

O Maravilhoso Mundo das Competições Capture the Flag (CTFs)

Álison "gnx" Bertochi
bertochi.com.br

Sobre mim

- * Capitão do Epic Leet Team (ELT), melhor time de CTF (Capture the Flag) da América Latina e time que comprometeu as Urnas Eletrônicas durante o TPS (Teste Público de Segurança do Sistema Eletrônico de Votação) 2017, organizado pelo TSE;
- * Coorganizador do Pwn2Win CTF, umas das principais competições do gênero do mundo, e CTF mais multidisciplinar de todos;
- * Mantenedor do Projeto CTF-BR;
- * Coorganizador do Encontro TecLand;
- * Pesquisador independente em infosec desde 2005;

Antes de mais nada...

... utilize seu *smartphone* e siga-nos as redes sociais!
:)



@capturetheflagbr



@ctfbr



reddit.com/r/ctfbr

Antes de mais nada...

... utilize seu *smartphone* e siga-nos as redes sociais!
:)



@ctfbr (Canal)

Temos também um Grupo Privado no Telegram (~440 membros), além de um canal no IRC (#ctf-br @ freenode)

O que é um CTF?

Capture the Flag é um tipo de competição que envolve diversas competências das equipes formadas por profissionais, estudantes ou entusiastas, para a realização de desafios relacionados à infosec (segurança da Informação) e lógica. Envolvem muito "pensar fora da caixa" para resolver os problemas de forma rápida e eficaz, e muito teamwork também.

O que é um CTF?



Vídeo que ilustra muito bem a ideia de CTFs:
"Pensamento fora da caixa".

Disponível também em

<https://ctf-br.org/files/Palestras/TcheLinux2019>

Quem organiza?

A maioria dos CTFs são feitos de times para times, ou ainda de empresas para times (Google, Facebook, Trend Micro, etc). Não há uma "Instituição" por trás, como a Association for Computing Machinery (ACM) que organiza o ICPC (Maratona Internacional de Programação). Qualquer um pode organizar e participar de CTFs. Nenhum dos que estão no CTFTIME tem custo de inscrição.

Qual sua duração?

Têm duração normalmente de 24 ou 48 **consecutivas (sem intervalo)**, sendo que algumas possuem as qualificatórias *online* e as finais *on-site (offline)*.

A estratégia de "logística" da equipe conta muito para se dar bem!

O que são as flags?

As flags nessas competições são **um código** que as equipes obtêm ao realizar os desafios. Com esse **código** em mãos, o time submete-o na plataforma do evento (dashboard) e obtêm os pontos referentes àquele desafio em específico.

Exemplos de flag

As competições têm tentado padronizar as flags nos últimos anos, colocando o nome do evento antes (**EVENTO{alguma_coisa_aqui}**). Em suma, o formato varia de competição pra competição, e as vezes dentro da própria competição.

Exemplos de flag

HITCON CTF:

HITCON{a755be06b165ed8fc4710d3544
fce942}

HITCON{SOOOOOOO_MaNy_7Ar_LeV
eLs}

Exemplos de flag

Pwn2Win CTF (BR):

CTF-

BR{TYPE_CONFUSION_ON_APIS_ARE_LOVELY_
WITH_XXE_DONT_U_THINK??}

CTF-BR{s00000_tight_for_my_BIG_sh3ll0dE_}

Exemplos de flag

DEF CON Quals:

```
000{if_u_Ar3_r34din6_7h15_yOu_  
4r3_7h3_m0z4rT_of_inf053c_Ch  
33rs2MP!}
```

Formatos de CTFs

1. Jeopardy-style
2. Attack/Defense
3. Híbridos

I. Jeopardy-style:

Estilo Quiz, possuem challenges de diversas categorias, níveis de dificuldade e pontuações. Tanto as categorias, como o formato de pontuação variam de evento pra evento. O **scoreboard** dinâmico está sendo adotado em todos CTFs Tier I. Com certeza é a maneira mais justa de definir a pontuação.

Categorias de desafios:

Em amarelo, as presentes em praticamente 100% das competições:

Forensics (Forense)

Reversing (Eng. Reversa)

Pwnable/Exploitation (Exploração de binários)

Networking (Redes)

Miscellaneous (Diversos)

Categorias de desafios:

Crypto (Criptografia)

Web Hacking

PPC (Professional Programming and Coding)

Alguns challenges podem ser de mais de uma categoria (ex: Crypto + Rev), e também existem outras, como Eletrônica/Hardware, mas nesse caso, dependendo da visão do organizador, podem colocá-los dentro de Reversing.

Pwn2Win 2014

Pwn2Win

ch1p Owners: 19 	70's Owners: 10 	Watson... Owners: 9	pkn1f3 Owners: 16 	p0llsh Owners: 14 
Misc 6 π Owners: 20 	Misc 20 Matroshka Owners: 20 	Networking 10 p23 Owners: 22 	Forensics 20 k1k0 Owners: 21 	Bônus 10 Bônus Owners: 17
Crypto 40 ch1q Owners: 2	Networking 20 p0r7s Owners: 3	Crypto 50 brut3 Owners: 4 	Networking 50 kn0ck1ng Owners: 0	Forensics 30 g30 Owners: 18 
Reversing 45 c4ll1t	Reversing 70 cr4ckm3	Forensics 50 fs	Misc 40 dlff	Misc 50 s3q

Pwn2Win 2017

News

MESSAGES

20

SOLVES

964

[22-10-2017 12:37:56] admin: 1 HOUR LEFT, submit your flags!
[22-10-2017 12:18:47] admin: For People Throwing 2, see the following diagram:
<https://static.pwn2win.party/pplthrowing2.jpg>
[22-10-2017 09:48:11] admin: Netscape hint: Good thing all browsers are updated automatically...
Or aren't they?
[22-10-2017 05:40:35] admin: Please guys, help us with your feedback: <https://goo.gl/mBz813>
[22-10-2017 04:28:10] admin: Botnet is online again, sorry!
[22-10-2017 03:42:53] admin: Botnet in the Wild is off for maintenance

Rank

1. Eat Sleep Pwn Repeat	7522
2. p4	5646
3. Dragon Sector	5418
4. 0x00C0FFEE	3452
5. HackingForSoju	3445

Challenges

Reversing Electronics Not a chall Crypto Exploitation PPC-M Web Recon Bonus Misc Forensics PPC Networking Attack Step Physics
Story

Achievement Unlocked

Total solves: 18

Score: 303

Reversing

Asymmetric Encryption

Total solves: 17

Score: 308

Crypto

Attack Step - Final

Total solves: 1

Score: 474

Attack Step

CSAW 2013

If you are not watching CSAW.tv, you are missing out!

Trivia

50

50

50

50

50

Recon

100

100

100

100

100

100

100

100

Web

100

200

300

Reversing

100

100

150

200

300

400

500

500

Exploitation

100

200

300

400

400

500

Miscellaneous

50

50

100

200

300

Crypto

100

300

500

CSAW 2014

https://ctf.isis.poly.edu/challenges#

4 ring

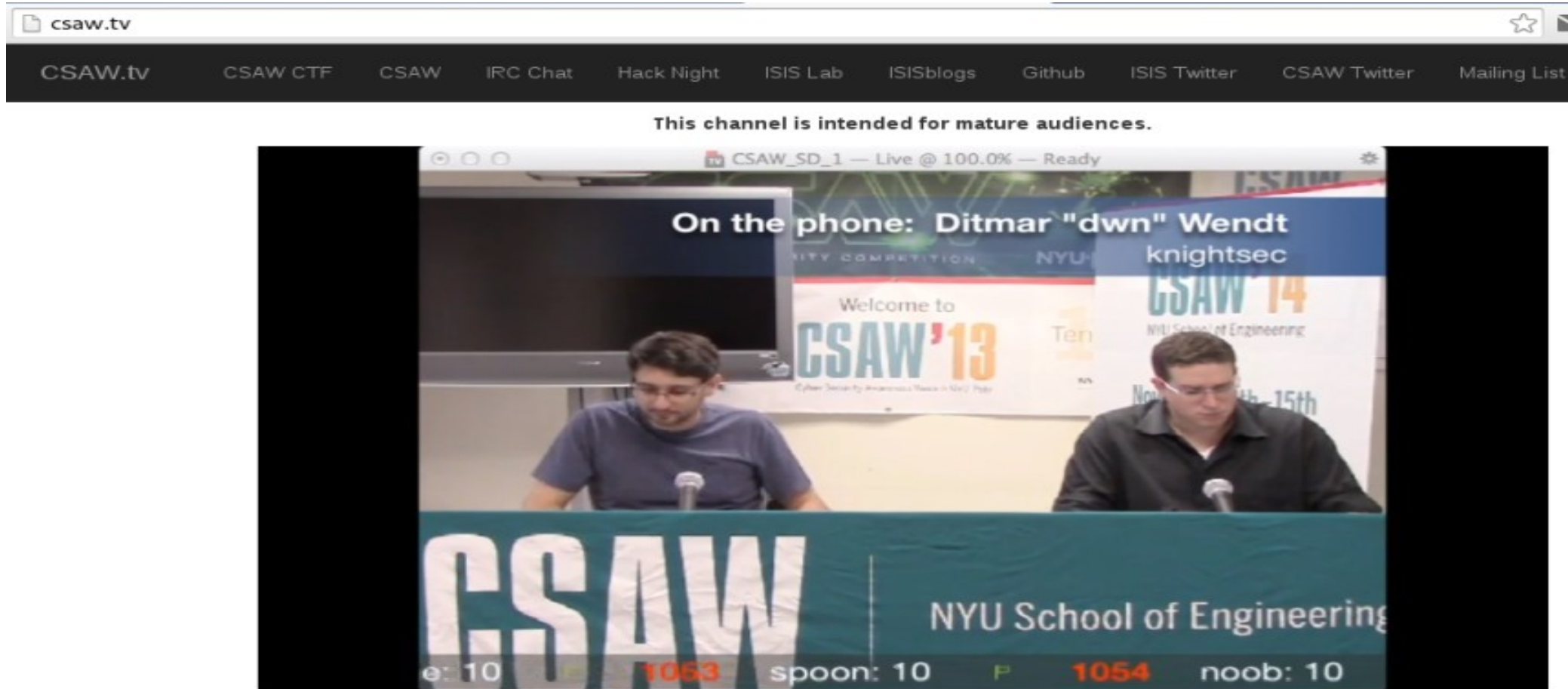
Home Rules Teams Judges Scoreboard Challenges Archives

CSAW TV

Challenges

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

CSAW 2014 - Narração



Time Epic Leet Team - 700pts

MiSc ellaneous	WeB application	ReV ersing	CrYpT ography	FoReN sics	BoNuS extra
100	100	100	100	100	10
200	200	200	200	200	10
300	300	300	300	300	10
400	400	400	400	400	10
500	500	500	500	500	10

3°

H
a
c
k
i
n
g
n'
R
o
l
l

2
0
1
3

The screenshot shows a web browser at the URL "scoreboard2019.ooverflow.io/#/". The page has a dark theme with purple accents. At the top, there's a navigation bar with links: TRAINING, RULES, SCOREBOARD (active), SOLVES, and LEADERBO... Below this, the main content area is divided into two columns. The left column is titled "FIRST CONTACT" with a robot icon. It lists five challenges: 1. 100 PTS, WELCOMING, WELCOME_TO_THE_GAME (COMPLETED BY 1252 CADETS). 2. 110 PTS, POTPOURRI, REDACTED-PUZZLE (COMPLETED BY 102 CADETS). 3. 108 PTS, INTRO, KNOW_YOUR_MEM (COMPLETED BY 122 CADETS). 4. 102 PTS, INTRO, RECON, WEB, CANT_EVEN_UNPLUG_IT (COMPLETED BY 390 CADETS). The right column is titled "DIPLOMACY" with a hand icon. It lists four challenges: 1. 135 PTS, PWN, REVERSE, GLORYHOST (COMPLETED BY 36 CADETS). 2. 201 PTS, CRYPTO, REVERSE, ASRYBAB (COMPLETED BY 14 CADETS). 3. 182 PTS, CRYPTO, TANIA (COMPLETED BY 17 CADETS). 4. A challenge with a pink background, handwritten text "KOT 34X", "WEX", "EAMT XX", "STREET STAKE", and "MYELLETT---". At the bottom, there are partial views of "FINAL FRONTIER" and "SPEEDRUN" sections.

Formatos de CTF

2. Attack/Defense:

De forma genérica, as equipes recebem uma VM com diversos serviços (alguns vulneráveis), e o objetivo é capturar as bandeiras alheias e proteger as do seu time com patches (SLA conta, não pode simplesmente "tirar o serviço do ar").

Formatos de CTF

2. Attack/Defense:

Como a infraestrutura nesse tipo de evento é um fator crítico, a maioria desses CTFs são *in loco*, e normalmente são as Finais de algum evento Jeopardy que teve qualificatória online. As exceções de CTFs Attack/Defense que acontecem online, são: RuCTFE, FAUST CTF, UCSB iCTF e ENOFLAG.

Formatos de CTF

2. Attack/Defense:



Vídeo "DEF CON Finals 2014" e Imagens do ambiente da final.

Disponível também em

<https://ctf-br.org/files/Palestras/TcheLinux2019/Attack&Defense>

Write-ups

São tutoriais que apresentam a resolução de um desafio por alguma equipe após a competição. É legal ver as mais diversas formas de resolver um *challenge*, de acordo com a criatividade de cada equipe.

Write-ups

Alguns repos de write-ups:

<https://ctftime.org/event/NUMERO-EVENTO/tasks/>

<https://github.com/ctfs>

<https://ctf-br.org/write-ups>

Hints

São dicas dadas para os challenges durante a competição. Depende da organização de cada evento querer ou não soltar. Na maioria dos CTFs Tier 1, hints são dadas para challs que ninguém conseguiu resolver, após decorrido um bom tempo de evento (1 dia, por exemplo).












Site referência no meio, onde os organizadores de CTFs, que normalmente são as próprias equipes, cadastram seus eventos. O capitão de cada time pode registrar o mesmo lá, e os membros, através de um hash, ingressam nele no site. O [CTFTime.org](https://ctftime.org) mantém um ranking anual das melhores equipes, e também armazena write-ups.

Team rating

2019

[2018](#)[2017](#)[2016](#)[2015](#)[2014](#)[2013](#)[2012](#)[2011](#)

Place	Team	Country	Rating
👑 1	Balsn		846,945
2	Dragon Sector		785,223
3	TokyoWesterns		738,337
4	Plaid Parliament of Pwning		712,667
5	Tea Deliverers		670,862
6	p4		638,825
7	r3kapig		620,971
8	dcua		620,139
9	Bushwhackers		615,464
10	LC4BC		598,572

[Full rating](#) | [Rating formula](#)

Upcoming events 📅

Past events 📅

[With scoreboard](#)[All](#)

📅 TokyoWesterns CTF 5th 2019


Set. 01, 2019 21:00 BRT | On-line | [Weight voting in progress](#)

Place	Team	Country	Points *
👑1	Balsn		194,160
2	A*0*E		143,699
3	CyKOR		124,862

[1003 teams total](#) | [Tasks and writeups](#)

📅 PASECA CTF 2019

Ago. 25, 2019 18:00 BRT | On-line

Place	Team	Country	Points
👑1	еще одна ctf команда		0,000
2	Nu93B34ch		0,000
3	fargate		0,000

[192 teams total](#) | [Tasks and writeups](#)

Por que você deveria jogar?

- Conhecimento → por ser uma competição extremamente multidisciplinar, se você trabalha com TI (ou é entusiasta da área), os benefícios de aprendizado são incomensuráveis

Por que você deveria jogar?

- Networking → CTFs te proporcionam conhecer os caras técnicos mais f()#@\$ do planeta

Por que você deveria jogar?

- Oportunidades de emprego → muitas empresas utilizam CTFs como processo seletivo ou como métrica pra selecionar os melhores candidatos. No Brasil, empresas gigantes como Itaú e Ernst & Young são exemplos de organizações que já utilizaram CTFs pra contratação

Por que você deveria jogar?

- Reunir a galera e se divertir → é muito legal ter alguns membros do time na mesma cidade
- Reconhecimento → times bons são referências na área de segurança em seus países e internacionalmente

Por que você deveria jogar?

- Dinheiro → já teve CTF com prize pool de 200k USD (RealWorld)
- Conhecer países e culturas diferentes → algumas qualificatórias pagam as despesas do time para a final

ELT

Se você ainda precisa de motivos pra jogar, conheça um pouco do meu time, o ELT.

- Formamos a equipe em 2012 e hoje somos a melhor da América Latina.

Overall rating place: **39** with **287,577** pts in 2018

Country place: **1**

ELT

- O sucesso da carreira do vice-capitão é praticamente 100% devido aos CTFs. Ele é o responsável do time pelos challs de *pwning* e *crypto*, e hoje trabalha no Google em Zurich (anteriormente passou pela Red Hat).

ELT

- Organizamos o Pwn2Win CTF, que é o mais multidisciplinar e um dos mais difíceis da cena internacional. O reconhecimento do nosso evento é gigantesco. Somos pioneiros em diversos tipos de *challenges*, ou seja, fomos os primeiros a explorar muita coisa na criação de desafios, como por exemplo, FPGA Reversing, Machine Learning, Engenharia Reversa de Circuitos Quânticos, etc.

ELT

- Participamos do Teste Público de Segurança do Sistema Eletrônico de Votação, organizado pelo TSE em 2017, e conseguimos comprometer completamente a Urna Eletrônica Brasileira. O nosso artigo "Execução de Código Arbitrário na Urna Eletrônica Brasileira" ganhou o prêmio George Cox de Melhor Artigo na SGSeg 2018.

Mais informações em <https://epicleet.team/urna-eletronica-comprometida>

ELT



ELT

- Fomos para o Japão em 2018 para representar o Brasil na Raimund Genes Cup, final do CTF da Trend Micro, cujo nos classificamos durante a H2HC (Hackers 2 Hackers Conference) 2019

Membros que jogaram no Japão

ELT

+

```
<BODY>  
<FORM name="gotolink">  
<INPUT TYPE="button" value=  
"Go to random ly
```

—

+

EPIC LEET TEAM
Brazil



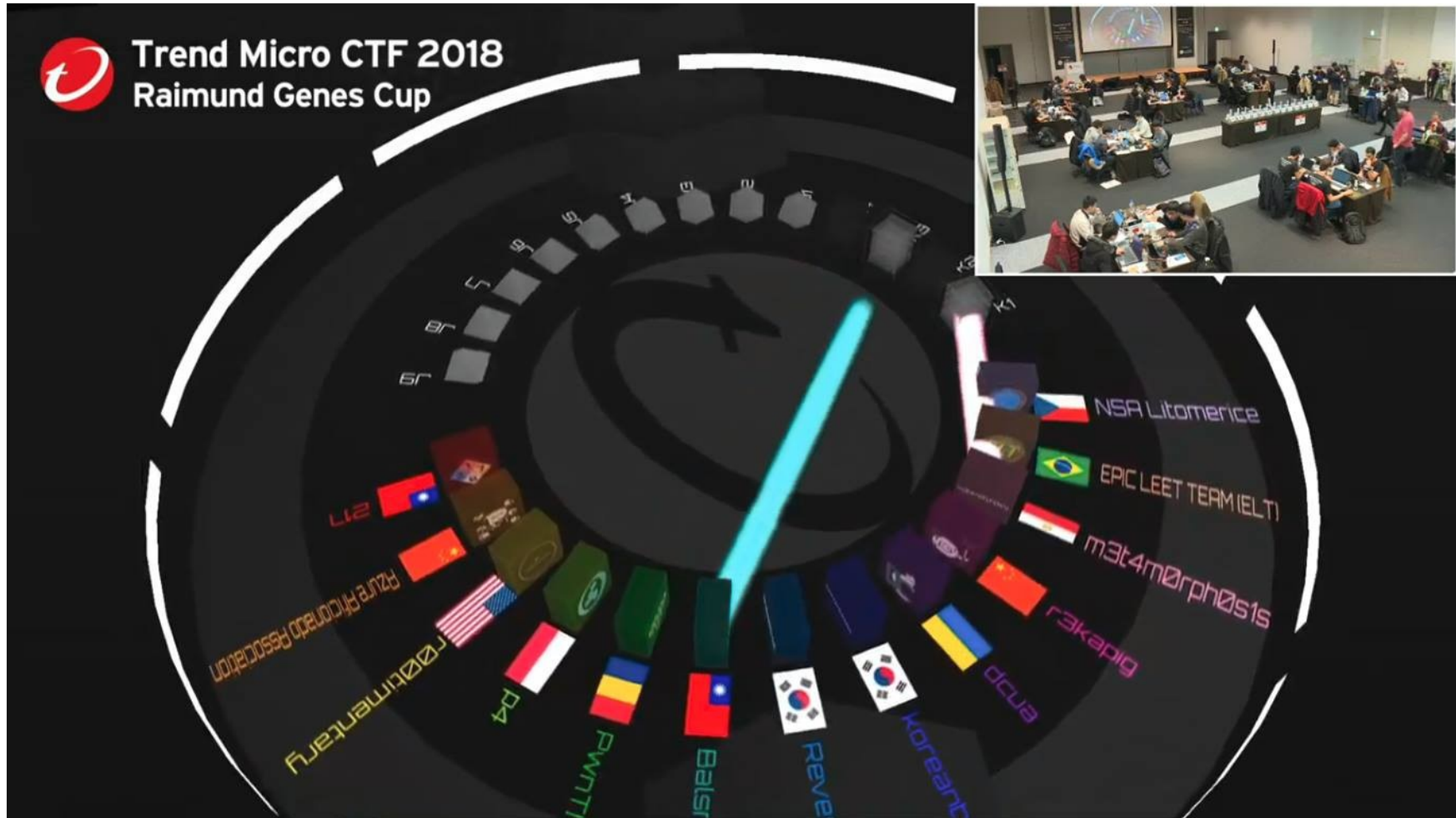
+

ELT

- Além de colecionarmos vários bons resultados, vitórias e premiações (dinheiro, eletrônicos, etc) em eventos nacionais e internacionais. Representar o Brasil nesse tipo de competição de alto nível é muito gratificante!

ELT

Muito orgulho ver a bandeira do Brasil!



ELT

Aos que se interessarem em ver a cobertura dessa Final, pesquisem por "Raimund Genes Cup" no YouTube:

- Primeiro dia: <https://www.youtube.com/watch?v=evx-gr24-aM>
- Segundo dia: https://www.youtube.com/watch?v=6XboxgC_PKk



Mas então, como começar?

- Treine bastante em sites de Wargames (em suma, são como "CTFs" porém que ficam online por tempo indeterminado). Alguns sites legais de wargames:
- <https://www.wechall.net/> → possui um "ranking global" com a pontuação de todos os outros sites de wargames
- <https://ringzer0ctf.com> (muitos challs divertidos)
- <https://root-me.org> (tem material de apoio)

Mas então, como começar?

- Veja muitos write-ups
- Tente juntar alguns amigos e se programe pra jogar algum CTF do [CTFTime.org](https://ctftime.org)
- Dê uma olhada nos links em <https://ctf-br.org/docs> e também <http://ctf-br.org/links-externos>

Projeto CTF-BR

O que é?

Um Projeto feito **pela** comunidade **para** a comunidade, com o intuito de disseminar a cultura dos CTFs pelo Brasil.

Projeto CTF-BR

Quem faz?

Voluntários de diversos times brasileiros. Você também pode participar e contribuir!

Principais objetivos:

1) Mostrar que esse tipo de competição é extremamente útil para a formação intelectual e profissional dos participantes, pois exercita o raciocínio lógico, trabalho em equipe, e capacita os *players* a pensar "fora do caixa" na resolução de problemas diversos de infosec (segurança da informação) e lógica;

Principais objetivos:

2) Disseminar a cultura do maravilhoso mundo das competições Capture the Flag no Brasil, tornando-as tão populares quanto as Maratonas de Programação. Visando cumprir esse objetivo, pretendemos dar palestras, utilizar redes sociais e outros recursos para chegar ao nosso público-alvo, que são estudantes, entusiastas e profissionais de TI;

Principais objetivos:

3) Manter um grande repositório BR de write-ups no Portal (<https://ctf-br.org/write-ups>) e de links de pessoas que produzem conteúdo relacionado à CTFs (<https://ctf-br.org/links-externos>).

Projeto CTF-BR

Como contribuir?

- Palestrando (temos o "Kit do Palestrante" em <https://github.com/ctf-br/>)
- Divulgando o Projeto e os CTFs brasileiros nas redes sociais
- Escrevendo *write-ups* ou fazendo vídeos resolvendo challenges

Projeto CTF-BR

Como contribuir?

- Traduzindo conteúdo interessante relacionado a CTFs. Temos um compilado de links em <https://ctf-br.org/docs> que pode servir de referência

Projeto CTF-BR

Como contribuir?

- Organizando eventos: por exemplo, em 2019 participamos da CPBR12 (Campus Party) como "Comunidade" com uma grade repleta de conteúdo bom, e isso só foi possível devido a iniciativa de um membro que tomou a frente e se propôs em organizar tudo (Chamada de Trabalhos, etc)

Projeto CTF-BR

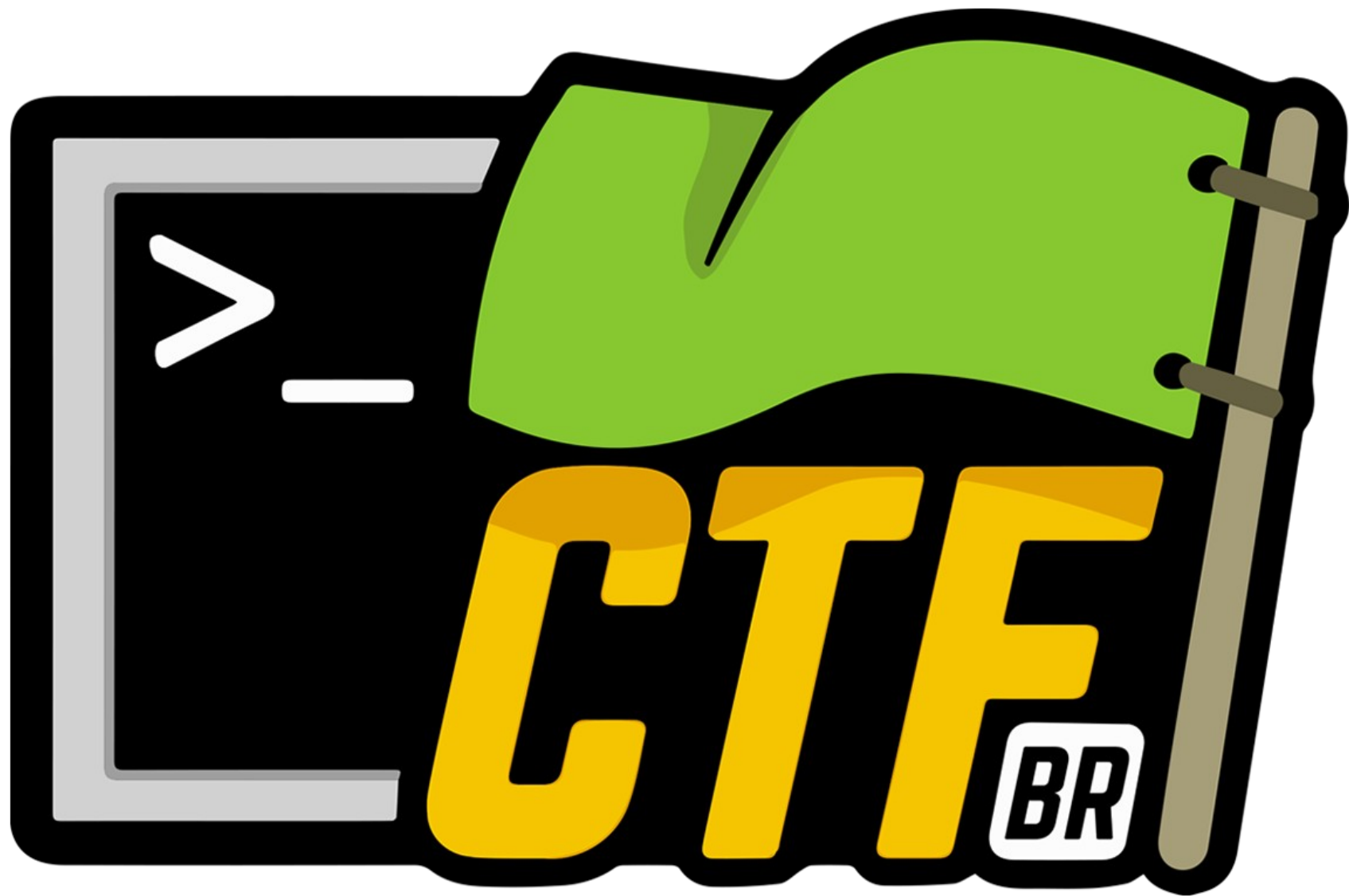
Como contribuir?

- Sendo proativo. Ao vermos que você tem interesse em ajudar, acharemos algo interessante em que você possa colaborar para a Comunidade!

O Projeto é de todos!

Resumo da Ópera

Joguem CTFs, ajudem no Projeto para fazer a Comunidade crescer e colham os frutos que essas sábias decisões irão trazer! :)



Mãos na massa!

Resolução de dois challenges simples, pra entenderem a ideia:

- coffee (Forensics)
- polish (Misc)

Dúvidas?

alisson@bertochi.com.br

alissonbertochi @ twitter

gnx @ freenode

gnx22 @ telegram

Follow us on Twitter:

@eltctfbr

@pwn2win