Introdução a *Capture The Flags* (CTFs) em Cibersegurança

Gabriel B. Sant'Anna
Egresso de CCO @ UFSC
Software / Firmware Dev. @ BRy Tecnologia
https://**baioc.github.io**/seccom-ctf/slides.pdf

DISCLAIMER

Toda a exposição de conteúdo nesta apresentação é feita de forma voluntária e **não implica na sua aprovação por outras entidades** (UFSC, BRy, etc).

Demonstrações serão realizadas **para fins exclusivamente educacionais**. **Replicar esses procedimentos em sistemas de terceiros pode ser ilegal** (vide artigos 154-A e 154-B do Código Penal).

Não existem garantias associadas aos procedimentos demonstrados. **O autor não será responsabilizado** por qualquer dano originado deles.

01 **Cybersec.**

Contexto nacional e internacional, *Ethical (white hat) Hacking*

02 **CTFs**

No contexto de cibersegurança

03 **Demonstração**

Sim, pode interromper e fazer perguntas

04 **Encerramento**

Recursos para continuar aprendendo

Cibersegurança

Kelly et al. 2021 (DOI: 10.3390/s21072433)

- Servidor web na nuvem
- *Honeypot* ativo por 3 semanas

Cibersegurança

Kelly et al. 2021 (DOI: 10.3390/s21072433)

- Servidor web na nuvem
- *Honeypot* ativo por 3 semanas
- Centenas de milhares de tentativas de invasão

Cibersegurança

- Vulnerabilidade na implementação do SMB da Microsoft
- NSA desenvolve o exploit *EternalBlue* em ~2012

WannaCry (src: securelist.com)

Cibersegurança

- Vulnerabilidade na implementação do SMB da Microsoft
- NSA desenvolve o exploit *EternalBlue* em ~2012
- Exploit foi vazado por hackers em 2017
- Ransomware Worm WannaCry afeta ~300k PCs

WannaCry (src: securelist.com)

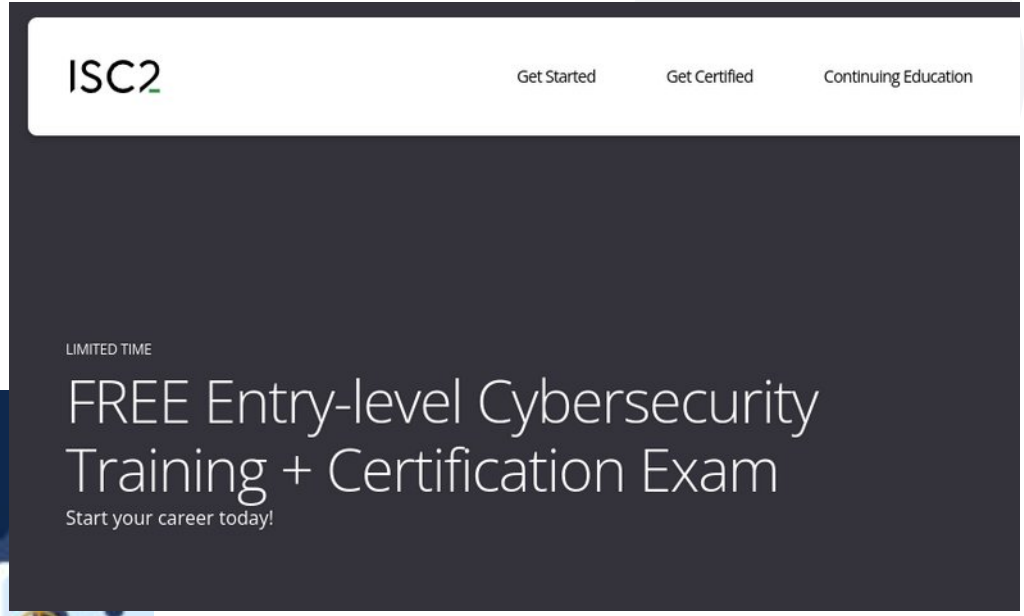
Cibersegurança

- Janeiro de 2021: dados de ~223 milhões de brasileiros sendo vendidos na Deep Web
- Fevereiro de 2021: ~102 milhões de números de telefone vazados

Vazamento “Serasa Experian” (src: tecnoblog.net)

80h de conteúdo + certificados digitais

Treinamento + exame
Pearson de U$199

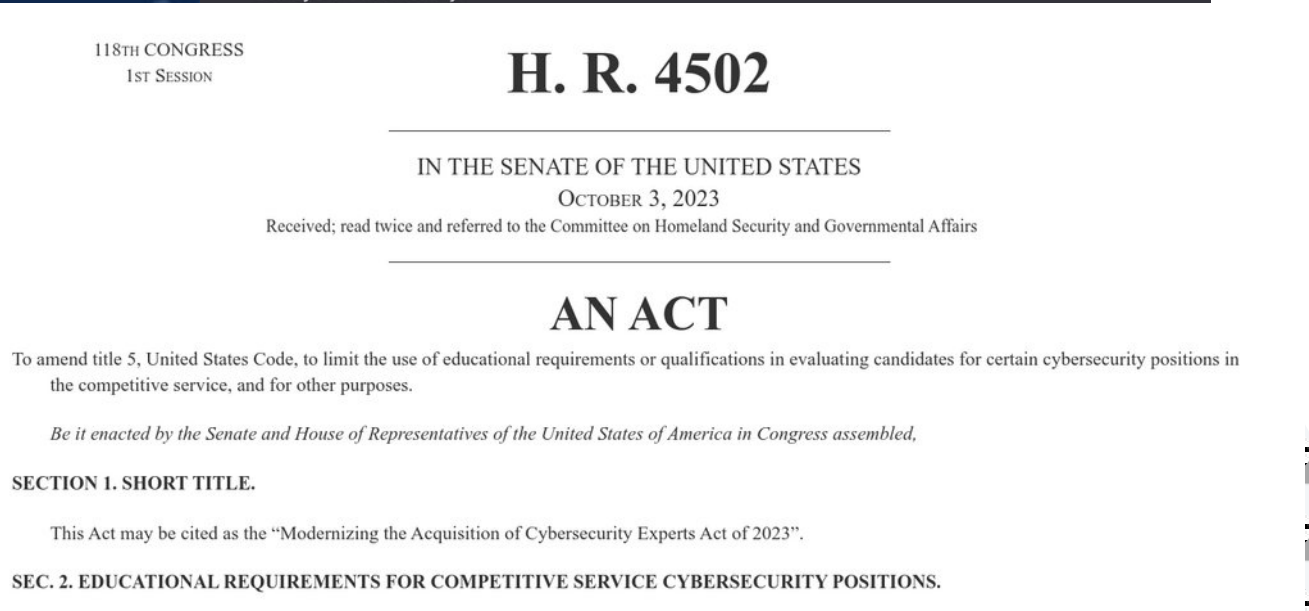


80h de conteúdo + certificados digitais

Treinamento + exame
Pearson de U$199

80h de conteúdo + certificados digitais

Senado americano reduz requisitos de formação para vagas em cybersec.



118TH CONGRESS
1ST SESSION

H. R. 4502

IN THE SENATE OF THE UNITED STATES
OCTOBER 3, 2023
Received; read twice and referred to the Committee on Homeland Security and Governmental Affairs

AN ACT

To amend title 5, United States Code, to limit the use of educational requirements or qualifications in evaluating candidates for certain cybersecurity positions in the competitive service, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

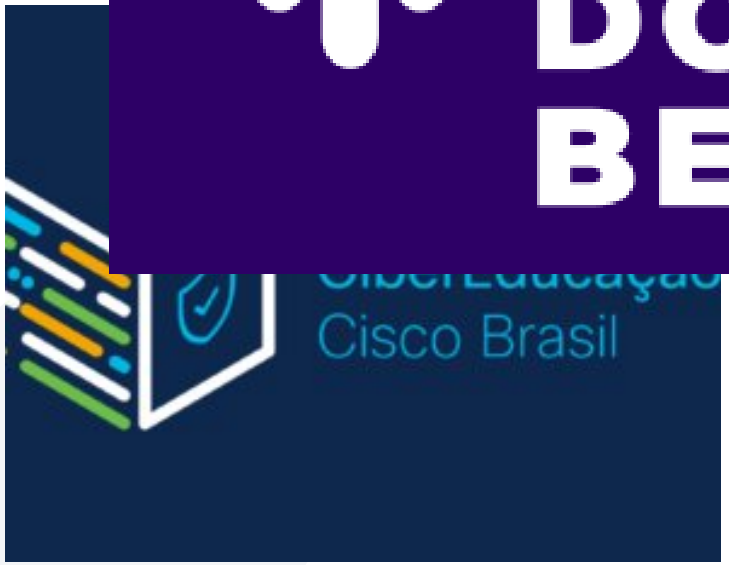
SECTION 1. SHORT TITLE.

This Act may be cited as the "Modernizing the Acquisition of Cybersecurity Experts Act of 2023".

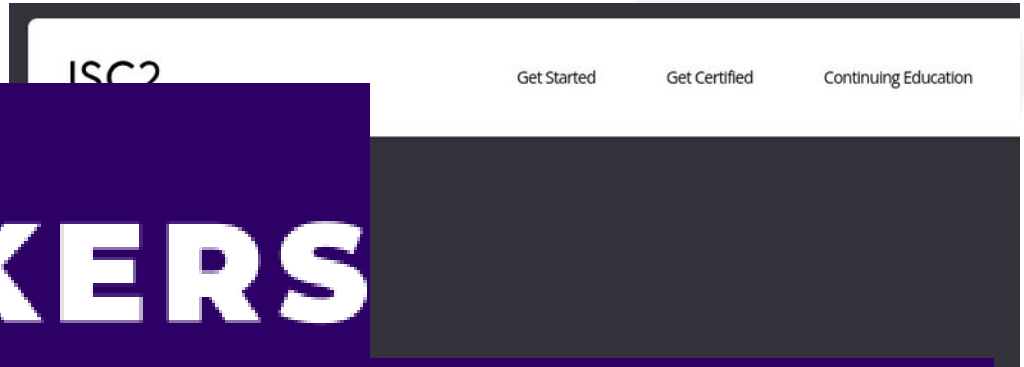
SEC. 2. EDUCATIONAL REQUIREMENTS FOR COMPETITIVE SERVICE CYBERSECURITY POSITIONS.

Treinamento + exame

80h



Senado americano reduz requisitos de formação para vagas em cybersec.



HACKERS DO BEM

R$ 32,6 milhões alocados pelo Ministério da Ciência, Tecnologia e Inovação

R. 4502

IN THE SENATE OF THE UNITED STATES

OCTOBER 3, 2023

Received; read twice and referred to the Committee on Homeland Security and Governmental Affairs

AN ACT

To amend title 5, United States Code, to limit the use of educational requirements or qualifications in evaluating candidates for certain cybersecurity positions in the competitive service, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "Modernizing the Acquisition of Cybersecurity Experts Act of 2023".

SEC. 2. EDUCATIONAL REQUIREMENTS FOR COMPETITIVE SERVICE CYBERSECURITY POSITIONS.

Tipos de “Hackers”

White Hat

Gray Hat

Black Hat

Tipos de “Hackers”

White Hat

Gray Hat

Black Hat

- *Script kiddies*
- Crime organizado
- Ciber-espionagem
- Ataques militares

Tipos de “Hackers”

White Hat

Gray Hat

- Pesquisadores independentes
- *Hacktivists*

Black Hat

- *Script kiddies*
- Crime organizado
- Ciber-espionagem
- Ataques militares

Tipos de “Hackers”

White Hat

- Grupos de pesquisa
- *Penetration testers*
- *Bounty hunters*

Gray Hat

- Pesquisadores independentes
- *Hacktivists*

Black Hat

- *Script kiddies*
- Crime organizado
- Ciber-espionagem
- Ataques militares

Tipos de “Hackers”

White Hat

- Grupos de pes
- *Penetration test*
- *Bounty hunters*

Black Hat

- *pt kiddies*
- me organizado
- Ciber-espionagem
- Ataques militares

Capture The Flag (CTF)

"Captura à Bandeira"

> Jogo ou esporte onde cada time possui uma bandeira e o objetivo é capturar a bandeira do outro time.
>
> Variantes incluem o CTF assimétrico (time ofensivo contra time defensivo) e jogos com múltiplas bandeiras.

CTFs em cybersec.

Assimétrico
red team vs *blue team*

CTFs em cybersec.

Assimétrico
red team vs *blue team*

Try Hack Me

CTFd

Treinamento em cybersec.
“gamificado”

HACKTHEBOX

CTF TIME

CTFs em cybersec.

Assimétrico
red team vs *blue team*

Try Hack Me

CTFd

Treinamento em cybersec.
“gamificado”

HACKTHEBOX

duolingo

CTFTIME

Categorias de CTF do HTB

Web

Enumeração de portas e serviços, identificação e exploração de vulnerabilidades em aplicações web

Cloud

Invasão e esclação de privilégios em serviços na nuvem

Crypto

Quebrar algoritmos de criptografia com implementações ou parâmetros vulneráveis

Pwn

Análise dinâmica de executáveis, seguida de exploração das suas vulnerabilidades lógicas e/ou físicas

Forensic

Investigação de logs, imagens de disco ou outros artefatos para identificar eventos ou descobrir informações escondidas

Reverse

Aplicação de engenharia reversa em programas, dados e processos

Fullpwn

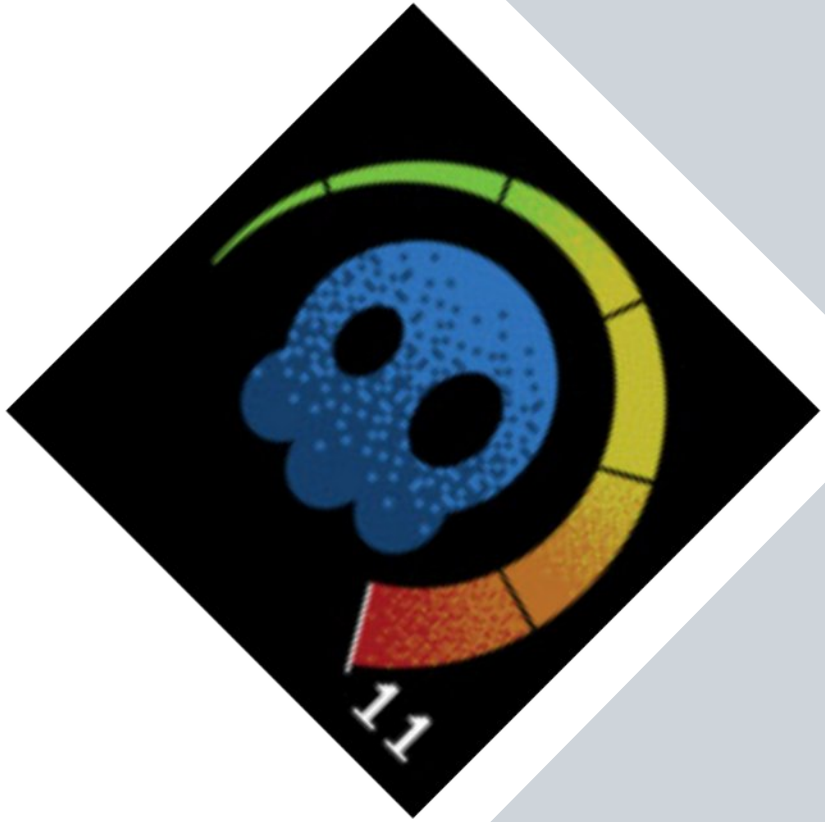
“Ataque completo” com enumeração, identificação de vulnerabilidades, exploração inicial para acesso remoto, pivoteamento e escalação de privilégios

Hardware

Análise e aplicação de métodos de ataque em objetos e mecanismos do dia a dia

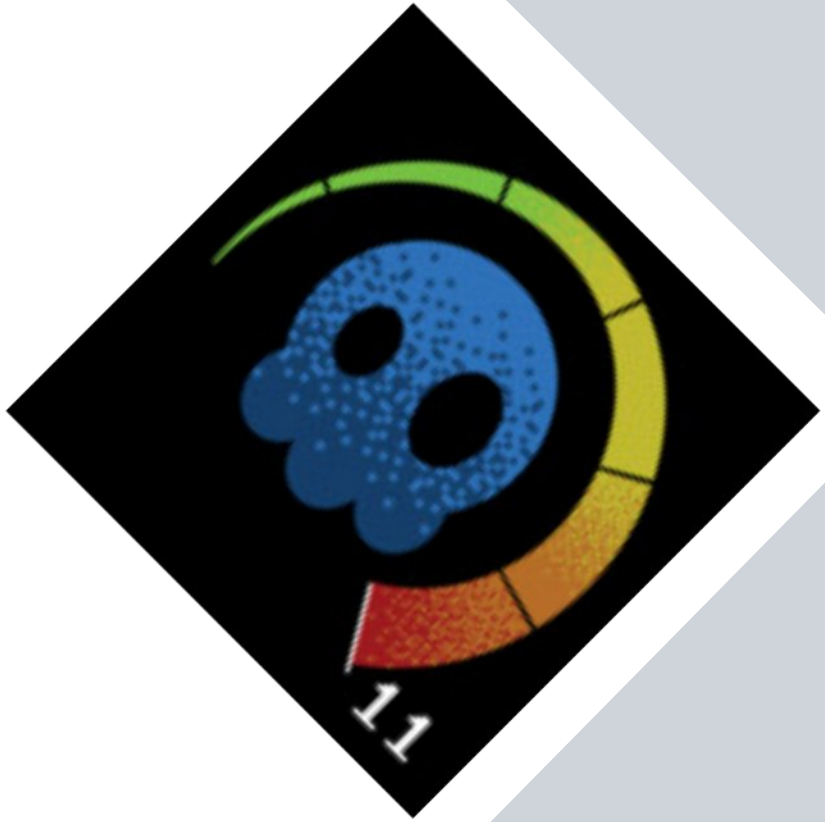
Exemplo de CTF: Prova de Cybersec. na *Université Grenoble Alpes*

- Laboratório de informática
- VM Kali Linux
- Um pacote ZIP por aluno



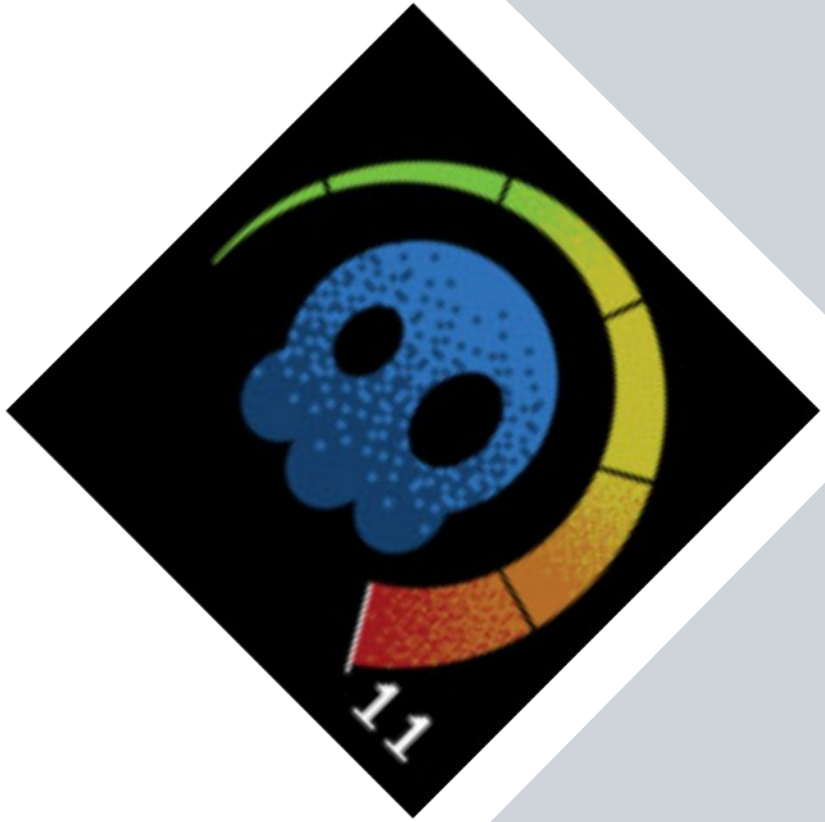
Exemplo de CTF: Prova de Cybersec. na *Université Grenoble Alpes*

- Laboratório de informática
- VM Kali Linux
- Um pacote ZIP por aluno
- 6 *flags* escondidas no pacote
- 4 horas de prova
- Objetivo: provar que encontrou suas flags



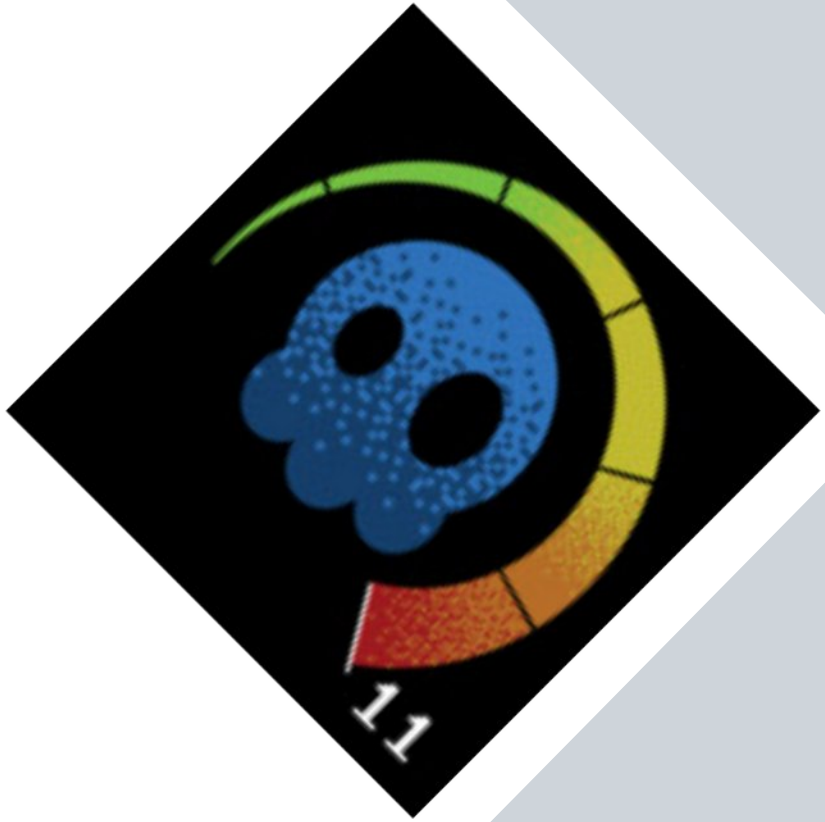
Exemplo de CTF: Prova de Cybersec. na *Université Grenoble Alpes*

- Laboratório de informática
- VM Kali Linux
- Um pacote ZIP por aluno
- 6 *flags* escondidas no pacote
- 4 horas de prova
- Objetivo: provar que encontrou suas flags
  - Primeiros 5 alunos a capturar as 6 flags = 100%
  - Próximos 5 alunos a capturar as 6 flags = 95%
  - Idem para 90% e 85%
  - 5 ou mais flags = 80% da nota
  - 3 ou mais flags = 50% da nota
  - <3 flags = recuperação



Exemplo de CTF: Prova de Cybersec. na *Université Grenoble Alpes*

- Laboratório de informática
- VM Kali Linux
- Um pacote ZIP por aluno
- 6 *flags* escondidas no pacote
- 4 horas de prova
- Objetivo: provar que encontrou suas flags
  - Primeiros 5 alunos a capturar as 6 flags = 100%
  - **Próximos 5 alunos a capturar as 6 flags = 95%**
  - Idem para 90% e 85%
  - 5 ou mais flags = 80% da nota
  - 3 ou mais flags = 50% da nota
  - <3 flags = recuperação



Forensic

Investigação de logs, imagens de disco ou outros artefatos para identificar eventos ou descobrir informações escondidas

Crypto

Quebrar algoritmos de criptografia com implementações ou parâmetros vulneráveis

Web

~~Enumeração de portas e serviços, identificação e exploração de vulnerabilidades em aplicações~~ web

Crypto

Quebrar algoritmos de criptografia com implementações ou parâmetros vulneráveis

Forensic

Investigação de logs, imagens de disco ou outros artefatos para identificar eventos ou descobrir informações escondidas

Reverse

Aplicação de engenharia reversa em programas, dados e processos

CTF de Demonstração na SECCOM 2023

- Formato das **flags**: `/cco{\w+}/`

```
<Flag> ::= 'cco' '{' <w> <Wp> '}'
<w>    ::= [a-z] | [A-Z] | [0-9] | '_'
<Wp>   ::= ε | <w> <Wp>
```

- Exemplo: **`cco{example_flag0}`**

CTF de Demonstração na SECCOM 2023

- Formato das **flags**: `/cco{\w+}/`

```
<Flag> ::= 'cco' '{' <w> <Wp> '}'
<w>    ::= [a-z] | [A-Z] | [0-9] | '_'
<Wp>   ::= ε | <w> <Wp>
```

- Exemplo: **`cco{example_flag0}`**

- **ATENÇÃO**: não tente atacar servidores ou outra infraestrutura digital. Esse CTF será conduzido de forma majoritariamente **offline**. Dar continuidade ao CTF na web requer apenas **OSINT**.

CTF de Demonstração na SECCOM 2023

- Formato das **flags**: `/cco{\w+}/`

```
<Flag> ::= 'cco' '{' <w> <Wp> '}'
<w>    ::= [a-z] | [A-Z] | [0-9] | '_'
<Wp>   ::= ε | <w> <Wp>
```

- Exemplo: **`cco{example_flag0}`**

- **ATENÇÃO**: não tente atacar servidores ou outra infraestrutura digital. Esse CTF será conduzido de forma majoritariamente **offline**. Dar continuidade ao CTF na web requer apenas **OSINT**.

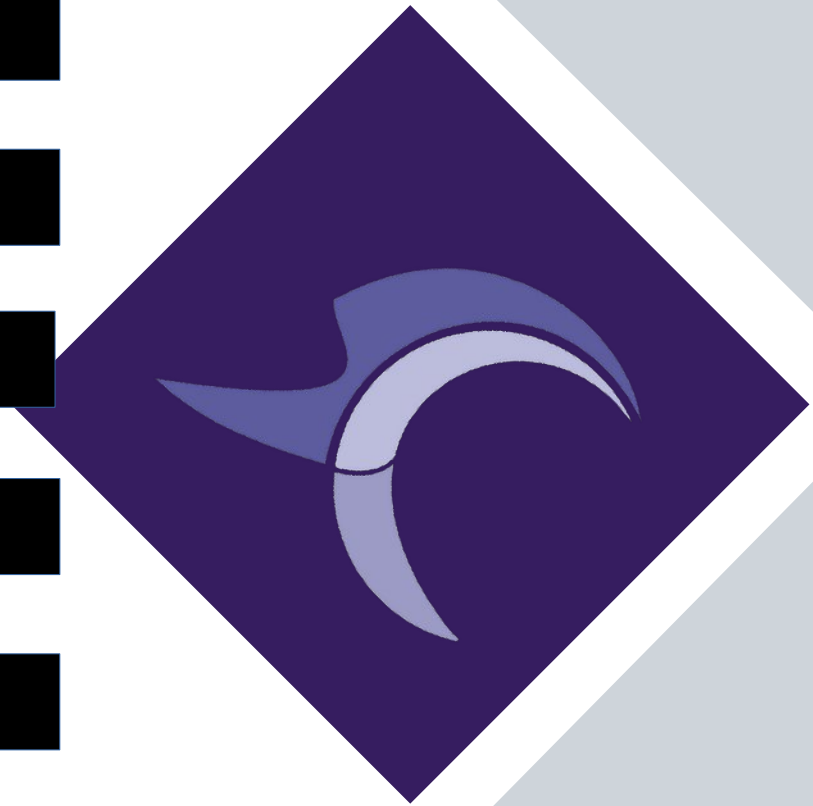
- Em troca, eu não vou colocar armadilhas no CTF :)

Introdução a *Capture The Flags* (CTFs) em Cibersegurança

Gabriel B. Sant'Anna
Egresso de CCO @ UFSC
Software / Firmware Dev. @ BRy Tecnologia
https://**baioc.github.io**/seccom-ctf/slides.pdf

CTF de Demonstração na SECCOM 2023

- cco{3[redacted]
- cco{8[redacted]
- cco{r[redacted]
- cco{H[redacted]
- cco{cc0[redacted]



Cybersec., CTFs e PenTesting
Onde aprender mais?

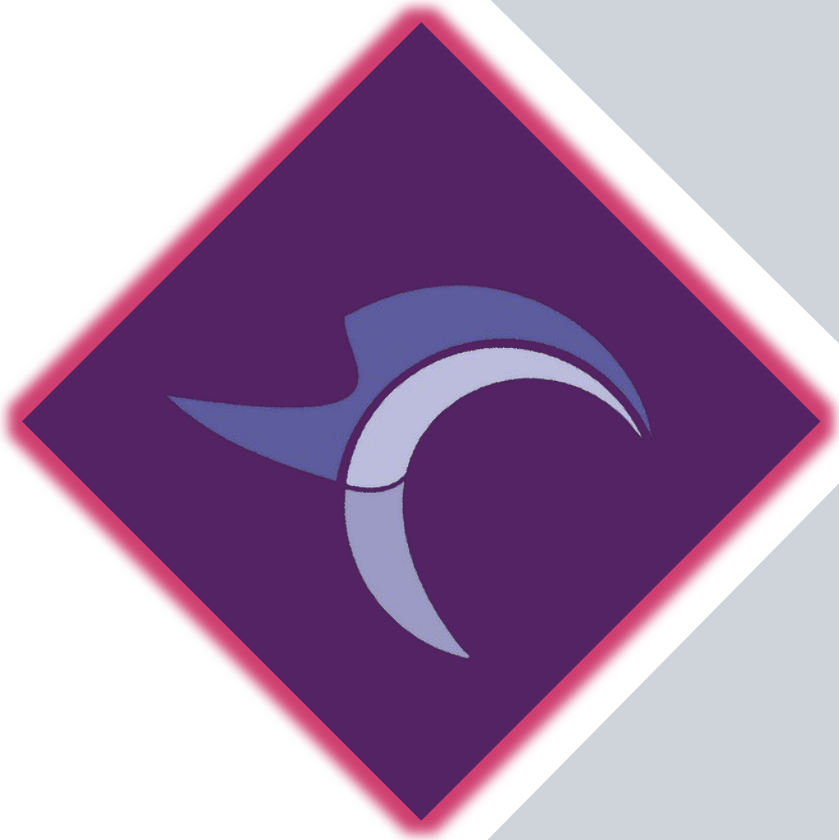
- **TryHackMe**: tryhackme.com/hacktivities
- **HackerOne**: www.hackerone.com/hackers/hacker101
- **HackTheBox**: hackthebox.com/hacker
- **TCM Security**: academy.tcm-sec.com/courses
- **Cyber Insecurity**: cyberinsecurity.tv

CTF de Desafio da SECCOM 2023

- Formato das **flags**: `/cco{\w+}/`

```
<Flag> ::= 'cco' '{' <w> <Wp> '}'
<w>    ::= [a-z] | [A-Z] | [0-9] | '_'
<Wp>   ::= ε | <w> <Wp>
```

- Exemplo: **`cco{example_flag0}`**



CTF de Desafio da SECCOM 2023

- Formato das **flags**: `/cco{\w+}/`

```
<Flag> ::= 'cco' '{' <w> <Wp> '}'
<w>    ::= [a-z] | [A-Z] | [0-9] | '_'
<Wp>   ::= ε | <w> <Wp>
```

- Exemplo: **`cco{example_flag0}`**

- **ATENÇÃO**: não tente atacar servidores ou outra infraestrutura digital. Esse CTF será conduzido de forma **100% offline** a partir do pacote ZIP inicial.

- Apenas o envio das flags capturadas exige conexão!

CTF de Desafio da SECCOM 2023

- Formato das **flags**: `/cco{\w+}/`

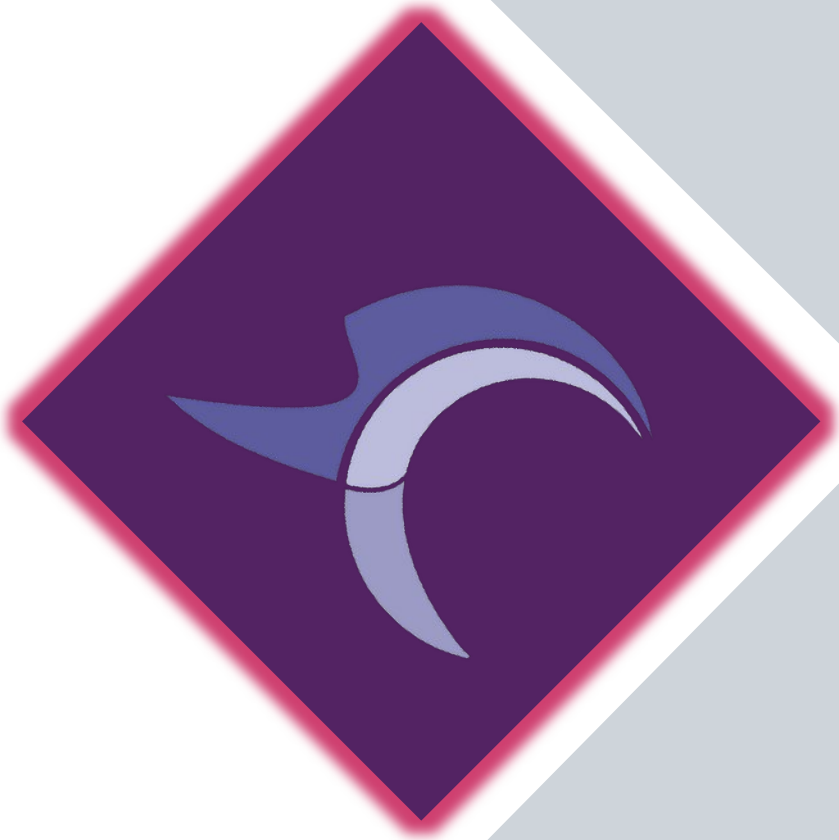
```
<Flag> ::= 'cco' '{' <w> <Wp> '}'
<w>    ::= [a-z] | [A-Z] | [0-9] | '_'
<Wp>   ::= ε | <w> <Wp>
```

- Exemplo: **`cco{example_flag0}`**

- **ATENÇÃO**: não tente atacar servidores ou outra infraestrutura digital. Esse CTF será conduzido de forma **100% offline** a partir do pacote ZIP inicial.
- Apenas o envio das flags capturadas exige conexão!
- Em troca, eu não vou colocar armadilhas no CTF :)

CTF de Desafio da SECCOM 2023

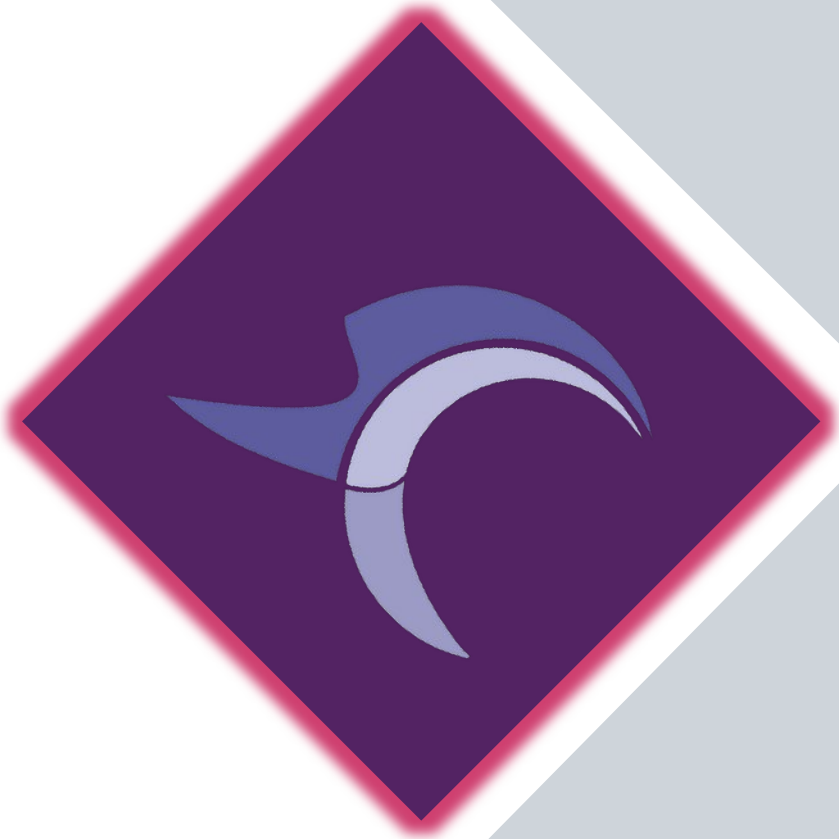
- Método de **envio das flags**:
  - E-mail para **baiocchi.gabriel@grad.ufsc.br**
  - Assunto = **Nome da Equipe**
  - Corpo da mensagem = flags capturadas
    - **Uma flag por linha**



CTF de Desafio da SECCOM 2023

- Método de **envio das flags**:
  - E-mail para **baiocchi.gabriel@grad.ufsc.br**
  - Assunto = **Nome da Equipe**
  - Corpo da mensagem = flags capturadas
    - **Uma flag por linha**

- Prazo final para envio: **09/11/2023 21h00**
  - Este email vai se autodestruir no 10/11



CTF de Desafio da SECCOM 2023

[Google@UFSC] Aviso de Remoção em 2 de 3 Inbox ×

Chamados@SeTIC - Notificacao <servicos.ti@sistemas.ufsc.br> Thu, 26 Oct, 13:46 (10 days ago)

to me

Olá,
Este chamado foi aberto automaticamente na SeTIC devido ao encerramento do seu vinculo com a UFSC.
Sua conta institucional no Google Workspace (baiocchi.gabriel@grad.ufsc.br) será encerrada no dia 2023-11-10.

Caso tenha dados que interessem a Servidores da UFSC entre em contato e repasse os dados mudando a propriedade (ownership) dos arquivos ou pastas, antes da data.

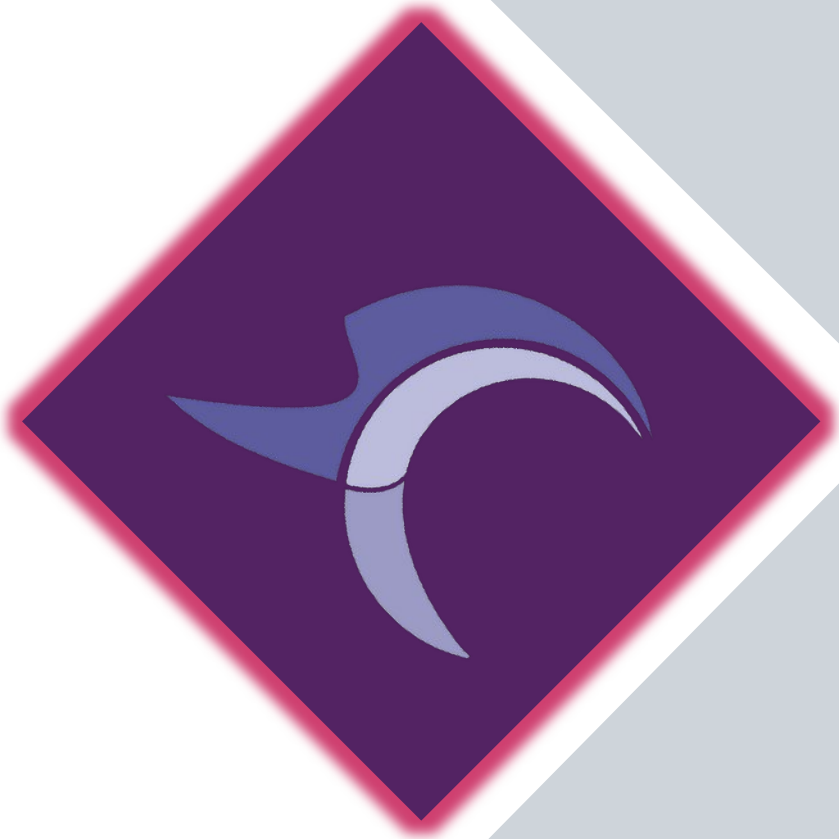
Sugerimos que faça uma cópia de segurança dos dados que estão em seu Google Drive (e outros serviços da plataforma) até o dia supracitado.
Após esta data todos os seus dados nesta plataforma serão excluídos.
Em caso de dúvidas, responda este e-mail ou abra um chamado na SeTIC em chamados.setic.ufsc.br.

Atenciosamente,
Equipes de atendimento e centro de dados da SeTIC

CTF de Desafio da SECCOM 2023

- Método de **envio das flags**:
  - E-mail para **baiocchi.gabriel@grad.ufsc.br**
  - Assunto = **Nome da Equipe**
  - Corpo da mensagem = flags capturadas
    - **Uma flag por linha**

- Prazo final para envio: **09/11/2023 21h00**
  - Este email vai se autodestruir no 10/11



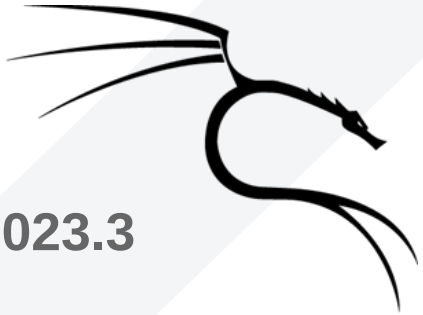
CTF de Desafio da SECCOM 2023

- Método de **envio das flags**:
  - E-mail para **baiocchi.gabriel@grad.ufsc.br**
  - Assunto = **Nome da Equipe**
  - Corpo da mensagem = flags capturadas
    - **Uma flag por linha**

- Prazo final para envio: **09/11/2023 21h00**
  - Este email vai se autodestruir no 10/11

- **ATENÇÃO**: não tente atacar ou spammar o servidor de emails. Envie apenas uma submissão por equipe.

Como começar?



- Baixe uma **VM** do **Kali Linux 2023.3**

- Vá para o 1o commit do repositório **https://github.com/baioc/seccom-ctf.git**

- Baixe o arquivo **ctf.zip** e transfira ele para a VM

- **Boa sorte!**

CTF inicial da SECCOM 2023

- cco{p[redacted]
- cco{2[redacted]
- cco{k[redacted]
- cco{y[redacted]
- cco{C[redacted]

Enviar flags capturadas para **baiocchi.gabriel@grad.ufsc.br**