Introduction aux CTFs

Philippe Grégoire

2023-02-01

whoami

- Philippe Grégoire
- Nom d'artiste : fob
- Diplômé du BIGL à l'UQAM
- Étudiant à la maitrise
- Chasseur de bogues professionnel depuis 4 ans
- Ancien membre de l'AGEEI (2017-2020)
- Gagnant de compétitions (CS Games, NorthSec, Hackfest, United CTF, etc.)
- Heureux détenteur d'une licorne de RingZer0 CTF et diverses certifications

Plan de la scéance

- Un CTF, c'est quoi ?
- Pourquoi s'intéresser des CTFs ?
- On y parle de quoi ?
- Ça s'adresse à qui ?
- Comment approcher un exercice ?
- Quelques exercices
- Comment devenir meilleur.e ?
- Quels CTFs faire ?

Un CTF, c'est quoi ?

- CTF == *Capture The Flag*
- C'est une compétition de sécurité[1] informatique
- Généralement de durée limitée (e.g. 72 heures, 1 semaine)
- Les participants doivent retrouver les *flags* en résolvant des problèmes
- Le *flag* est une information secrète, protégée par le problème

[1] certains réutilisent la formule pour des exercices de programmation

Pourquoi s'intéresser aux CTFs ?

- Découvrir ou se familiariser avec des technologies
- Améliorer sa capacité à résoudre des problèmes
- En apprendre sur la sécurité informatique
- Gagner des prix
- Étoffer son CV

Dans un CTF, on parle de quoi ?

Il y a différents types d'exercices, pour différents domaines.

- Web
- *reverse engineering*, *reverse*, *re*, rétro-ingénierie
- *pwn*, exploitation binaire
- cryptographie/cryptologie
- *forensics*, "informatique légale", "cyber-enquêtes"
- stéganographie
- applications mobiles
- analyse de données
- réseautique
- *hardware*, matériel
- *trivia*, de la culture générale
- etc.

Qui participe ?

Les CTFs sont généralement ouverts à tous, mais peuvent s'adresser à un public spécifique :

- les étudiants du secondaire (pour commencer)
- les étudiants au baccalauréat (pour continuer)
- les amateurs (pour se faire plaisir)
- les professionnels (pour avoir mal à la tête)

Pro tip: dirigez-vous vers les événements à votre mesure.

L'approche générale

On cherche les bogues. Les bogues de sécurité.

- On reçoit un énoncé de programmation avec quelques cas d'utilisation
- On prépare des tests en fonction des cas d'utilisation
- On programme pour le *happy path*, le chemin normal
- On chasse les bogues! Tous ce qui n'est pas sur le *happy path*

On sort des sentiers battus pour trouver les bogues, et on regarde si et comment ça nous avantage.

Exercices 1 - Web

- http://138.197.132.10/
- Qu'est-ce qu'on ne voit pas ?
- Qu'est-ce qu'on nous cache ?
- Qu'est-ce qu'on contrôle ?

Exercices 1 - Web (solution)

- Afficher le code source de la page

`FLAG-82573a73dba4901cf77c34f6d0981e22`

Exercices 1 - Web (solution)

- Afficher le code source de la page
- Consulter `/robots.txt` pour découvrir une page cachée

`FLAG-7e990addc6d653b84e5e8218e85f0551`

Exercices 1 - Web (solution)

- Afficher le code source de la page
- Consulter `/robots.txt` pour découvrir une page cachée
- Modifier le cookie (`admin=1`) pour devenir administrateur

`FLAG-63afb057a5097a1c830071a509a39b82`

Exercice 2 - Forensics

http://138.197.132.10/intro.pcap

- On tente d'extraire de l'information à partir de données collectées d'un événement.
- Un `pcap` est un fichier contenant une capture de paquets réseau.
- On analyse les échanges de données pour extraire un *flag*.
- Wireshark est un outil permettant d'analyser ces captures.

Ici, on veut récupérer le fichier `flag.txt`.

Exercice 2 - Forensics (solution)

Démonstration

Comment devenir meilleur.e ?

- Familiariser vous avec des technologies
- Lire des *write-ups*!
- INF1070 (Linux/UNIX)
- INF1132 (Logique)
- INF2171 (Assembleur, systèmes ordinés)
- INF3080 (SQL)
- INF3135 (C)
- INF3173 (Systèmes d'exploitation)
- INF3190 (Web)
- INF3271 (Réseautique)
- INF600C (shell, Web, binaire)

Il y a toujours plus à apprendre !

Quelques recommandations de CTFs et d'outils

Sans ordre particulier :

- https://overthewire.org/wargames/
- https://ctf.ageei.org/
- https://www.csaw.io/
- https://hackthebox.com/
- https://ringzer0ctf.com/
- https://nsec.io/competition/
- https://root-me.org/

Quelques outils :

- https://gchq.github.io/CyberChef/
- https://ghidra-sre.org/