Visit <https://ctfs.github.io/resources/> or read the following paragraphs to learn the knowledge about CTF.

**CTF Resources**

This repository aims to be an archive of information, tools, and references regarding CTF competitions.

CTFs, especially for beginners, can be very daunting and almost impossible to approach. With some general overviews of common CTF subjects and more in-depth research and explanation in specific topics both beginners and veterans can learn, contribute, and collaborate to expand their knowledge.

**What is a CTF?**

CTFs are computer security/hacking competitions which generally consist of participants breaking, investigating, reverse engineering and doing anything they can to reach the end goal, a "flag" which is usually found as a string of text.

DEF CON hosts what is the most widely known and first major CTF, occuring annualy at the hacking conference in Las Vegas. Many different competitions have branched off since then, and numerous ones are available year round. One of the best places to see when CTFs are being scheduled is ctftime, an active website with calendars and team rankings.

**Example**

A very simple type of CTF challenge consists of looking at the source code of websites or programs to find flags and/or hints. For example, can you find the flag hidden on this page?

**Using These Docs**

These docs are organized broadly along the lines by which CTF tasks are organized. Inside each folder in the topics section is a README like this one explaining the basics of the technology and what the tasks generally involve. Alongside these READMES are folders with more information regarding specific technologies and topics. Many of these articles link to the tools folder, where more detailed explanations can be found for tehcnologies used throughout CTF competitions.

The best way to use these docs is to participate in an actual CTF! Join a CTF or attempt some old tasks and try to solve them. Use the information in this repository to get you started with finding some flags. If you feel like there is insufficient information to help you solve a task, bring up an issue on this repository and someone can try to clarify it.

**Moving On**

You may be able to solve some CTF challenges after looking through the documents in this repository and understanding the basics of the technologies and subjects covered, but you won't be very proficient or successful for long. To be an adept CTF competitor you have to be able to combine many different strategies and tools to find the flag. Developing the ability to find flags quickly takes practice more than anything, and participating in numerous CTFs will allow you to expand your understanding and abilities, leading you to success.

**Conclusion**

Now that you know the basics of CTFs, you can visit ctftime and try out a CTF! Using your background knowledge and the information on this page you'll be able to develop a solid basis in computer security.

**Cryptography**

Cryptography is the practice and study of techniques for secure communication in the presence of third parties. - Wikipedia

In the case of CTFs, the goal is usually to crack or clone cryptographic objects or algorithms to reach the flag.

**Example**

If you look around the folders in this page you should be able to find a suitable way to solve this simple cipher:

Hint: Julius Caesar's favorite cipher

kxn iye lbedec

**Steganography**

Steganography is the art or practice of concealing a message, image, or file within another message, image, or file. - Wikipedia

In the context of CTFs steganography usually involves finding the hints or flags that have been hidden with steganography. Most commonly a media file will be given as a task with no further instructions, and the participants have to be able to uncover the message that has been encoded in the media.

**Example**

Images are a very common medium for steganography, as they are easy to manipulate and simple to view and transport. Files in Images give a good introduction for beginner steganography.

**Getting Started**

A rudimentary knowledge of media filetypes (e.g. jpg, bmp, png for pictures and wav, mp3 for sound) is essential to steganography, as understanding in what ways files can be hidden and obscured is crucial. Also, understanding basic linux is important, as a multitude of tools are specifically for bash.

**Web**

Web challenges in CTF competitions usually involve the use of HTTP (or similar protocols) and technologies involved in information transfer and display over the internet like PHP, CMS's (e.g. Django), SQL, Javascript, and more. There are many tools used to access and interact with the web tasks, and choosing the right one is a major facet of the challenges. Although web browsers are the most common and well known way of interacting with the internet, tools like curl and nc allow for extra options and parameters to be passed and utilized.

**Getting Started**

Command Line and the Web

If you are running linux and want extended functionality (like passing custom headers) in web challenges, bash (terminal) commands are your best bet. cURL is a simple but extensible command-line tool for transferring data using various protocols, and allows users to use HTTP to interact with servers, including POST and GET methods.

**Example**

To see curl at work, you can simply run curl 8.8.8.8 (Google), and the html of Google's home page should appear.

There are many other options and flags that can be passed to curl, making it an extremely useful tool in CTFs.

**Miscellaneous**

Many challenges in CTFs will be completely random and unprecedented, requiring simply logic, knowledge, and patience to be solved. There is no sure-fire way to prepare for these, but as you complete more CTFs you will be able to recognize and hopefully have more clues on how to solve them.

**Examples**

In recent CTFs the sheer variety of miscellaneous tasks has been highly exemplified, for example:

In the Sochi Olympic CTF 2014, there was a low-point miscellaneous challenge which only provided a jumbled string of words. Instead of being a typical crypto challenge, the answer required competitors to draw out the word SOCHI on their keyboards.

RuCTF had a challenge which presented a single picture of shredded strips of paper jumpled up in a random order. The best way of solving this was by hand! No computer knowledge was even needed for its completion, only patience and a good eye.