ACxx.xx – Proposer une architecture sécurisée de système d'information pour une petite structure

Mise en place lors de la SAE CTF

📌 Contexte

Dans le cadre de la **SAE CTF**, l'objectif était de concevoir et déployer une **architecture réseau sécurisée** pour une **petite structure** en intégrant des solutions adaptées aux besoins en **sécurité, connectivité et administration**. Cela impliquait le choix et la mise en place des équipements réseau et systèmes tout en assurant la **haute disponibilité**, la **supervision** et la **protection contre les cybermenaces** (IDS/IPS, pare-feu, VPN, segmentation réseau, etc.).

📚 Savoir mis en œuvre

- **Concepts de sécurité des systèmes d'information** : principes de défense en profondeur, segmentation réseau, contrôle des accès, durcissement des systèmes.
- **Sécurisation réseau** : pare-feu, VLANs, IDS/IPS, VPN, filtrage web et proxy.
- **Matériels et solutions de protection** : choix de composants comme **switchs managés**, **routeurs**, **firewalls**, **Wi-Fi sécurisé**, etc.
- **Surveillance et supervision** : intégration d'une solution de **SIEM** pour la collecte et l'analyse des logs réseau.
- **Gestion des accès** : mise en place d'un **contrôle d'accès strict** (authentification multi-facteurs, gestion des droits utilisateurs).

🛠️ Savoir-faire mis en œuvre

✅ **Définition des besoins** : identification des besoins en connectivité et sécurité de la structure.
✅ **Conception de l'architecture réseau** : élaboration d'un schéma détaillé intégrant VLANs, pare-feu, IDS/IPS et VPN.
✅ **Déploiement des équipements** : configuration des switchs, routeurs, firewalls et points d'accès Wi-Fi sécurisés.
✅ **Configuration d'un IDS/IPS** : mise en place de **Wazuh** pour la détection des intrusions.

✅ **Mise en place d'un VPN sécurisé** : installation et configuration d'un VPN **OpenVPN** pour l'accès distant sécurisé.
✅ **Surveillance du réseau** : intégration de **Wazuh** pour la supervision des logs et détection des anomalies.
✅ **Test et validation** : simulations d'attaques pour vérifier la résilience de l'architecture.

🎭 **Savoir-être mis en œuvre**

- **Rigueur** : respect des bonnes pratiques en matière de sécurité réseau.
- **Analyse** : évaluation des vulnérabilités et proposition de solutions adaptées.
- **Réactivité** : adaptation aux incidents et amélioration continue de la solution.
- **Collaboration** : travail en équipe pour assurer l'interopérabilité des équipements et services.

✅ **Tâches réalisées et résultats**

📌 **Tâches effectuées**

✅ **Conception d'un plan d'architecture réseau sécurisé**, avec segmentation des différents services (serveurs, postes clients, Wi-Fi invité, etc.).
✅ **Mise en place d'un pare-feu avec filtrage avancé** pour contrôler le trafic entrant et sortant.
✅ **Configuration d'un IDS/IPS avec Wazuh** pour détecter et bloquer les menaces en temps réel.
✅ **Déploiement d'un VPN sécurisé** pour permettre un accès distant aux collaborateurs.
✅ **Installation d'une solution de supervision réseau** (Wazuh + ELK) pour centraliser et analyser les logs.
✅ **Tests de cybersécurité** pour évaluer la résistance aux attaques (scan de ports, attaques de type Man-in-the-Middle, tentatives d'intrusion).

🎯 **Résultats obtenus**

- Une **infrastructure réseau sécurisée** avec un **pare-feu filtrant**, un **IDS/IPS**, et une segmentation via **VLANs**.
- Une **authentification forte et sécurisée** pour les utilisateurs grâce à un VPN avec certificats.

- Une **surveillance proactive** du réseau et des systèmes via Wazuh et ELK.
- Une **capacité de détection et réponse aux menaces** grâce aux logs et aux alertes automatisées.
- Une **réduction des risques d'attaques externes** grâce au **filtrage avancé** et aux **politiques de sécurité strictes**.