Rapport d'étude des systèmes IDS/IPS

Par Hugo LOURREIRO et
Alexandre BEROT-ARMAND
IUT Nord-Franche Comté - 2023

TABLE DES MATIERES

INTRODUCTION

Le but de se rapport d'étude est de comparer plusieurs solutions de système de détection d'intrusion (IDS) et de système de prévention d'intrusion (IPS) et de voir quels sont les différentes propositions présente sur le marché dans le but d'intégrer ce système dans la sécurité informatique d'un hôpital.

Un IDS est un système qui analyse le réseau et qui émet une alerte en cas de detection d'activité malicieuse. Les détections se font par signature (SIDS) via des bibliothèques de motifs d'attaque ou par anomalie (AIDS) avec une phase d'apprentissage des comportements du réseau et une phase de détection des évènements anormaux vis-à-vis de ses connaissances. L'IDS s'arrête au stade d'émettre une alerte et c'est à l'administrateur de prendre les mesures pour régler le problème.

Les IPS suivent le même principe que les IDS mais rajoute une couche de sécurité en agissant sur le système : bloquer une adresse IP d'un utilisateur qui va sur un site non-autorisé, supprimer un fichier qui a l'exacte signature d'un virus…
L'IPS ira plus loin dans sa manière de gérer le trafic en temps réel.

Dans le panel des solutions de sécurités disponible sur le marché, nous en avons sélectionnés 3 en rajoutant la solution obligatoire :

- Snort
- Zeek
- Suricata
- Security Onion

COMPARATIF DES SOLUTIONS

Snort

Snort est un des plus anciens IDS/IPS ce qui signifie que le produit est fiable, avec sa première release en 1998. De plus, la boite de développement d'origine a été racheté par Cisco, preuve de son fonctionnement. Il dispose d'une grosse communauté présente sur leur forum, YouTube ou Reddit ce qui signifie qu'il y a un nombre substantiel de tutoriel sur le sujet.
Snort dispose aussi d'une bonne compatibilité sur Windows ou Linux et il y a aussi une possibilité de le coupler avec différents pare-feux (comme pfSense). Son plus gros défaut était sa conception Single-Threaded qui a été corrigé récemment.

Suricata

Suricata est un IDS/IPS a publié sa première release en 2010 avec comme objectif la performance. Le produit a eu le temps de gagner en popularité et dispose aussi d'une grande communauté avec des tutoriels présent sur beaucoup de média.
Suricata est compatible sur plusieurs systèmes d'exploitation tel Linux et Windows aussi. Il existe aussi des plugins pour l'utiliser sur des pare-feux (comme IpFire).

Zeek

Zeek, anciennement Bro, est un IDS orienté réseau (NIDS) datant aussi de 1998 pour sa première release. Sa communauté, certes plus petite, reste présente avec de nombreux tutoriels.
Si son fonctionnement ressemble à Snort, il faut noter que le logiciel permet aussi la cartographie du réseau avec des générations de modèles.
Il est moins maintenant que les autres IDS présenté du fait qu'il est maintenu par une équipe de chercheur mais il reste dans le haut du panier.
Il n'y a pas de plugin proposé pour l'intégrer dans des pare-feux.

Security Onion

Securité Onion se classerais plus dans la catégorie des solutions complète de sécurité que dans des IDS/IPS pure. C'est une solution qui va coupler plusieurs logiciels ensemble tel que Suricata et Zeek (déjà présenté) avec d'autres logiciels tel que la suite ELK (Elasticsearch, Logstash et Kibana) pour la gestion de logs ou TheHive pour la gestion d'incident.

Sa communauté est plus restreinte mais on trouve suffisamment de tutoriels pour l'installation des points clefs.

Il reste a noté que la solution est assez lourde à mettre en place avec 100Go de disque dur pour l'utilisation d'une VM.

CONCLUSION

Le marché des IDS/IPS est assez large et le panel sélectionné permet d'avoir un choix conséquent parmi les plus connus.

Dans un souci d'économie, nous avons sortie les entreprises couteuses du lot tel qu'IBM, Cisco et autres.

Dans la liste proposée, Suricata et Snort sortent du lot par leurs position de leader open source sur le marché.

Zeek intègre des outils différents qui peuvent avoir de la valeur mais sur le côté IDS/IPS, il reste en retrait.

Security Onion est plus une solution lourde complète qu'un simple IDS, IDS qui se trouve être Suricata, il en récupère donc une grande partie des avantages mais derrière un poids assez lourd niveau place.

Pour finir, l'ensemble des tutoriels trouvé pour ces différentes solutions annonce des temps entre 25 minutes et 1 heure pour la mise en place des IDS et les premiers résultats. Elles se valent donc toutes plus ou moins.