Intro au CTF

Le CTF, c'est quoi?

- Terme devenu générique pour désigner une compétition de sécurité informatique

- Chaque compétition est unique

- Pas de règles fixes

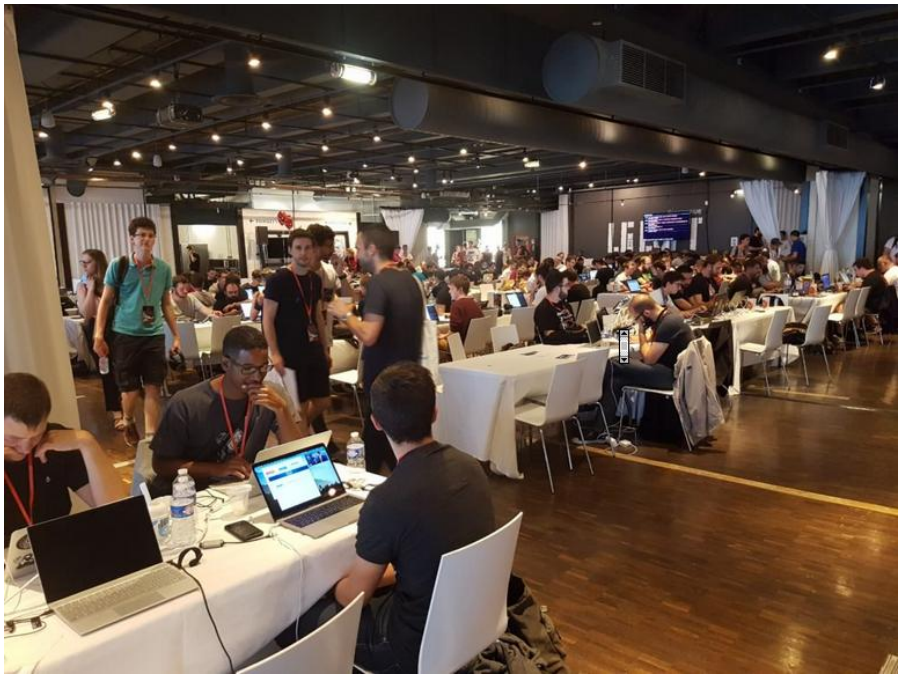
Types de CTF

- Jeopardy
  - Challenge unitaires sur un thème, une vuln, un exercice de style… Il faut trouver un « flag » qui montre qu'on a réussi le challenge
  - Entre 3h et 48h

- Attack & defense
  - Chaque équipe dispose d'un SI qu'elle doit protéger tout en attaquant celui des autres
  - Entre 10 et 24h

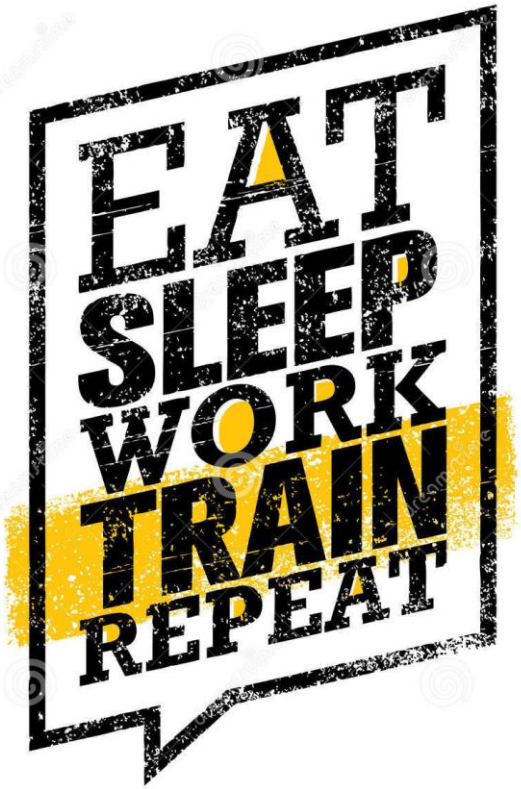
- Spying challenge, qui veut gagner des bitcoins, badge challenge, Hack ATM ou voiture, escape games…

Et le Wargame de le Hack?



- Jeopardy
- De 20h à 6h
  du matin
- Cette année
  quelques challenges spécial débutants
- L'équipe d'orga est là pour toute question!

Comment on flag?

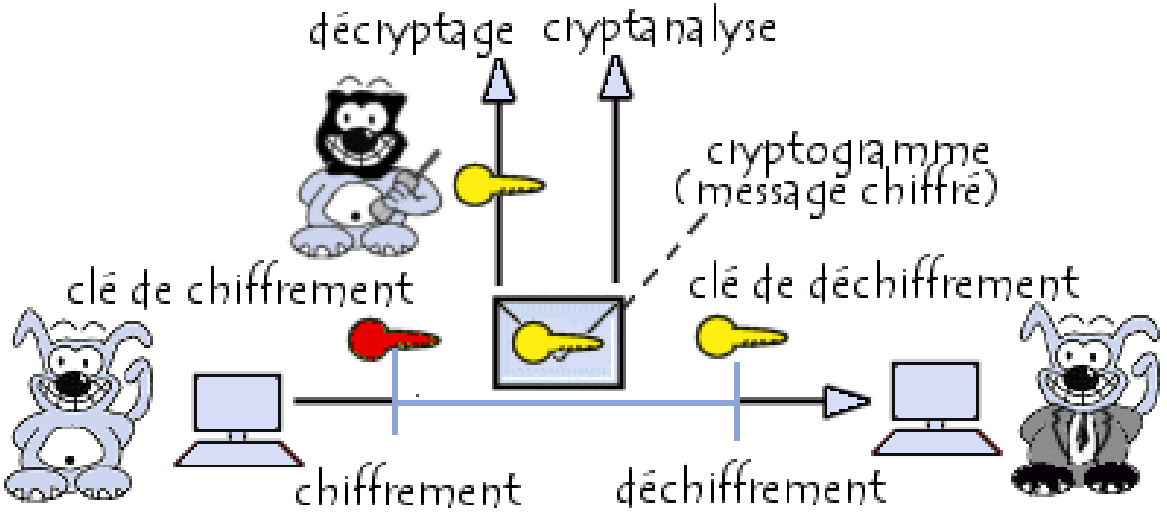


- Chaque challenge se voit en général attribué une catégorie
- Pour chaque catégorie, la manière de récupérer le flag est en général similaire

Comment on flag? - crypto

- Message chiffré avec de la crypto qui présente une vulnérabilité

- Pas de méthode particulière
- Outils: openssl, rsatools, python



Comment on flag? - reverse

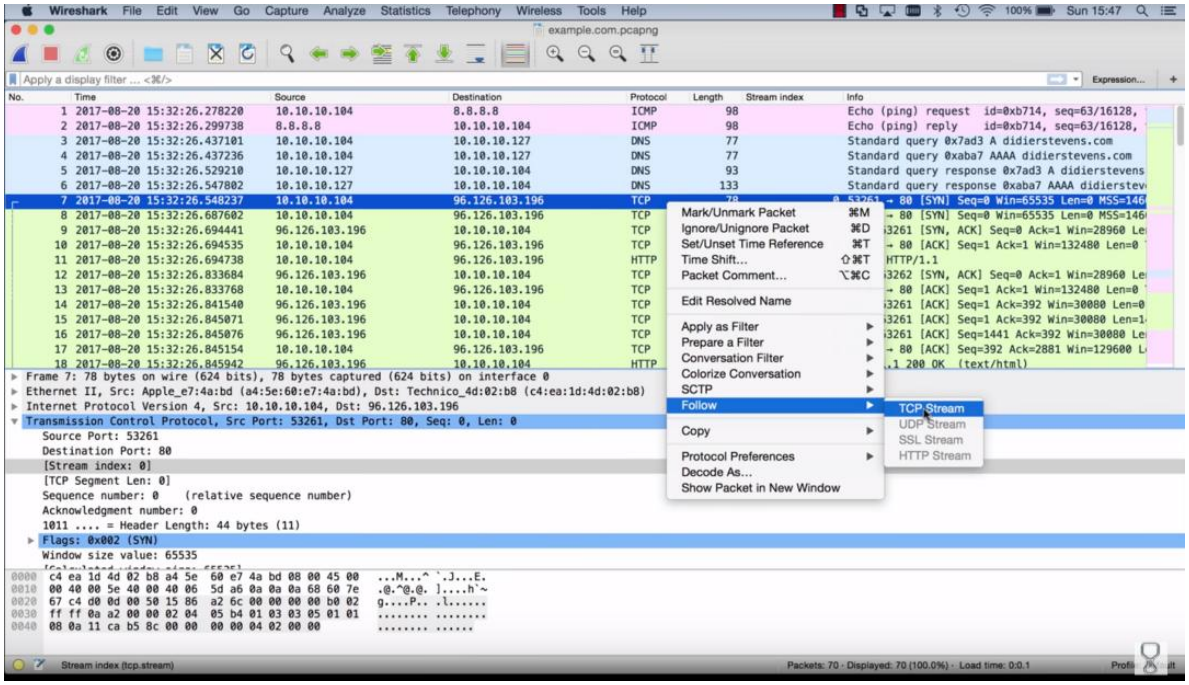
- En général un binaire qui nous demande un mot de passe, qui sert de flag.

1. Utiliser toute technique de reverse engineering pour comprendre la logique de validation du mot de passe
2. Inverser cette logique pour retrouver le mot de passe

- Outils: IDA, gdb, python, radare2

Comment on flag? - réseau

- En général une capture réseau. Le flag est alors souvent un mot de passe transmis dans la capture quelque part



- Outils: wireshark, python

Comment on flag? - web

- Assez souvent, il faut accéder à la partie d'administration d'un site en exploitant une vulnérabilité web, ou alors lire un fichier particulier ou la base de données

- Outils: burp, votre navigateur

Pour ce soir

- Mettez vous en **équipe,** c'est plus sympa!

- Ne pas attaquer les challenges difficiles!
  - Plus un challenge est compliqué et plus il vaut de point. Sélectionner les challenges avec peu de points
  - Ne pas se décourager : réussir un ou deux challenges est suffisant. Il faut apprendre à utiliser les outils notamment, ce qui prend du temps.

- **Prévoir nourriture + eau**, attention à la **fatigue**

- Selon comment se passe la compétition, je pourrais faire des explications de résolution des challenges débutants


LET'S GO!!!!!
memegenerator.net