Titre du projet : Système de détection d'anomalies et de gestion de logs pour la sécurité des réseaux

Objectif : Créer un système de détection d'anomalies et de gestion de logs pour identifier les menaces potentielles et améliorer la sécurité des réseaux.

Outils utilisés :

- Système de détection d'intrusions et de prévention (IDS/IPS) : Snort, Wazuh, etc.
- syslog-ng : collecteur de logs
- Elasticsearch : base de données pour la gestion des logs
- Kibana : interface utilisateur pour la visualisation des logs
- Une machine (virtuelle) Linux.

Architecture du projet :

1. **Collecte des logs** : syslog-ng collecte les logs de sécurité provenant des équipements réseau et les envoie vers Elasticsearch.
2. **Détection d'anomalies** : IDS/IPS de votre choix analyse les logs collectés pour détecter les anomalies et les menaces potentielles.
3. **Gestion des logs** : Elasticsearch stocke les logs collectés et les rend accessibles pour la recherche et l'analyse.
4. **Visualisation des logs** : Kibana fournit une interface utilisateur pour visualiser les logs et les anomalies détectées.

Avantages du projet :

- Amélioration de la sécurité des réseaux
- Détection en temps réel des anomalies et des menaces potentielles
- Meilleure visibilité et réponse aux menaces
- Réduction des coûts et de la complexité de la gestion des logs de sécurité

Vous devez implémenter au moins cinq cas différents d’intrusion et montrer la détection de ces intrusions en utilisant ce projet de gestion de logs et de détection d'anomalies. Voici un exemple possible d’intrusion (Snort est choisi dans l’exemple):

***Cas d'intrusion** :*

Un attaquant tente d'accéder à un serveur web interne en utilisant une vulnérabilité connue dans le logiciel serveur. L'attaquant envoie une requête HTTP malveillante qui contient un code d'exploitation pour la vulnérabilité.

***Détection de l'intrusion** :*

1. ***Collecte des logs** : Le serveur web envoie les logs de sécurité à syslog-ng, qui les collecte et les envoie à Elasticsearch.*
2. ***Analyse des logs** : Snort analyse les logs collectés et détecte la requête HTTP malveillante. Ce même IDS/IPS identifie la requête comme une tentative d'intrusion et génère une alerte.*
3. ***Gestion des logs** : Elasticsearch stocke les logs collectés et les rend accessibles pour la recherche et l'analyse.*
4. ***Visualisation des logs** : Kibana fournit une interface utilisateur pour visualiser les logs et les anomalies détectées. L'administrateur système peut voir l'alerte générée par Snort et analyser les logs pour comprendre l'origine et la nature de l'intrusion.*

***Exemple de log** :*

Voici un exemple de log qui pourrait être généré par le serveur web lors de l'intrusion :

192.168.1.100 - - [10/Mar/2023:14:30:00 +0000] "GET /index.php?exploit=1 HTTP/1.1" 200 1234

Ce log montre que l'attaquant a envoyé une requête HTTP GET pour accéder à la page /index.php avec un paramètre exploit=1, qui est une tentative d'exploiter la vulnérabilité.

***Alerte Snort** :*

Voici un exemple d'alerte qui pourrait être générée par Snort lors de l'intrusion :

Alert: [1:100000:1] "WEB-MISC PHP exploit attempt" [Classification: Attempted Administrator Privilege Gain] [Priority: 1]

Cette alerte montre que Snort a détecté une tentative d'intrusion et a généré une alerte avec une classification et une priorité.

***Visualisation des logs avec Kibana** :*

Voici un exemple de visualisation des logs avec Kibana :

+---------------+---------------+---------------+

| Date | Source IP | Destination IP |

+---------------+---------------+---------------+

| 10/Mar/2023 | 192.168.1.100 | 192.168.1.200 |

+---------------+---------------+---------------+

Cette visualisation montre les logs collectés par syslog-ng et stockés dans Elasticsearch. L'administrateur système peut analyser ces logs pour comprendre l'origine et la nature de l'intrusion. Une notification par message texte ou par courriel sera nécessaire dès la détection d'un cas confirmé d'intrusion.

Barème :

Déploiement du projet : **25 points**

1. Installation d'un IDS/IPS et de syslog-ng sur les équipements réseau : 6 points
2. Configuration de syslog-ng pour collecter les logs de sécurité : 4 points
3. Installation d'Elasticsearch et de Kibana pour la gestion et la visualisation des logs : 6 points
4. Configuration de l' IDS/IPS pour détecter les anomalies et les menaces potentielles : 4 points
5. Intégration des outils de visualisation pour améliorer la visibilité et la réponse aux menaces : 5 points

Fonctionnalités du projet : **45 points**

- Détection d'anomalies en temps réel : 5 scénarios différents avec une description complète et une justification des choix des scénarios : 20 points
- Collecte et gestion des logs prioritaires en sécurité en relation avec les 5 scénarios avec justification : 10 points
- Visualisation des logs des anomalies détectées et explication des menaces représentées par les 5 scénarios : 10 points
- Alertes et notifications pour les anomalies détectées avec des explications à l'administrateur du système : 5 points

Documentation GitHub : 20 points

- Structure claire du dépôt (README, dossiers, organisation du code et configs) : 5 points
- Documentation de l'installation pas-à-pas (IDS/IPS, syslog-ng, ELK) : 10 points
- Guide d'utilisation : comment lancer, reproduire et tester les scénarios déjà décrits ailleurs : 5 points
- Visualisation : intégration de captures Kibana + explication de leur lecture : 5 points
- Analyse et conclusion : limites du projet, améliorations possibles, perspectives (veille technologique) : 5 points

Points bonus : 10 points
Attribués aux équipes qui intègrent des fonctionnalités supplémentaires ou des améliorations allant au-delà des exigences minimales du projet. Des exemples :

- Dashboard Kibana personnalisé (au lieu du dashboard par défaut) : +5 points
- Automatisation des alertes (script pour envoi d'alertes Slack, Teams, e-mail) : +5
- Schéma d'architecture clair et bien intégré (Mermaid, draw.io, etc.) : +3 points

- Intégration d’un outil complémentaire (par ex. Suricata en plus de Snort, ou Wazuh pour enrichir la collecte) : +5 points