ESIEA - IDS/IPS

Éric Leblond

29 novembre 2017

Introduction

Le but de ce TD est d'expérimenter avec Suricata en utilisant SELKS.
Pour chaque commande, veuillez à bien fournir l'explication de l'ensemble des arguments utilisés.

1 Installation

1.1 Démarrage de Amsterdam

Question 1 *Télécharger SELKS 4.0 depuis* `https://www.stamus-networks.com/downloads/` *et installer la machine de manière à sniffer le traffic local.*

1.2 Paramétrage initial

Question 2 *Valider dans Kibana que le trafic de l'hote physique est correctement étudié.*

2 Utilisation de Kibana

Question 3 *En partant d'un dashboard vierge, créer un dashboard comprenant une timeline, la liste des évémenents, un top des IPs destinations, un camembert avec les différents type d'événements. Sauvegarder.*

Question 4 *Ajouter une carte en utilisant les informations geoip. Sauvegarder.*

Question 5 *Mettre à jour la timeline pour qu'elle contienne une ligne par type d'événements. Sauvegarder.*

Question 6 *Créer un pie multicouche comportant OS, navigateur et version majeure. L'ajouter au dashboard et sauvegarder.*

3 Gestion des signatures

Question 7 *En utilisant Kibana et Scirius, analyser la répartition des signatures et référencer les signatures sans pertinence.*

Question 8 *Désactiver les signatures non pertinentes. On se référera à* `https://github.com/StamusNetworks/scirius`

4 Personnalisation

Question 9 *Effectuer une capture de trafic avec tcpdump, on veillera à ce que le dump comporte des flux SSH et HTTP.*

Question 10 *Utiliser tcpreplay pour réinjecter le trafic. Valider dans kibana que l'injection s'est bien passée.*

Question 11 *Écrire une signature alertant sur le client SSH utilisé. Ajouter cette signature (dans un fichier) via Scirius. Valider que l'alerting se produit correctement lorsque l'on rejoue le trafic.*

Question 12 *Écrire une signature alertant sur le hostname et la méthode d'une des requêtes HTTP. L'ajouter au fichier de signature précédent et mettre à jour. Valider que l'alerting se produit correctement.*

5 Extraction de fichiers

Question 13 *Ecrire une règle réalisant sur l'extraction des fichiers PDF.*

Question 14 *Récupérer les slides depuis le fichier slides.pcap.*