{Capture The Flag}

Hélder Fernandes

Patrocinadores **Platina**

Patrocinadores **Ouro**

Patrocinadores **Prata**

Organização

Agenda

e-Jornadas 2020

- O que é um CTF
- Para que servem os CTFs ?
- Tipos de CTF mais comuns
- Plataformas para CTF
- Exemplos
- Desafio Stega300 - Summer 2020 CTF

O que é um CTF (Capture the Flag) ?

e-Jornadas 2020

- Competição focada em utilização de técnicas e provas de conceito relacionadas com temas que envolvem a segurança de informação

- Tipicamente o objetivo destas competições é obter o maior número de flags no menor tempo possível

- Flag é uma espécie de hash, que serve de resposta ao desafio e comprova que o participante cumpriu o objetivo do desafio.

Para que servem os CTFs ?

e-Jornadas 2020

Competir, treinar e melhorar a capacidade de:

- ❑Análise de código
- ❑Análise de vulnerabilidades em sistemas
- ❑Técnicas de penetração em sistemas

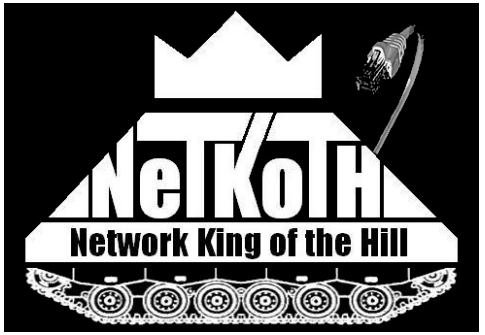
Tipos mais comuns de CTF

e-Jornadas 2020

Attack-Defence

Jeopardy-style

Network King of the Hill



Jeopardy Style

e-Jornadas 2020

- Focado em desafios tipo pergunta / resposta
- Normalmente abrange diversos temas tais como web-hacking, criptografia, reverse-engineering, steganography, forensics, etc.
- A instalação de plataformas para este tipo de desafios são de complexidade reduzida

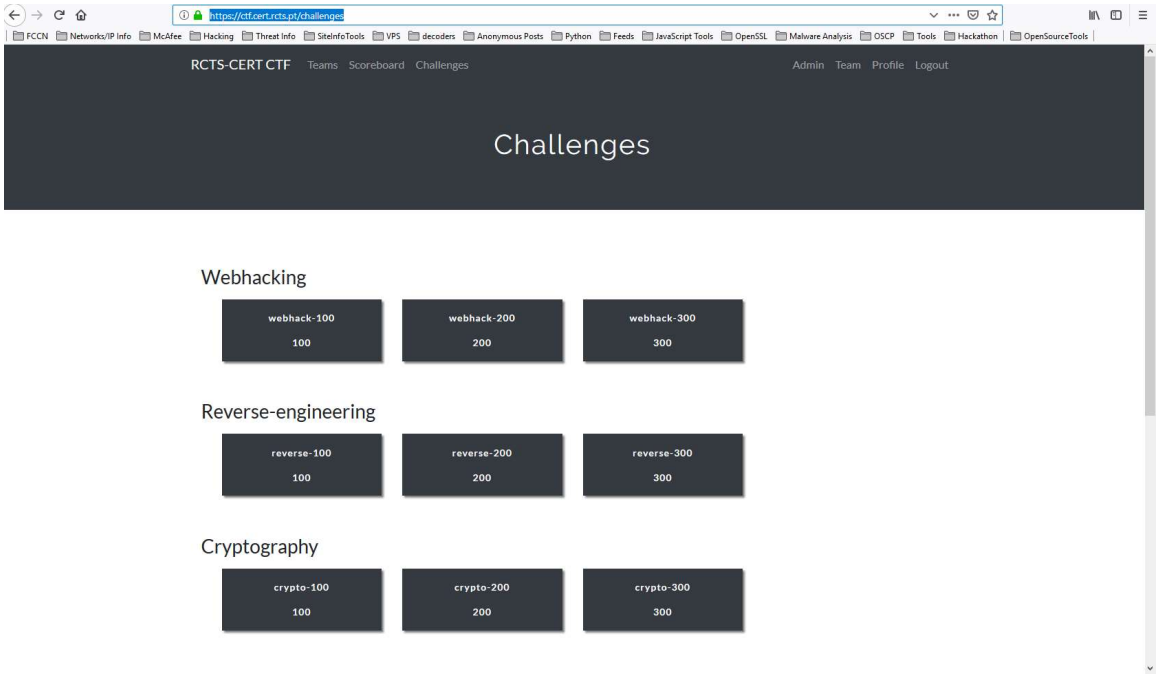
CHALLENGES

Binary	Forensics	Network	Pwnables	Web
BIN100	FOR100	NET100	PWN100	WEB100
BIN200	FOR200	NET200	PWN200	WEB200
BIN300	FOR300	NET300	PWN300	WEB300

Jeopardy Style

e-Jornadas 2020

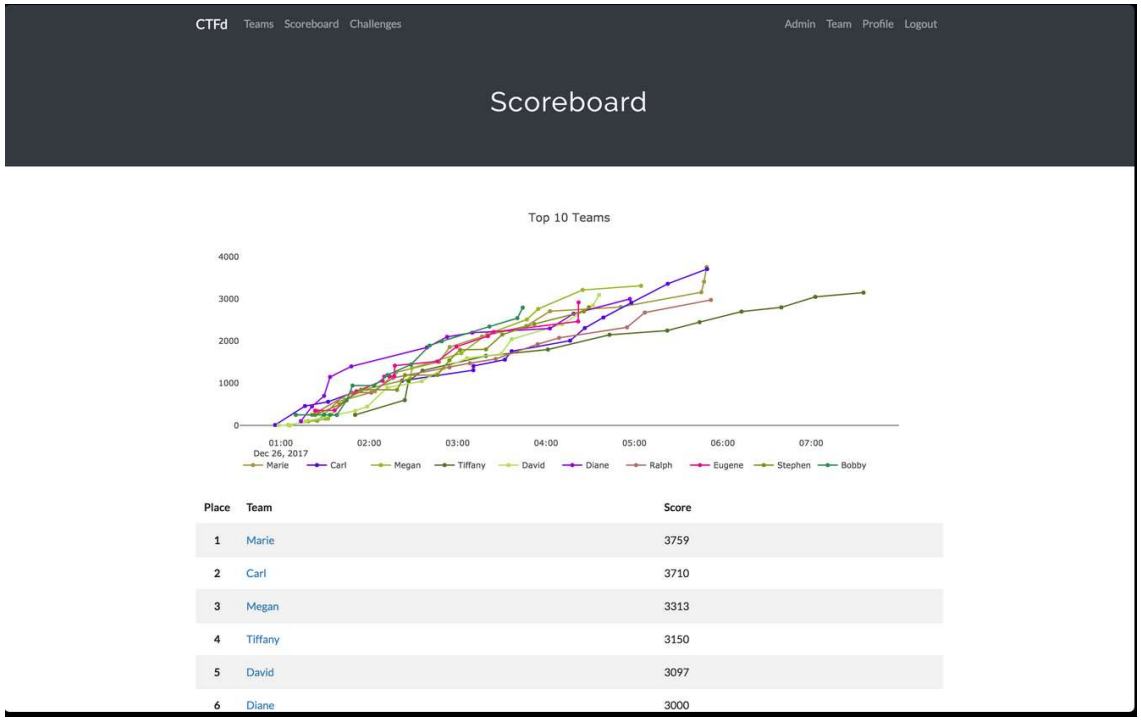
CTFd



Jeopardy Style

e-Jornadas 2020

CTFd

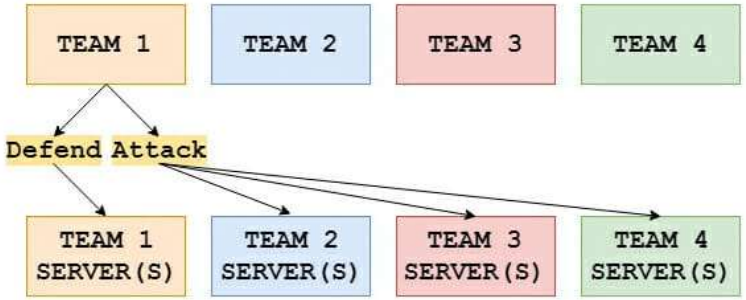


Place	Team	Score
1	Marie	3759
2	Carl	3710
3	Megan	3313
4	Tiffany	3150
5	David	3097
6	Diane	3000

Attack-Defence

e-Jornadas 2020

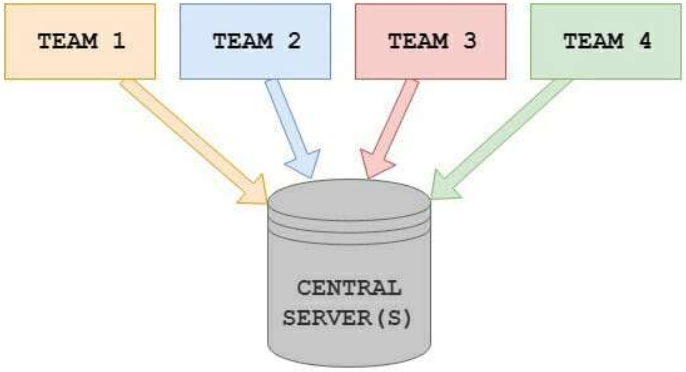
- A competição restringe-se a uma “Red Team” e uma “Blue Team”
- Red team tem como objetivo enumerar e explorar vulnerabilidades nos sistemas
- Blue team tem como objetivo mitigar ataques e corrigir vulnerabilidades
- Maior complexidade na elaboração deste tipo de desafios



Network King of the Hill (NetKotH)

e-Jornadas 2020

- Muito idêntico ao modo Attack-Defence
- A grande diferença é que quando um participante ganha acesso a uma máquina terá que mantê-lo e impedir os ataques das outras equipas



Plataformas OpenSource

- CTFd – Jeopardy style CTFs
- FBCTF – Plataforma para alojar CTF do Facebook
- Scorebot – Plataforma para CTFs usado no DEFCON (LegiBS)

https://github.com/apsdehal/awesome-ctf#awesome-ctf

Informações sobre CTFs

e-Jornadas 2020

- Resultados de competições
- Informações sobre competições a nível mundial
- Calendários

https://ctftime.org/ctfs

CTF Jornadas FCCN 2018

e-Jornadas 2020

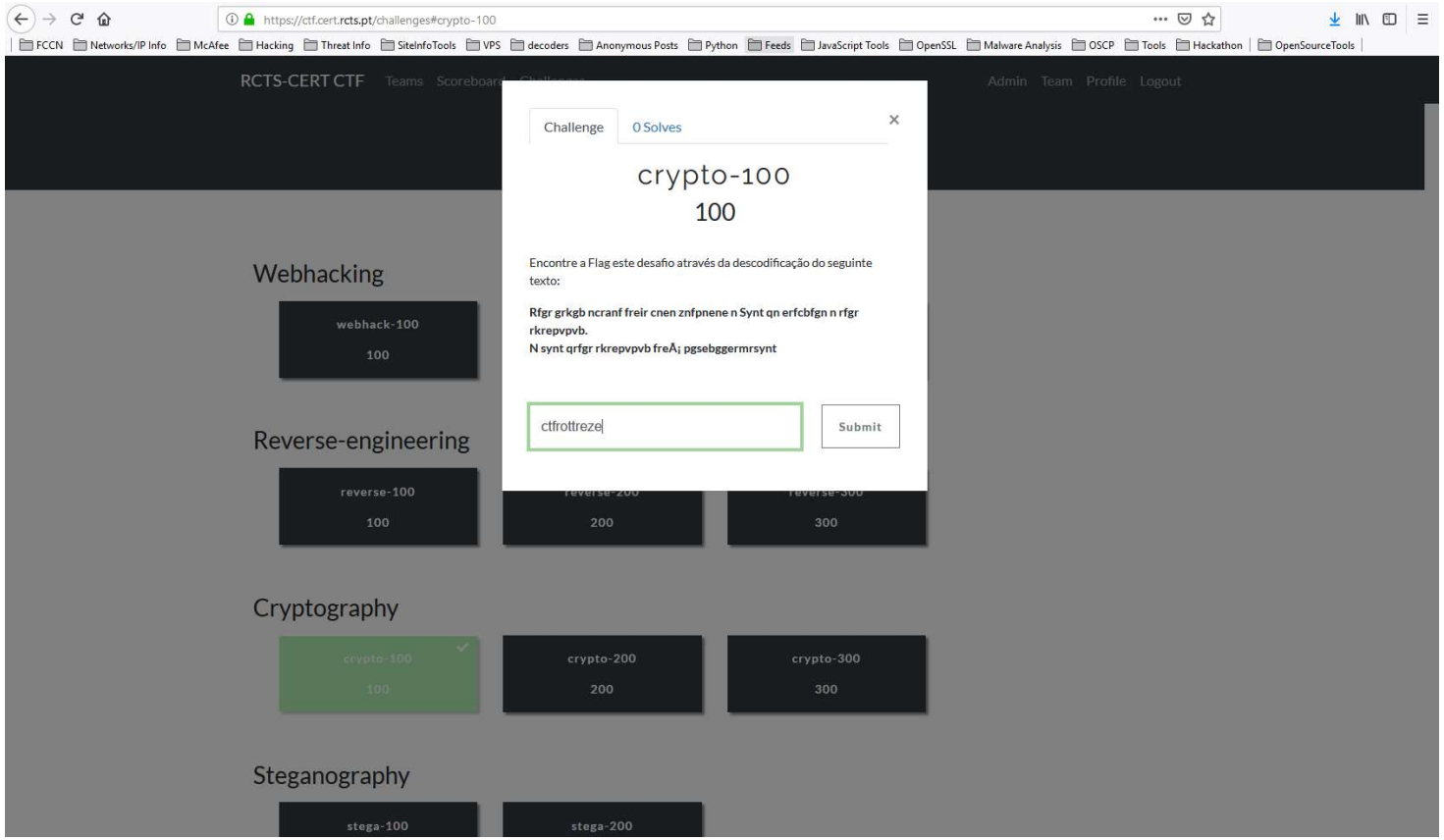
- 14 Exercícios

- Cryptography, Reverse, Forensics, Steganography, web hacking, wifi

Durante as Jornadas FCCN o RCTS CERT vai organizar um *CTF Challenge* (*Capture The Flag*), uma competição com vários desafios de segurança que os participantes terão que ultrapassar para chegarem ao fim.

CTF Jornadas FCCN 2018

e-Jornadas 2020



Summer 2020 RCTS CERT CTF

e-Jornadas 2020

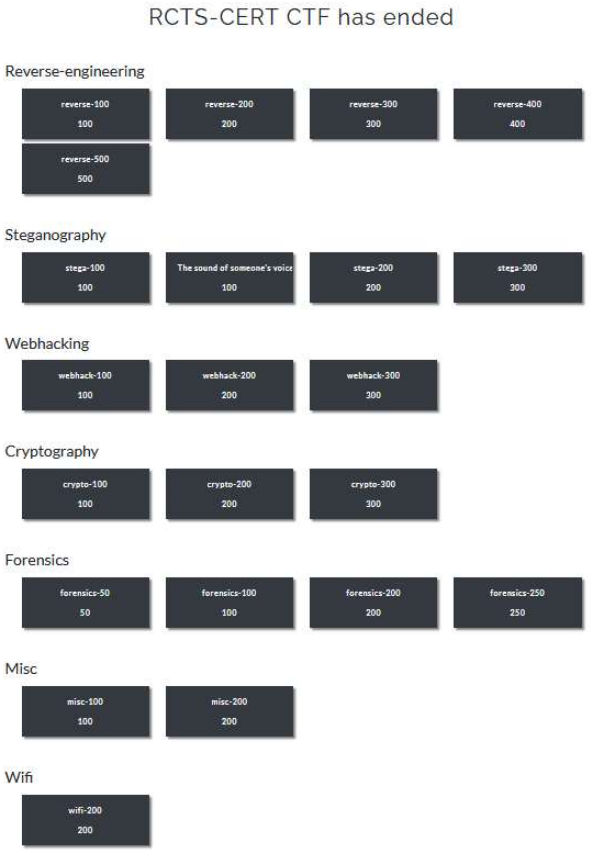
Summer 2020 RCTS CERT CTF

Summer 2020 RCTS CERT CTF

- 50 equipas registadas, mas apenas 27 pontuaram
- 22 Desafios
- Apenas 4 equipas completaram todos os desafios

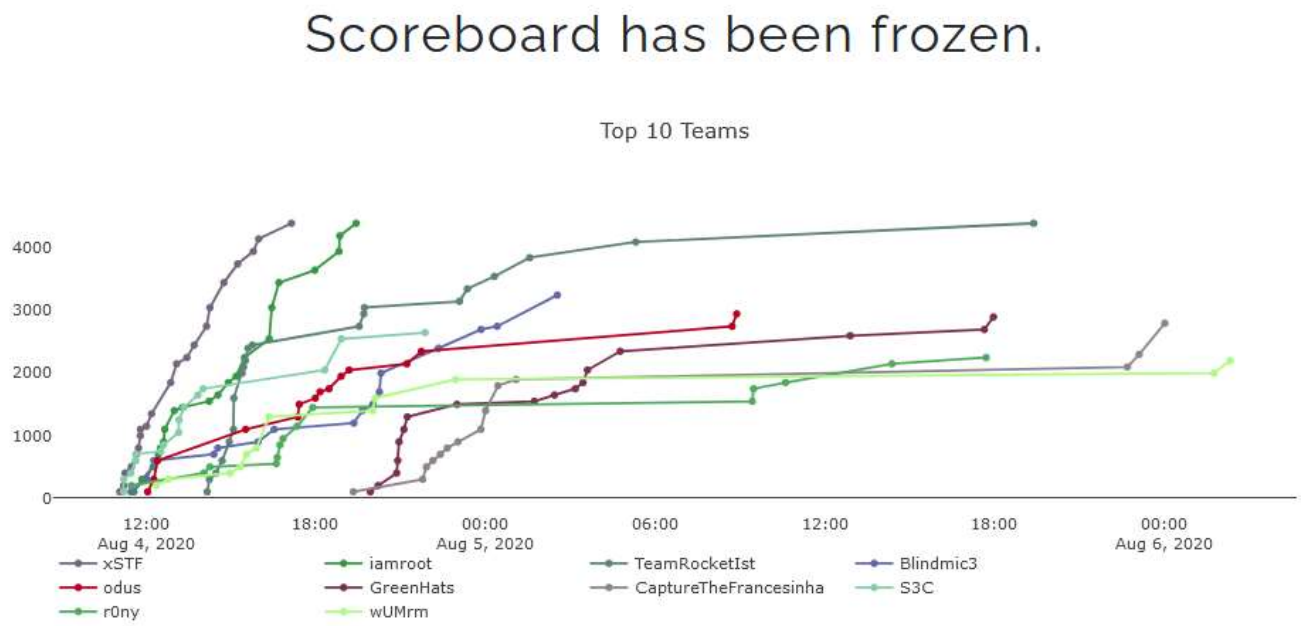
Summer 2020 RCTS CERT CTF

e-Jornadas 2020



Summer 2020 RCTS CERT CTF

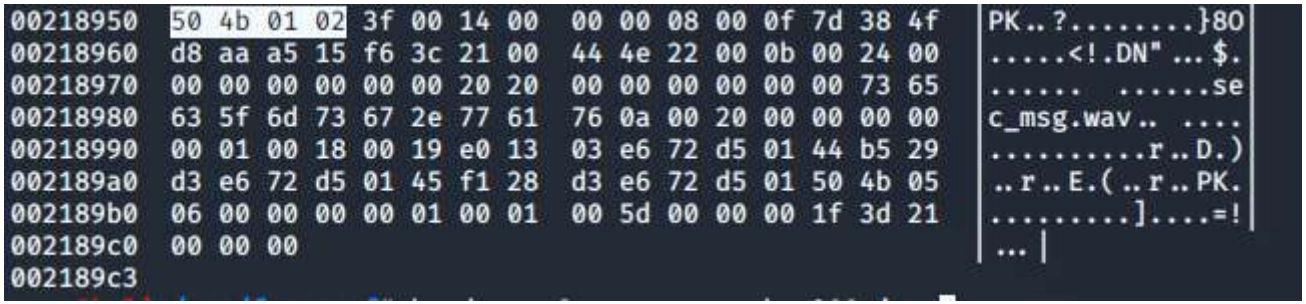
e-Jornadas 2020



Summer 2020 RCTS CERT CTF
Solução – Stega300

e-Jornadas 2020

- É fornecido um ficheiro JPG que contém a respetiva flag escondida
- O ficheiro JPG contém um ficheiro zip embebido, mas como o cabeçalho do zip está corrompido é mais difícil de identificar
- Fazendo um hexdump ao ficheiro, era possível confirmar a existência do ficheiro zip, tendo em conta a assinatura no final do ficheiro (50 4b 01 02)

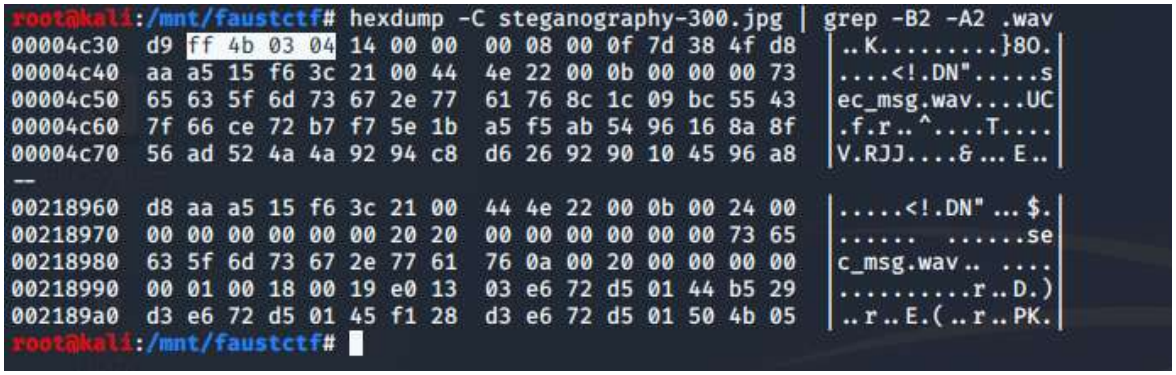


Summer 2020 RCTS CERT CTF
Solução – Stega300

e-Jornadas 2020

- Sabendo que os ficheiros zip normalmente contêm o nome dos ficheiros comprimidos no inicio e no fim do ficheiro, fazendo uma pesquisa por “sec_msg.wav” são encontradas duas localizações no ficheiro com este padrão, que neste caso indica o inicio do zip e o fim do zip

- Este informação foi obtida através do seguinte comando:
  “hexdump –C steganography-300.jpg | grep -B2 -A2 .wav



Summer 2020 RCTS CERT CTF
Solução – Stega300

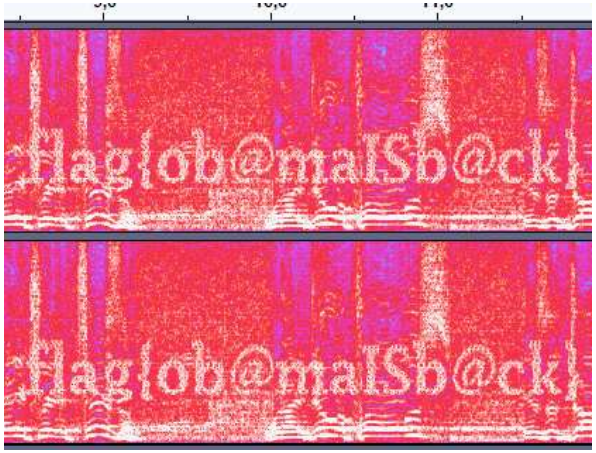
- Ao corrigir o header (“Alterar o byte FF para 50”) e excluindo o restante conteúdo que não pertence ao zip, era possível descomprimir conteúdo e obter o ficheiro “sec_msg.wav”

- A flag para este desafio encontra-se escondida no espectrograma do áudio, isto porque é possível converter imagens em ficheiros de áudio, sendo a imagem visível através do espectrograma. A ferramenta utilizada para fazer esta conversão chama-se “audacity” (https://www.audacityteam.org/)

Summer 2020 RCTS CERT CTF
Solução – Stega300

- Para visualizar a flag era necessário ver o espectrograma do áudio, através do audacity ou outra qualquer ferramenta que tenha esta funcionalidade.

FLAG: **flag{ob@maISb@ck}**



e-Jornadas
2020

e-Jornadas
2020

Thank You