

L'apprentissage par la pratique

CHALLENGES, WARGAMES & CTFs

\$ whois

- **Alexandre CHÉRON**
- Digital Forensics Analyst
- Pentester
- (wannabe) Developer
- @axcheron  



*Photo non contractuelle.

Wargame vs. CTF

- Les « Wargames » sont permanents
 - Nombreux sur Internet
 - Individuel
 - Pas de limite de temps
- Les « CTF » sont temporaires
 - Durant un évènement
 - Généralement en équipe

WARGAMES

Capture The Flag

- Capture The Flag
 - Bataille de « skill » en équipe
 - Composé d'une variété de challenges
 - L'objectif est d'obtenir des « flags »
- Le « flag » ou drapeau
 - Généralement une chaîne de caractères aléatoire
 - Preuve de la résolution d'un challenge
 - Possède une valeur selon la difficulté du challenge

Types de CTF

- Jeopardy (HackFest)
 - Ensemble de challenges
 - Différentes catégories
 - En ligne / On-site
- Attaque/Défense (DEFCON)
 - Chacun possède un ensemble de serveurs vulnérables
 - Temps alloué pour l'audit et les correctifs
 - La compétition commence...
 - Généralement on-site (en ligne sur <https://ctf365.com>)



Catégories de challenges

- Logique
- Web
- Cryptographie
- Reverse engineering (CrackMe)
- Exploitation
- Stéganographie
- Forensics
- Dev
- Autres (hardware, etc.)



Pourquoi ?

- “*Knowing is not enough; we must apply. Willing is not enough; we must do.*” - Johann Wolfgang von Goethe



Apprentissage

- Blog - (<https://axcheron.github.io/trainings/>)
 - Modern Binary Exploitation
 - Malware Analysis
 - Offensive Computer Security
 - Web Security Academy
 - etc.
- Lire des « *writeups* »
 - <https://github.com/apsdehal/awesome-ctf/>

Prochaines étapes

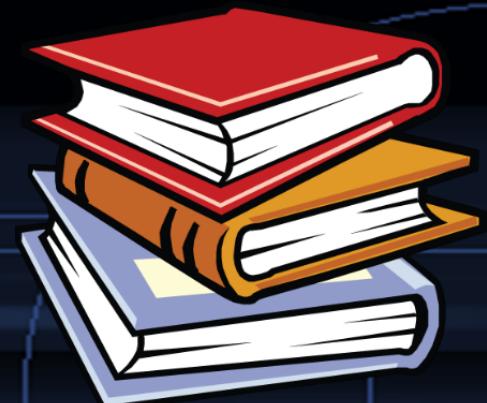
- Faire un wargame
 - Écrire un *writeup*
 - On rince et on répète
-
- S'inscrire à un CTF !

DEMO



Références

- <https://www.wechall.net>
- <https://www.newbiecontest.org>
- <https://overthewire.org/wargames/>
- <https://www.zenk-security.com>
- <http://pwnable.kr>
- <https://crackmes.one/>
- <https://www.root-me.org>



Questions ?

MERCI !

@axcheron

