CTF INEAT

Edition #1

Ineat

NEW TECHNOLOGY, NEW LEADERS

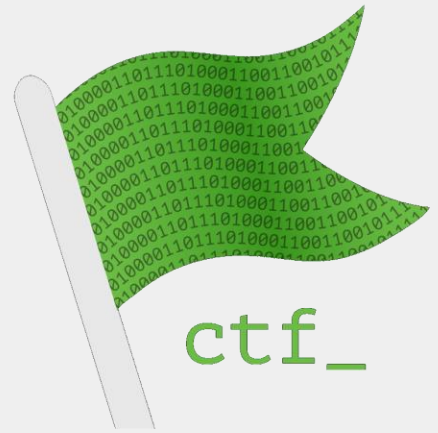
Disclaimer

Je décline toute responsabilité pour toutes les actions qui seront effectuées dans le cadre de ce CTF. Chaque participant est responsable de ses actes.

Le techniques, méthodes et outils découverts durant cet événement
sont à utiliser avec parcimonie et uniquement sur des environnements
qui vous appartiennent ou avec l'accord de leurs propriétaires.

Il est strictement interdit d'attaquer de quelques manières que ce soit les infrastructures INEAT.

Présentation générale



CTF : **C**apture **T**he **F**lag

Ensemble de challenges dont le but est de récupérer un « flag » par challenge.

Un flag est systématiquement sous la forme d'une chaine de caractères.

L'événement s'inscrit dans un esprit de cybersécurité.
Il va donc falloir creuser, réfléchir, chercher à comprendre le fonctionnement voire détourner le comportement normal des applications proposées pour récupérer ce « flag »

Il faut valider le challenge avec ce flag pour gagner les points correspondants.

Quel public ?

« White Hat »

- Les « gentils »
- Chercheurs en sécurité
- Hackers éthiques

« Nous »

- Noob
- Pour le plaisir
- S'entrainent
- Jouent aux CTFs !

« Black Hat »

- Les « méchants »
- Piratent pour l'argent, le plaisir, détruisent, font du tord, volent…
- Ransomware, Virus, Extorsion

Seul ou en équipe

Il est possible de participer seul ou en équipe.

Dans ce cas d’une participation en équipe, les validations comptent pour l’équipe entière.

Savoir vivre

L'environnement que je vous présente est mutualisé !

→ Cela signifie que vous travaillez tous sur la même machine..

1 machine unique ⟷ 20+ participants

<u>Deux règles</u> :

1. Restez discret – Effacez vos traces
2. Ne cassez rien (pas de « *rm –rf* » trop invasif, pas de DOS, pas de brute force, ..)

Challenges, Points et Indices

Chaque challenge rapporte des points.

Entre 10 et 150 points

Certains challenges possèdent des indices.
Chaque indice coûte des points.

Entre 10 et 15 points

Il y a **42 challenges** à débloquer pour un total de **2500 pts**

Challenges bonus *

Il y a **6 challenges** qui possèdent un ** à la fin de leur nom.

Si vous finissez ces 6 là, vous obtiendrez **100 points** supplémentaires !

Bon à savoir.

Dix catégories de challenge

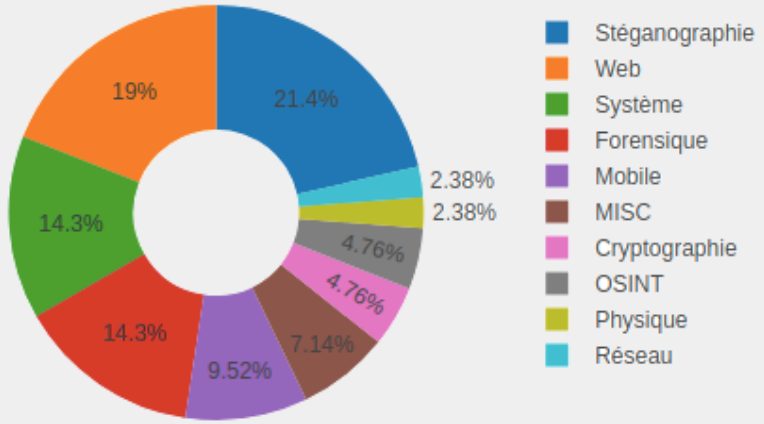
Web
Echange client / serveur

Forensique
Analyse et investigation de manière large

Système
Challenge autour des OS

OSINT
Open Source Intelligence / Stalking

Cryptographie
Chiffrement et Déchiffrement de données



Mobile
Android

Stéganographie
L'art de cacher des données dans des données

Physique
Challenge hardware

Réseau
Echange de données entre machines

MISC
Tout le reste

Les types de flag

Les flags peuvent-être sous deux formats différents :

- **APRK{**********}**
- **INEAT{**********}**

Quand ? Où ?

L’événement sera en ligne

Du **12 novembre à 12h30** Au **30 novembre à 23h59**

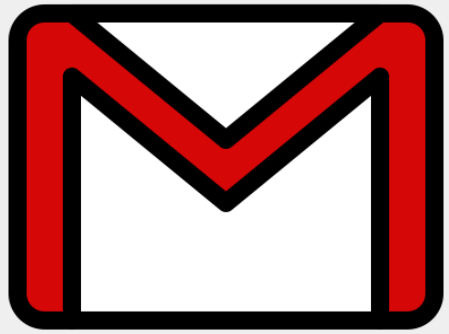
Sur

https://ctf.ineat.fr

Communication

slack

*Chaine **#ctf***



jdouliez@ineat.fr

Cadeaux

(1 cadeau par équipe)

Remerciements

Un grand merci à

Adeline GALASSO et **Maxime RENAUD**

qui m’ont aidé à créer quelques uns de ces challenges

Go !!