

# Introduction à la cybersécurité via les Capture The Flag (CTF)

Ugo Proietti et François Vion

Université de Mons

16 février 2022

- 1 Qu'est-ce qu'un CTF ?
- 2 Les différents domaines de CTF
- 3 Mise en pratique
- 4 Plateformes et évènements
- 5 Conseils généraux

Les Capture The Flag sont des compétitions durant lesquelles il faut trouver des flags dans des fichiers, sites, applications, etc. Les flags sont des chaînes de caractère qui suivent un format standard en fonction de l'évènement. Par exemple : {CPU69420}.

Chaque flag rapporte un certain nombre de points en fonction de sa difficulté.

Il existe un grand nombre de catégories ayant chacune leurs caractéristiques. Nous allons vous présenter les plus connues.

- Stéganographie
- Cryptographie
- Web
- Programmation
- Réseau
- Forensic
- Reverse Engineering

## Explication

La Stéganographie est l'art de la dissimulation. Il s'agit en général de cacher une information là où on ne s'y attend pas.

## Explication

La Stéganographie est l'art de la dissimulation. Il s'agit en général de cacher une information là où on ne s'y attend pas.

## Exemples

- Cacher un message dans un fichier audio
- Cacher une message sur une image
- Cacher une image dans une autre image

## Explication

La Stéganographie est l'art de la dissimulation. Il s'agit en général de cacher une information là où on ne s'y attend pas.

## Exemples

- Cacher un message dans un fichier audio
- Cacher un message sur une image
- Cacher une image dans une autre image

## Compétences utiles

- Observation
- Utilisation de scripts
- Connaissance des divers formats de fichier

## Explication

La Stéganographie est l'art de la dissimulation. Il s'agit en général de cacher une information là où on ne s'y attend pas.

## Exemples

- Cacher un message dans un fichier audio
- Cacher un message sur une image
- Cacher une image dans une autre image

## Compétences utiles

- Observation
- Utilisation de scripts
- Connaissance des divers formats de fichier

**Difficulté** : 1/5



## Explication

La cryptographie est l'art de rendre un message illisible pour toute personne n'ayant pas la clé pour le déchiffrer. Elle est différente de la stéganographie qui consiste simplement à faire passer un message inaperçu.

## Explication

La cryptographie est l'art de rendre un message illisible pour toute personne n'ayant pas la clé pour le déchiffrer. Elle est différente de la stéganographie qui consiste simplement à faire passer un message inaperçu.

## Exemples

- Cryptage et décryptage d'un message

## Explication

La cryptographie est l'art de rendre un message illisible pour toute personne n'ayant pas la clé pour le déchiffrer. Elle est différente de la stéganographie qui consiste simplement à faire passer un message inaperçu.

## Exemples

- Cryptage et décryptage d'un message

## Compétences utiles

- Connaissance de divers formats d'encodage
- Connaissance de diverses méthodes de cryptage et de décryptage

## Explication

La cryptographie est l'art de rendre un message illisible pour toute personne n'ayant pas la clé pour le déchiffrer. Elle est différente de la stéganographie qui consiste simplement à faire passer un message inaperçu.

## Exemples

- Cryptage et décryptage d'un message

## Compétences utiles

- Connaissance de divers formats d'encodage
- Connaissance de diverses méthodes de cryptage et de décryptage

**Difficulté** : 2/5

## Explication

Un site web peut contenir un mot de passe, un fichier ou une faille permettant de s'y connecter sans autorisation.

## Explication

Un site web peut contenir un mot de passe, un fichier ou une faille permettant de s'y connecter sans autorisation.

## Exemples

- Un message caché dans le code HTML
- Un lien sur le site qui mène à une ressource cachée
- Un faille de sécurité dans un système de connexion

## Explication

Un site web peut contenir un mot de passe, un fichier ou une faille permettant de s'y connecter sans autorisation.

## Exemples

- Un message caché dans le code HTML
- Un lien sur le site qui mène à une ressource cachée
- Un faille de sécurité dans un système de connexion

## Compétences utiles

- Connaissance d'HTML, JavaScript et PHP
- Connaissance de la structure d'un site web

## Explication

Un site web peut contenir un mot de passe, un fichier ou une faille permettant de s'y connecter sans autorisation.

## Exemples

- Un message caché dans le code HTML
- Un lien sur le site qui mène à une ressource cachée
- Un faille de sécurité dans un système de connexion

## Compétences utiles

- Connaissance d'HTML, JavaScript et PHP
- Connaissance de la structure d'un site web

**Difficulté** : 2/5



## Explication

On peut trouver des flags dans un programme en comprenant son fonctionnement et en exploitant les failles de celui-ci.

## Explication

On peut trouver des flags dans un programme en comprenant son fonctionnement et en exploitant les failles de celui-ci.

## Exemples

- Faille dans la méthode `input()` de Python 2
- Contournement du mot de passe d'une application Android

## Explication

On peut trouver des flags dans un programme en comprenant son fonctionnement et en exploitant les failles de celui-ci.

## Exemples

- Faille dans la méthode `input()` de Python 2
- Contournement du mot de passe d'une application Android

## Compétences utiles

- Maîtrise de divers langages de programmation

## Explication

On peut trouver des flags dans un programme en comprenant son fonctionnement et en exploitant les failles de celui-ci.

## Exemples

- Faille dans la méthode `input()` de Python 2
- Contournement du mot de passe d'une application Android

## Compétences utiles

- Maîtrise de divers langages de programmation

**Difficulté** : 3/5

## Explication

Surveiller un réseau peut révéler des informations concernant les clients connectés et les données qui y sont échangées.

## Explication

Surveiller un réseau peut révéler des informations concernant les clients connectés et les données qui y sont échangées.

## Exemple

- Récupérer des identifiants de connexion en interceptant les paquets

## Explication

Surveiller un réseau peut révéler des informations concernant les clients connectés et les données qui y sont échangées.

## Exemple

- Récupérer des identifiants de connexion en interceptant les paquets

## Compétences utiles

- Maîtriser un analyseur de réseau
- Connaître les protocoles réseaux les plus communs

## Explication

Surveiller un réseau peut révéler des informations concernant les clients connectés et les données qui y sont échangées.

## Exemple

- Récupérer des identifiants de connexion en interceptant les paquets

## Compétences utiles

- Maîtriser un analyseur de réseau
- Connaître les protocoles réseaux les plus communs

**Difficulté** : 4/5



## Explication

L'analyse forensic consiste a retrouver des infomations sur une machine qui a subit un accident.

## Explication

L'analyse forensic consiste a retrouver des infomations sur une machine qui a subit un accident.

## Exemples

- Analyse de la mémoire qui peut contenir des mots de passe utilisés par l'OS ou des tokens de connexion utilisés par le navigateur web.
- Analyse des logs générés par l'OS

## Explication

L'analyse forensic consiste à retrouver des informations sur une machine qui a subi un accident.

## Exemples

- Analyse de la mémoire qui peut contenir des mots de passe utilisés par l'OS ou des tokens de connexion utilisés par le navigateur web.
- Analyse des logs générés par l'OS

## Compétences utiles

- Maîtrise de divers formats d'encodage
- Maîtrise de manipulation de bits
- Utilisation d'un langage de script (e.g. Python)

## Explication

L'analyse forensic consiste à retrouver des informations sur une machine qui a subi un accident.

## Exemples

- Analyse de la mémoire qui peut contenir des mots de passe utilisés par l'OS ou des tokens de connexion utilisés par le navigateur web.
- Analyse des logs générés par l'OS

## Compétences utiles

- Maîtrise de divers formats d'encodage
- Maîtrise de manipulation de bits
- Utilisation d'un langage de script (e.g. Python)

**Difficulté** : 4/5

## Explication

Le reverse engineering est le fait de décompiler un programme pour pouvoir voir son fonctionnement interne.

## Explication

Le reverse engineering est le fait de décompiler un programme pour pouvoir voir son fonctionnement interne.

## Exemples

- Analyse du fonctionnement interne d'un programme pour en tirer des informations
- Modification du code source d'un programme

## Explication

Le reverse engineering est le fait de décompiler un programme pour pouvoir voir son fonctionnement interne.

## Exemples

- Analyse du fonctionnement interne d'un programme pour en tirer des informations
- Modification du code source d'un programme

## Compétences utiles

- Maîtrise de langage machine et assembleur (C, x86, etc)
- Utilisation de décompilateurs

## Explication

Le reverse engineering est le fait de décompiler un programme pour pouvoir voir son fonctionnement interne.

## Exemples

- Analyse du fonctionnement interne d'un programme pour en tirer des informations
- Modification du code source d'un programme

## Compétences utiles

- Maîtrise de langage machine et assembleur (C, x86, etc)
- Utilisation de décompilateurs

**Difficulté** : 5/5



Essayez de trouver les flags dans les fichiers du drive !

Le lien : [shorturl.at/lvzD3](https://shorturl.at/lvzD3)

Les flags suivent le format `¡CPU...¿`

Conseil : Faites des recherches internet

- [root-me.org](https://root-me.org)
- [overthewire.org](https://overthewire.org)
- [hackthebox.com](https://hackthebox.com)
- [ctftime.org](https://ctftime.org)



- Compétition CTF inter-écoles belges
- Par équipe de 4 (de la même école)
- Du 10 au 11 mars 2022
- Finales du 25 au 26 mars 2022

CYBER  
SECURITY

CHALLENGE  
BELGIUM

**ONE TEAM**  
4 Players

**MANY CHALLENGES**

CRYPTOGRAPHY  
WEB SECURITY  
MOBILE SECURITY  
NETWORK SECURITY  
REVERSING  
DIGITAL FORENSICS  
OPEN SOURCE  
INTELLIGENCE



10 & 11 March – Online

## QUALIFIERS

REMOTE CHALLENGES OPEN TO EVERYONE (+18).



25 March – Brussels

## PRE-FINALS

TOP ELIGIBLE TEAMS.



25 & 26 March – Brussels

## FINALS

TOP 16 TEAMS.

- Utilisez Linux (VM ou installation complète)

- Utilisez Linux (VM ou installation complète)
- Persévérez et faites beaucoup de recherches

- Utilisez Linux (VM ou installation complète)
- Persévérez et faites beaucoup de recherches
- Avoir des connaissances générales dans tout les domaines de l'informatique (être polyvalent)



- Utilisez Linux (VM ou installation complète)
- Persévérez et faites beaucoup de recherches
- Avoir des connaissances générales dans tout les domaines de l'informatique (être polyvalent)
- Prendre note des solutions des ctf qui pourront sans doute servir plus tard