I realized the data is in base64 format because of ==. So, I go to cyber chef website and decode the text and submitted the decoded text in the chatbot and I got the flag.











Flag: CSCUU{Discord_Bot_Verification_Success}

Doublehexa

Category: Cryptography

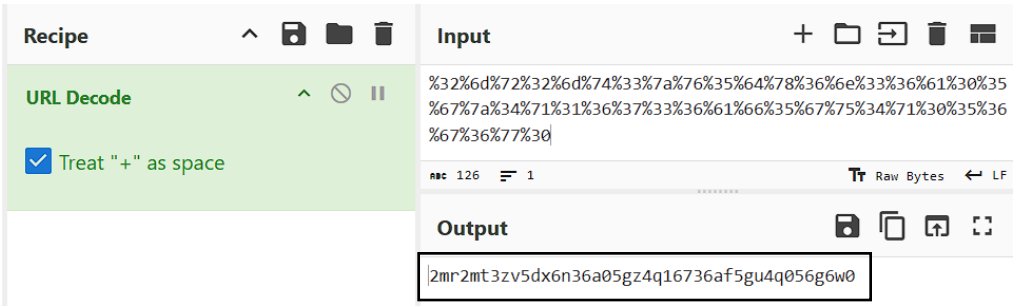
Flag Format: CSCUU{Something_here}

Description:

Cipher Text:
%32%6d%72%32%6d%74%33%7a%76%35%64%78%36%6e%33%36%61%30%35%67%7a%34%71%31%36%37%33%36%61%66%35%67%75%34%71%30%35%36%67%36%77%30

Approach:

After seeing the chipper text, I realized this text is encrypted by URL format because of %. So, I went to cyber chef website and use URL decode method and I got a decoded cipher text. But I don't know which format is in the decoded text.



After getting the decoded cipher text I went to Cipher Identifier. After a moment I see the highest probability, it could be a twin hex cipher.

Then I went to twin hex cipher decoder and put the text on that and I got the flag.

Flag: CSCUU{hey_this_is_twin_hex}