Document d'Etude 2024 – SAE503

27 NOVEMBRE

PAQUELET Etienne
OCKANDJI Ardy

Contexte

Le CHU Livrac souhaite mener une refonte totale du système informatique afin de l'améliorer et de le sécuriser face à de potentielles attaques. A cette fin, une étude du système d'information a été mené par un groupe d'expert composé de M. OCKANDJI et M. PAQUELET de la société PloufTech Solution. Cette étude comprend un audit de l'infrastructure existante, une sélection de différentes solutions d'IDS/IPS présentes sur le marché, un comparatif des solutions existantes ainsi que la nouvelle infrastructure réseau qui sera mise en place.

Audit de l'infrastructure existante

Une analyse de l'architecture actuelle du CHU Livrac a été réalisé. Nous vous présentons ci-dessous les résultats de cet audit. Les points positifs de cette infrastructure sont les suivants :

- Séparation du serveur de base de données du serveur web.
- Isolation des serveurs par rapports aux stations clientes.
- Politique de NAT sur le routeur central, permettant de sécuriser un minimum le réseau local d'internet.

Nous relevons cependant les points négatifs suivants :

- L'isolation des serveurs par rapports aux stations clientes est mal réalisé et peut être optimisé en utilisant moins de matériel physique par la création de VLAN.
- L'excès de matériel physique (deux routeurs et un switch superflu) utilisé pour le cloisonnement entraîne des coûts supplémentaires et une consommation énergétique inutile pour maintenir l'isolation actuelle.
- Le serveur de base de données contient seulement la base de données du serveur web. Dans le but d'économiser un serveur qui pourrait être utilisé pour réaliser des sauvegardes, la base de données pourrait être migrée sur le serveur web.
- Un manque de sécurité apparaît également sur l'infrastructure actuelle. En effet, pas de pare-feu, ou d'IDS/IPS ont été installés, rendant ainsi le réseau informatique vulnérable aux attaques.
- Il manque une redondance au niveau des systèmes (serveur web/base de données) ainsi qu'au niveau du réseau. En effet, une panne du routeur central entraînerait une interruption complète, faute d'équipement capable de prendre le relais. Il est donc essentiel d'implémenter des solutions de redondance réseau pour garantir une disponibilité continue.
- Le réseau actuel ne dispose pas de solution de supervision du réseau. Cela empêche donc d'avoir une vision claire de l'état des serveurs et matériels réseaux.

Solution IDS/IPS

Suite à cet audit, nous avons recherché sur Internet différents IDS/IPS qui pourraient répondre aux besoins du CHU Livrac. Ces IDS/IPS ont été sélectionné en fonction du critère suivant de l'open source. Les IDS/IPS que nous avons sélectionné sont les suivants :

- Snort
- Suricata
- Zeek

Un IDS (Intrusion Detection System ou Système de Détection d'Intrusion) est un logiciel ou un équipement réseau conçu pour analyser le trafic réseau afin d'identifier les menaces connues et les activités suspectes ou malveillantes. Le mécanisme de détection repose souvent sur des signatures : il analyse les paquets transitant par le réseau pour repérer ceux correspondant à des signatures malveillantes préenregistrées. Lorsqu'il détecte des risques ou des menaces de sécurité, l'IDS alerte les équipes informatiques et de sécurité, leur permettant de prendre des mesures correctives.

En complément des fonctionnalités d'un IDS, un IPS (Intrusion Prevention System) ajoute la capacité de bloquer activement les paquets malveillants détectés, renforçant ainsi la sécurité en empêchant les intrusions en temps réel.

Etude comparative des solutions retenues

Nous allons présenter dans cette partie présenter les différents IDS/IPS que nous avons sélectionné et comparer leurs fonctionnalités.

Critères	Snort	Suricata	Zeek
Type de système	IDS/IPS basé sur les signatures	IDS/IPS hybride (signatures + comportement)	IDS basé sur l'analyse comportementale
Avantages	- Leader du marché depuis longtemps - Large bibliothèque de signatures - Documentation complète - Intégré dans plusieurs pares-feux et appliance - Multithreading intégré dans Snort 3.	- Multithreading natif (meilleur pour les gros volumes de trafic) - Compatible avec les règles Snort - Bonne gestion des alertes - Plus rapide dans les environnements multicœur - Flexible : possibilité de personnalisation des règles pour un type de menace particulier	- Analyse approfondie des protocoles - Génère des logs détaillés - Utile pour l'investigation - Flexibilité pour personnaliser les scripts d'analyse
Inconvénients	- Moins adapté aux environnements modernes - Plus lourd dans le traitement	- Plus complexe à configurer et optimiser	- Courbe d'apprentissage plus élevée (basé sur des scripts) - Moins axé sur les signatures
Performances	Bonne pour des débits moyens (avec des optimisations)	Excellente pour les débits élevés grâce au multithreading	Performances variables en fonction de la complexité des scripts et des logs générés
Communauté	Très large et bien établie - Soutien actif de Cisco	Grande et en croissance constante - Soutien actif de l'OISF	Communauté universitaire et professionnelle - Moins nombreuse mais active
Documentation	Riche et accessible	Bonne documentation, mais moins intuitive que Snort	Documentation détaillée, mais plus technique
Cas d'utilisation	Environnements stables et classiques - Petits à moyens réseaux - Détection en temps réel des menaces	Réseaux à haut débit - Scénarios où le multithreading est critique	Analyse forensic - Réseaux où une visibilité approfondie des protocoles est essentielle
Réputation	Leader historique en IDS/IPS	Alternative moderne, de plus en plus adopté	Réputé pour son analyse approfondie et son utilité dans la recherche
Données d'utilisation	Principalement basé sur les règles (peu ou pas d'analyse comportementale)	Combinaison de signatures et d'analyse comportementale	Log et analyse comportementale avancée
Facilité d'intégration	Facilement intégrable avec des appliances comme pfSense	Compatible avec les systèmes basés sur Snort et facile à remplacer dans ces contextes	Moins d'intégrations standards, mais personnalisable avec des outils spécifiques
Coût	Gratuit (version Community) - Possibilité de licence payante avec Cisco	Gratuit (Open Source), financé par l'OISF	Gratuit (Open Source)
Support	Support gratuit par la communauté et possibilité d'un support Cisco (payant).	Support disponible via des partenaires (OISF)	Support limité, surtout dans le cadre académique ou open source

Conclusion

Nous venons d'étudier différentes solutions logicielles d'IDS/IPS. Le marché des IDS/IPS est vaste, et le panel sélectionné offre un éventail significatif parmi les solutions les plus réputées. Afin de maîtriser les coûts, nous avons exclu les entreprises onéreuses, telles qu'IBM, Cisco, et d'autres. Snort et Suricata se ressemble par leurs fonctionnalités et leurs communautés respective et leur prédominance. Zeek, quant à lui, se distingue par son approche différente, axée sur l'analyse comportementale et la capacité à générer des logs détaillés, ce qui le rend particulièrement utile pour des environnements nécessitant une analyse approfondie et une visibilité étendue sur les protocoles réseau. Cependant, il demande une courbe d'apprentissage plus importante et des compétences spécifiques pour être configuré et exploité efficacement.