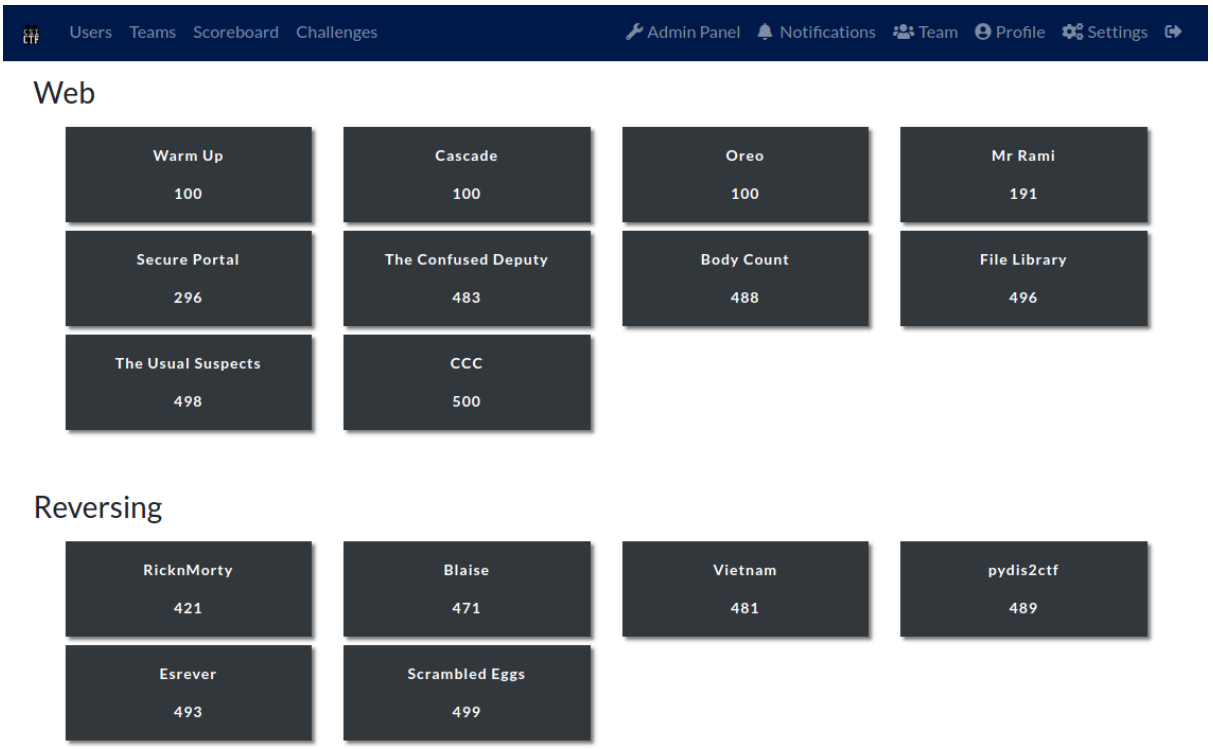
Les CTF

Qu'est-ce qu'un CTF en cybersécurité ?

Un CTF (Capture The Flag) en cybersécurité est un exercice pratique basé sur des défis où les participants doivent résoudre des problèmes de sécurité pour "capturer" des "drapeaux" virtuels. Ces drapeaux sont généralement des morceaux de texte cachés que l'on découvre en exploitant des vulnérabilités, en effectuant de l'ingénierie inverse ou en analysant le trafic réseau.



Sur cette image, l'interface principale d'un CTF où on voit les défis, les catégories et le nombre de points.

Qu'est-ce qu'un flag ?

Un flag est une chaîne de caractères spécifique qui sert de preuve pour valider la résolution d'un défi. Il suit généralement un format précis défini par les organisateurs du CTF, souvent sous forme : `CTF{texte_ou_hash}` ou `flag{texte_ou_hash}`. Par exemple, après avoir exploité une faille SQL dans une application web, vous pourriez trouver un flag comme : `CTF{SQL_1nj3ct10n_M4st3r_2024}`. La soumission de ce flag exact prouve que vous avez réussi le défi.

Types de CTF

1. Style Jeopardy : Les participants résolvent, en équipe ou individuellement, des défis classés par catégories (cryptographie, ingénierie inverse, forensic, exploitation web, exploitation binaire, etc.). Chaque défi contient un drapeau à capturer.
2. Attaque-Défense (Rouge vs Bleu) : Les équipes doivent attaquer les systèmes des autres tout en défendant les leurs. Ce type de CTF simule des scénarios de cyberattaque du monde réel.
3. Mixte : Une combinaison des deux types ci-dessus, avec des défis de style Jeopardy et des éléments d'attaque-défense.

Objectifs des CTFs

- Développement de compétences : Pratiquer et améliorer des compétences techniques (hacking éthique, forensic, ingénierie inverse, etc.).
- Expérience d'apprentissage : Acquérir une expérience pratique des concepts de cybersécurité.
- Collaboration en équipe : Encourager le travail d'équipe et la résolution de problèmes dans des délais serrés.
- Compétitions : Souvent organisés lors de conférences (comme DEFCON) ou lors d'événements autonomes où les participants concourent pour des prix, de la reconnaissance ou des opportunités professionnelles.

Qui devrait essayer les CTFs ?

- Débutants : Excellente manière d'apprendre et de mettre en pratique les concepts de sécurité.
- Passionnés et étudiants en cybersécurité : Pour affiner leurs compétences en hacking.
- Professionnels : Pour tester et améliorer leur expertise technique.

Ce qu'un CTF n'est pas :

- Un audit de sécurité professionnel ou une recherche de vulnérabilités (*bug bounty*) sur des systèmes en production: Les CTF utilisent des environnements contrôlés spécifiquement conçus pour l'apprentissage.
- Une formation complète en cybersécurité: Les CTF se concentrent souvent sur des aspects techniques spécifiques et ludiques, laissant de côté des compétences essentielles comme la gestion des risques ou la conformité.
- Une reproduction fidèle d'attaques réelles: Les défis sont simplifiés et isolés pour se concentrer sur des concepts précis, contrairement aux incidents réels qui sont plus complexes et interconnectés.

- Une activité illégale: Les CTF se déroulent dans des cadres éthiques et légaux stricts, avec des cibles désignées et des règles claires.
- Une compétition pour hackers confirmés uniquement: Les CTF existent pour tous les niveaux, y compris les débutants, et constituent un excellent outil d'apprentissage.

Catégories communes dans les CTF

- Web: Exploitation de vulnérabilités web comme XSS, SQLi, LFI, command injection, broken authentication, et désérialisation. Nécessite des connaissances en HTTP, JavaScript, PHP et architectures web.
- Binary Exploitation (pwn): Exploitation de binaires pour obtenir des accès non autorisés. Couvre le buffer overflow, ROP chains, format string, heap exploitation. Requiert des bases en assembleur et C.
- Reverse Engineering: Analyse de binaires pour comprendre leur fonctionnement sans accès au code source. Utilise des désassembleurs et débogueurs. Demande des connaissances en programmation bas niveau.
- Cryptographie: Casser ou exploiter des implémentations cryptographiques faibles. Couvre les chiffrements classiques et modernes, hashing, et protocoles cryptographiques. Nécessite des bases en mathématiques.
- Forensics: Analyse de fichiers, mémoire, trafic réseau et systèmes pour trouver des preuves. Utilise des outils d'analyse comme Volatility, Wireshark. Demande une bonne méthodologie d'investigation.
- Steganographie: Découverte d'informations cachées dans des fichiers média. Analyse de fichiers images, audio, et vidéo. Utilise des outils spécialisés pour détecter et extraire des données.
- Mobile: Exploitation d'applications Android/iOS. Couvre le reverse engineering d'APK, analyse de trafic mobile, et vulnérabilités spécifiques aux plateformes mobiles.
- Hardware: Exploitation de systèmes embarqués et circuits. Analyse de protocoles comme I2C/SPI, radio (SDR), et firmware. Demande des connaissances en électronique.
- OSINT: Recherche d'informations à partir de sources publiques. Couvre la reconnaissance passive, analyse de métadonnées, et investigation sur les réseaux sociaux.
- Miscellaneous: Défis variés ne rentrant pas dans les autres catégories. Peut inclure la programmation, les casse-têtes logiques, ou l'automatisation.

Comment trouver des CTF auxquels participer ?

astuce

CTF Time est la plateforme de référence dans le monde des CTF, servant à la fois de calendrier global des compétitions et de système de classement des équipes.

- PicoCTF: PicoCTF est un CTF éducatif créé par Carnegie Mellon University, spécialement conçu pour les débutants et les étudiants.
- Hackfest (Québec, QC): L'un des plus grands événements de sécurité informatique au Canada, se déroulant annuellement à Québec.
- NorthSec (Montréal, QC): Plus grand CTF technique au Canada, organisé à Montréal, combinant conférence et compétition intensive.

Que fait-on après un CTF ?

Les *write-ups* sont des documents détaillés qui expliquent la résolution d'un challenge ou d'une machine de CTF étape par étape. Ils décrivent la méthodologie utilisée, les outils employés, les vulnérabilités découvertes et la manière de les exploiter pour obtenir le flag. Ces ressources sont précieuses pour apprendre de nouvelles techniques, comprendre les erreurs commises et découvrir des approches différentes.

Il est courant que les participants partagent leurs write-ups après la fin d'un CTF, contribuant ainsi à l'apprentissage collectif de la communauté. Les plateformes comme CTFTime et Medium regorgent de write-ups qui constituent une véritable base de connaissances en cybersécurité. Cependant, il est recommandé d'essayer de résoudre les challenges par soi-même avant de consulter les write-ups, afin de maximiser l'apprentissage.