ESILV
ENGINEERING SCHOOL
DE VINCI PARIS

DaVinciCode

DaVinciCTF 2023: Cahier des charges

1 Introduction

Une compétition Capture The Flag (CTF) est une compétition de cybersécurité, dans laquelle les participants doivent énumérer et exploiter des failles informatiques dans des environnements délibérément vulnérables afin de retrouver des flags (des chaînes de caractères formatées et donc facilement repérables, tel que `ESILV{c3c1_3st_1_fl4g}`) qui leur permet d'obtenir des points.
Ces compétitions regroupent plusieurs catégories, telles que la cryptographie, la stéganographie, le web, l'algorithmie, etc. Les CTF s'adressent aux personnes intéressées par la sécurité informatique et qui souhaitent s'exercer et apprendre : les participants partagent leurs solutions des challenges à la fin de la compétition. Nous proposons d'organiser un tournoi CTF, pour :

- développer la majeure IOS
- faire découvrir la cybersécurité aux étudiants qui n'ont toujours pas choisi de majeure
- faire découvrir l'ESILV aux participants souhaitant poursuivre leurs études dans une école d'ingénieur

2 Informations pratiques

2.1 Années recherchées

- A2
- A3
- A4
- A5

2.2 Connaissances pré-requises

- Participation à des CTF et/ou wargames (root-me, THM, HTB)
- Maîtrise d'un langage de programmation pertinent pour une catégorie de challenge
  - Reverse : C, C++, C#, Go, Rust ...
  - Web : PHP, Javascript, Python, .NET ...
  - Pwn : C
  - Cryptographie : Python, Sage
  - Android : Java, Kotlin
  - Programmation : Python...
  - Web3 : Solidity...
- Maîtrise de l'anglais lu

2.3 Connaissances appréciées

- Maîtrise particulière d'une catégorie commune ou non en CTF (il existe des challenges sur Discord, sur Minecraft, etc.)
- Containerisation (Docker)
- Gitlab CI/CD

3 Détail du projet

Nous voulons réaliser un tournoi CTF en ligne qui soit accessible aux personnes débutantes. Pour cela, nous allons devoir:

- Héberger un site web (landing page, plateforme CTF et challenges) avec l'utilisation du framework CTFd.
- Créer des challenges intéressants dans plusieurs catégories et rédiger (tout ou en partie) leurs solutions. Un total d'environ une trentaine de challenge serait souhaitable, réparti plus ou moins également dans les catégories choisies (pas de challenge seul dans une catégorie ni de catégorie trop dominante). Les challenges pourront varier en difficulté pour pouvoir rendre le CTF abordable aux débutants comme aux confirmés.
- Administrer un serveur discord
- Tenter de trouver des sponsors pour financer les prix et/ou l'hébergement.
- Communiquer sur l'existence de ce tournoi.

4 Détails techniques

Les challenges devront être classifiés dans une des catégories suivantes : Web, Forensics, Reverse, Pwn, OSINT/Recon, Programmation, Hardware/Réseau, Stéganographie, Cryptographie, Blockchain/S3, Misc. Toutes les catégories ne devront pas forcément être représentées. Toute autre catégorie non mentionnée ici devra être approuvée par l'association.
Les flags devront tous suivre le format suivant (et en respectant la casse): `dvCTF{ascii}`.
Plusieurs contraintes techniques vont être présentes pour la création des challenges.

4.1 Challenges dynamiques

Les challenges dits « dynamiques » sont des challenges ayant besoin d'une connexion à internet (très souvent dans les catégories pwn, web, cryptographie).

- Chaque challenge devra être soumis par son créateur sous la forme d'un ou plusieurs conteneurs docker (avec des permissions minimums, voir ce lien et autres documentations pour éviter tout problèmes en cas de compromission de la machine) pour une mise en production et un redémarrage plus rapide en cas de problèmes.
- Un seul serveur sera mis à disposition de l'équipe pour faire leurs tests. Ce serveur sera accessible à travers un VPN Wireguard pour éviter les regards indiscrets (participants ayant accès aux challenges avant le début du CTF). Un deuxième serveur, plus performant, sera disponible pendant et

après le CTF pour les challenges dynamiques, et le premier sera monté en gamme pour permettre l'hébergement du CTFd (plateforme de soumissions des flags) ainsi que de la base de données avec les challenges statiques.

4.2 Challenges statiques

Les challenges statiques sont des challenges qui se présentent sous la forme d'énoncés, souvent joints de fichiers.

- Si les fichiers sont trop volumineux, pensez à les compresser avec un algorithme de compression (gzip, xz).