4. Projet : conception d'un orchestrateur de scanners de vulnérabilités

L'objectif de ce projet est de concevoir et implémenter un **orchestrateur** permettant de **contrôler à distance plusieurs scanners de vulnérabilités** (à savoir **Nmap, OWASP ZAP et Nikto**). Cet orchestrateur doit permettre l'exécution, la collecte et la centralisation des résultats des analyses de sécurité sur un ou plusieurs hôtes cibles.

Fonctionnalités attendues

1. **Orchestration des scanners**
    - L'orchestrateur doit être capable d'envoyer des commandes aux scanners distants et de récupérer leurs résultats.
    - Les scanners supportés sont **Nmap**, **OWASP ZAP** et **Nikto**.
    - Il doit permettre de configurer les paramètres de scan (cibles, types de tests, options spécifiques à chaque outil).
2. **Agent distant pour exécuter les scans**
    - Un **agent distant** devra être développé pour exécuter les scanners sur différentes machines.
    - L'agent devra recevoir des instructions depuis l'orchestrateur et lui transmettre les résultats après exécution.
    - La communication entre l'orchestrateur et les agents devra être chiffrée pour garantir la confidentialité et l'intégrité des échanges**.**
3. **Collecte et synthèse des résultats**
    - L'orchestrateur doit agréger les résultats des différents scanners.
    - Il doit fournir une vue synthétique des vulnérabilités détectées.

Autres consignes

- Le projet doit être **développé en C** avec une architecture reposant sur un **orchestrateur central** et des **agents distants**. La communication entre l'orchestrateur et les agents doit être **sécurisée**.
- **Important** : il est impératif que toutes les expérimentations soient effectuées dans un **environnement contrôlé et isolé**. Il est strictement interdit d'utiliser les scanners sur un réseau réel, que ce soit un réseau de l'école, d'un hébergeur, ou d'Internet. Pour éviter tout impact involontaire sur des systèmes externes, vous devez obligatoirement utiliser une **infrastructure virtualisée** comme **docker**, une machine virtuelle locale (VirtualBox, VMware) ou un **cyber-range** dédié.
- L'objectif est de comprendre le fonctionnement de scanners dans un cadre pédagogique et sécurisé, sans causer de perturbations ou de dommages. Toute infraction à cette règle peut avoir des **conséquences légales et disciplinaires**.

Références

- **Scanner Nmap** : https://nmap.org/
- **Scanner OWASP ZAP** : https://www.zaproxy.org/
- **Scanner Nikto** : https://cirt.net/nikto2