Mohamed Horma MOHAMED EL MOKHTAR

COMPÉTENCES

- Programmations: C, Java, Python
- Web : HTML, CSS, JAVASCRIPT
- Basse de données: SQL, PostgreSQL
- Mathématiques
- Algorithmique

Sujet de Stage : Mise en place d'une Infrastructure à Clé Publique (PKI) pour la sécurisation des systèmes d'information

Contexte :

Dans un contexte de digitalisation croissante, la sécurisation des échanges électroniques est un enjeu stratégique pour les entreprises et institutions. La mise en place d'une Infrastructure à Clé Publique (PKI) permet de garantir l'authenticité, la confidentialité, l'intégrité et la non-répudiation des communications et des documents numériques.

Objectif du stage :

Concevoir et mettre en œuvre une solution PKI interne, conforme aux standards internationaux, pour répondre aux besoins de sécurité de l'organisation : signature électronique, chiffrement des emails, authentification forte, etc.

Missions principales :

1. Étude théorique et veille technologique sur les infrastructures PKI, les certificats X.509 et les normes associées (RFC, ETSI, eIDAS…).
2. Analyse des besoins de l'entreprise : cas d'usage, niveaux de sécurité, types de certificats (serveurs, utilisateurs, machines…).
3. Choix des outils et solutions (ex : EJBCA, Microsoft ADCS, OpenXPKI, HashiCorp Vault PKI, etc.).
4. Mise en œuvre de l'architecture PKI : racine, sous-autorité(s), politiques de certification (CP/CPS), génération et gestion des clés, CRL, OCSP.
5. Intégration avec les services existants (LDAP, SSO, VPN, messagerie…).
6. Élaboration de la documentation technique et des procédures d'exploitation.
7. Formation des utilisateurs administrateurs sur la gestion des certificats.

Résultats attendus :

- Une PKI fonctionnelle et sécurisée déployée dans un environnement de test ou de préproduction.
- Une documentation complète (technique et utilisateur).
- Une analyse des risques et des recommandations pour l'environnement de production.

Profil recherché :

- Étudiant(e) en dernière année d'école d'ingénieur ou Master 2 en cybersécurité, systèmes ou réseaux.
- Connaissances en cryptographie, protocoles de sécurité, systèmes Linux/Windows.
- Capacité à rédiger une documentation claire et structurée.

Durée : 4 à 6 semaines
Lieu : Siège SMART
Encadrement : Équipe IT/Sécurité de l'entreprise