Contexte
Entreprise X
Projet
Alert'Intrusion
Présentation rapide du projet
Proposer une solution facilitant la détection d'intrusion dans le LAN et la DMZ
Professeur responsable
Mme PITOIS
Planning d'intervention
Présentation du projet : 7 Avril 2026
Objectifs
Proposer une solution de détection d'intrusions dans la zone DMZ. Proposer une solution de centralisation des journaux des équipements réseaux et des serveurs côté LAN ainsi que la mise place d'un proxy SSL. Proposer un jeu de tests pour vérifier le bon fonctionnement du système mis en place. Rédiger une documentation sur l'utilisation de la solution mise en œuvre.
Ressources
BLOC3 – séquence6.pdf /Dossier technique Wazuh

Présentation de la mission

I/ Définition du besoin

Définition de l'objet

Votre entreprise dispose d'une DMZ dans laquelle se trouve un serveur hébergeant une application Web permettant d'enregistrer les commandes/réservations de vos clients. Il est donc crucial d'être très réactif en cas de coupure du service web. Une haute disponibilité est à l'étude mais il faut également limiter la surface d'attaque par la mise en place d'un dispositif permettant de détecter toute forme de trafic suspect. Le responsable du service informatique vous demande donc après étude de mettre en place une solution de détection d'intrusions dans la zone DMZ.

En parallèle à la suite d'un audit de sécurité réalisé sur la partie LAN, deux problématiques devront être gérées qui permettront également de gérer un trafic suspect tel qu'un ransomware

La première : une solution de centralisation des journaux d'évènements des équipements réseaux et des serveurs côté LAN paraît indispensable.

La seconde : une solution proxy SSL qui permettra d'apporter une protection antivirale et un filtrage URL des flux HTTPS vers des serveurs C&C

II/ Cahier des charges

Point n°1 :

Zone DMZ :

Dans un premier temps votre responsable vous demande de commencer par une veille technologique sur les outils utilisés sur le marché en matière de solutions HIPS, NIDS et NIPS.

Dans second temps il vous demande de réaliser la mise en place d'une solution HIPS.

Enfin vous devrez réaliser des tests pour vérifier l'efficacité du HIPS :
- Utilisation des commandes suivantes à destination du serveur web situé en DMZ.
nmap -sS
nmap -sU
nmap –sV

-Simulation d'une attaque ayant pour objectif de rendre le service web indisponible avec hping3 par exemple

Point n°2 :

Zone LAN :

Problématique n°1 :

Votre responsable vous demande de commencer par une solution de centralisation des journaux de la zone LAN. Vous devrez proposer une solution qui permettra de pouvoir regrouper l'ensemble des journaux des switchs et serveurs du LAN. Votre responsable aimerait que vous testiez la solution Wazuh.

Problématique n°2 :

Votre responsable vous demande de mettre en place une solution en utilisant un boitier Stormshield SN160

III/ Activités

A1 : Planification des tâches : Diagramme de Gantt et Gestion de projet sur Trello
A2 : Veille technologique sur les solutions HIPS
A3 : Veille technologique sur les solutions NIDS
A4 : Veille technologique sur les solutions NIPS
A5 : Veille technologique sur les solutions SIEM
A6 : Mise en œuvre de la solution HIPS sur la zone DMZ
A7 : Mise en œuvre de la solution de centralisation des journaux dans la zone LAN (Wazuh)
A8 : Etude de fonctionnement d'un proxy SSL
A9 : Mise en œuvre de la solution de proxy SSL dans la zone LAN
A10 : Tests du HIPS
A11 : Traitement des données obtenues grâce à la centralisation des journaux
A12 : Tests du proxy SSL
A13 : Documentation technique de la solution HIPS
A14 : Documentation technique de la solution de centralisation de journaux