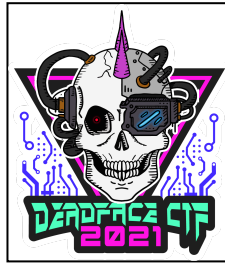


DEADFACE CTF (15/10/2021)



Write up made by @informaticapau.

Starter

Hello there! We're so glad you're able to help us thwart DEADFACE this year. Let's get you spun up on where to get started.

We found out DEADFACE is likely targeting a company called De Monne Financial. They've targeted them in the past and based on some OSINT research, we're sure they're targeting De Monne again this year.

One of our partners found a forum page where DEADFACE discusses their activity. We managed to gain access to the forum and opened it up to be viewed publicly, but you won't be able to create an account. The forum site is called [Ghost Town](#). There's a lot of information on this forum that might help you.

Thanks for participating in this year's DEADFACE CTF! Before you begin, please take a look at our [rules](#) and submit the flag found on that page. Submitting the flag is an acknowledgement of the rules and your compliance. Thank you and enjoy the CTF!

I found the flag reading the rules section:

Rules

To ensure that all players have a safe and fun experience during this event, certain rules must be followed. Please follow the rules listed below. If you have any questions, please contact the staff in Discord or email us at info@cyberhacktics.com

- Players **MUST NOT** attempt to hack or manipulate off-limits devices and resources. The following are considered off-limits and **may not** be attacked or exploited:
 - The scoring server (ctf.deadface.io)
 - Other players
- Players **MUST NOT**:
 - manipulate or modify flags.
 - perform any denial of service (DoS) on any portion of the environment.
 - attack other players.
 - compete on more than one team.
 - share flags with another team.
 - share an account with another player.
- Players **MUST** be respectful, courteous, professional, and display proper sportsmanship.

An **attack** is considered any activity which renders resources unavailable or disrupts other players' ability to advance in the competition.

These rules exist to ensure a fair and enjoyable competition for all of our players. Players will receive a warning on their first infraction. Recurring infractions will result in the team's disqualification. Mods can ban players from Discord at their discretion. If you have questions or concerns, you can contact us at info@cyberhacktics.com

Awards Eligibility

If you are a US-based team competing for one of the cash prizes, you **MUST** indicate your country as US on your profile. If you do not identify as a US-based team on your profile, we **WILL NOT** be able to guarantee that you'll be awarded a cash prize for 1st, 2nd, or 3rd place.

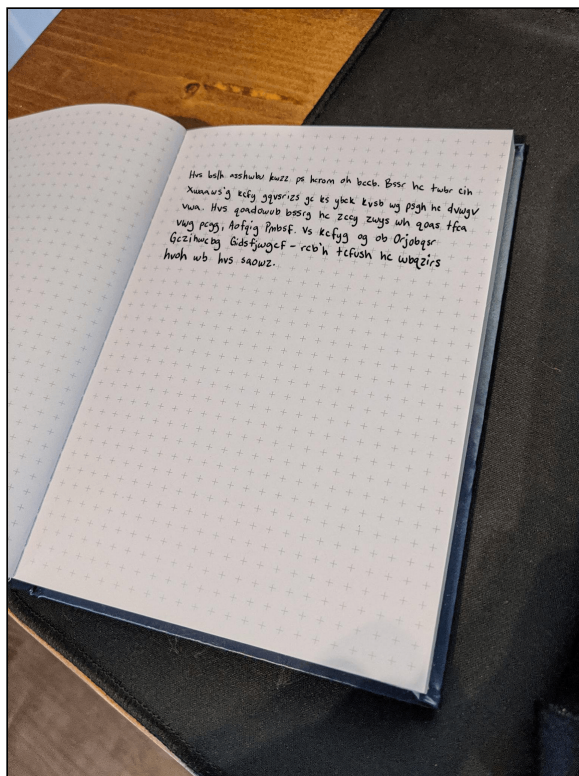
[View the rules](#)

```
flag{themz_the_ru1es}
```

Cryptography

Big boss

An anonymous tipster sent us this photo alleging that it's a note written by **b3li3f1203**. The tipster claims that the note was intended for someone who works at De Monne Financial. They also said it's likely that it has something to do with a phishing campaign. Provide the name of the target individual as the flag in this format: `flag{FirstName_LastName}`.



The image contains the following text:

Hvs bslh asshwbu kwzz ps hcrom oh bccb. Bss hc twbr cih xwaaws'g kcfy gqvsrizz gc ks ybck kvsh wg psgn hc dhwgv vwa. Hvs qoadowub bssrg hc zccy zwys wh qoas tfca vwg pcgg, Aofqig Pmbfsf. vs kcfyg og ob orjobqsr Gczihwcbg GidsfjwgcF-rcb'h tcfush hc wbqzirs hvoh wb hvs saowz.

Using a [cipher identifier](#) we can find out that the text is using Caesar Cipher. Knowing this we can easily find out that the key is 14 and get the plain text:

The next meeting will be today at noon. Nee to find ouz jimmie's work schedule so we know whet is best to phish him. The campaign needs to look like it came from his boss, Marcus Byner. he works as an Advanced Solutions Supervisor-don't forget to include that in the email.

Flag:

`flag{Marcus_Byner}`

Poor MEGAN!

Oh, NO! Poor Megan! She's just been bitten by a ZOMBIE! We can save her if we act fast, but the formula for the antidote has been scrambled somehow. Figure out how to unscramble the formula to save Megan from certain zombification. Enter the answer as `flag{here-is-the-answer}`.

The formula for the antidote: `j2rXjx9dkhw9eLKsnMR9cLDVjh/9dwz1QfGXm+b9=wKs1L1zpb45`.

To solve this challenge we have to decode the string from base64 using the Megan35 alphabet. The online tool [Cyberchef](#) detects this type of encoding and gives us the flag:

```
flag{Six-Parts-Honey-One-Part-Garlic}
```

To Be Xor Not to Be

`.$)/3<'e-)<e':e&'<e<'e-)<5`

Since the title suggests that the text is encrypted using XOR, I looked for an [online tool](#) to decrypt it by brute force since the key is unknown.

Flag:

```
flag{to-eat-or-not-to-eat}
```

Forensics

Blood Bash

We've obtained access to a system maintained by `bl0ody_mary`. There are five flag files that we need you to read and submit. Submit the contents of `flag1.txt`.

Username: `bl0ody_mary`

Password: `d34df4c3`

`bloodbash.deadface.io:22`

After connecting with the machine via SSH I found the file using the `find` command:

```
bl0ody_mary@663a12f28f95:~$ find / -type f -name "flag1.txt" 2>/dev/null
/home/bl0ody_mary/Documents/flag1.txt
```

Then I read it with the `cat` command:

```
bl0ody_mary@663a12f28f95:~$ cat /home/bl0ody_mary/Documents/flag1.txt
flag{cd134eb8fbd794d4065dcd7cfa7efa6f3ff111fe}
```

OSINT

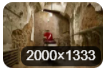
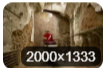
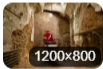
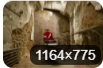
Meetup

A member of DEADFACE suggested that they all meet up at some point. With this information, we'd be able to contact law enforcement to get them all at once! What does the picture say about their meetup location, though?

Submit the flag as: `flag{location}`.



I checked the image's metadata with `exiftool` but I didn't find anything interesting. After that I searched it on [Yandex](#) and the results gave the location I was looking for:

Sites containing information about the image	
 2000x1333	J GOES PLACES: Eastern State Penitentiary in Philadelphia, 05/27/17 NEPA Scene nepascene.com Philadelphia, PA.
 2000x1333	Eastern Penn State Related Keywords & Suggestions - Eastern Penn State Long Tail Keywords keywordbasket.com
 1200x800	#тюрьма - Twitter Search twitter.com
 1164x775	Underrated Ghost Stories And Mythical Creatures All Over The World: Ninth Stop - Pennsylvania Underrated Ghost Stories And Mythi werewoofs.com A photo showing the Mad Chair.

Flag:

```
flag{Eastern State Penitentiary}
```

Programming

Unfinished

There seems to be something wrong with this code. Can you figure out how to make it return the flag? Modify the code to show the flag. Submit the flag as: `flag{flag-goes-here}`.

```
#!/usr/bin/env python3
from binascii import unhexlify as u

def get_flag():
    flag = '666c61677b30682d6c6f6f6b2d612d466c61477d'
    return u(flag).decode('utf-8')

print(f'The flag is: ')
```

To finish the code we have to call the `get_flag` function after the string in the `print` function:

```
#!/usr/bin/env python3
from binascii import unhexlify as u

def get_flag():
    flag = '666c61677b30682d6c6f6f6b2d612d466c61477d'
    return u(flag).decode('utf-8')

print(f'The flag is: {get_flag()}')
```

After we run the code we get the following output:

```
The flag is: flag{0h-look-a-FLAG}
```

SQL

Body Count

One of our employees, Jimmie Castora, kept database backups on his computer. DEADFACE compromised his computer and leaked a portion of the database. Can you figure out how many customers are in the database? We want to get ahead of this and inform our customers of the breach.

Submit the flag as `flag{#}`. For example, `flag{12345}`.

We are given a file named `demonne.sql`. We can create the database using it and some SQL server. In my case I used MySQL.

```
mysql -u <user> -p <password> < demonne.sql
```

After I created the database I checked its tables:

```
show tables;
```

Among the results, the `customers` table appeared and I used the following query to get the number of customers:

```
SELECT COUNT(*) FROM customers;
```

Output:

```
+-----+
| count(*) |
+-----+
| 10000 |
+-----+
```

Flag:

```
flag{10000}
```

Steganography

Send in the Clowns

There is a secret hidden somewhere in this image. Can you find it? Submit the flag as `flag{this-is-the-flag}`.



To solve this challenge we had to check the image's metadata. I used exiftool for this and found a field "Comment" with the flag:

```
flag{s3nd_in_the_k10wns}
```

VoicE

A friend of mine sent me an audio file which supposes to tell me the time of our night out meeting, but I can't comprehend the voice in the audio file. Can you help me figure it out? I want to hang out with my friends.

We are given a WAV file. To find the flag I used a [Spectrum Analyzer](#).



Flag:

```
flag{1257}
```

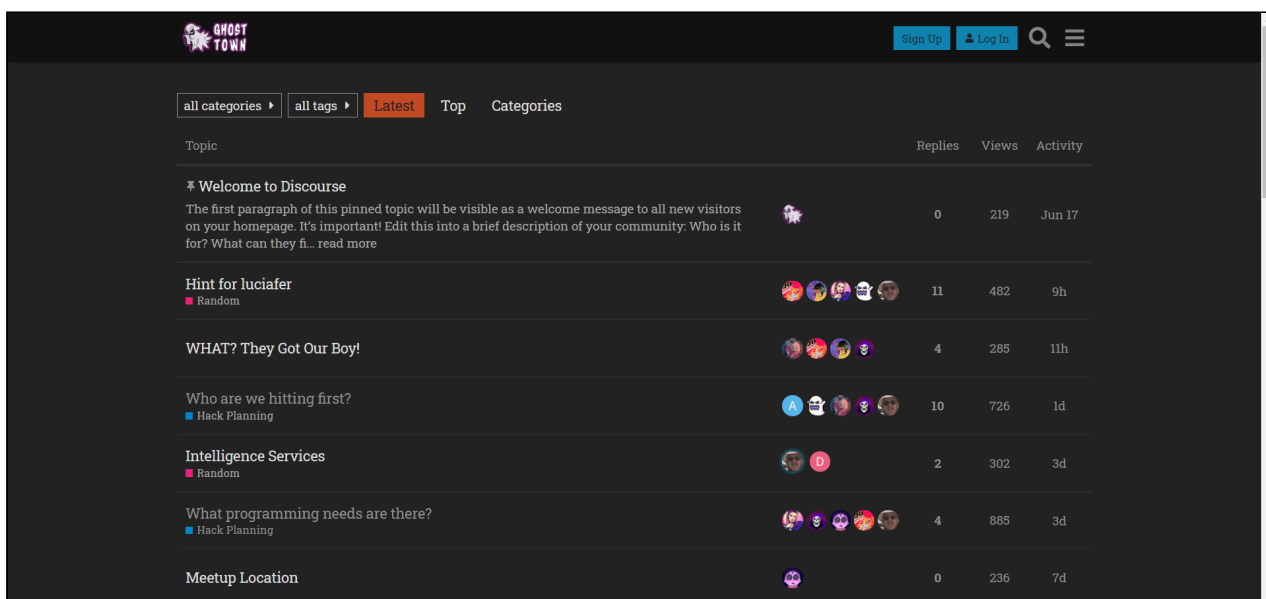
Bonus

Jailbird

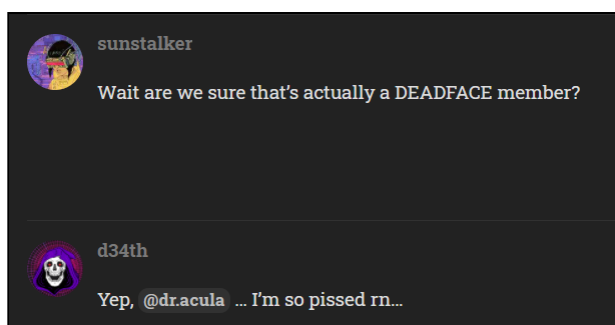
It looks like authorities arrested a member of DEADFACE. But who was it?

Submit the member's username as the flag: `flag{username}`

For this challenge I had to go to DEADFACE's website Ghost Town:



There was a thread named "WHAT? They Got Our Boy!". Reading it I found the flag.



Flag:

```
flag{dr.acula}
```