REPUBLIQUE DU BENIN

****

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

****

UNIVERSITE D'ABOMEY-CALAVI

****

INSTITUT DE FORMATION ET DE RECHERCHE EN INFORMATIQUE

BP 526 Cotonou Tel : +229 21 14 19 88 http://www.ifri.uac.bj

Courriel : contact@ifri.uac.bj

Cahier de charges

Pour l'obtention du

Diplôme de Licence en Informatique

Option: Sécurité Informatique

Mise en œuvre d'un système de détection d'intrusion hôte axé sur l'identification des fichiers malicieux et le monitoring des répertoires critiques

Présenté par :

HOUNGBETODE Ange

Sous la supervision de :

M. H. ACAKPO

Année académique : 2023-2024

Sujet

Mise en œuvre d'un système de détection d'intrusion hôte axé sur l'identification des fichiers malicieux et le monitoring des répertoires critique*s*

Contexte

Notre écosystème numérique fait de plus en plus face aux cyber menaces. Ces attaques informatiques se soldent souvent par le vol, la destruction ou la modification de certains fichiers sensibles et critiques sur la machine des victimes. Les rançongiciels en sont une preuve palpable. Pour lutter contre ces incidents de sécurité, nous envisageons concevoir une solution HIDS qui détectera non seulement les fichiers malicieux et suspects mais aussi s'assurera de veiller sur les répertoires déclarés sensibles par l'utilisateur en vue de détecter toute tentative d'intrusion affectant ces dossiers. La suite du document sera consacrée à une description détaillée du cahier de charges de ce projet.

.

Objectifs spécifiques

Cette solution vise à atteindre les objectifs suivants :

- ***Développement d'un IDS hôte :*** Concevoir un système de détection d'intrusion qui opère au niveau des hôtes (machines utilisateurs) pour veiller sur les répertoires et fichiers déclarés sensibles.
- ***Détection de fichiers malicieux*** : Identifier et générer un rapport détaillé sur les fichiers trouvés suspects et malicieux dans les répertoires surveillés
- ***Protection des données sensibles*** : Assurer la sécurité et l'intégrité des données sensibles présents dans les fichiers et répertoires surveillés.

Fonctionnalités principales

- ***Surveillance en temps réel*** : Monitoring actif des répertoires déclarés sensibles pour la détection des activités suspectes et modifications de fichiers
- ***Analyse de contenu*** : Utilisation des méthodes d'analyse de contenus pour identifier les fichiers malicieux en nous basant non seulement sur les signatures d'attaque mais aussi sur les comportements et anomalies.
- ***Notification d'alertes*** : Envoi d'alertes en temps réel ou de rapports périodiques aux administrateurs en cas de détection d'une activité suspecte.
- ***Intégration avec des systèmes de sécurité existants*** : Intégration du HIDS à d'autres solutions de sécurité existantes pour renforcer la sécurité globale de l'organisation.
- ***Gestion des logs*** : Enregistrer en toute sécurité les événements et les activités à des fins d'analyse post-incident et pour répondre aux exigences de conformité.

- ***Gestion des versions précédentes de fichiers*** : Stocker en toute sécurité les versions antérieures des fichiers et restaurer rapidement une version antérieure si un compromis est détecté à la demande de l'utilisateur.

Compétences requises

Ce projet nécessite des compétences en :

- ***Programmation classique*** : Python a été choisi pour sa simplicité et sa multipolarité.
- ***Plateforme de déploiement*** : La solution sera déployée sur les systèmes d'exploitation Linux et Windows.
- ***Sécurité*** : Des mesures de sécurité robustes seront mises en œuvre pour protéger le système IDS contre les tentatives d'intrusion et les attaques.
- ***Performance*** : Nous ferons de notre mieux pour assurer une performance optimale du système IDS sans compromettre les ressources du système ou la réactivité.

Méthode d'étude

Le succès de ce projet nécessite :

- L'étude des solutions similaires existantes ;
- La conception de l'architecture de la solution HIDS ;
- La sélection des technologies et outils appropriés ;
- La description des cas d'utilisation de la solution HIDS ;
- L'implémentation de la solution en conformité avec les exigences de la sécurité et la confidentialité des données utilisateurs ;
- Mettre en place un système de test et de validation pour identifier les points d'échecs et zones d'amélioration.

Livrables

Les livrables attendus à la fin de cette présentation sont :

- Un mémoire de licence.
- Le code du programme.
- Un guide d'utilisation.