CTF Techniques

Por Carlos Velez

Introduction

01

What is it, why is it important?

Types of CTF

02

Many options with different difficulty levels

Challenges

03

Some of the challenges of the most important CTFs

Statistics

04

It is growing and recruiters are looking for talent

Tools

05

Some of the essential tools for CTF Competitions

Resources

06

Lots of information, writeups, repos

INTRO

CTF

What is it?

Children game where each team attempt to capture the opposing team’s flag (Persil).

British soldiers capturing French flag (Pinterest).

INTRO

CTF

What is it?

- …is a computer security competition where teams/individuals compete to solve challenges of varying difficulty (usually increasing) to score points.
- Realistic problems with realistic solutions.
- Some of the famous CTFs (CTFtime).

FACEBOOK PRESENTS CAPTURE THE FLAG CTF

DEFCON CTF

CTF MITRE

Google CTF

TYPES OF CTFs

Wargames

overthewire

Hack quest

SANS holyday Challenge

Jeopardy

National Cyber League

Attack & Defend

National Collegiate Cyber Defense

- Single-user vs. multi-user
- Single targets vs. multiple targets
- Competitive vs. collaborative
- Short and focused vs. long-term
- Local vs. remote
- Defensive, offensive, analytical

TYPES OF CHALLENGES (CATEGOERIES)

Cryptography

Lots of math!

Exploitation

Break it!

Reverse Engineering

How it works, what can you get?

Forensics

Looking for evidence

Web Applications

Get information!

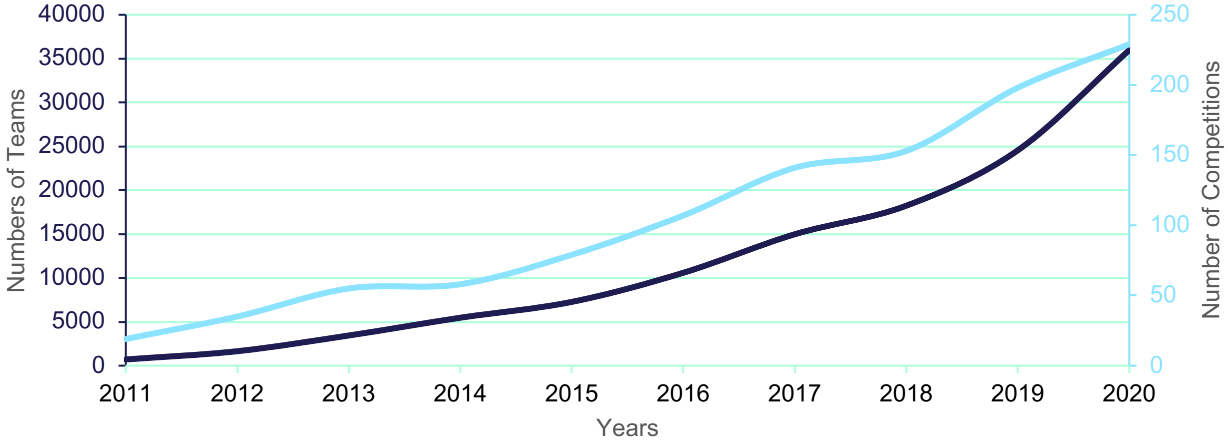
CTF Characteristics:

- divides a problem into smaller pieces (challenges, flags)
- measure progress (score)
- create a sense of accomplishment (rewards, achievements)
- instill a sense of competition (leader board)
- directly applies theory
- is great fun!

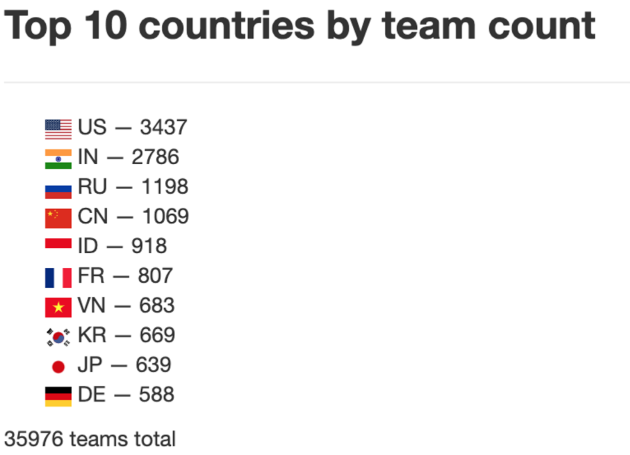
Why CTF?

- To practice your hacking skills in a realistic environment
- Compete with other hackers
- Getting good at it = find a good job opportunity
- Is great fun!

CTFtime



CTFtime.org Teams Total



Top 10 countries by team count

US	3437
IN	2786
RU	1198
CN	1069
ID	918
FR	807
VN	683
KR	669
JP	639
DE	588

35976 teams total

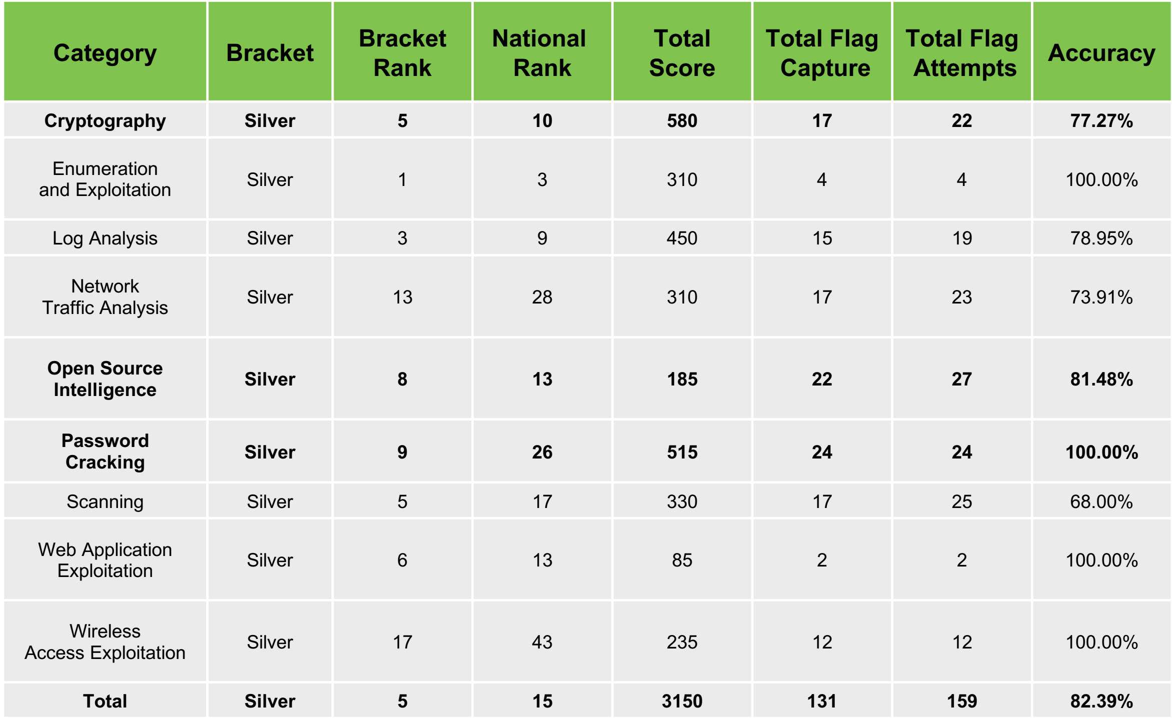
Nacional Cyber League (NCL) (Spring 2017) Report

- Must be affiliated to a US institution

- Defensive and offensive puzzles

- Based on CompTIA Security+ and EC-Council CEH exams

- **Open Source Intelligence**, Scanning, Enumeration and Exploitation, **Password Cracking**, Traffic Analysis, Log Analysis, Wireless Security, **Cryptography**, and Web Application Security.



Category	Bracket	Bracket Rank	National Rank	Total Score	Total Flag Capture	Total Flag Attempts	Accuracy
Cryptography	**Silver**	**5**	**10**	**580**	**17**	**22**	**77.27%**
Enumeration and Exploitation	Silver	1	3	310	4	4	100.00%
Log Analysis	Silver	3	9	450	15	19	78.95%
Network Traffic Analysis	Silver	13	28	310	17	23	73.91%
Open Source Intelligence	**Silver**	**8**	**13**	**185**	**22**	**27**	**81.48%**
Password Cracking	**Silver**	**9**	**26**	**515**	**24**	**24**	**100.00%**
Scanning	Silver	5	17	330	17	25	68.00%
Web Application Exploitation	Silver	6	13	85	2	2	100.00%
Wireless Access Exploitation	Silver	17	43	235	12	12	100.00%
Total	**Silver**	**5**	**15**	**3150**	**131**	**159**	**82.39%**

Requirements:

- Problem solving skills
- Network knowledge
- Web vulnerabilities
- Programming (no language preference) ***python***
- *Keep up with the Tools*
- *In addition: math, algorithms, protocols, Linux, shell script, automation*

Forensic Challenge Tools

- Network
  - Wireshark (packet analyzer)
  - Tcpdump (packet analyzer)
  - Network Miner (network forensics analysis tool)
- File
  - 010 (hex editor)
  - Scalpel (file system recovery)
- **Disk Image**
  - Autopsy
  - VMs
  - FTK
- **Image Steganography**
  - Stegsolve
  - Zsteg

RE Tools

- Decompilers
- IDA Pro
- Binary Ninja
- Gidra (free... from NSA)
- programmer knowledge and patience

Encoding vs Ciphers vs Hashing

- Encoding
  - Base64
  - Morse
  - Braille
  - Fictional language

- Ciphers (Classic)
  - Atbash
  - ROT13
  - Caesar
  - Vigener

- Ciphers (Mecanical)
  - Enigma cipher
  - Lorenz ciphers

- Ciphers (Modern)
  - Block ciphers
  - Stream ciphers

- Tools
  - John (pass. Cracking)
  - Hashcat (lots of hash types, GPU)
  - OphCrack (rainbow tables)
  - THC Hydra (online)

Tools for web app security

- Web Browser!
- Web Proxying Tool(s)
  - Burp Suite
  - Fiddler
  - mitmproxy
  - Nikto
  - ZapProxy
- SQLMap - Automatic SQL injection and database takeover tool
- Ysoserial - tool for exploiting unsafe object deserialization vulnerabilities
- SSLyze - deep analysis of the SSL/TLS configuration of web servers/applications.

RESOURCES

- **https://github.com/zardus/ctf-tools**
- **https://github.com/MrMugiwara/CTF-Tools** (Repos of useful tools)

- **http://icyberchef.com/** (encrypt, decrypt, base conversion, more, open source on GitHub)

- **https://www.kali.org/** (pentesting tools already installed on a Linux environment)

- **https://overthewire.org/wargames/** (practice Linux command line interface)

REFERENCES

Annual Security Conference Proceedings

- Alicea, Y. (2017). Cybersecurity Competitions as Effective Cybersecurity Teaching Tools. In Proceedings of the Annual Information Institute Conference, Eds. G. Dhillon and S. Samonas, April, 18-20, 2017. Las Vegas, NV. USA.

ACM

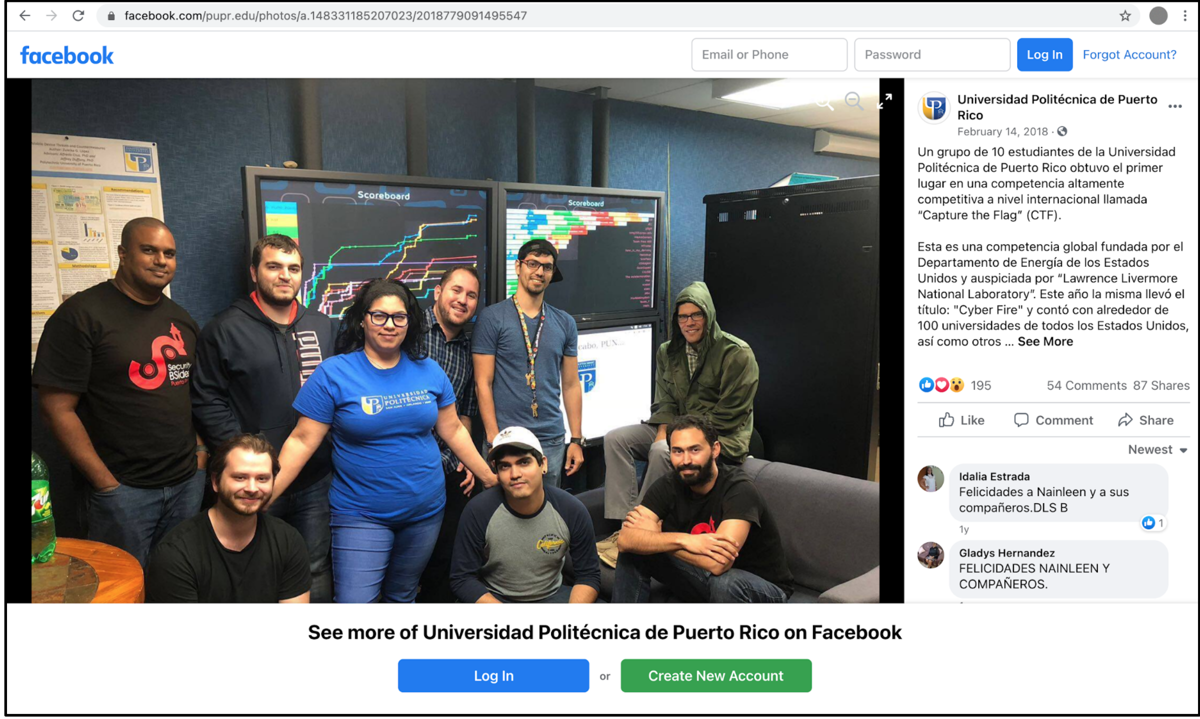
- Nathan Backman. 2016. Facilitating a Battle Between Hackers: Computer Security Outside of the Classroom. In Proceedings of the 47th ACM Technical Symposium on Computing Science Education (SIGCSE '16). ACM, New York, NY, USA, 603-608.
- Kees Leune and Salvatore J. Petrilli, Jr.. 2017. Using Capture-the-Flag to Enhance the Effectiveness of Cybersecurity Education. In Proceedings of the 18th Annual Conference on Information Technology Education (SIGITE '17). ACM, New York, NY, USA, 47-52.

IEEE

- L. McDaniel, E. Talvi and B. Hay, "Capture the Flag as Cyber Security Introduction," 2016 49th Hawaii International Conference on System Sciences (HICSS), Koloa, HI, 2016, pp. 5479-5486.
- R. Raman, S. Sunny, V. Pavithran and K. Achuthan, "Framework for evaluating Capture the Flag (CTF) security competitions," International Conference for Convergence for Technology-2014, Pune, 2014, pp. 1-5.

THANKS!

Do you have any questions?
velez.carlos.y@gmail.com


facebook.com/pupr.edu/photos/a.1483311852O7023/2018779091495547
facebook
Email or Phone
Password
Log In
Forgot Account?

Universidad Politécnica de Puerto Rico
February 14, 2018 ·

Un grupo de 10 estudiantes de la Universidad Politécnica de Puerto Rico obtuvo el primer lugar en una competencia altamente competitiva a nivel internacional llamada "Capture the Flag" (CTF).

Esta es una competencia global fundada por el Departamento de Energía de los Estados Unidos y auspiciada por "Lawrence Livermore National Laboratory". Este año la misma llevó el título: "Cyber Fire" y contó con alrededor de 100 universidades de todos los Estados Unidos, así como otros ... See More

Idalia Estrada
Felicidades a Nainleen y a sus compañeros.DLS B
1y

Gladys Hernandez
FELICIDADES NAINLEEN Y COMPAÑEROS.

See more of Universidad Politécnica de Puerto Rico on Facebook

CREDITS: This presentation template was created by **Slidesgo**, including icons by **Flaticon**, infographics & images by **Freepik** and illustrations by Stories