

FCT

Fundação para a Ciência e a Tecnologia
MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E ENSINO SUPERIOR

FCCN

Computação
Científica Nacional

{CAPTURE THE FLAG}

João Machado



Agenda

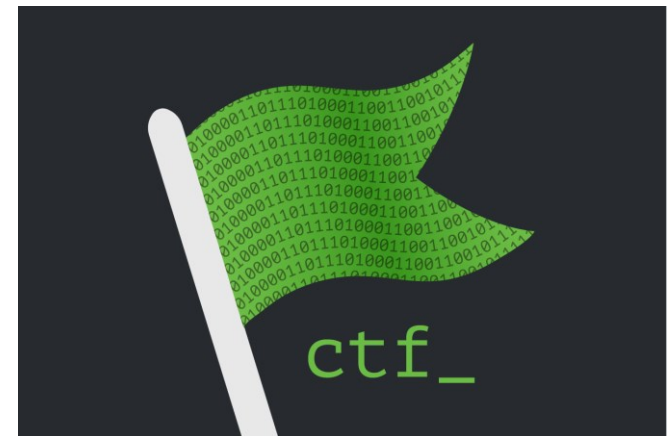
- O que é um CTF?
- Como criar um CTF?
- Exemplos de Exercícios



O QUE É UM CTF?

O que é um ctf?

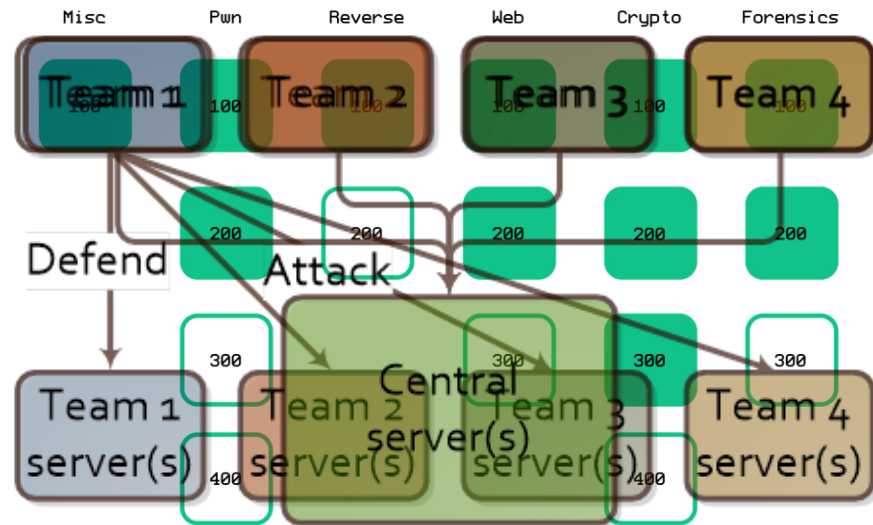
- É uma competição de Ciber-Segurança.
- Podem durar entre horas a vários dias.
- Atraem estudantes, entusiastas ou mesmo profissionais.
- Pontos são atribuídos com base em submissões de flags.



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 respectivas correções.



Plataformas 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 de desafios de CTF

- 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

LET'S GET
STARTED



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 específicas do CTF.



EXEMPLOS DE EXERCÍCIOS

Exercícios

- Nahamcon2021 – ChickenWings (Cryptography)



Exercícios

- Cyber Apocalypse 2021 – Nintendo Base64 (Cryptography)

```
Input                                                                    length: 1005
                                                                           lines: 9
Vm          0w          eESGbFdWw          GhT          V0d4VvYwZ
G9          XV          mx          yWk          ZOv          BaV          WRH
          YW          xa          c1          Nswl dS          M1          JQ wV          d4
S2RHHVkljRm Rp UjJoMlZrZH p1RmRHV m5WaV3tU1 hUVEZLZVZk V1VrZFpWmu pHVDFaV1Z tSkdXazlXYW twd1 Yx Wm Fj bHBfVmxwT1Z
Xdz Bwa 2M xVT FSc 1d uTl hi R2h XwW taS 1dG VXh Xbu ZTT VdS elYy cz FwM kY2VmtwV2
JU RX dZ ak Zr U0 ZOc2JGwm1S a3 BY V1 d0 YV 1V MH hj RVpYYlVaVFRWw mF 1V mt 3V
lR GV 01 ER kh Zak 5rVj JFe VR Ya Fdha 3BIV mpGU 2NtR kdx bWx oT TB KW VYxW lNSM
Wx XW kV kV mJ Gw1RZ bXmxY2xWc 1V sZ FRiR1J5VjJ 0a1YySkdj RVpWVmxKV 1V GRT1QUT09

Output                                                                    time: 13ms
                                                                           length: 38
                                                                           lines: 1
CHTB{3nc0d1ng_n0t_3qu41_t0_3ncrypt10n}
```

Exercícios

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



Exercícios

- Cyber Apocalypse 2021 – Passphrase (Reverse)

The screenshot displays a reverse engineering tool interface with three main panels:

- Program Trees:** Shows the file structure of the binary, including sections like .bss, .data, .got, .dynamic, .fini_array, and .init_array.
- Listing:** Displays the assembly code for the `passphrase` function. The code defines a `hex_string` array of 20 hexadecimal values and iterates through them to build an output string `out`.
- Debugger Console:** Shows the execution of the program. The user is prompted with "You do not look familiar.." and "Tell me the secret passphrase:". The input "3xtr4t3rR3stR14L5_VS_hum4n5" is entered, and the program responds with "Sorry for suspecting you, please transfer this important message to the chief: CHTB{3xtr4t3rR3stR14L5_VS_hum4n5}".

Below the console, the **Data Type Manager** and **Flow Graph** are visible, showing the program's control flow and variable declarations.

Exercícios

- RCTS_CERT CTF 2021 - Well Hello there (Pwn)

```
(jmachado@kali) - [~/Desktop/RCTS_CERT_CTF_2021]
$ ./program
Hello there! What is your name?
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
flag{buff3r_0v3rfl0w_r0cks}

loc_11E0:
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)

```
L$ curl https://raw.githubusercontent.com/ZedZini/secretkey/main/0xE0B6528-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  0  0  0  0  0  0  0  0  0  0  0  0  0
  0     0 19488    0     0     0     0      0  0  0  0  0  0  0  0  0  0  0  0  0
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}

```
SzChR0Jt3vI7BjA3wV1xQp94XTqRqFrjtJkS2I3n03I94jhLu0AwFoiskKzyl+tQ
lexhE31arP/MEYV9VfPSxqR23rm+shIdeKP+9G9XR3Z1rp00+1P78o7uvRG/7oPR
POw6CAh0eXLP3P18irvjnH3VekS0g9a/d/7hhyVkRtsH4vAd8038Z3QB2dWws5J
... cut ...
=0o5F
-----END PGP PUBLIC KEY BLOCK-----
```

Dummy-Repo Public

Will be used later, or perhaps never...

Updated on Feb 15

secretkey Public

It is a public key. Not really a secret, right?

Updated on Feb 15

Exemplos de exercícios de CTF

- InCTF 2021 - Listen (Network)

Maecenas vel ante ex. Ut rutrum mi ullamcorper eros facilisis rhoncus. Quisque tortor metus, aliquam in ligula et, tempor placerat eros. Maecenas eget commodo lorem. Quisque v elit nisi, pretium vitae tempor non, molestie ac risus. Nam vehicula, leo a vestibulum ornare, orci tellus mattis est, eget viverra lorem purus ut purus. Pellentesque venenati s blandit augue id bibendum. Nulla facilisi. Nunc finibus neque libero, sed placerat mi ultrices et. Mauris cursus pellentesque molestie. Nullam sed ligula libero. Nulla ex se m, lacinia quis sem nec, rhoncus consequat nibh. Nunc maximus magna neque, vel pulvinar elit blandit nec. `inctf{s0_y0u_finally_d3cid3d_t0_listen!!}` Lorem ipsum dolor sit amet, consectetur adipiscing elit. Duis molestie sapien ac tortor sodales malesuada. Suspendisse efficitur rhoncus massa, a eleifend sapien porttitor semper. Sed ac cursus quam, ornare aliquam ipsum. Aenean ut urna pret

pit nisl posuere quis. Proin facilisis justo metus, eu congue ex ultricies auctor. Aenean consectetur enim nec leo vehicula pellentesque. In ut sollicitudin est. Aliquam erat volutpat. Praesent cursus sem eget sapien sagittis, non hendrerit ex vehicula. Quisque malesuada, lectus in dignissim tincidunt, mi erat tristique eros, et consectetur tortor

volutpat. Praesent cursus sem eget sapien sagittis, non hendrerit ex venenata. Quisque malesuada, lectus in dignissim tincidunt, mi erat tristique eros, et consectetur tortor metus sed est. Ut vestibulum eget odio facilisis fringilla. Donec dolor neque, rhoncus laoreet sem vitae, bibendum congue nibh.								ACK=1 win=64256 len=1313 rsv=1286000
172.30.0.14	31690	128	8,192	64	3,456	64	4,736	
172.30.0.14	31491	128	8,192	64	3,456	64	4,736	
172.30.0.14	31769	132	8,448	66	3,564	66	4,884	
172.30.0.14	32286	132	8,448	66	3,564	66	4,884	
172.30.0.14	32062	136	8,704	68	3,672	68	5,032	
172.30.0.14	31394	136	8,704	68	3,672	68	5,032	
172.30.0.14	31683	136	8,704	68	3,672	68	5,032	
172.30.0.14	32194	138	8,832	69	3,726	69	5,106	
172.30.0.14	32097	140	8,960	70	3,780	70	5,180	
172.30.0.14	31336	70,810	4,551 k	35,402	1,911 k	35,408	2,639 k	
172.30.0.14	31337	71,422	4,584 k	35,709	1,928 k	35,713	2,655 k	

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