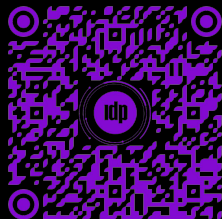


IDP CTF



idp

CAPTURE THE FLAG (CTF)

idp

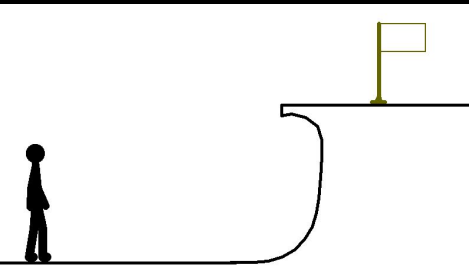
O que é

- CTF é um tipo de competição que envolve diversas competências na realização de desafios relacionados à Segurança da Computação (e Computação como um todo)



Objetivo

- O objetivo é capturar uma “flag”
 - Algo que comprove que você atingiu um objetivo
 - Acesso indevido a um computador, desvendou um enigma, automatizou algo, etc



Flag

- Flags são um código que a equipe obtém e é convertida em pontuação na competição
 - É algo que o competidor tem a capacidade de perceber que é uma flag



Flag

- Costumam possuir um padrão. Exemplos:
 - GCTF{parabens}
 - 3DSCTF{c1fra_s3cr3ta}
 - 4ac0be71b877b8687ac748f1016a9cd7
 - DEFCON{4ac0be71b877b8687ac748f1016a9cd7}
 - IDP{exemplo_de_flag_da_apresentacao}

Tipos de CTF

Ataque/Defesa



Jeopardy



Tipos de CTF - Ataque e Defesa

- Cada equipe recebe um conjunto vulnerável
 - servidor, software, máquina virtual, etc
- Há um tempo para se proteger (ou não)
- Times atacam uns aos outros por pontos
- Indisponibilidade é penalizada

Tipos de CTF - Jeopardy

- Estilo perguntas e respostas
- Dividido em categorias
- Pontuação de acordo com dificuldade
- Maioria dos CTFs está aqui

ARTISTA	QUEM DISSE?	FILME	LUGAR	LIVRO
10	10	10	10	10
20	20	20	20	20
30	30	30	30	30
40	40	40	40	40
50	50	50	50	50

Tipos de CTF - Jeopardy

- Criptografia (CRYPTO/STEGO)
- Engenharia Reversa (REV)
- Exploração de Binários (PWN)
- Forense (FOR)
- Jail (JAIL)
- Open Source Intelligence (OSINT)
- Redes (NET)
- Web (WEB)
- Programação (PPC)
- Miscelânea (MISC)
- Trivia (TRIVIA)
- LLM Injection (LLM)

Duração de CTFs

- Normalmente de 24 a 48 horas consecutivas
 - Por quê? (porque ocorre aos finais de semana)
- Algumas organizações e instituições gerenciam competições que duram mais tempo (<https://www.hackyeaster.com/>)
- Em eventos (conferências, seminários) costuma durar 5 horas

Composição de Times

- Pode ser jogado de maneira individual
- Times com tamanho definido (estamos aqui!!!)
- Online
 - Sem controle



Quem joga e quem organiza?

- Times normalmente são formados por estudantes, profissionais e, principalmente, curiosos
- Organizadores são entusiastas e profissionais ~~que não tem nada melhor pra fazer no final de semana~~

COMPETIÇÃO E REGRAS

idp

Regras (1/2)

- O CTF será no formato Jeopardy
- As flags estão no formato IDP{.+}
- Não é permitido ataque à infraestrutura do CTF
 - Servidores web que executam a plataforma
 - Servidores onde estão os desafios
 - Dispositivos na rede do evento
 - Se você não tem certeza, pergunte a um organizador do CTF



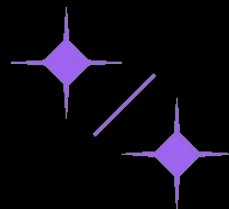
Regras (2/2)

- Não ataque, prejudique ou aja de forma a prejudicar outros competidores (todos querem aproveitar o evento)
- Não tente submeter as flags através de força bruta
- Lave as mãos
- Beba água
- Se divirta!



Regras (2/2)

- O que não está proibido, está liberado
 - Mas, tenham parcimônia ~~(esse ano o coordenador tá aqui)~~
- Está fora dos limites:
 - Aquário (inventei esse nome ano passado)
 - Manicômio (não quebrem nada, plmdds)
 - Piscina
 - Ligar para taxistas (eles não tem nenhuma flag)



WORKSHOPS

idp

Workshops

- Durante a realização da competição, serão ministrados dois mini workshops, cada um em um tópico diferente utilizado na competição, como forma de introduzir e guiar os competidores em alguma área que é desconhecida para os mesmos

Workshops

- Horários:
 - Eu vou notificar vocês pela própria plataforma
 - O previsto é:
 - 22:00h
 - 10:00h

DESAFIO DE IMERSÃO

idp

Desafio de Imersão

- Durante a competição, as equipes participarão de um desafio de imersão
- O objetivo é vocês receberem um desafio que exige um pouco de lógica e a solução seja contra o tempo (mais ainda)

Desafio de Imersão



Desafio de Imersão

- São dois desafios diferentes
- Os times participarão duas vezes (apenas)
 - Até duas pessoas na cabine ao mesmo tempo
 - Um participante só poderá jogar duas vezes se o companheiro de equipe abrir mão
- Solução para o desafio pontua na plataforma

Desafio de Imersão



Desafio de Imersão

- Regras:
 - Pode levar material de anotação
 - Pode levar eletrônico para anotar
 - Não pode tirar foto
 - Não pode gravar
- Um detalhe importante, é que por mais que vocês estejam curiosos sobre o desafio, tira boa parte da graça ficar perto acompanhando outros times (o objetivo é aproveitar)

Desafio de Imersão

- Horários previstos:
 - Rodada 01: 20h às 00h
 - Rodada 02: 10 às 14h
- Os times vão receber uma notificação na plataforma com a ordem de participação
- Duração do desafio é em torno de 15 minutos

CREDENCIAIS E PLATAFORMA

idp

Credenciais

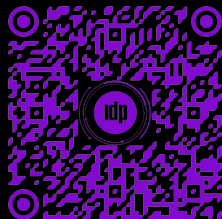
- Será entregue uma folha com a senha de todo os membros da equipe
 - O login é por `_matricula`

Plataforma

- <https://idp-ctf.online/>



IDP CTF



idp