TP : Support, Mise à Disposition et Cybersécurité

Ce TP combine deux domaines essentiels : le support/mise à disposition d'infrastructures et la cybersécurité. Vous travaillerez en équipes transversales pour simuler un cycle complet de vie d'une application, de son déploiement à sa sécurisation.

Objectifs des Missions

Le projet se déroule en plusieurs étapes où chaque équipe passera par différents rôles :

1. **Infrastructure/Support** : Mise en place de l'environnement.
2. **Red Team (Attaque)** : Audit et exploitation des failles.
3. **Blue Team (Défense)** : Remédiation et sécurisation (étape suivante).

Déroulé du TP

Étape 1 : Déploiement et création des comptes

Instructions :

- Se mettre en équipe (garder les équipes du "hackathon").
- Déploiement de **3 nouvelles VM Debian** :
  - **VM 1 : GLPI** (Gestion des incidents et inventaire).
  - **VM 2 : Backend** (Serveur API PHP).
  - **VM 3 : FrontEnd** (Interface utilisateur statique).
- Configuration du réseau pour que les machines communiquent entre elles.
- Création des comptes utilisateurs sur GLPI pour l'équipe Red Team.

Ressources :

- ISO Debian serveur (Image d'installation).
- Repository GitHub Backend : API PHP.
- Repository GitHub Frontend : HTML/CSS/JS.

Résultat attendu :

- 3 VM Debian fonctionnelles avec 3 adresses IP distinctes et accessibles.
- Instance GLPI configurée avec les comptes utilisateurs pour la Red Team.

Étape 2 : Red Team — Audit, détection de failles & rapport sur GLPI

Instructions :

- **Audit de sécurité** : Identifier le maximum de failles sur l'infrastructure d'une autre équipe (périmètre autorisé uniquement).
- **Périmètre** : Attaquer exclusivement l'adresse IP fournie par l'équipe adverse.

- **Référencement** : Chaque faille trouvée doit être documentée précisément via un ticket sur le GLPI de l'équipe auditée.

Ressources :

- Fiches mémo et PDF explicatifs sur les types d'attaques (DDoS, XSS, Injections SQL, IDOR, etc.).
- Outils d'audit (Nmap, Burp Suite, etc.).

Résultat attendu :

- Un ensemble de tickets GLPI détaillant chaque vulnérabilité trouvée (description, preuve de concept, criticité).

Étape 3 : Blue Team — Remédiation (À venir)

Cette étape consistera à corriger les failles signalées dans GLPI pour sécuriser l'infrastructure.