Les épreuves de Passe ton hack d'abord 2025

Sommaire

Mission brief

Le CTF Passe ton hack d'abord est réalisé par le Commandement de la cyberdéfense (COMCYBER) du ministère des Armées et des anciens combattants, en partenariat avec le ministère de l'Éducation nationale. Renseignez-vous ici sur les opportunités d'études dédiées à la cyberdéfense (bac+2, bac+3, bac+5). Pour garder contact, suivez-nous sur le compte Instagram du CTF @Passetonhack.

Vous pouvez retrouver le règlement complet du challenge sur le site Eduscol :

ici

.

Scénario

Osland, partenaire historique de la France, est sous la menace directe du pays voisin Tobana. Ce dernier a basculé récemment sous un régime dictatorial et menace ouvertement la souveraineté de son voisin Osland. La principale raison en est économique, car Osland possède des mines de métaux rares ainsi que des puits de pétrole au large de ses côtes.

Au-delà des déplacements de troupes militaires tobanaises à ses frontières sous couvert d'exercices d'ampleur annuels et prévus de longue date, Osland constate une recrudescence d'incidents cyber, notamment sur ses infrastructures pétrolières. Depuis plusieurs semaines, elles subissent de nombreux DDOS ainsi que d'attaques de type Phishing. Ne possédant pas de capacité cyber suffisante, Osland fait appel à la France pour l'assister dans la sécurisation de ses réseaux.

Un GIC (Groupe d'Intervention Cyber) est déclenché à Rhyode sur les SI du groupe pétrolier national, qui semble être sous feu cyber ennemi. Ce fait est confirmé par le GIC, qui tente de contenir l'attaque et de maintenir les capacités de production d'Osland.

Le matériel d'analyse sur site n'étant pas suffisamment dimensionné, la décision est prise de conduire les prélèvements à la capitale Alryne afin de mener des investigations plus approfondies sur les malwares découverts dans les infrastructures réseaux du site. Durant son acheminement, l'hélicoptère conduisant le GIC subit une avarie et se crashe en territoire Tobanais.

Nous sommes actuellement sans nouvelles de l'équipage. Un commando est dépêché sur la zone du crash afin de localiser l'hélicoptère. Il faut impérativement retrouver l'équipe et sécuriser les données critiques qu'elle transporte.

Principe

Le CTF « Passe ton Hack d'abord » est constitué de 15 épreuves accessibles en ligne et portant sur des sujets de sécurité informatique (sécurité web, sécurité réseau, programmation, etc.). Dans ce cadre :

- chaque épreuve dispose d'un descriptif cadrant les attendus et scénarisant l'épreuve ;
- excepté pour les épreuves de type tutoriel, chaque épreuve nécessite de trouver un code de victoire caché ou « flag » ;
- les épreuves ont été spécifiquement étudiées pour être résolues par un public lycéen, certaines ont cependant un niveau de

difficulté plus élevé afin de départager les élèves.

Afin d'accomplir les différents challenges, vous pourrez vous aider des outils suivants :

- Outils de développement de votre navigateur
- Python
- Ghidra
- FTK Imager

Règles

1. 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.

2. Il est interdit :

   * d'attaquer la plateforme de compétition ou tout système qui n'est pas explicitement identifié comme cible ; * de partager les flags avec d'autres équipes ; * de donner accès à la plateforme ou de communiquer ses identifiants et mots de passe à toute personne n'appartenant pas à son équipe ; * de mener toute action non-conforme aux documents contractuels en vigueur de la plateforme du CTF ; * de partager des solutions ou de publier tout ou partie du contenu accédé lors de la compétition ;

Tout manquement à ces règles pourra entraîner l'exclusion de la personne et/ou de son équipe.

1. Le joueur est averti qu'un système de sécurité sera mis en place sur la plateforme de jeu.

Calcul des points

- les points sont attribués par épreuve en fonction de leur complexité. Le classement est actualisé en temps réel sur la plateforme de jeu. Le classement s'effectue en fonction du nombre de points et de la rapidité. En cas d'égalité de points entre deux équipes, l'avantage sera donné à l'équipe ayant été la plus rapide pour compléter l'intégralité des épreuves ou, à défaut de complétude intégrale, ayant été la plus rapide à résoudre les épreuves complétées (il ne sera pas pris en compte le temps effectif passé sur la plateforme, mais la date de complétude de la dernière épreuve réalisée) ;
- le classement sera arrêté par la DGESCO et le COMCYBER dans les jours suivants, et au maximum trois (3) semaines ouvrées, après la fin du CTF (soit avant le 28 février 2024). Le classement général sera divisé en 3 catégories : la catégorie « Lycées de la Défense » (tous niveaux), la catégorie « pré-BAC » et la catégorie « post-BAC » ;
- à l'issue de l'évènement Cinq (5) équipes gagnantes seront identifiées selon les critères suivants : trois (3) équipes « pré-BAC », une (1) équipe « post-BAC », et une (1) équipe « Lycées de la Défense » ;
- la remise des prix s'effectuera au courant du mois de mars au Campus Cyber. La date est sujette à modification en fonction notamment de la disponibilité des autorités présentes à la remise des prix et aux capacités de déplacement des élèves et enseignants des équipes gagnantes.