Projet Final - Cyber

Contexte

Votre client est la société Company01 représentée par M. Jean Truc, Directeur du système d'information. Il vous a directement contacté afin que vous puissiez procéder à des certaines vérifications de sécurité au sein de son environnement car celui-ci a besoin d'appui afin de dresser sa roadmap sécurité.

Pour le moment, le projet ne porte que sur une application unique qui est en cours de développement en interne chez Company01, il s'agit du AlexCloud. Une solution ayant comme ambition de remplacer les solutions de stockage en Cloud hébergé comme NextCloud ou OwnCloud.

Ce projet est divisé en plusieurs grandes parties :

Partie 1 - Audit

Le client souhaite que vous commenciez par une étude de l'existant et du niveau de sécurité actuel de l'application. Pour ce faire, il sera nécessaire de décomposer votre analyse en deux points de vue distincts, une vision offensive et une vision défensive.

Vision offensive (pentest) :

Votre rôle est de découvrir et recenser l'intégralité des vulnérabilités visibles et potentiellement exploitables par un attaquant.

Le client a une exigence stricte sur le rendu et souhaite qu'il suivre un modèle qui vous sera fourni pour l'occasion.

Vision défensive (durcissement) :

Votre rôle est de découvrir tous les problèmes d'implémentation et de configuration des services présents sur la machine.

Dans le cadre de cet audit défensif, il vous est demandé de vous reposer exclusivement sur les travaux de l'ANSSI et du CIS. Toute utilisation d'un autre référentiel de sécurité devra être motivé et fortement défendu lors de la restitution.

> Note : Cette vision défensive s'appelle un audit de conformité. Il existe des solutions permettant de faciliter cet audit (Nessus, OpenVAS, ...)

Pour ces deux visions, il sera nécessaire d'inclure dans vos retours les recommandations d'actions à mener pour améliorer le niveau de sécurité global de la solution ainsi que le niveau de priorité correspondant.

Chaque vulnérabilité devra faire l'objet d'un score de sévérité logique utilisant les métriques du NIST à ce sujet : https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator

Partie 2 - Sécurisation

Vous ne pouvez pas vous arrêter simplement sur le listing des vulnérabilités présentes. Il vous est demandé de fournir des solutions concrètes aux problèmes et d'améliorer fortement le modèle d'implémentation de l'application et de les mettre en oeuvre.

Cette mise en œuvre se fera également en deux temps :

1. La mise en place des correctifs directement sur la machine fournie afin de démontrer la mise en application simple de ceux-ci aussi bien au niveau du code source que des configurations du système qui supporte l'application
2. Le redéploiement global de la machine dans un meilleur contexte de sécurité

La phase de redéploiement doit inclure l'implémentation de modules de sécurité complémentaires sur la machine. A ce titre, M. Truc a son idée sur la question et souhaite vous faire des propositions :

- Implémentation d'un système de centralisation des journaux
- Implémentation d'un WAF au niveau du service web
- Implémentation d'un service de détection d'anomalie dans les journaux
- Implémentation d'un SIEM
- Implémentation d'un scan automatisé régulier des vulnérabilités
- Implémentation d'un HIDS sur la machine
- Implémentation d'un NIDS sur la machine
- Implémentation d'un cluster de base de données

M. Truc sait cependant bien qu'il va être compliqué d'implémenter correctement l'ensemble de ces solutions. Il vous demande au minimum de vous renseigner sur chacun de ces besoins et de proposer des solutions avec un comparatif des différents éléments importants pour la sécurité au sein de ces solutions.

Un point doit absolument être implémenté : un système de centralisation des journaux dans l'optique de créer un SIEM par la suite. Pour le reste, le client souhaite voir un maximum de PoC et pourquoi pas des implémentations complètes au sein de l'environnement de l'application.

Il sera important de garder en tête que ces solutions devront pouvoir être déployées sur tout le parc informatique de M. Truc.

Partie 3 - Sécurisation

M. Truc commence à réaliser que le problème vient en premier lieu de la manière dont ses équipes de développement travaillent. Il souhaite vous mettre en concurrence avec sa propre équipe afin de voir qui peut être en mesure de proposer la meilleure version de l'application AlexCloud.

Aucun cahier des charges ne vous sera fourni, il sera donc nécessaire de procéder à la rétro ingénierie de l'application pour en comprendre son fonctionnement et son modèle d'implémentation logicielle.

Tous vos développements devront par contre absolument suivre un modèle de développement sécurisé. Il vous sera demandé de démontrer la manière dont vous avez assuré les meilleures pratiques de développement et d'implémentation de votre nouvelle version de l'application.

Gestion de projet

Le client souhaite ne travailler qu'avec des professionnels accomplis. Pour ce faire, il souhaite notamment pouvoir vous suivre et suivre l'avancée du projet qu'il vous a confié.

Il vous est donc demandé de produire dès le départ un planning prévisionnel d'avancée des différentes tâches qui composent le projet.

Egalement et étant donné la durée du projet dans le temps, M. Truc souhaite passer en revue régulièrement votre avancée au travers de pré-recettes qui auront lieu en fin de chaque semaine de projet. Il sera alors nécessaire lors de ces échanges de présenter votre système de planification ainsi que les dérives potentielles par rapport aux éléments prévisionnels.

M. Truc est connu pour ses humeurs changeantes, il n'est pas impossible qu'il décide pendant ces échanges de modifier des grosses parties du projet, il sera donc de votre devoir de cadrer ces changements pour qu'ils ne vous empêchent pas d'accomplir pleinement vos tâches. Ne vous engagez pas sur une réalisation complémentaire qui pourrait mettre en péril le projet dans sa globalité.

Le dernier jour du projet sera dédié à une présentation générale de tous les éléments du projet devant M. Truc qui s'assurera que ses différentes directives au cours du projet ont bien été suivies et que le projet est pleinement finalisé.