TLS-SEC

Exercices d'examen

Décembre 2015

Détection d'intrusion

Exercice 1 *(1 point)*

Expliquez à quoi correspond un « vrai négatif » dans le domaine de la détection d'intrusion.

Exercice 2 *(5 points)*

Voici une signature de détection réseau utilisable avec le logiciel Snort pour détecter des messages électroniques présentant des caractéristiques spécifiques :

```
alert tcp $EXTERNAL_NET any -> $SMTP_SERVERS 25 (msg:"cyber-drrck"; flow:to_server,
established; content:"terroriste"; nocase; content:"islam"; within:30; nocase;
content:"voiture"; within:30; nocase; content:"nitrate"; within:30; nocase;
reference:nsa,765432;  classtype:string-detect; rev:2;)
```

Question 1 *(1 point)* : Expliquez sur quels critères Snort détecte un message électronique avec cette signature (type de flux réseau, caractéristiques des données) ?

On considère que la France compte 65 millions d'habitants environ. Faisons l'hypothèse que :

- chaque citoyen français utilise la messagerie électronique 5 fois par an en moyenne ;
- et parmi eux, il y a 10 individus malveillants et dangereux.

Question 2 *(1 point)* : Si la fiabilité de détection d'une signature Snort du type ci-dessus, utilisée pour repérer des communications malveillantes, est de 99,9 % : combien d'alarmes vont être générées ? Est-ce que tous les terroristes seront détectés ? Combien d'alarmes seront des faux positifs ?

Question 3 *(1 point)* : Quel taux de détection doit-on avoir pour ne plus avoir *que* de vraies alarmes ?

Question 4 *(1 point)* : Supposons que la détection soit effectuée par des mots-clefs. Supposons que les services de renseignement chargés de la mise en œuvre estiment que chaque mot-clef supplémentaire (judicieux bien évidemment) augmente la sélection des « bons » candidats d'un facteur 20. *Combien faut-il de mots-clefs* dans une signature pour atteindre le taux de détection obtenu ci-dessus (au 3 si possible, au 2 sinon). Pour mémoire : $X^n = e^{n \cdot \ln(X)}$

Question 5 *(1 point)* : Discutez votre résultat.