MINISTÈRE
DE L'ÉDUCATION
NATIONALE

Liberté
Égalité
Fraternité

Challenge Cybersécurité : **Passe Ton Hack d'abord** – Un challenge **'Capture The Flag'**

Organisé par le Commandement de la cyberdéfense (COMCYBER) du ministère des Armées et des anciens combattants en partenariat avec l'Éducation Nationale (Degesco).

Pour **toutes les lycéennes** et tous les lycéens de la seconde à Bac+2.

Inscription :

L'inscription au « CTF » est ouverte à toute classe de lycée de voie générale, technologique ou professionnelle, mentions complémentaires jusqu'au BTS en lycée.

Objet du challenge :

Le but de l'évènement est de :

- Résoudre les différents challenges proposés et découvrir les codes de victoire ou « flag ». Le format de soumission des flags est indiqué dans le descriptif de l'épreuve ;
- Valider ces flags afin d'obtenir des points. Le nombre de points accordés pour chaque épreuve est indiqué sur la plateforme du CTF. Un classement final sera établi à la fin des épreuves.

Modalité de participation et règlement :

https://eduscol.education.fr/document/53682/download

Lien d'inscription : https://magistere.education.fr/dgesco/

Compétences ciblées et références aux filières CIEL (Cybersécurité, **I**nformatique et réseaux, **EL**ectronique**) :**

Le challenge met en avant des compétences comme la recherche de vulnérabilités, le décryptage, ou encore l'analyse de systèmes, qui sont des éléments-clés du programme de la filière CIEL.

Le challenge est une forme de mise en pratique concrète des notions abordées en cours (sécurisation des données et des réseaux, etc.). Pour les futurs étudiants de la filière CIEL, ce type de défi peut agir comme un tremplin, leur permettant d'évaluer leurs aptitudes tout en se projetant dans des métiers spécifiques à la cybersécurité. Les modules de la filière CIEL (par exemple, ceux liés à l'administration des systèmes ou la gestion des risques) trouvent un écho direct dans les épreuves du challenge.

Pour illustrer les activités et tâches demandées aux participants on peut citer une liste non exhaustive d'actions à mener :

- Décrypter un message ;
- Pirater un mot de passe ;
- Écrire en langage codé Python ;
- Tester la sécurité d'un site web ;
- Rechercher dans les logs les tentatives de connexion depuis une même adresse IP ;
- Analyser les enregistrements ;
- Identifier si l'attaquant a réussi à accéder au système ;
- …

Liens avec la filière CIEL (Bac-Pro, BTS, Mentions Complémentaires) et liste non exhaustive de activités :

Modules d'analyse réseau et sécurité :

- Études des protocoles réseau (TCP/IP, HTTP) pour comprendre les schémas d'attaque.
- Utilisation d'outils d'analyse de trames de données et/ou un gestionnaire de logs pour décoder les données.

Cybersécurité proactive :

- Apprentissage des mécanismes de vulnérabilités et sécurisation des réseaux et des applications (Pare-feu, IDS/IPS, authentification).
- Gestion et analyse des données et traitements des incidents de sécurité.

Programmation et automatisation :

- Écriture de scripts simples en Python pour traiter les fichiers de logs automatiquement (exemple : repérer des motifs répétitifs dans les IP ou les timestamps).

Gestion des risques :

- Rédaction de recommandations pour améliorer la sécurité, comme enseigné dans les volets méthodologiques et organisationnels du programme.