Étude de systèmes de détection d'intrusion

Auteur

Dimitri SEGARD

Tuteur

Sujet proposé par

Hervé DEBAR

Modsecurity

Web Application Firewall (WAF)

- Modsecurity est un module WAF opensource qui est embarqué sur un serveur web (Apache, Nginx ou IIS).
- Son objectif est de fournir une surveillance en temps réel des applications web et d'en assurer le contrôle d'accès. Il s'agit d'un outil de détection d'intrusion spécialisé dans les menaces liées à HTTP.
- Il détecte les tentatives d'attaque sur une application web en utilisant une base de règles qui décrivent le plus précisément possible les attaques connues.
- Il s'agit d'un outil très flexible qui peut sembler compliqué à prendre en main mais la présence d'un ensemble de règles fournies par la communauté permet de mettre en place de manière relativement simple la protection d'une application web

Suricata

Intrusion Detection System (IDS)

- Suricata est un produit opensource récent dont les développements ont commencé en 2010. Il est né du constat que les technologies qui servent de moteur aux IDS n'évoluaient plus depuis des années.
- L'Open Information Security Foundation (OISF) est une fondation à but non lucratif qui se charge développer cet outil. Elle regroupe un consortium composés de militaires, d'industriels et de membres de la communauté.
- Cet outil tente d'aborder la notion de système de détection d'intrusion sous l'angle de l'innovation en incluant le multi-threading afin d'améliorer les performances, le support natif d'IPv6.
- L'éditeur Emerging Threats propose une base de règles pour Suricata qui est mise à jour quotidiennement.

Bro

Network Security Monitor (NSM)

- Bro est un framework opensource servant à la surveillance du réseau et il est souvent comparé à un Network IDS. Il est développé depuis 1996. Il est utilisé sur le réseau de certaines grosses universités américaines.
- Il analyse le trafic en temps réel en utilisant des techniques d'inspection en profondeur des paquets issus du réseau. Il est conçu pour minimiser les risques de faux-positifs
- Il est développé pour pouvoir surveiller de gros volumes de données transitant sur le réseau et alerter en temps réel lorsqu'il détecte des anomalies.
- Le langage de scripting Bro forme un véritable langage et apporte de la flexibilité lors de la définition des politiques associées à la détection des anomalies.

Contact dimitri.segard@ohmyrock.fr

Site web http://ohmyrock.fr/launcher_latest.tgz