

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

Ugo Proietti et François Vion

Université de Mons

26 février 2024

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

# Principe

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.

# Catégories

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

# Stéganographie

## 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.

# Stéganographie

## 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

# Stéganographie

## 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 et d'outils
- Connaissance des divers formats de fichier

# Cryptographie

## 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.



# Cryptographie

## 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

- Chiffrement et déchiffrement d'un message
- Exploiter des paramètres mal choisis

# Cryptographie

## 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

- Chiffrement et déchiffrement d'un message
- Exploiter des paramètres mal choisis

## Compétences utiles

- Connaissance de divers formats d'encodage
- Connaissance de diverses méthodes de chiffrement

# Web

## Explication

Un site web mal codé peut contenir des failles de sécurité ou des informations sensibles visible de tous.

## Explication

Un site web mal codé peut contenir des failles de sécurité ou des informations sensibles visible de tous.

## 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 mal codé peut contenir des failles de sécurité ou des informations sensibles visible de tous.

## 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
- Utilisation d'outils de visualisation de requête

# Programmation

## Explication

Comme un site web, un programme peut contenir des failles de sécurité permettant d'exploiter le contenu de celui-ci.

# Programmation

## Explication

Comme un site web, un programme peut contenir des failles de sécurité permettant d'exploiter le contenu de celui-ci.

## Exemples

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

# Programmation

## Explication

Comme un site web, un programme peut contenir des failles de sécurité permettant d'exploiter le contenu de celui-ci.

## Exemples

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

## Compétences utiles

- Maîtrise de divers langages de programmation



## 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
- Récupérer des fichiers échangés

## 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
- Récupérer des fichiers échangés

## Compétences utiles

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

# Forensic

## Explication

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

## 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

## 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

- Utilisation d'outils d'analyse forensic
- Connaissance approfondie de la structure de fichier d'un système

# Reverse Engineering

## Explication

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

# Reverse Engineering

## 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



# Reverse Engineering

## 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 de bas niveau et assembleur (C, x86, etc)
- Utilisation de décompilateurs

## Explication

L'open source intelligence est le fait de récolter des informations publiques sur un individu ou une chose et d'en déduire des informations non explicites.

## Explication

L'open source intelligence est le fait de récolter des informations publiques sur un individu ou une chose et d'en déduire des informations non explicites.

## Exemples

- Retrouver une personne
- Localisation d'image

## Explication

L'open source intelligence est le fait de récolter des informations publiques sur un individu ou une chose et d'en déduire des informations non explicites.

## Exemples

- Retrouver une personne
- Localisation d'image

## Compétences utiles

- Google dorks (filetype,...)
- Connaissance de logiciels adaptés

## Mise en pratique

Inscrivez vous sur le site **45.155.169.253 :8000** et créez un compte pour une équipe de 2 ou 3 personnes

Trouvez le plus de flag possible avant demain 18h et faites grimper votre équipe dans le classement !

Les flags suivent le format <CPU...>

Conseil : Faites des recherches internet

# A titre indicatif

## Facile

- De beaux chats
- Complètement décalé
- Fonctio enjoyer
- Top 10 Linux facts
- Un dossier bizarre
- Détournement d'avion

## Moyen

- L'attention du détail
- Plusieurs alphabets
- Mot de passe solide
- Code obfusqué
- Voyage voyage
- Connexion admin
- Il aurait pu se cacher le steg

## Difficile

- Stagiaire mystérieux
- Nouvel utilisateur
- Site professionnel
- Permutations

# Plateformes

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



- Compétition CTF inter-écoles belges
- Par équipe de 4 (de la même école)
- Du 8 au 9 mars 2024
- Finales du 22 au 23 mars 2024



CYBER  
SECURITY

CHALLENGE  
BELGIUM

**ONE TEAM**  
4 Players

**MANY CHALLENGES**

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

# Conseils généraux

- Utilisez Linux (VM ou installation complète)

# Conseils généraux

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

# Conseils généraux

- 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)

# Conseils généraux

- 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

# Outils pratiques

- Steganographie
  - ▶ exiftool
  - ▶ steghide
- Cryptographie
  - ▶ dcode.fr
  - ▶ CyberChef
- Réseau
  - ▶ Wireshark
  - ▶ Nmap
- Forensic
  - ▶ volatility
- Reverse engineering
  - ▶ Ghidra
  - ▶ Cutter
- OS Linux
  - ▶ Kali
  - ▶ Parrot OS
  - ▶ Black Arch