168h - Fiche Projet

Sommaire

Contextualisation

Dans le cadre de notre programme de formation, nous avons une semaine dédiée au projet appelée les 168H. Au cours de cette semaine, l'objectif de ce projet est de concevoir un outil capable d'identifier les vulnérabilités de sécurité dans les systèmes informatiques..

Problématique

Imaginez une entreprise qui néglige la collecte régulière de données sur les vulnérabilités de ses systèmes informatiques. Au fil du temps, des failles de sécurité se développent sans être détectées, exposant ainsi l'entreprise à des risques croissants d'attaques informatiques. Lorsqu'une tentative d'intrusion survient, l'absence de mise à jour des données sur les vulnérabilités rend difficile l'interprétation des résultats du scan. Les équipes de sécurité se retrouvent dans l'incapacité de réagir rapidement et efficacement pour corriger les failles de sécurité, laissant ainsi les systèmes et les données de l'entreprise vulnérables aux attaques. La solution, utiliser des outils de scan de port et de vulnérabilité pour couvrir 100% des besoins cette méthode nécessite cependant d'utiliser plusieurs outils afin de couvrir l'ensemble des vulnérabilités.

Plus Value Technique

À partir d'outils d'analyses, d'un outil de scan de ports, services et autres détections de vulnérabilités, nous voulons apporter un rapport plus détaillé que ce que peut offrir un simple scan aujourd'hui. La plus value technique réside dans la centralisation d'outils qui permettent de balayer un large spectre pour la détection de vulnérabilités. Le développement de cette solution permettra de développer des compétences techniques comme du développement réseau, du développement web pour la mise en place d'une interface graphique de ce rapport, la maîtrise de plusieurs outils open Source utilisés dans le domaine de la sécurité des systèmes ainsi que de la connaissance réseau pour utiliser ces mêmes outils.

Description du projet

Notre solution

La solution proposée est un outil de sécurité informatique complet qui offre plusieurs fonctionnalités essentielles pour évaluer et renforcer la sécurité des systèmes informatiques. Voici une description détaillée de chaque fonctionnalité :

Scan des ports et services : Cet outil est capable de scanner les ports ouverts sur un ordinateur ou un réseau. Il utilise des techniques de balayage pour identifier les ports qui sont actuellement accessibles et les services qui y sont associés. Cela permet aux administrateurs de systèmes de comprendre quels services sont exposés et de prendre des mesures pour sécuriser les ports non nécessaires.

Détection des vulnérabilités : L'outil est équipé d'une base de données de vulnérabilités connues dans les logiciels et les systèmes d'exploitation. En analysant les configurations système et les versions logicielles, il peut identifier les vulnérabilités potentielles qui pourraient être exploitées par des attaquants. Cette fonctionnalité est cruciale pour anticiper les failles de sécurité et les corriger avant qu'elles ne soient exploitées.

Évaluation des risques : Une fois les vulnérabilités détectées, l'outil évalue le niveau de risque associé à chacune d'elles. Il prend en compte divers facteurs tels que la criticité de la vulnérabilité, la probabilité d'exploitation et l'impact potentiel sur le système. Cette évaluation permet aux administrateurs de hiérarchiser les correctifs et de se concentrer sur les vulnérabilités les plus critiques en premier.

Génération de rapports : Enfin, l'outil génère des rapports détaillés sur les vulnérabilités détectées. Ces rapports incluent des informations sur les vulnérabilités spécifiques, les services affectés, les risques associés et des recommandations pour les corriger. Ces rapports sont précieux pour les équipes de sécurité informatique, car ils fournissent une vue d'ensemble claire de l'état de la sécurité du système et des mesures à prendre pour l'améliorer.

Rapport automatisé : Une évolution facultative sera de mettre en place un lancement automatisé des analyses et d’automatiser l’envoie des rapports, on pourra également envoyer des alertes en cas de vulnérabilités importantes détectées.

En résumé, cette solution offre une approche holistique de la sécurité informatique en identifiant les vulnérabilités, en évaluant les risques et en fournissant des recommandations pour renforcer la sécurité des systèmes informatiques. Elle est essentielle pour les entreprises et les organisations cherchant à protéger leurs actifs numériques contre les menaces potentielles.

Les technologies utilisées

La solution repose sur un ensemble de technologies open source et un langage de programmation puissant et flexible pour fournir une solution complète de sécurité informatique :

Nmap : Utilisé pour le scan des ports et la découverte de services, Nmap est un outil open source largement reconnu dans le domaine de la sécurité informatique. Il offre une gamme de fonctionnalités pour identifier les ports ouverts, les services qui y sont associés et d'autres informations essentielles sur les systèmes cibles.

Nessus et OpenVAS : Ces deux outils open source sont spécialisés dans la détection de vulnérabilités. Ils utilisent des bases de données de vulnérabilités connues pour analyser les systèmes et identifier les failles de sécurité potentielles. Nessus et OpenVAS fournissent des rapports détaillés sur les vulnérabilités détectées, aidant ainsi les équipes de sécurité à prendre des mesures correctives appropriées.

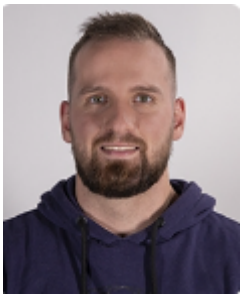
Python : En tant que langage de programmation puissant et flexible, Python est utilisé pour intégrer et automatiser les fonctionnalités des outils mentionnés ci-dessus. Grâce à sa syntaxe claire et à sa vaste gamme de bibliothèques, Python est idéal pour le développement d'outils de sécurité personnalisés, la création de scripts pour l'automatisation des tâches de sécurité et l'analyse des données de sécurité.

En combinant Nmap pour le scan des ports et la découverte de services, Nessus et OpenVAS pour la détection de vulnérabilités, et Python pour l'intégration et l'automatisation, cette solution offre une approche complète pour évaluer et améliorer la sécurité des systèmes informatiques. Elle permet aux équipes de sécurité de détecter les vulnérabilités, d'évaluer les risques associés et de prendre des mesures correctives appropriées pour renforcer la sécurité globale des systèmes.

Description de l’équipe

Composition de l’équipe

Elie
Dev-Back



Anthony
Front

Gwendal
Réseau

Emeric
Full-Stack

Responsabilité de chacun dans le projet

Elie :

- Récupérer les logs des outils
- Traiter la donnée
- Veille technique

Anthony :

- Mettre en valeur la donnée
- Vulgariser la donnée pour un public pas forcément technique
- S’assurer que le produit soit fini et déployée

Gwendal :

- Déployer les outils de vulnérabilités

- Manipuler ces outils (scanner les ports, les services, …)
- Veille technique

Emeric :
- Intégration front / back
- Renfort sur les équipes au besoin
- S’assurer que le produit soit fini et déployée

Nous aurons tous la responsabilité de maintenir sa documentation à jour.

Méthodologie de travail

Nous utiliserons la méthode kanban qui permet d’avoir une mise en place de notre organisation rapidement puisque le projet dure environ une semaine. De plus, nous pourrons attribuer facilement des tâches à chacun et avoir un suivi visuel de qui fait quoi et qui en est où. Cela évitera de se perdre lors de l’avancée du projet mais également de se responsabiliser chacun dans son travail.