Jornadas Computação Científica 2021

{CAPTURE THE FLAG}

João Machado

2021/10/21

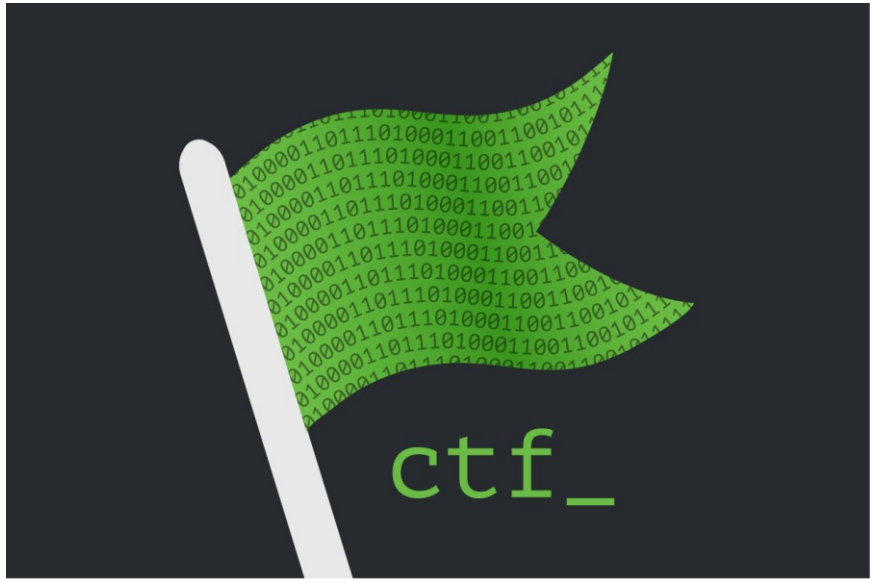
AGENDA

- O que é um CTF?
- Como criar um CTF?
- Exemplos de Exercícios

O QUE É UM CTF?

O QUE É UM CTF?

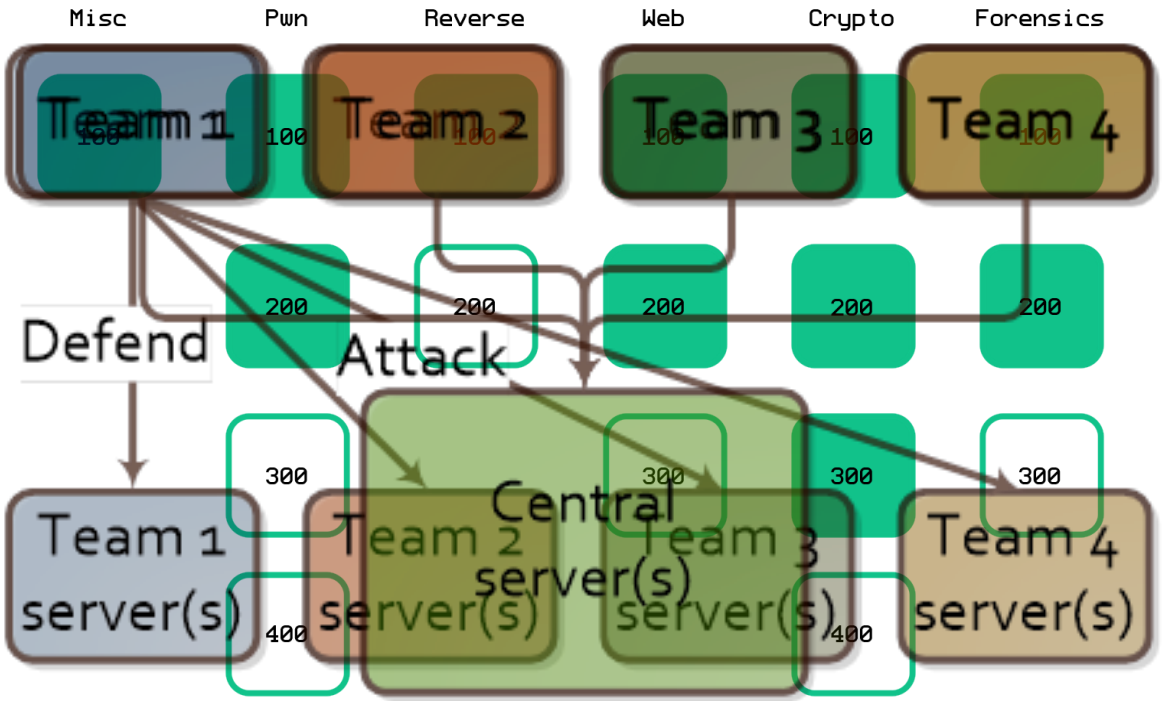
- É uma competição de Ciber-Segurança.
- Podem durar entre horas a vários dias.
- Atraem estudantes, entusiastas ou mesmo profissionais.
- Pontos são atribuídos com base em submissões de flags.



Flag{Th1s_1s_4_Fl4G}

TIPOS DE CTF

- Jeopardy
- Attack & Defense
- King of the Hill



QUAL O PROPÓSITO DE UM CTF?

- Ferramenta para treino.
- Team building e Soft Skills.
- Entender vulnerabilidades e respetivas correções.

PLATADORMAS DE CTF CONHECIDAS

- picoCTF (https://www.picoctf.org)
- Hack This site (https://www.hackthissite.org)
- HackTheBox (https://www.hackthebox.eu)
- VulnHub (https://www.vulnhub.com)
- TryHackMe (https://tryhackme.com)
- HackerOne (https://ctf.hacker101.com)
- Entre outros…

INFORMAÇÕES SOBRE CTFS

- Resultados de competições
- Informações sobre competições a nível mundial
- Calendários e próximos eventos
- Resoluções de exercícios de CTF anteriores
- Acessível em https://ctftime.org/

COMO CRIAR UM CTF?

COMO COMEÇAR?

- Participar frequentemente em desafios de CTF
- Ler Write-ups de exercícios e entender as vulnerabilidades
- Começar a criar exercícios!
- Usar frameworks para criar um CTF com os exercícios criados

FERRAMENTAS

Treino

- OWASP Juice Shop (https://owasp.org/www-project-juice-shop)
- Damn Vulnerable Web Application (DVWA) (https://dvwa.co.uk)
- picoCTF (https://github.com/picoCTF/picoCTF)

FERRAMENTAS

Criação de CTFs

- Facebook's CTF Framework (https://github.com/facebookarchive/fbctf)
- picoCTF (https://github.com/picoCTF/picoCTF)
- SecGen (https://github.com/cliffe/SecGen)
- CTFd (https://ctfd.io)

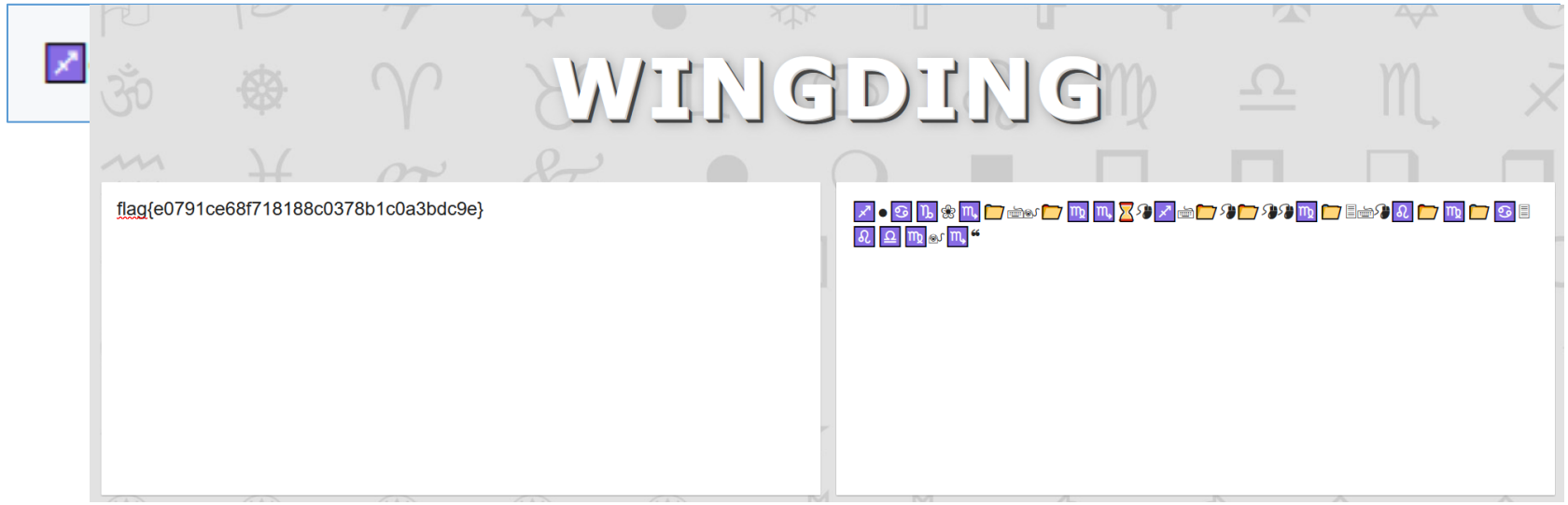
CUIDADOS A TER

- Regras específicas em ambientes Cloud
- Evitar colocar sistemas vulneráveis expostos à internet
- Definir sempre o contexto e as regras especificas do CTF.

EXEMPLOS DE EXERCÍCIOS

EXERCÍCIOS

- Nahamcon2021 – ChickenWings (Cryptography)

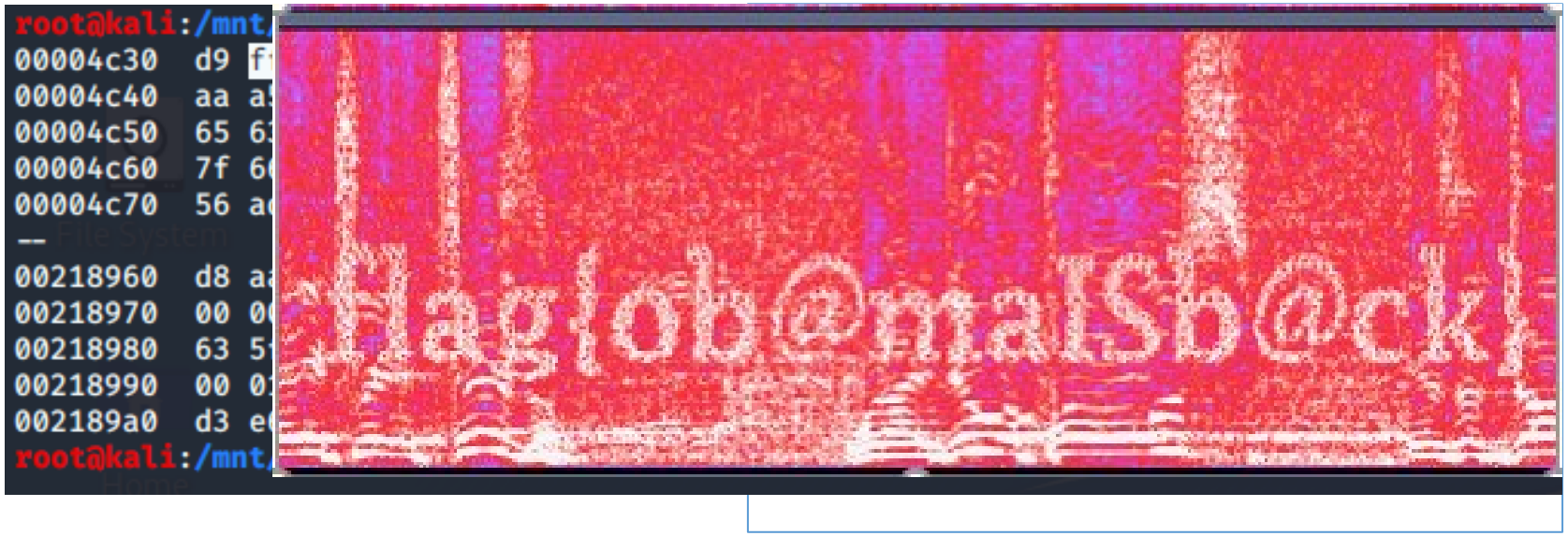


EXERCÍCIOS

- Cyber Apocalypse 2021 – Nintendo Base64 (Cryptography)

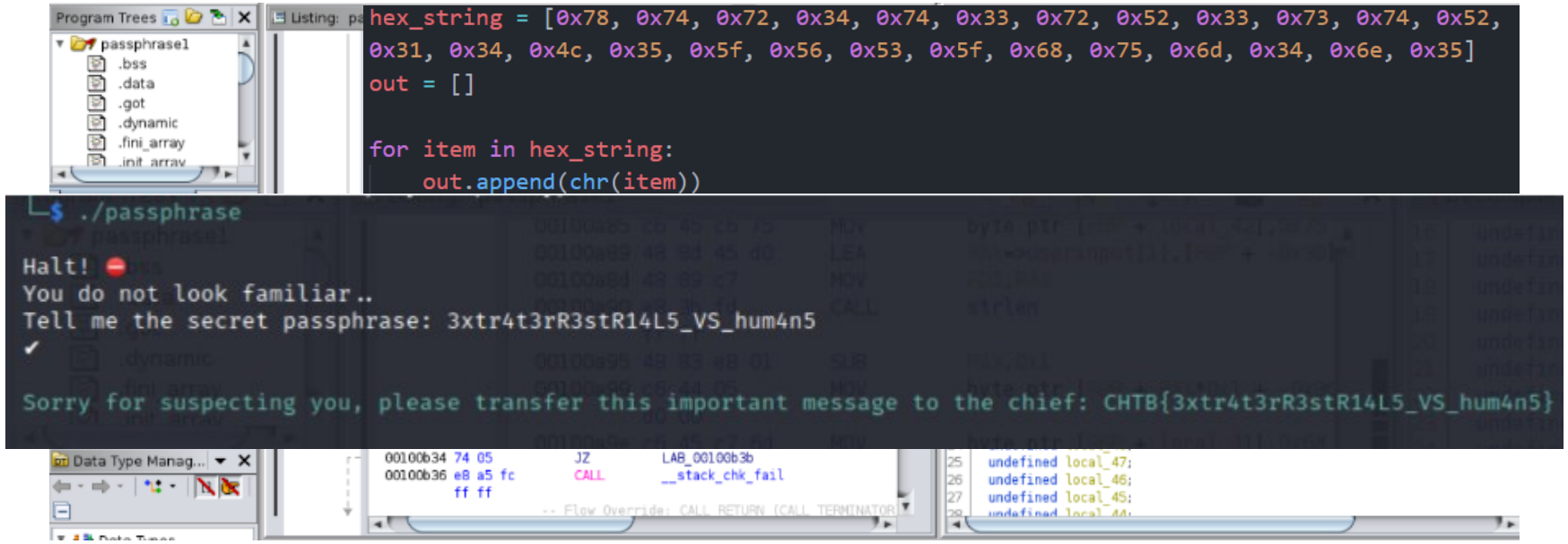
EXERCÍCIOS

- Summer 2020 RCTS CERT CTF – Stega 300 (Forensics)



EXERCÍCIOS

- Cyber Apocalypse 2021 – Passphrase (Reverse)



EXERCÍCIOS

- RCTS_CERT CTF 2021 - Well Hello there (Pwn)

```
┌──(jmachado㉿kali)-[~/Desktop/RCTS_CERT_CTF_2021]
└─$ ./program
Hello there! What is your name?
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
flag{buff3r_0v3rfl0w_r0cks}
```

```
mov     edi, 0Ah
call    _putchar
mov     eax, 0
add     rsp, 58h
retn
```

```
call    _gets
mov     eax, [rsp+58h+var_C]
test    eax, eax
jnz     short loc_11E1
```

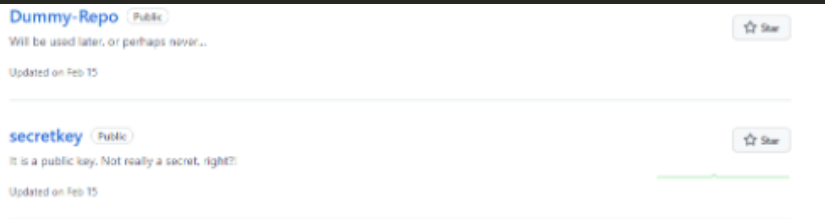
EXERCÍCIOS

- TMUCTF 2021 - Foreign Student (OSINT)

```
└─$ curl https://raw.githubusercontent.com/ZedZini/secretkey/main/0xEB0B6528-pub.asc | gpg --import
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
  0     0    0     0    0     0      0      0 --:--:-- --:--:--100  6139  100  6139    0     0  19488      0 --:--:-- --:--:--100  6139  100  6139
    0     0  19488      0 --:--:-- --:--:-- --:--:-- 19427
gpg: key 586DD615EB0B6528: public key "Zedmondo Zaberini (Nothing to say...) <Z3dm0nd0_Z4b3r1n5k1_15_My_R34l_N4m3@zaberini.com>" imported
gpg: Total number processed: 1
gpg:               imported: 1
```

flag{Z3dm0nd0_Z4b3r1n5k1_15_My_R34l_N4m3@zaberini.com}

```
SzChR0Jt3vI7BjA3WVlxQp94XTqRqFrjtJkS2I3nO3I94jhLu0AwfoiskKzyl+tQ
lexhE31arP/MEYV9VfPSxqR23rm+shIdeKP+9G9XR3Z1rpO0+1P78o7uvRG/7oPR
POw6CAh0eXLpM3P18irvjnH3VekSOg9a/d/7hhyVkRtsH4vAd8O38Z3QB2dWWs5J
... cut ...
=oo5F
-----END PGP PUBLIC KEY BLOCK-----
```



EM RESUMO

- ✓ Os desafios CTF podem ser usados para treino.
- ✓ A criação de um CTF pode ser usado para demonstrar vulnerabilidades.
- ✓ Podem ser usadas como ferramentas de team building e de melhoria de soft e hard skills.

Obrigado