lordsudo.xyz

Irisctf osint challenge

5–7 minutes

Challenge 1:Czech Where?

Description

Iris visited this cool shop a while back, but forgot where it was! What street is it on?

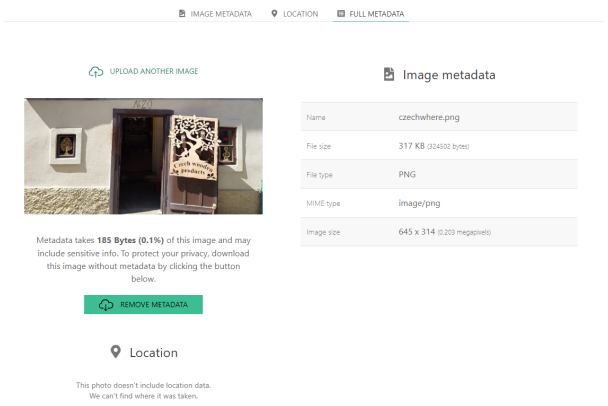
This is the image of the shop.

Hint

FYI: flag is all lowercase and _ for spaces. Please remove all accent marks if there are any. Wrap your answer in irisctf{}.

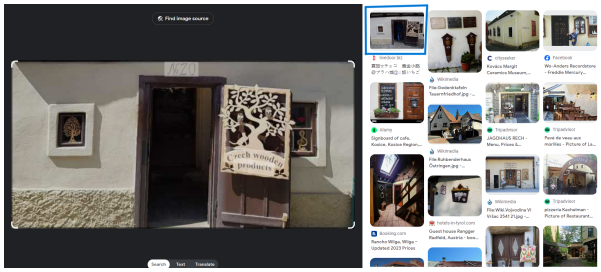
Solution

The first thing that comes to mind is to check the image metadata for any probable location information, though in most cases it is usually stripped off the image.



Just as we thought, the location data has been stripped from the image.

We can now do a reverse search with the image and we see an article with the same image. The article points to Golden Lane,Prague castle.

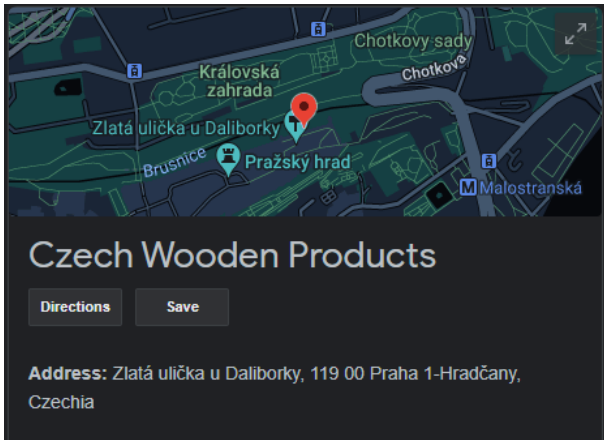


December 21, 2019 22:30 czech 2019

Summer trip ☆ Czech Golden Lane @ Prague Castle ①

Next was Koganekoji.
Traditional houses line the narrow lanes inside Prague Castle.
Most of the places are souvenir shops, and even though they are included in th e ticket, you can't enter unless you pay.
I wonder if they don't let you in for free in the sense that you can see old hous es.

A further google search with the shop name leads us right to the address.



This gives us the flag: *irisctf{zlata_ulicka_u_daliborky}*

Challenge 2: Away on Vacation

Description

Iris and her assistant are away on vacation. She left an audio message explaining how to get in touch with her assistant. See what you can learn about the assistant.

The Audio file was provided and its transcript too

Transcript

```
Hello, you've reached Iris Stein, head of the HR department! I'm currently away on vacation, please contact my assistant Michel. You can reach out to him at michelangelocorning0490@gmail.com. Have a good day and take care.
```

Solution

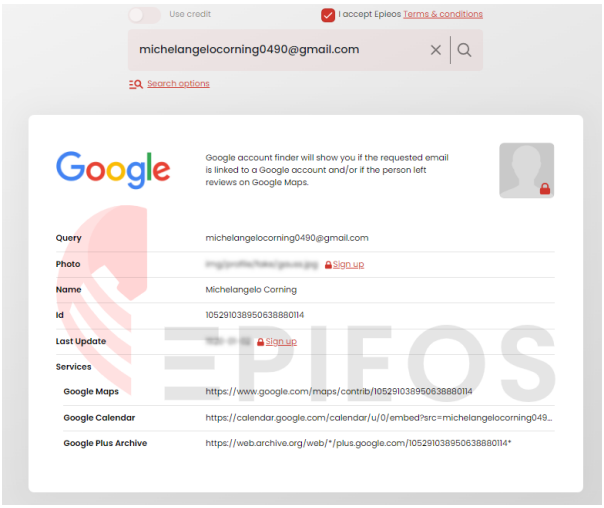
Out of Curiosity I sent an email to Michel and got the following response.

Dear,

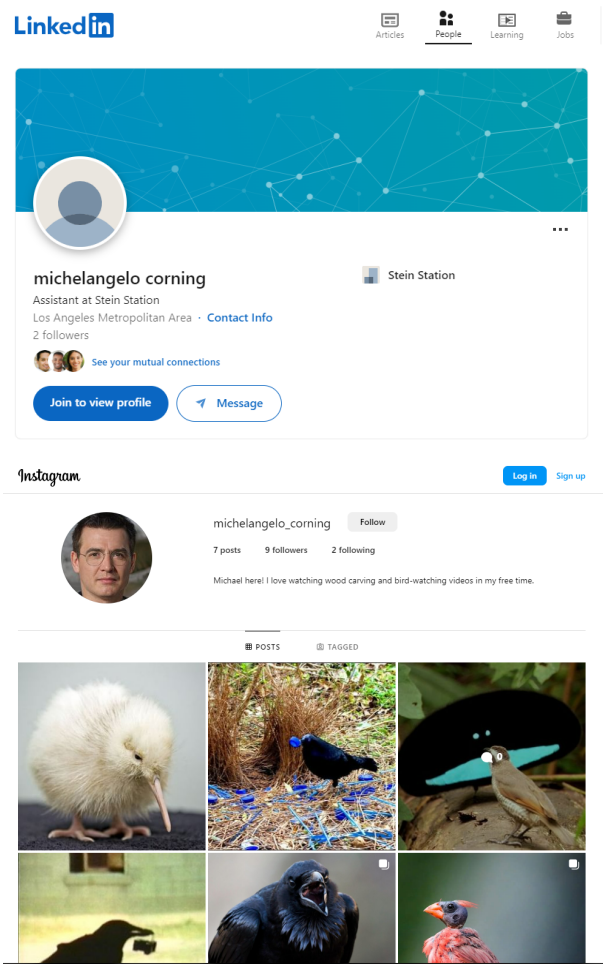
Thank you for the email. I'm currently away on vacation to celebrate New Years! If you would like a quicker response, feel free to reach out to my social media. I mostly talk about birds on it.

Have a great start to the year, and take care!

We can use `epieos.com` and find out what data we can get from there and this gives us the full name of the google account in question.



A google search with the name shows us two social media accounts i.e LinkedIn and Instagram



We can confirm that the instagram account belongs to him since its all about birds and thats what he hinted towards in his email. Scrolling through the posts we come across a very interesting one that gives us the flag.

This gives us the flag: *irisctf{pub1ic_4cc0unt5_4r3_51tt1ng_duck5}*.

Challenge 3: Personal Breach

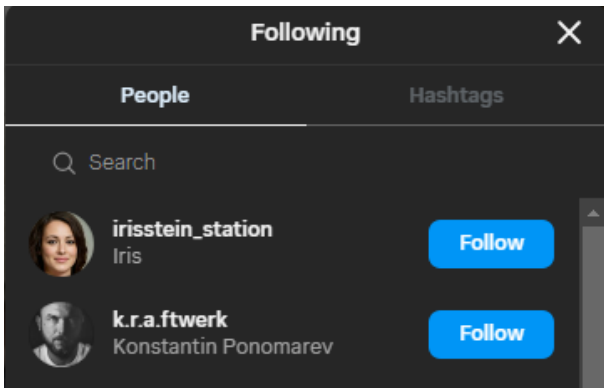
Description

Security questions can be solved by reconnaissance. The weakest link in security could be the people around you.

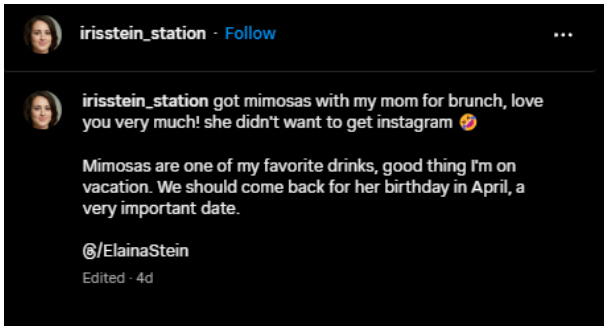
This challenge provides us with a link to a web page where we are required to provide some information.

Solution

Going back to Michel's page, we can check his following which leads us to Iris' Instagram handle.

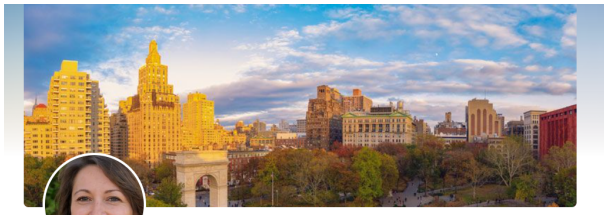


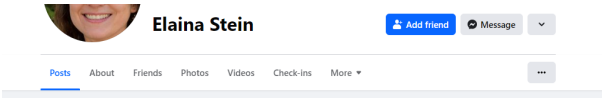
Perusing through her feed there isnt much of help apart from a single post where she mentions her mum and also tags a handle.



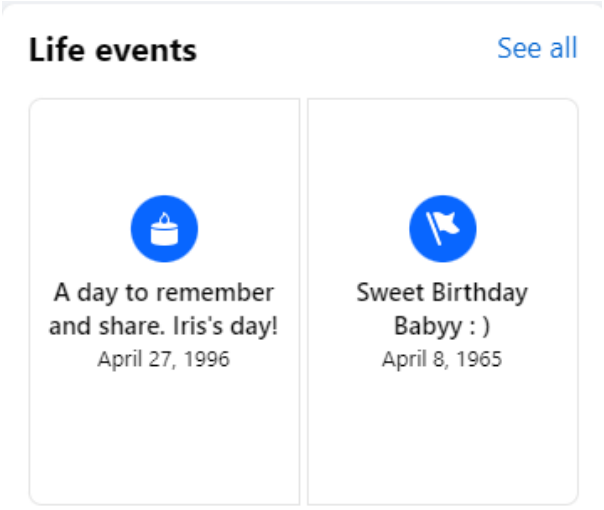
Searching for that username on Instagram bore no fruits, so i decided to shift my focus to the most obvious platform used by the "Elders" - Facebook.

Searching through facebook gave various accounts but finding the exact one was really easy.



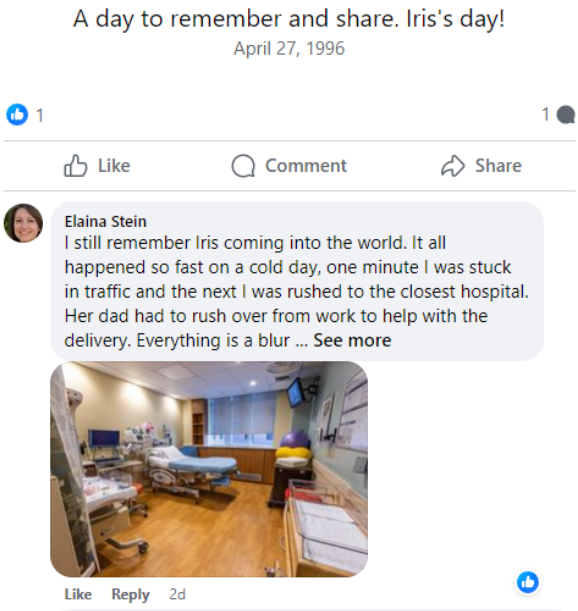


Scrolling down through her profile we hit basically a gold mine.



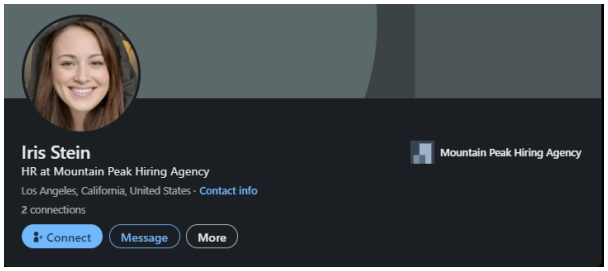
We have a hit on Iris' Birthdate which gives us her age - 27yrs

In the comments of the birthday post, we basically hit another gold mine as we can now find the hospital she was born in.



A reverse search of the image gives us the hospital or alternativley we could search by the leading statement from the mum's comment "best maternity hospital in Manhattan" This search gives us results from Yelp which leads us to the answer.

Now for the final answer, we can do a search on LinkedIn for Iris And we get a hit. Information from the previous question tells us that she works in the HR department and thus we can verify that it indeed is her profile and get her company.



Using all the details found we can now enter the answers on the web page to get our flag.

This gives us the flag: *irisctf{s0c1al_m3d1a_1s_an_1nf3cti0n}*

Challenge 4: A Harsh Reality of Passwords

Description

Recently, Iris's company had a breach. Her password's hash has been exposed. This challenge is focused on understanding Iris as a person.

Hash: $2b$04$DkQOnBXHNLw2cnsmSEdM0uyN3NHLUb9I5IIUF3akpLwoy7dlhgyEC

The flag format is irisctf{plaintextPassword}

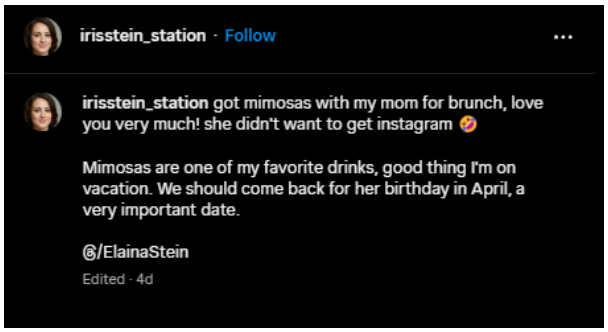
Hint

Focus on Iris and what she finds important! There are three words (not letters, but words), and a certain amount of numbers following it. There's no leet words, proper capitalization nothing like (ExAmPLE), no special characters as well like -,! etc. If you find a specific date, do not include the month'a name into your word list. Just use the numbers!!

Solution

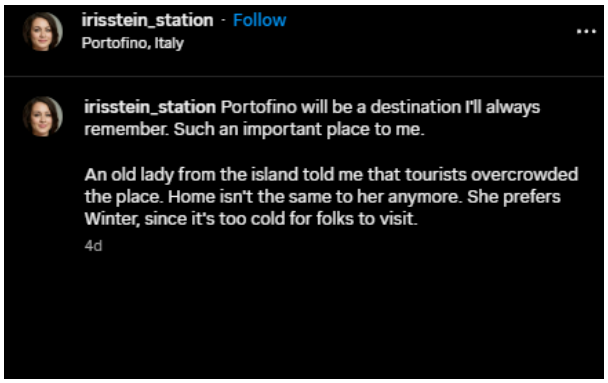
We start with a hash and need to decrypt it for which we shall require a wordlist. This needs us to gather key information to include in the wordlist.

Scouring through her Instagram, she mentioned her Mum's birthday being an important date and we can get this from the mum's facebook. This should be our numbers - as per the hint.



She also mentioned having ‘mimosas’, and we can add that too. As we keep scrolling she mentions she has an obsession with ‘Tiramisu’ and we can take note of this too.

In another post, she mentions how ‘Portofino’ will always be a destination to remember.



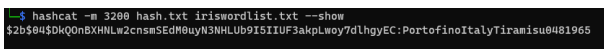
Going through all the posts and various things that may be important we can gather enough information to create a wordlist.

We can generate the wordlist using a python script

```python
from itertools import permutations

def generate_combinations(words, num_str):
    word_combinations = permutations(words, 3)
    all_word_combinations = [''.join(combo) for combo in word_combinations]

    num_combinations = permutations(num_str, len(num_str))
    all_num_combinations = [''.join(combo) for combo in num_combinations]

    combined_results = [word_combo + num_combo for word_combo in all_word_combinations for num_combo in all_num_combinations]

    return combined_results

def write_to_file(results, filename):
    with open(filename, 'w') as file:
        for result in results:
            file.write(result + '\n')

def main():
    words = ["Iris", "Stein", "Elaine", "Tiramisu", "Portofino", "Mimosas", "Italy"]
    date_numbers = "8041965"

    all_combinations = generate_combinations(words, date_numbers)

    write_to_file(all_combinations, 'iriswordlist.txt')

if __name__ == "__main__":
    main()
```

We now have a wordlist file that we can run against the hash. The hash is input in a text file and run against hashcat

```
hashcat -m 3200 hash.txt iriswordlist.txt
```



```
└─$ hashcat -m 3200 hash.txt iriswordlist.txt --show
$2b$04$DkQOnBXHNLw2cnsmSEdM0uyN3NHLUb9I5IIUF3akpLwoy7dlhgyEC:PortofinoItalyTiramisu0481965
```

This gives us the matching password PortofinoItalyTiramisu0481965

The flag: irisctf{PortofinoItalyTiramisu0481965}

Nos vemos en mi próximo artículo…