



**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

© LARZUL JULIEN, 2025

TABLE DES MATIÈRES

LISTE DES FIGURES	1
INTRODUCTION	2
CHAPITRE I – MISE EN PLACE DE L’ENVIRONNEMENT	3
1.1 ENVIRONNEMENT DE TRAVAIL	3
1.2 BRIQUES LOGICIELLES NÉCESSAIRES	3
1.3 INSTALLATION DES COMPOSANTS	4
1.4 AUTOMATISATION PAR ALIAS	5
CHAPITRE II – CONFIGURATION ET INTÉGRATION	6
2.1 CONFIGURATION DE SURICATA	6
2.1.1 VÉRIFICATION DU CHEMIN DES RÈGLES	6
2.1.2 AJOUT D’UNE RÈGLE LOCALE	7
2.1.3 TEST DE CONFIGURATION	7
2.1.4 RELANCE DU SERVICE	7
2.1.5 GÉNÉRATION DE TRAFIC ICMP	8
2.1.6 VÉRIFICATION DES ALERTES GÉNÉRÉES	9
CHAPITRE III – SCÉNARIOS D’INTRUSION (5 CAS)	10
CHAPITRE IV – VISUALISATION ET ALERTES	11
CHAPITRE V – ANALYSE ET DISCUSSION	12
CONCLUSION	13
APPENDICE A – PREMIÈRE ANNEXE	14

LISTE DES FIGURES

FIGURE 2.1 – VÉRIFICATION DU CHEMIN DES RÈGLES ET INCLUSION DE LOCAL.RULES..	6
FIGURE 2.2 – RÈGLE ICMP DE TEST AJOUTÉE AU FICHIER LOCAL.RULES. . . .	7
FIGURE 2.3 – VALIDATION DE LA CONFIGURATION DE SURICATA.	7
FIGURE 2.4 – RELANCE DE SURICATA EN MODE DÉMON SUR L'INTERFACE ENS160.	8
FIGURE 2.5 – GÉNÉRATION DE TRAFIC ICMP AVEC LA COMMANDE PING. . .	8
FIGURE 2.6 – ALERTE GÉNÉRÉE DANS FAST.LOG SUITE AU PING ICMP. . . .	9

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

2.1 CONFIGURATION DE SURICATA

2.1.1 VÉRIFICATION DU CHEMIN DES RÈGLES

Pour commencer, nous avons vérifié que le fichier `/etc/suricata/suricata.yaml` pointe bien vers le répertoire `/var/lib/suricata/rules`, et que le fichier `local.rules` est inclus dans la section `rule-files` :

```
$ grep -n "default-rule-path" /etc/suricata/suricata.yaml
```

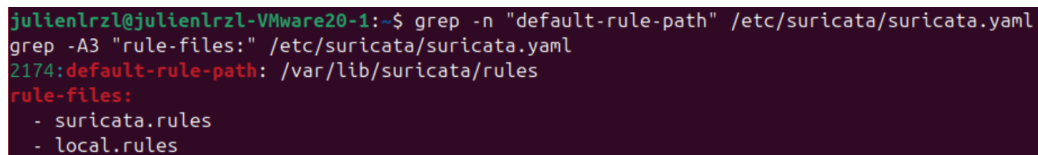
```
2174:default-rule-path: /var/lib/suricata/rules
```

```
$ grep -A3 "rule-files:" /etc/suricata/suricata.yaml
```

```
2176:rule-files:
```

```
2177:  - suricata.rules
```

```
2178:  - local.rules
```



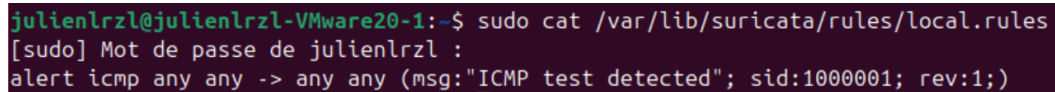
```
julienlrzl@julienlrzl-VMware20-1:~$ grep -n "default-rule-path" /etc/suricata/suricata.yaml
grep -A3 "rule-files:" /etc/suricata/suricata.yaml
2174:default-rule-path: /var/lib/suricata/rules
rule-files:
- suricata.rules
- local.rules
```

FIGURE 2.1 : Vérification du chemin des règles et inclusion de `local.rules`.

2.1.2 AJOUT D'UNE RÈGLE LOCALE

Une règle de détection ICMP a été ajoutée dans le fichier `local.rules` :

```
alert icmp any any -> any any (msg:"ICMP test detected"; sid:1000001; rev:1;)
```



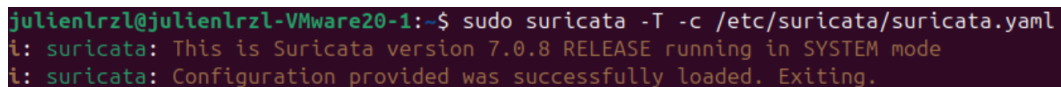
```
julienlrzl@julienlrzl-VMware20-1:~$ sudo cat /var/lib/suricata/rules/local.rules
[sudo] Mot de passe de julienlrzl :
alert icmp any any -> any any (msg:"ICMP test detected"; sid:1000001; rev:1;)
```

FIGURE 2.2 : Règle ICMP de test ajoutée au fichier `local.rules`.

2.1.3 TEST DE CONFIGURATION

Un test de configuration a permis de vérifier que le fichier YAML est valide et que les règles sont correctement chargées :

```
$ sudo suricata -T -c /etc/suricata/suricata.yaml
-- Configuration OK --
```



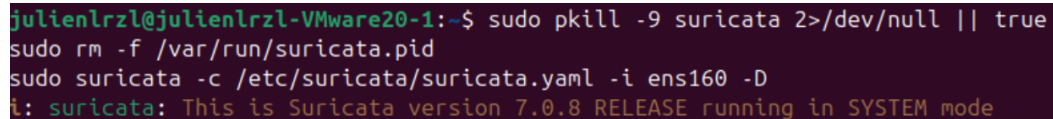
```
julienlrzl@julienlrzl-VMware20-1:~$ sudo suricata -T -c /etc/suricata/suricata.yaml
i: suricata: This is Suricata version 7.0.8 RELEASE running in SYSTEM mode
i: suricata: Configuration provided was successfully loaded. Exiting.
```

FIGURE 2.3 : Validation de la configuration de Suricata.

2.1.4 RELANCE DU SERVICE

Suricata a ensuite été relancé en mode démon :

```
$ sudo pkill -9 suricata 2>/dev/null || true  
$ sudo rm -f /var/run/suricata.pid  
$ sudo suricata -c /etc/suricata/suricata.yaml -i ens160 -D
```



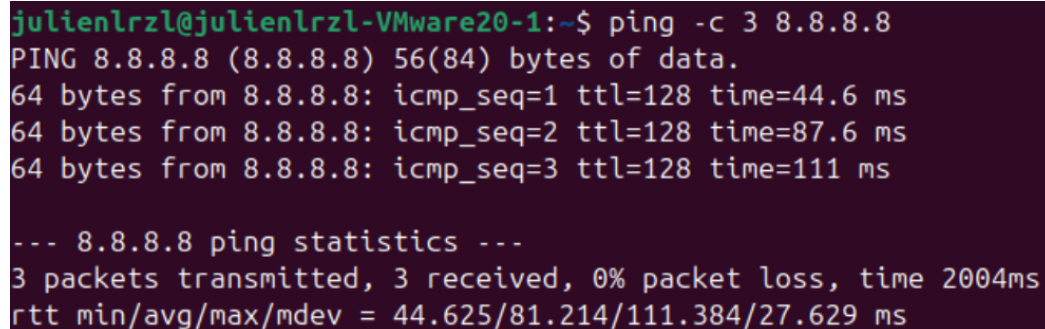
```
julienlrzl@julienlrzl-VMware20-1:~$ sudo pkill -9 suricata 2>/dev/null || true  
sudo rm -f /var/run/suricata.pid  
sudo suricata -c /etc/suricata/suricata.yaml -i ens160 -D  
i: suricata: This is Suricata version 7.0.8 RELEASE running in SYSTEM mode
```

FIGURE 2.4 : Relance de Suricata en mode démon sur l'interface ens160.

2.1.5 GÉNÉRATION DE TRAFIC ICMP

Un simple ping vers l'adresse publique de Google (8.8.8.8) a été utilisé pour générer du trafic ICMP :

```
$ ping -c 3 8.8.8.8
```



```
julienlrzl@julienlrzl-VMware20-1:~$ ping -c 3 8.8.8.8  
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.  
64 bytes from 8.8.8.8: icmp_seq=1 ttl=128 time=44.6 ms  
64 bytes from 8.8.8.8: icmp_seq=2 ttl=128 time=87.6 ms  
64 bytes from 8.8.8.8: icmp_seq=3 ttl=128 time=111 ms  
  
--- 8.8.8.8 ping statistics ---  
3 packets transmitted, 3 received, 0% packet loss, time 2004ms  
rtt min/avg/max/mdev = 44.625/81.214/111.384/27.629 ms
```

FIGURE 2.5 : Génération de trafic ICMP avec la commande ping.

2.1.6 VÉRIFICATION DES ALERTES GÉNÉRÉES

L'analyse du fichier `/var/log/suricata/fast.log` montre bien que la règle locale a déclenché une alerte pour les paquets ICMP observés :

09/25/2025-19:16:40.523467 **[**]** [1:1000001:1] ICMP test detected **[**]** {ICMP}

↪ 172.16.150.130:8 -> 8.8.8.8:0

```
julienlrzi@julienlrzi-Vmware20-1: $ tail -f /var/log/suricata/fast.log
09/25/2025-19:58:25.005565 [**] [1:2231000:1] SURICATA QUIC failed decrypt [**] [Classification: Generic Protocol Command Decode] [Priority: 3] (UDP) 172.16.150.130:59815 -> 3.161.2
13.64:443
09/25/2025-19:58:25.005582 [**] [1:2231000:1] SURICATA QUIC failed decrypt [**] [Classification: Generic Protocol Command Decode] [Priority: 3] (UDP) 172.16.150.130:59815 -> 3.161.2
13.64:443
09/25/2025-19:58:25.005577 [**] [1:2231000:1] SURICATA QUIC failed decrypt [**] [Classification: Generic Protocol Command Decode] [Priority: 3] (UDP) 172.16.150.130:59815 -> 3.161.2
13.64:443
09/25/2025-19:58:25.005590 [**] [1:2231000:1] SURICATA QUIC failed decrypt [**] [Classification: Generic Protocol Command Decode] [Priority: 3] (UDP) 172.16.150.130:59815 -> 3.161.2
13.64:443
09/25/2025-19:59:19.690675 [**] [1:1000001:1] ICMP test detected [**] [Classification: (null)] [Priority: 3] (ICMP) 172.16.150.130:8 -> 8.8.8.8:0
09/25/2025-19:59:19.690684 [**] [1:1000001:1] ICMP test detected [**] [Classification: (null)] [Priority: 3] (ICMP) 172.16.150.130:8 -> 8.8.8.8:0
09/25/2025-19:59:19.690691 [**] [1:1000001:1] ICMP test detected [**] [Classification: (null)] [Priority: 3] (ICMP) 172.16.150.130:8 -> 8.8.8.8:0
09/25/2025-19:59:19.735235 [**] [1:1000001:1] ICMP test detected [**] [Classification: (null)] [Priority: 3] (ICMP) 8.8.8.8:0 -> 172.16.150.130:0
09/25/2025-19:59:19.735235 [**] [1:1000001:1] ICMP test detected [**] [Classification: (null)] [Priority: 3] (ICMP) 8.8.8.8:0 -> 172.16.150.130:0
09/25/2025-19:59:19.735235 [**] [1:1000001:1] ICMP test detected [**] [Classification: (null)] [Priority: 3] (ICMP) 8.8.8.8:0 -> 172.16.150.130:0
```

FIGURE 2.6 : Alerte générée dans `fast.log` suite au ping ICMP.

En conclusion, Suricata est correctement configuré pour charger les règles locales et détecter du trafic ICMP simple, démontrant sa capacité à identifier des anomalies sur le réseau.

CHAPITRE III
SCÉNARIOS D'INTRUSION (5 CAS)

CHAPITRE IV
VISUALISATION ET ALERTES

CHAPITRE V
ANALYSE ET DISCUSSION

CONCLUSION

APPENDICE A
PREMIÈRE ANNEXE

Lorem ipsum dolor sit amet, consectetur adipisicing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Lorem ipsum dolor sit amet, consectetur adipisicing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.