UQAC
Université du Québec
à Chicoutimi

SYSTÈME DE DÉTECTION D'ANOMALIES ET DE GESTION DE LOGS POUR LA SÉCURITÉ DES RÉSEAUX

PAR LARZUL JULIEN

RAPPORT DE RECHERCHE PRÉSENTÉ À L'UNIVERSITÉ DU QUÉBEC À CHICOUTIMI COMME EXIGENCE PARTIELLE EN VUE DE L'OBTENTION DU GRADE DE MAÎTRE ÈS SCIENCES EN INFORMATIQUE

QUÉBEC, CANADA

TABLE DES MATIÈRES

LISTE DES FIGURES

INTRODUCTION

Dans ce contexte, ce projet a pour objectif la conception et le déploiement d'un *système de détection d'anomalies et de gestion de logs*. L'approche consiste à mettre en place une chaîne complète allant de la collecte des journaux jusqu'à leur visualisation et leur analyse via une interface conviviale. L'architecture retenue repose sur quatre briques logicielles complémentaires :

— **Suricata**, un système de détection d'intrusions (IDS/IPS) chargé d'analyser le trafic réseau et de générer des alertes en temps réel ;

— **syslog-ng**, utilisé pour centraliser les journaux du système et des applications ;

— **Elasticsearch**, base de données NoSQL permettant l'indexation et la recherche rapide des événements collectés ;

— **Kibana**, une interface web offrant des fonctionnalités de visualisation et de création de tableaux de bord.

Le projet doit également inclure l'implémentation de plusieurs scénarios d'attaque simulés. Ces cas d'intrusion permettront de valider la capacité du système à détecter différents comportements malveillants et à générer des alertes exploitables par l'administrateur.

Ce rapport présente dans un premier temps l'environnement mis en place et les choix technologiques retenus. Il détaille ensuite la configuration et l'intégration des outils, avant de décrire et d'analyser cinq scénarios d'intrusion représentatifs. Enfin, une partie est consacrée à la visualisation des résultats, à l'évaluation des limites du système et aux perspectives d'amélioration.

CHAPITRE I

MISE EN PLACE DE L'ENVIRONNEMENT

1.1 ENVIRONNEMENT DE TRAVAIL

Le projet a été réalisé par une équipe de quatre personnes. Chaque membre a travaillé sur une machine hôte différente (Windows ou macOS), mais l'ensemble du projet a été uniformisé à travers l'utilisation d'une machine virtuelle Ubuntu. Ce choix garantit un environnement cohérent, reproductible et isolé, permettant de tester des scénarios d'attaques sans risque pour les machines personnelles.

L'environnement retenu est le suivant :

— **Système d'exploitation invité** : Ubuntu 22.04 LTS (Linux)

— **Hyperviseurs utilisés** : VMware Fusion (macOS) et VMware Workstation/VirtualBox (Windows)

— **Ressources allouées** : 2 vCPU, 4 Go de mémoire vive, 40 Go de disque

— **Interface réseau** : `ens160`, configurée en mode NAT

Ce choix d'architecture permet de travailler de manière collaborative tout en garantissant que les configurations, les scripts et les fichiers produits sont compatibles sur toutes les machines de l'équipe.

1.2 BRIQUES LOGICIELLES NÉCESSAIRES

Le projet repose sur quatre composants principaux :

— **Suricata** : un système de détection et de prévention d'intrusions (IDS/IPS), chargé d'analyser le trafic réseau et de générer des alertes.

— **syslog-ng** : un collecteur de logs, utilisé pour centraliser les journaux générés par le système et par Suricata.

— **Elasticsearch** : une base de données orientée recherche, permettant d'indexer et de stocker les logs collectés.

— **Kibana** : une interface web de visualisation connectée à Elasticsearch, permettant d'explorer et d'analyser les logs.

1.3 INSTALLATION DES COMPOSANTS

L'installation a été réalisée en ligne de commande sur Ubuntu. Les principales étapes sont résumées ci-dessous.

SURICATA

```
sudo apt install -y suricata suricata-update
sudo suricata-update
sudo systemctl restart suricata
```

La commande `suricata -build-info` permet de vérifier que l'installation est correcte.

SYSLOG-NG

```
sudo apt install -y syslog-ng
systemctl status syslog-ng
```

ELASTICSEARCH

Téléchargement et extraction de la version ARM64 :

```
curl -LO https://artifacts.elastic.co/downloads/elasticsearch/elasticsearch
    ↪ -8.15.3-linux-aarch64.tar.gz
tar -xzf elasticsearch-8.15.3-linux-aarch64.tar.gz
cd elasticsearch-8.15.3
./bin/elasticsearch -E discovery.type=single-node -E xpack.security.enabled=
    ↪ false
```

KIBANA

Téléchargement et extraction :

```
curl -LO https://artifacts.elastic.co/downloads/kibana/kibana-8.15.3-linux-
    ↪ aarch64.tar.gz
tar -xzf kibana-8.15.3-linux-aarch64.tar.gz
cd kibana-8.15.3
./bin/kibana
```

1.4 AUTOMATISATION PAR ALIAS

Afin de simplifier le lancement des différents composants, des alias ont été définis dans le fichier `/.bashrc`. Ces raccourcis permettent à l'équipe de démarrer ou d'arrêter les services (Elasticsearch, Kibana, Suricata) avec des commandes simples, plutôt que de retaper à chaque fois des lignes longues et complexes. Cette approche améliore la lisibilité, réduit les erreurs de saisie et accélère les tests.

CHAPITRE II

CONFIGURATION ET INTÉGRATION

CHAPITRE III

SCÉNARIOS D'INTRUSION (5 CAS)

CHAPITRE IV

VISUALISATION ET ALERTES

CHAPITRE V

ANALYSE ET DISCUSSION

CONCLUSION