# An introduction to CTF

Sandra Siby



#### What is a CTF?

- Information security competition
- Usually organized by a university/security organization
- Solve security challenges and earn points by 'finding the flag'
- Compete with teams all over the world
- Fun way to learn about security!

### Types of CTF events

#### Jeopardy

- Most popular type
- Questions in different categories
- Gain points by solving the questions

				1		
	tta	<b>/</b> _	a		10	
	1 7 7 0 1		u			

- Teams have their own network and services
- Goal is to attack other teams (attack points) and protect your services (defense points)
- You can have a mix of styles as well

CATEGORY 1	CATEGORY 2	CATEGORY 3	CATEGORY 4	CATEGORY 5	CATEGORY 6
\$100	\$100	\$100	\$100	\$100	\$100
\$200	\$200	\$200	\$200	\$200	\$200
\$300	\$300	\$300	\$300	\$300	\$300
\$400	\$400	\$400	\$400	\$400	\$400
\$500	\$500	\$500	\$500	\$500	\$500



### When and where?

#### When

- Events are organized throughout the year
- Usually during weekends
- Check upcoming events on: ctftime.org

#### Where

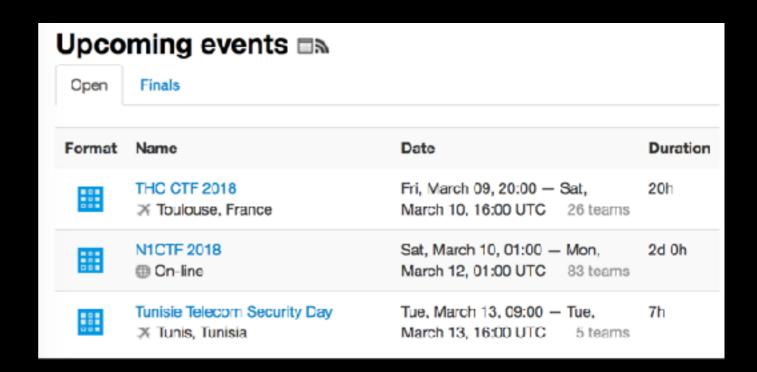
- Usually online
- Occasionally, you have live events as well

#### How does it work?

- Sign up for a team
- Register team on <u>ctftime.org</u>
- Pick an event and register the team for it
- Log in when the event starts and solve challenges
- You can work on challenges till the end time of the event
- Team ranking is published on <u>ctftime.org</u>
- Points over all events are aggregated for global team ranking
- Discuss/write about the challenges you solved/found interesting

# ctftime.org

- Past and upcoming events
- Teams and rankings (country/ university/global)
- Write-ups
  (solutions) to
  challenges
- Ratings of past CTF events



Team rating									
2018	2017	2016	2015	2014	2013	2012	2011		
Place	Team					Country		Rating	
<b>± 1</b>	dcua							228.917	
2	noraneco					•		152.550	
3	Harekaze					•		138.981	
4	Epic Leet	Team				•		138.396	
5	Made In N	MIM				_		113.828	

## What can I expect?

- Challenges are in various categories
- Challenges will have varying difficulty (and hence varying number of points)
- Common categories (and examples):
  - Crypto (attack poorly implemented/vulnerable crypto protocol)
  - Reverse Engineering (analysis of binary files)
  - Forensics (discover hidden information in images/audio files/ network traffic etc.)
  - Web (exploit vulnerabilities in websites)
  - Misc (can be anything!)

## What can I expect?

- Questions can be quite challenging.
- It is very possible that you spend an entire CTF and don't manage to solve anything.
- Training outside of CTFs can be very helpful
  - Websites with mock CTF challenges
  - Training sessions with teammates

## What can I expect?

- Time commitments
  - Not binding participate whenever possible
  - More members = more events/more player rotation/more players per event = More points
- Background in security
  - Not required basic CS knowledge and programming sufficient to get started
  - Beginners are welcome!
  - You do not need to be familiar with all categories!

A typical CTF team consists of players having varying skill levels in various categories

### A few resources to get started

- OverTheWire <u>overthewire.org/wargames/</u>: Practice challenges for different skill levels
- http://pwnable.kr/: Practice challenges in exploitation
- https://w3challs.com/: Practice challenges for different skill levels (with forums)
- Video (from Stevens): Building a Competitive Hacking [CTF] Team <a href="https://www.usenix.org/conference/enigma2016/conference-program">https://www.usenix.org/conference-program</a>

## Next steps!

- Create an EPFL CTF team :)
- Name? Register on <u>ctftime.org</u>
- Member list
- Communication channels
  - Mailing list for important announcements
  - Slack for discussion during events/training

## Next steps!

- Training
  - Share resources
  - Find experienced players or trainers in various categories
- Pick events to participate in
  - Frequency
  - Number of players
  - Difficulty level

# Thank you!

# Questions/Suggestions?