# ESIEA - IDS/IPS - TD2

Éric Leblond

18 décembre 2017

## Introduction

Le but de ce TD est d'expérimenter l'écriture de règles. Pour chaque signature, veuillez à bien fournir l'explication de l'ensemble des arguments utilisés.

## 1 Extraction de fichiers

**Question 1** *Ecrire une règle réalisant sur l'extraction des fichiers PDF.*

**Question 2** *Récupérer les slides depuis le fichier slides.pcap.*

## 2 Command line for ever

**Question 3** *Utiliser jq pour faire un top des alertes*

**Question 4** *Utiliser jq pour faire un top des alertes par sources*

On pourra utiliser le site `https://badssl.com/` pour se connecter à des sites mal configurés.

**Question 5** *Détecter les certificats autosignés avec une commande jq.*

## 3 Échauffement

**Question 6** *Écrire et activer une règle réalisant le stockage des certificats signés par Verisign pour du trafic sur le port 443.*

**Question 7** *Réaliser un dashboard dédié aux alertes avec :*
- *Alerte par HTTP hostname*
- *Alerte par type de fichier*

## 4 Make France great again

**Question 8** *Écrire une signature alertant lorsque qu'un certificat est signé par une autorité française.*

**Question 9** *Écrire une signature alertant lorsque qu'un certificat délivré pour un site .fr n'est pas signé par une autorité française.*

**Question 10** *Écrire une signature alertant lorsque qu'un certificat délivré pour une entité française n'est pas signé par une autorité française.*

# 5 xbits

**Question 11** *Télécharger* `http://testmyids.com/CVE.old/AR/CVE-2010-2883.pdf` *et procéder à l'analyse des alertes liées à cet action.*

Ce PDF déclenche le téléchargement d'un exécutable.

**Question 12** *Télécharger* `wgethttp://d.7-zip.org/a/7z1701-x64.exe`.

Cet enchainemenent est classique et la capture de l'exécutable est intéressante.

**Question 13** *Écrire un ensemble de signatures détectant un download d'un PDF infecté suivi d'un téléchargement d'un exécutable. La signature stockera l'exécutable.*

Le téléchargement de l'exécutable est très souvent fait par un analyste et cela entrainera donc des alertes inutiles.

**Question 14** *Mettre à jour les signatures précédentes pour ne pas alerter si le téléchargement est fait par* `wget`.