Let's Play a CTF, Part 1

David Zero
zero-one@zer0-one.net

January 29, 2018

Table of Contents

Presentation Overview

This presentation series is meant to introduce you to the wonderful world of security CTFs. The gist of this series is that it's:

- Targeted at beginners
- Meant to introduce you to common challenge types
- Meant to introduce you to common solution techniques

Where there's some bigger lesson to be had from these challenges with regard to practical security, we'll talk a bit about it.

If you have pertinent questions, interrupt me. I like things loosey-goosey.

CTF Overview

CTF \see-tee-eff \\
A competition in which infosec (un)professionals get to exercise their talents for fun and profit. The basic premise is that a competitor is tasked with finding "flags", which are worth points. The competitor with the most points at the end of the competition wins.

Sometimes it's a team game, and sometimes you're required to go solo.

- *Sometimes* a cash prize is up for grabs.
- *Sometimes* there's a lucrative career up for grabs.
- There are *always* bragging rights up for grabs.

Flags

A "flag" in this context usually refers to a specially-formatted and/or specially placed text token which serves as proof-of-completion of a particular challenge/task. They can be a plaintext token like this:

ZeroCTF{THi5_i5_A_fLaG}

or maybe a hash token like this:

ab0bfd73daaec7912dcdca1ba0ba3d05

or maybe even something like this:

(͡° ͜ʖ ͡°)

ZeroCTF{swigg1ty_sw00ty}

Note: Flags can't always be formatted according to a given CTF's own standards. Some challenges just make it technically impossible for one reason or another. In these cases, a CTF will usually expect you to properly format the flag yourself.

For example, if you find: **THi5_i5_A_fLaG**

you may need to wrap it with **ZeroCTF**{} manually before submitting it.

CTF Types

There are two common types of CTF:

- Jeopardy
- Attack-Defend

Attack/Defend-Style CTF

In attack/defend CTFs, competitors are given a network running some identical set of services (mail, ftp, etc.). As they find vulnerabilities in their services, they can patch those vulnerabilities, and exploit them in networks belonging to other competitors.

The exploit will give the player some level of elevated access, and they'll use that access to hunt for a flag, which may be present in a file on disk, in process memory, or in any number of other locations.

This type of CTF is uncommon because of how much effort it takes to run one. Notable examples include:

- **Defcon CTF**

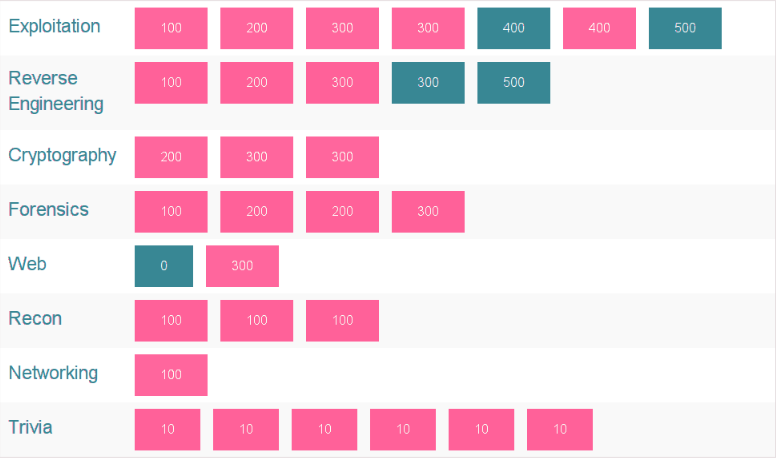
Jeopardy-Style CTF

In a jeopardy style CTF, competitors are presented with a Jeopardy board populated with infosec-related categories like:

- Cryptography
- Reverse-engineering
- Forensics
- Pwnable (i.e remote exploitation)
- Programming
- Web (everyone's favorite)

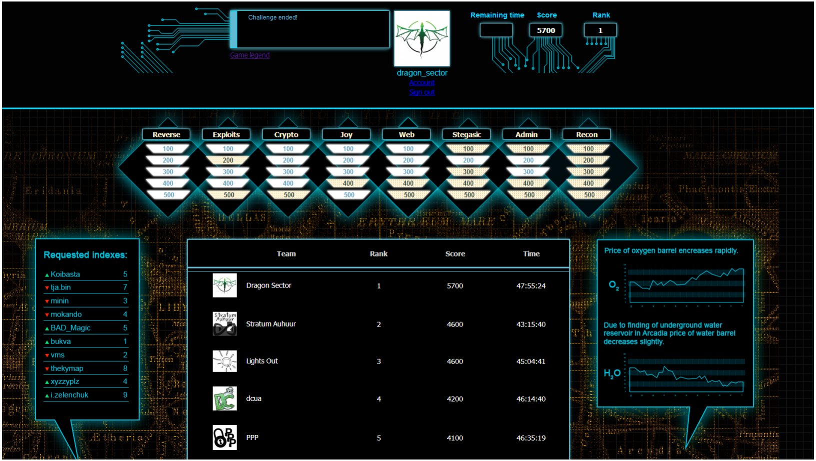
Just as in Jeopardy, each category contains challenges of varying difficulty, with the more difficult challenges worth more points and vice-versa.

Jeopardy-Style CTF Board Example #1



Exploitation	100	200	300	300	400	400	500
Reverse Engineering	100	200	300	300	500		
Cryptography	200	300	300				
Forensics	100	200	200	300			
Web	0	300					
Recon	100	100	100				
Networking	100						
Trivia	10	10	10	10	10	10	

Jeopardy-Style CTF Board Example #2



Challenge ended!

Game legend

dragon_sector
Account
Sign out

Remaining time	Score	Rank
	5700	1

Reverse	Exploits	Crypto	Joy	Web	Stegasic	Admin	Recon
100	100	100	100	100	100	100	100
200	200	200	200	200	200	200	200
300	300	300	300	300	300	300	300
400	400	400	400	400	400	400	400
500	500	500	500	500	500	500	500

Requested indexes:

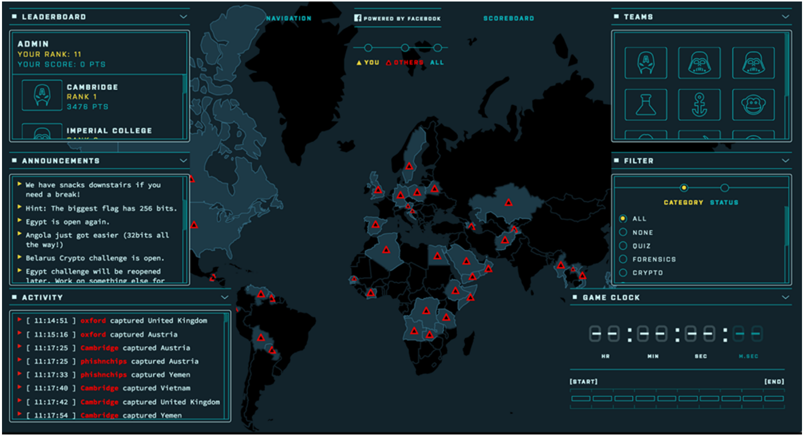
▲ Koibasta	5
▼ tja.bin	7
▼ minin	3
▼ mokando	4
▲ BAD_Magic	5
▲ bukva	1
▼ vms	2
▼ thekymap	8
▲ xyzzyplz	4
▲ i.zelenchuk	9

Team	Rank	Score	Time
Dragon Sector	1	5700	47:55:24
Stratum Auhuur	2	4600	43:15:40
Lights Out	3	4600	45:04:41
dcua	4	4200	46:14:40
PPP	5	4100	46:35:19

Price of oxygen barrel encreases rapidly.

Due to finding of underground water reservoir in Arcadia price of water barrel decreases slightly.

Jeopardy-Style CTF Board Example #3



ADMIN
YOUR RANK: 11
YOUR SCORE: 0 PTS

CAMBRIDGE
RANK 1
3476 PTS

IMPERIAL COLLEGE

- We have snacks downstairs if you need a break!
- Hint: The biggest flag has 256 bits.
- Egypt is open again.
- Angola just got easier (32bits all the way!)
- Belarus Crypto challenge is open.
- Egypt challenge will be reopened later. Work on something else for

```
[ 11:14:51 ] oxford captured United Kingdom
[ 11:15:16 ] oxford captured Austria
[ 11:17:25 ] Cambridge captured Austria
[ 11:17:25 ] phishnchips captured Austria
[ 11:17:33 ] phishnchips captured Yemen
[ 11:17:40 ] Cambridge captured Vietnam
[ 11:17:42 ] Cambridge captured United Kingdom
[ 11:17:54 ] Cambridge captured Yemen
```

● ALL
○ NONE
○ QUIZ
○ FORENSICS
○ CRYPTO

-- : -- : -- : --

How to Find a CTF

There's pretty much only two ways you're gonna find CTFs:

- **ctftime** (or a similar online calendar/league/directory)
- Word of mouth

Let's take a quick tour of ctftime.

CTF Challenge #1

This brings us to our first challenge. The flag format we'll use through this series is:

ZeroCTF{*flag_contents*}

You can find the first challenge **here**. The flag is worth 100 points. When you solve it, **DO NOT SPOIL THE SOLUTION FOR OTHERS, LET THEM SUFFER**.

CTF Challenge #1 BONUS

BONUS: There are one or more flags hidden within the presentation (file?) itself. The first person(s) to email me with a bonus flag that no-one else has yet found scores 50 bonus points.

As mentioned earlier, if you find a flag that isn't wrapped in "ZeroCTF{}", then make sure to properly format it yourself before sending it, otherwise it won't be worth any points.