Mason Competitive Cyber

Introduction to CTF’s

Proud Sponsors

CACI

EVER VIGILANT

VOLGENAU SCHOOL

MASON

ENGINEERING

WarCollar

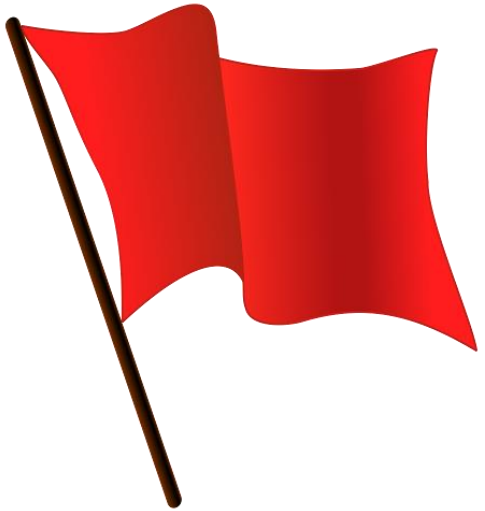
industries

Capture the Flag Competitions

- Usually online
- Jeopardy style
  - Questions worth varying amounts of points
  - Complete tasks to find the answer, called the “flag”
    - Web exploitation
    - Forensics
    - Cryptography
    - Reverse engineering

- Attack/Defense style
  - Option 1: server that everyone tries to control
  - Option 2: protect your own machine, capture other people’s machines

What is this Flag thing?

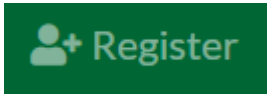


- Normally the solution to the challenge
- Has a specific format unique to the CTF
  - Commonly in the form ctfname{The Flag}
  - For the MasonCC training CTF, format is masoncc{Flag}

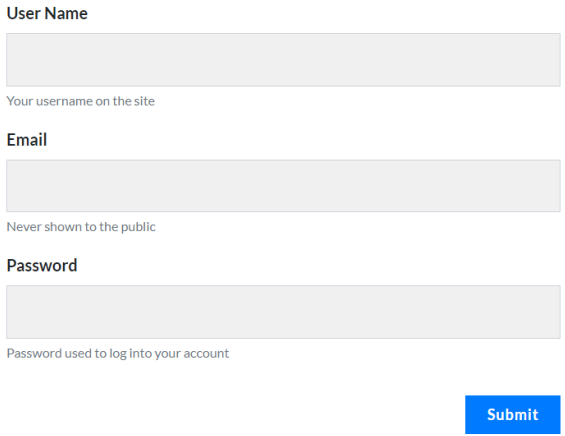
- Sometimes the flag is already formatted, sometimes it's not
  - You may find a flag in the form flag{}
  - Other times flag will need to be put into the flag format

- Example: "What year was the Statue of Liberty Built?"
  - Put you answer in the form masoncc{}
  - In this case, the flag will be the year it was built.
  - masoncc{1875}

Joining Your First CTF



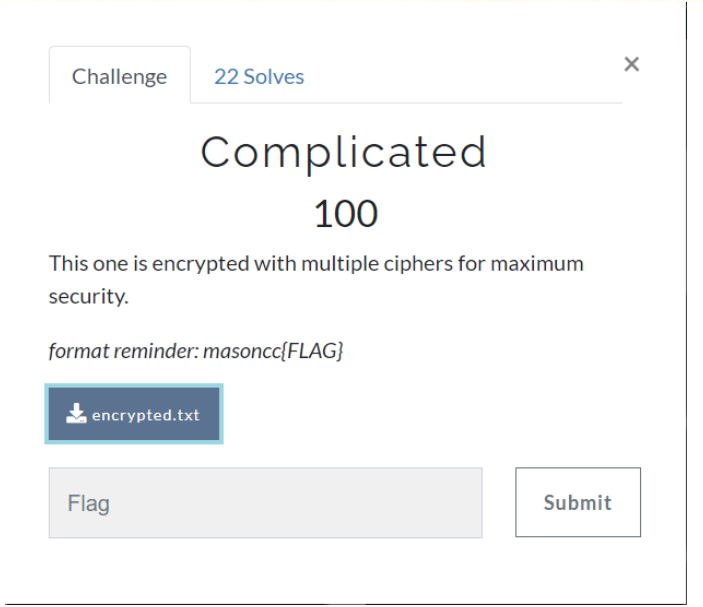
- For Today, we will be joining the MasonCC Training CTF, TCTF
- To get started, go to https://tctf.competitivecyber.club/ and click on register
  - Choose a Username, password, and Use your @gmu.edu email
  - Choose Wisely, everyone will see it

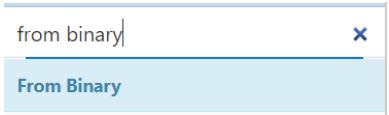


- After Registering, click challenges
  - Wow, that's a lot of challenges
  - Almost all of them were written by MasonCC Members
  - Contacting the author may help if your stuck

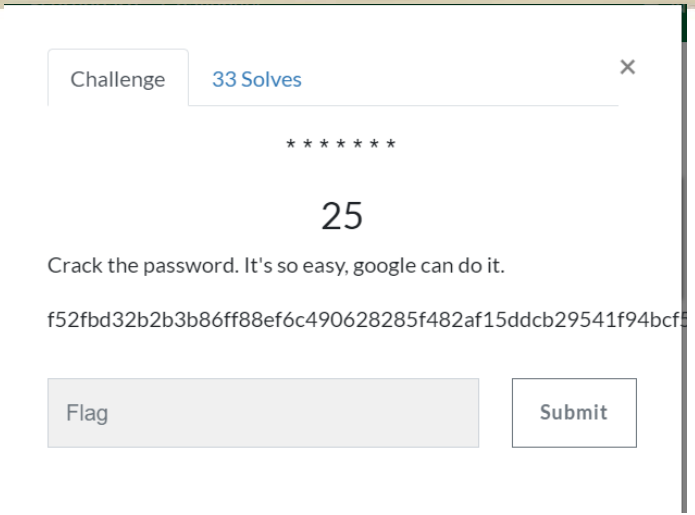
Let's Solve a Challenge

- The name of the challenge is "Complicated", remember this.
  - Many times, the title and description give you hints
- Let's download the attached file and see what we get.
- File Contents appear to be Binary
- Let's try using a tool called [CyberChef]
- Drag the "From Binary" operation into the recipe
- Output doesn't look like plain text, does it? Read the challenge description again.
- Try adding another operation to finish the challenge.





Let’s Solve Another One



- This challenge is a cracking challenge.
- Goal is to crack the provided hash
- First step, identify hash type
  - Online Sites
  - Hash ID in Kali
- Ok, now we know the hash type, let’s crack it.
- Again, we can use an online site, or a dedicated tool.
- In the spirit of the challenge description, let’s use an online tool called Crack Station.
- Crack Station can crack very common hashes but tends to fail on custom ones.

- bb7d2e9629ef27214756d0d03db455f2ef73a3e59684b385bd64e28424b45e04

Land Before Time

- This image contains Steganographic data.
- Steganography is the technique of hiding data in files.
- Some nice tools to have:
  - Foremost (detects file headers to extract files)
  - Zsteg (Runs an automated set of scripts)
  - strings (looks for strings in the input file)

The Image with hidden data

- Let’s try running the jpg through some tools
- First place to start is strings
- From there, let’s run zsteg to do a “deeper” analysis

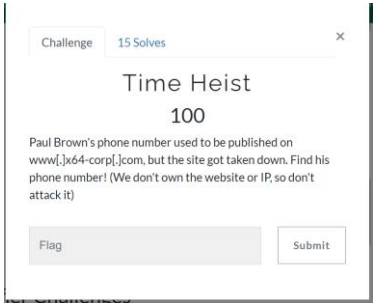
OSINT Challenges

- OSINT (Open-Source Intelligence) is a category that tasks you with finding information using open-source channels (Social media, google, public records, etc.)
- Some useful tools:
    - Plain old Google, use modifiers (Search Google Dorking for more)
    - Whois lookups are a great tool for finding domain registration info
    - Recon-ng is an all-in-one web recon platform built in Python that supports modules for drop in functions.
    - Trying to find a site that no longer exists? Try using the Way Back Machine.
    - For a detailed list, check out this great list on GitHub https://github.com/jivoi/awesome-osint

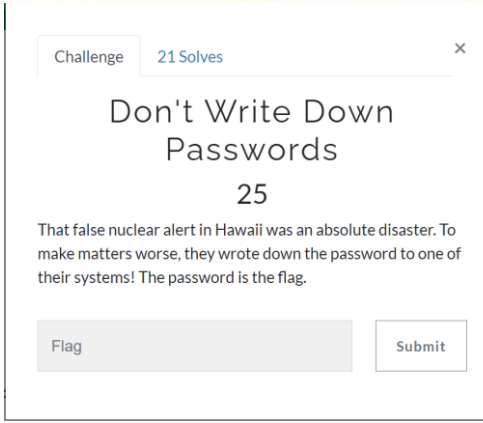
Audience Participation Time

On your own, (or with a friend), try and see if you can solve “Don't Write Down Passwords” and “Time Heist” on TCTF under the Recon section.

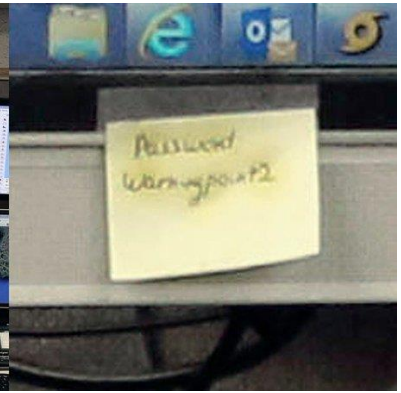
- In a couple of minutes, we will solve it as a group.
- Remember, Google is your friend. From the previous slide:
  - Whois lookups are a great tool for finding domain registration info
  - Trying to find a site that no longer exists? Try using the Way Back Machine.
  - For a detailed list, check out this great list on GitHub https://github.com/jivoi/awesome-osint



Don’t Write Down Passwords

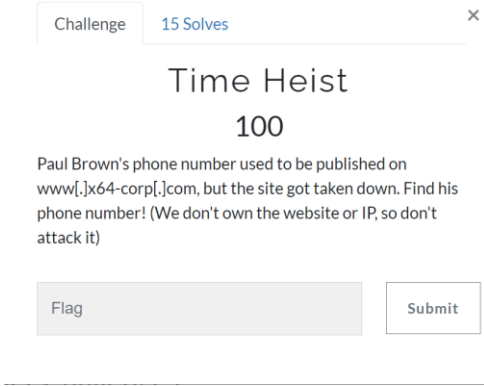


- First things first, lets just search for this on google and see what we get
- Searching yields this image
- Zooming in, we can se it says “warningpoint2” on the sticky note.
- If you weren’t 100% sure, or just couldn’t be bothered to try and decipher the chicken scratching. Further searching shows multiple articles that have it typed out.



- Score! An easy 25 points.
- Make sure to put it in the format masoncc{Flag}

Time Heist



- This challenge asks us to find a phone number on a now dead site.
- Remember back 2 slides to the tools, which tool can do this?
- Way back machine allows us to look at archived versions of a site.

- Putting it into wayback machine, we are given several archive dates, Let's just choose the oldest.
- And like that, we have the phone number!

- Again, make sure to format it in the masoncc{} format.

Where to Find CTFs?

- Watch out in the #ctf-watch slack channel for announcements for CTFs
- There are a few long running CTFs that are good practice.
  - PicoCTF is a good beginner oriented CTF
  - Our very own TCTF
  - MicroCorruption-Embedded Security Challenges
  - Ctf101.com