



Antes de mais nada...

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



@capturetheflagbr



@ctfbr



reddit.com/r/ctfbr

Agenda

- Afinal, o que é CTF?
- Flags? Como são? Onde vivem?
- Formatos de CTF
- Eventos
- Como participar?
- Projeto CTF-BR
- Conclusão

Afinal, o que é CTF?

Capture the flag (Capture a bandeira)

O que é? Competição individual ou em equipe que envolve diversas competências de Computação. Normalmente acontecem nos fins de semana e tem duração entre 24h-48h.

Objetivos? Resolver problemas (geralmente relacionados com infosec). Aprender.

Quem participa? Estudantes, professores, programadores, hackers, profissionais de segurança da informação, entusiastas etc.

Afinal, o que é CTF? (Termos comuns)

- Challenges/tasks - Desafios/tarefas
- Flag - Bandeira. Informação secreta (mais adiante...)
- Scoreboard - Rank das equipes
- Write-up - Explicação de como um desafio foi resolvido por uma equipe. Liberado apenas no final da competição!!!
- Hint - Dicas que os organizadores dão sobre algum desafio.

Flags? Como são? Onde vivem?

Flags?

Informação secreta que comprova a resolução de um problema.

Flags? Como são? Onde vivem?

Como são?

Depende da competição. Ultimamente existe uma tentativa de padronizar um formato.

Ex:

- a8db1d82db78ed452ba0882fb9554fc9
- This_is_an_example_of_flag
- flag{a8db1d82db78ed452ba0882fb9554fc9}
- key{w00t_you_g0t_it}
- CTFBR{S0m3_S3cr3t_T3XT}

Flags? Como são? Onde vivem?

Onde vivem?

- Em servidores (WEB, FTP, DNS etc...)
- Em arquivos criptografados
- Em arquivos binários
- Em arquivos de captura de pacote (PCAPs)
- Em imagens
- Em audios
- Em qualquer lugar :P

Formatos de CTF

- Jeopardy
- Attack/Defense
- Híbridos

Formatos de CTF (Jeopardy)

- Múltiplos problemas
- Várias categorias
- Diferente níveis de dificuldade
- Problemas mais difíceis = Maior pontuação

Formatos de CTF (Jeopardy)

Categorias:

- **F**orensics (Forense)
- **R**eversing (Eng. Reversa)
- **P**wnable/Exploitation (Exploração de binários)
- **N**etworking (Redes)
- **M**iscellaneous (Diversos)
- **T**rivia (Triviais)
- **C**rypto (Criptografia)
- **W**eb Hacking

Formatos de CTF (Jeopardy)

| CSAW CTF | | | | | | |
|--|-----|-----|-----|-----|-----|-----|
| About Rules Judges Register Competitors Scoreboard Challenges Archives CSAW Conference You are logged as | | | | | | |
| CSAW CTF 2012 Challenges | | | | | | |
| The competition has ended! | | | | | | |
|  Trivia | 100 | 100 | 100 | 100 | 100 | |
|  Recon | 100 | 100 | 100 | 400 | 400 | |
|  Web | 100 | 200 | 300 | 400 | 500 | 600 |
|  Reversing | 100 | 200 | 300 | 400 | 500 | |
|  Exploitation | 200 | 300 | 400 | 500 | | |
|  Forensics | 200 | 200 | 500 | | | |
|  Networking | 100 | 200 | 300 | 400 | | |

Formatos de CTF (Jeopardy)

2014年5月19日 上午7:59:39 <global>
30 SECONDS, SUBMIT THAT SHIT #DEFCON #CTF

2014年5月19日 上午7:44:56 <global>
YOU'VE GOT FIFTEEN MINUTES TO QUALIFY FOR #DEFCON #CTF. JUST SAYING. SOLVE THAT SHIT. GOOD LUCK.
ET CETERA.

2014年5月19日 上午7:39:15 <global>
holy shit Gallopsled solved rebaby [Jymbolia] for 3 points. #defcon #ctf

2014年5月19日 上午7:38:00 <global>

0:00:-8

Baby's First 1 1 1 1

Duchess 2

Gynophage 2 3 4

HJ 2 3 4

Jymbolia 2 3

Lightning 5 5

Selir 2 3

Sirgoon 2 4

Vito Genovese 2 3 4

[What are these categories?](#)

| | |
|----------------------------|-----------|
| Gallopsled | 49 |
| Dragon Sector | 40 |
| 9447 | 39 |
| Reckless Abandon | 39 |
| tomcr00se | 37 |
| Routards | 35 |
| More Smoked Leet Chicken | 34 |
| raon_ASRT | 34 |
| KAIST GoN | 32 |
| shellphish | 29 |
| CodeRed | 29 |
| HITCON | 28 |
| blue-lotus | 27 |
| HackingForChiMac | 27 |
| Rainbow Pixies of Delight | 27 |
| (Mostly) Men in Black Hats | 27 |
| w3stormz | 27 |
| Samurai | 26 |
| Robot Mafia | 26 |
| int3pids | 24 |
| Stratum Auhuur | 24 |
| ReallyBataika | 24 |
| OMGACM | 23 |
| SpamAndHex | 22 |
| 0x8F | 21 |

Formatos de CTF (Jeopardy)

hnr4.hackingroll.com/scoreboard/m500/

Time/Habilidades
Instruções
História
Para sair, clique [aqui](#)

Matrix

Alice e Bob estão com um problema matemático para conseguir entrar nas defesas da Digital Chip Munks [Download](#)

Resolvido por: 2 Equipes

| MiSc ellaneous | WeB application | ReV ersing | FoReN sics | ReCoN naissance | BoNuS extra |
|-------------------|--------------------|---------------|---------------|--------------------|----------------|
| 100 | 100 | 100 | 100 | 100 | 10 |
| 200 | 200 | 200 | 200 | 100 | 10 |
| 300 | 300 | 300 | 300 | 100 | 10 |
| 400 | 400 | 400 | 400 | 100 | 10 |
| 500 | 500 | 500 | 500 | 100 | 10 |


1. Epic Leet Team - 5150
2. dcua - 4750
3. Pão de Batãta - 4650
4. TheGoonies - 3000
5. InsertPIZZAintoCACTUS - 2940
6. TimeZero - 2530
7. RaulHC - 2350
8. NullByte - 1730
9. H3x Pr0phets - 1630
10. Django's Team - 1520

Formatos de CTF (Jeopardy)

Pwn2Win

12/10 01:15:33 Comunicado A noite é uma criança: muitos challenges pela frente ainda: ,D

12/10 00:54:58 Parabenização Pontos extras da [Bônus] r1ckr0ll1ng para o RaulHC | +30

| | | | | |
|---|--|--|--|---|
| Misc 5 d4t3 Owners: 19  | Misc 5 oldsch00l Owners: 30  | Misc 10 N1MB3R5 Owners: 2 | Misc 700 Etapa de Attack Owners: 2 | Misc 10 61f Owners: 32  |
| Forensics 15 mln14tur3 Owners: 15  | Misc 5 sux Owners: 31  | Misc 6 Clichê Owners: 26  | Misc 8 flrs7 Owners: 13 | Misc 7 m4g Owners: 14  |
| Misc 8 ch1p Owners: 19  | Reversing 15 70's Owners: 10  | Crypto 35 Watson... Owners: 9 | Misc 7 pkn1f3 Owners: 16  | Misc 12 p0llsh Owners: 14  |

ctf.tecland.com.br/Pwn2Win/#questao2

Formatos de CTF (Jeopardy)

Exemplo

Nome: Uma fácil

Categoria: Misc

Descrição:

426f6d2074726162616c686f2120436f6e73656775697520313020706f6e746f7321204171756920737
56120666c61673a2043544642527b3865623930656331353262643330663461353366313562663830
3537383364637d

Formatos de CTF (Jeopardy)

>>>

```
'426f6d2074726162616c686f2120436f6e7365677569752031302  
0706f6e746f732120417175692073756120666c61673a2043544  
642527b38656239306563313532626433306634613533663135  
626638303537383364637d'.decode('hex')
```

'Bom trabalho! Conseguiu 10 pontos! Aqui sua flag:
CTFBR{8eb90ec152bd30f4a53f15bf805783dc}'

Formatos de CTF

(Attack/Defense)

Equipes recebem/montam máquinas virtuais com diversos serviços (alguns vulneráveis).

As equipes devem atacar as máquinas dos concorrentes.

As equipes devem proteger os serviços de suas máquinas.

Formatos de CTF (Híbridos)

Jeopardy + Attack/Defense

Eventos

Nacionais

- Hacking n' Roll (Organizado pelo INSERT)
- Pwn2Win (Organizado pelo ELT)

Internacionais

- DEF CON Quals e Finals
- Codegate Quals e Finals
- HITCON CTF
- CSAW CTF
- PlaidCTF

Como participar?

- Junte uma galera;
- Registre um time em algum CTF;
- Compre umas pizzas :P
- Divirta-se!

Saiba sobre os próximos CTFs em:

<https://ctftime.org/event/list/upcoming>

Como "ficar bom"?

- Participando de muitos CTFs;
- Lendo *write-ups*;
- Fazendo *write-ups*;
- Praticando em sites com desafios de dificuldade crescente, como pwnable.kr, ctf.katsudon.org, w3challs.com...

Como "ficar bom"?

- Praticando na rede social brasileira dos CTFs, o Shellter Labs (shellterlabs.com)



Projeto CTF-BR

- Projeto para movimentar a cena de CTF no Brasil;
- Projeto da comunidade e para a comunidade;
- Iniciativa para levar os CTFs para as Universidades;
- Integração dos times brasileiros;
- Repositório centralizado de write-ups;

Visite!

<https://www.ctf-br.org/>

CTF-BR University

Você deseja um **CTF introdutório** na sua Universidade?

Nós podemos proporcioná-lo!
Utilizando a mesma plataforma do **Pwn2Win CTF**, e com 12 challenges (6 iniciantes e 6 avançados), podemos organizar um CTF na sua Instituição e estimular os alunos a trabalhar em equipe e pensar "fora da caixa"!

Não perca essa oportunidade, **contate-nos!**

Conclusão

- CTFs são divertidos
 - CTFs são ótimas fonte de conhecimento
 - CTFs te fazem conhecer pessoas legais
 - CTFs te ensinam a trabalhar em equipe
 - CTFs podem te levar para outros países
 - CTFs podem ser lucrativos
-
- Entrose com a galera no IRC:
 - #ctf-br @ freenode