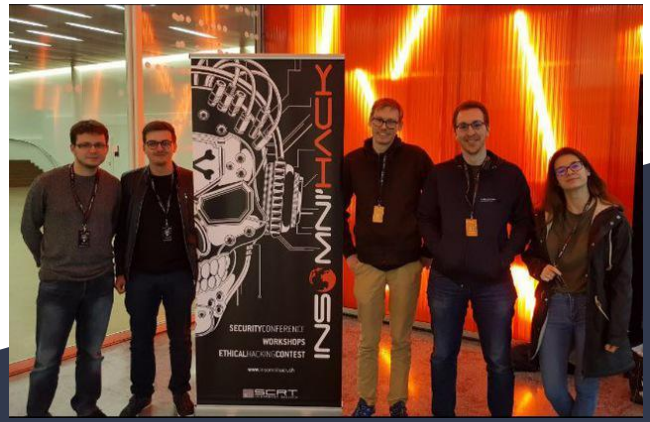
Introduction aux CTF



Roh Steven, Pannatier Yvan,
Da Rocha Micaela, Constantin Jérémie

Sommaire

- Qu’est ce qu’un CTF ?
- Les types de CTF
- Débuter dans les CTF
- Pratique

LOCAL GHOST

Qu’est ce qu’un CTF ?

Les bases

- Un CTF est une compétition de sécurité informatique

- Comment capturer un drapeau ?
  - Introduction dans un système informatique
  - Devenir admin
  - Lire un fichier, une bdd

- À quoi ressemble un drapeau ?
  - `flag{17s_0k_8i7s_n3v4r_fL!p_1RL}`

- Durée
  - 24h-48h-72h, parfois une semaine
  - Voire quelques heures : 4h, 6h etc..

LOCAL HOST

Qu’est ce qu’un CTF ?

Les bases

Objectifs

- Casser des programmes
- Apprendre à réaliser des pentest
- Penser out of the box
- Sensibiliser à la sécurité informatique

Règles

- Pas de partage de flag
- Pas de bruteforce
- Pas d’attaque contre l’infrastructure
- Règles spécifiques à l’organisateur

LOCAL HOST

Les types de CTF

Online-onsite

Onsite

- Attaque par équipe (attaque / défense)
- Jeopardy
- Hacking Quest
- Hardware

Online

- Jeopardy
- Attaque / défense

LOCAL HOST

Les types de CTF

Online vs onsite

LOCAL HOST

Les types de CTF

Les catégories

Liste des catégories

- Cryptographie
- Stéganographie
- Reverse engineering
- Binary exploitation
- Web
- Forensic
- Réseau
- Programmation
- Reconnaissance / OSINT
- Hardware
- Quest

LOCAL HOST

Les types de CTF

Les catégories

Cryptographie

- Déchiffrer un message chiffré
- Input de type binaire, script, texte

Exemple

```
input: cvpbPGS{guvf_vf_pelcgb!}

alphabet:
ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrst
uvwxyz

rot13 alphabet:
NOPQRSTUVWXYZABCDEFGHIJKLMnopqrstuvwxyzabcdef
ghijklm

output: picoCTF{this_is_crypto!}
```

LOCAL HOST

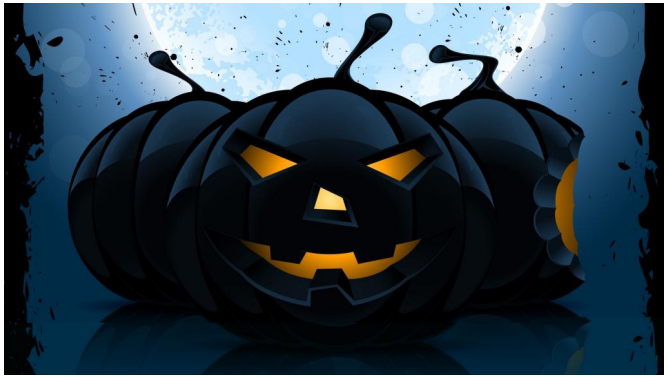
Les types de CTF

Les catégories

Stéganographie

- Flag dans une image, un fichier audio, un texte

Exemple



strings <file>

```
Mun`~2cc
flag-SpookyPumpkinIsSpooky=
RU%JJ/[
```

LOCAL HOST

Les types de CTF

Les catégories

Reverse engineering

- Analyser un programme pour comprendre comment il fonctionne

Binary exploitation

- Analyser un programme afin de trouver des vulnérabilités, changer une partie du code, exploiter une faille
  - Buffer Overflow
  - ret2libc
- Nécessite souvent de faire du reverse engineering
- Attention à l'architecture ⚠️ ARM, x86/x64, etc..

LOCAL HOST

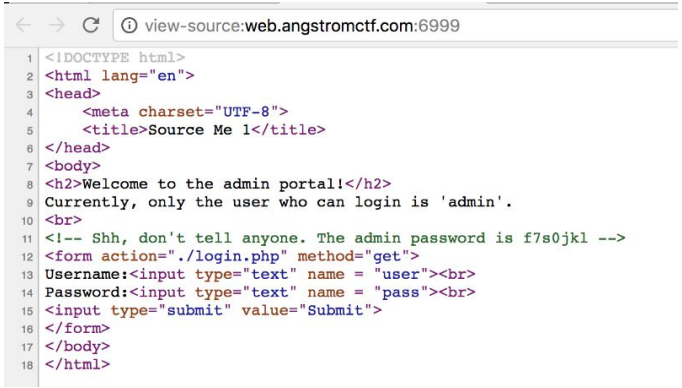
Les types de CTF

Les catégories

WEB

- Analyser un site web pour exploiter une faille
- Commentaires HTML, backup, XSS, SQli, CSRF, directory indexing ...

Exemple



Les types de CTF

Les catégories

Forensic

- Réaliser une recherche d'information sur des données
- Il s'agit souvent d'expliquer une attaque ou de connaître les informations exfiltrées, contient parfois de la stéganographie
- Analyses de dump mémoires, de captures réseau, de logs ...

Réseau

- Analyse de captures réseau

LOCAL HOST

Les types de CTF

Les catégories

Recon /OSINT

- Récupérer des informations depuis des sources en libre accès pour récupérer le flag
- Sur des réseaux sociaux, sites web ...

Exemple

- Retrouver le profile Facebook d'une personne, lequel mentionne son compte Spotify contenant le flag

LOCAL HOST

Les types de CTF

Les catégories

Hardware

- Challenge physique offline, nécessite de se connecter à un périphérique
- Débugger une carte Arduino, UART, hacker une voiture

Quest

- Une sorte de jeux de piste
- Déverrouillage de serrures, lecture de codes QR, ouverture de salles, de coffres

LOCAL HOST

Débuter dans les CTF

Warmup

S'entraîner

- **https://www.root-me.org** (fr)
- https://pwnable.tw/
- http://pwnable.kr/
- https://ctflearn.com/
- https://w3challs.com/ (fr)
- https://www.hackthissite.org/
- https://www.hackthebox.eu/

Ressources

- https://www.google.com/
- https://github.com/zardus/ctf-tools
- https://github.com/apsdehal/awesome-ctf
- http://forensicswiki.org/wiki/Main_Page
- https://www.owasp.org/index.php/Main_Page

LOCAL HOST

Débuter dans les CTF

Rejoindre ou créer un team

CTF Time

- Plateforme en ligne
- Calendrier CTF
- Classement des équipes
- Writeups

LOCAL HOST

Débuter dans les CTF

Les outils

Crypto

- featherduster
- findmyhash
- crackstation
- rsatool
- xortool
- hashcat
- john the ripper
- ophcrack

Forensics

- aircrack
- volatility

LOCAL HOST

Débuter dans les CTF

Les outils

Réseau

- wireshark
- zmap
- nmap

Reverse

- apktool
- binwalk
- gdb
- javadecompilers
- radare2
- windbg
- ghidra

LOCAL HOST

Débuter dans les CTF

Les outils

Stegano

- audacity
- exiftool
- imagemagick
- StegCracker
- steghide

WEB

- **burp**
- OWASP_Zed
- postman
- sqlmap
- w3af
- F12
- tamper-data

LOCAL HOST

Débuter dans les CTF

Conseils

- Participer à des CTF
- Travailler en groupe
- S’entraîner sur des sites spécialisés
- Participer à des Bugs-Bounties
- Lire beaucoup de Write-Ups (voir CTF Time)
- Être curieux !

LOCAL HOST

Pratique

Root-me.org

LOCAL HOST