

CTF for Beginners

What is CTF and how to get started!

#security #ctf #beginners



atan

Mar 28, 2019 Updated on May 07, 2020 • 3 min read

CTFs are one of my favorite hobbies. I love the feeling of solving a particularly difficult task and seeing all the puzzle pieces click together. I'd like this post to serve as an introduction to CTF for those in the dev.to community that may not know what it is.

So what is CTF?

CTF (Capture The Flag) is a kind of information security competition that challenges contestants to solve a variety of tasks ranging from a scavenger hunt on wikipedia to basic programming exercises, to hacking your way into a server to steal data. In these challenges, the contestant is usually asked to find a specific piece of text that may be hidden on the server or behind a webpage. This goal is called the flag, hence the name!

Like many competitions, the skill level for CTFs varies between the events. Some are targeted towards professionals with experience operating on cyber security teams. These typically offer a large cash reward and can be held at a specific physical location. Other events target the high school and college student range, sometimes offering monetary support for education to those that place highly in the competition!

[CTFtime](#) details the different types of CTF. To summarize, Jeopardy style CTFs provide a list of challenges and award points to individuals or teams that complete the challenges, groups with the most points wins. Attack/Defense style CTFs focus on either attacking an opponent's servers or defending one's own. These CTFs are typically aimed at those with more experience and are conducted at a specific physical location.

CTFs can be played as an individual or in teams so feel free to get your friends onboard!

I'd like to stress that CTFs are available to everyone. Many challenges do not require programming knowledge and are simply a matter of problem solving and creative thinking.

Challenge types

Jeopardy style CTFs challenges are typically divided into categories. I'll try to briefly cover the common ones.

- Cryptography - Typically involves decrypting or encrypting a piece of data
- Steganography - Tasked with finding information hidden in files or images

- Binary - Reverse engineering or exploiting a binary file
- Web - Exploiting web pages to find the flag
- Pwn - Exploiting a server to find the flag

Where do I start?

If I managed to pique your curiosity, I've compiled a list of resources that helped me get started learning. CTF veterans, feel free to add your own resources in the comments below!

Learning

- <http://ctfs.github.io/resources/> - Introduction to common CTF techniques such as cryptography, steganography, web exploits (Incomplete)
- <https://trailofbits.github.io/ctf/forensics/> - Tips and tricks relating to typical CTF challenges/scenarios
- <https://ctftime.org/writeups> - Explanations of solutions to past CTF challenges

Resources

- <https://ctftime.org> - CTF event tracker
- <https://github.com/apsdehal/awesome-ctf> - Comprehensive list of tools and further reading

Tools (That I use often)

- [binwalk](#) - Analyze and extract files
- [burp suite](#) - Feature packed web penetration testing framework
- [stegsolve](#) - Pass various filters over images to look for hidden text
- [GDB](#) - Binary debugger
- The command line :)

Practice

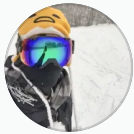
Many of the "official" CTFs hosted by universities and companies are time-limited competitions. There are many CTFs however that are online 24/7 that can be used as practice and learning tools. Here are some that I found to be friendly for beginners.

- <https://ctflearn.com> - A collection of various user-submitted challenges aimed towards newcomers
- <https://overthewire.org/wargames/> - A series of progressively more difficult pwn-style challenges. (Start with the bandit series)
- <https://2018game.picoctf.com/> - Yearly time-limited CTF now available to use as practice

Conclusion

CTF is a great hobby for those interested in problem-solving and/or cyber security. The community is always welcoming and it can be a lot of fun tackling challenges with friends. This is my first post, if I was able to spark interest with even a single person, I'd consider it a success 😊. Thank you for reading!

Posted on Mar 28 '19 by:



atan

@atan

Application Security Engineer based in Japan. Penetration Testing and general hackery fun.

Follow



Discussion

Subscribe

Add to the discussion

Boris Quiroz 

May 2 ...

Hello! Just to mention that seems to be a typo in `https://cftime.org` - CTF event tracker.
(Missing t between c and f?) :)



2

REPLY

atan 

Author

May 7 ...

Sheesh that typo has been there for way too long! Thanks for checking out this ancient post!



3

REPLY

ASM   

Jul 13 ...

thank so much 😊



1

REPLY





Ochirgarid Chinzorig

Sep 9 '19

Thank you, The sources are wonderful, I think adding some video tutorials to the list like "LiveOverflow" channel on Youtube



REPLY



saktipong

Dec 23 '19

Thank so much.



REPLY



Saad Takieddine

Dec 15 '19

Thanks !



REPLY



Musab

May 28

Thank you this cleared up many things



[REPLY](#)

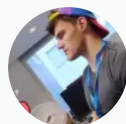
[code of conduct](#) - [report abuse](#)

Read Next



Keep a Brag Document

Shikhar Sachdev - Jun 29



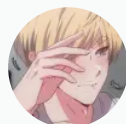
Programming is easy!

Rus Kuzmin - Jun 28



CSS Best Practices and Advice for beginners

JoelBonetR - Jun 28



15 ANGULAR PROJECT IDEAS: BEGINNER TO EXPERT [WITH FREE TUTORIAL]

Muhammad Ali (Nerdjfb) - Jun 30

More from atan

Solving a CTF challenge

[#security](#) [#beginners](#) [#ctf](#)

DEV

A constructive and inclusive social network. Open source and radically transparent.



DEV Community copyright 2016 - 2020

Built on [Forem](#) — the [open source](#) software that powers [DEV](#) and other inclusive communities.

Made with love and [Ruby on Rails](#).

[Home](#)

[Listings](#)

[Podcasts](#)

[Videos](#)

[Tags](#)

[Sign In/Up](#)

[Code of Conduct](#)

[FAQ](#)

[About](#)

[Privacy policy](#)

[Terms of use](#)

[Contact](#)

[Sponsors](#)

[DEV Shop](#)