INSA

Exercices d'examen

Décembre 2014

Détection d'intrusion

Exercices proposés avec corrigé

Exercice 1 *(2 points)*

Question 1 : Expliquez à quoi correspond un « faux négatif » dans le domaine de la détection d'intrusion.

Question 2 : Est-il plus important de s'y intéresser qu'à un faux positif ?

Corrigé

1. Un faux négatif est une situation dans laquelle aucun message d'alerte n'est émis par un outil de détection d'intrusion (IDS ou antivirus) alors qu'une intrusion est en cours ou qu'un programme malveillant est en train de s'exécuter dans le système surveillé (virus par exemple).

2. (Un faux positif est un message d'alerte émis par un outil de détection alors qu'aucune attaque n'est en cours.)

L'impact d'un faux positif, c'est de créer une charge d'exploitation inutile pour l'opérateur du système de détection. C'est dommageable, mais l'impact global dépend de la quantité de faux positifs rencontrés et du travail inutile qu'ils génèrent. C'est d'abord un signe de la qualité du système de détection. (Il peut aussi y avoir un impact sur la sécurité s'il est facile pour un utilisateur de « fabriquer » ces déclenchements de fausses alarmes ; mais c'est déjà plus élaboré.)

Un faux négatif est lui par contre directement une défaillance du système de détection dans sa fonction primaire de sécurité. Idéalement, il est donc prioritaire de s'intéresser d'abord à l'absence de faux négatifs dans un IDS avant de s'intéresser à son niveau de qualité (faible taux de faux positifs).

Exercice 2 *(4 points)*

Voici deux signatures de détection d'intrusion réseau utilisables par le logiciel Snort pour détecter des flux réseaux présentant des caractéristiques spécifiques :

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"Pirate propaganda";
content:"Host : "; content:"eveoganda.blogspot.fr|0d 0a|"; nocase; content:"GET";
http_method; classtype:gamification; sid:98765; rev:1;)

alert udp $HOME_NET any -> $HOME_NET 53 (msg:"Pirate propaganda dns request";
flow:to_server; content:"|01 00 00 01 00 00 00 00 00 00|"; depth:10; offset:2;
content:"|09|eveoganda|08|blogspot|02|fr"; nocase; classtype:gamification;
sid:98766; rev:1;)
```

Question 1 *(1 point)* : Indiquez la caractéristique commune à ces 2 signatures et donc le type de flux que l'on souhaite identifier.

Question 2 *(2 points)* : Présentez à présent les 2 différents types de flux réseau que chaque signature permet de repérer dans la communication. Discutez les différences entre les types de détection permis par chacune de ces signatures.

Corrigé

1. Les 2 signatures s'intéressent à la détection d'un trafic réseau à destination de l'hôte identifié par le nom de domaine eveoganda.blogspot.fr[1].

2. La première signature cherche l'identification du nom de domaine de la machine à l'intérieur du flux HTTP (dans les attributs). Elle va donc repérer le démarrage d'une communication Web avec cette machine – via un canal TCP sortant du réseau surveillé.

La deuxième signature repère une requête DNS portant sur le nom de domaine en question, émise sur le réseau interne (dans un message UDP).

Cette détection arrive avant l'établissement d'une connexion TCP (sur HTTP ou sur autre protocole) vers l'hôte en question.
Remarque : Cette signature concerne les demandes DNS et va donc s'activer même si le nom de domaine ciblé n'est pas/plus attribué (ce qui peut être voulu, ou non).

Voici une autre signature de détection d'intrusion réseau extraite de la base des signatures Snort pour détecter un type de flux spécifique :

```
alert udp $EXTERNAL_NET any -> $HOME_NET 53 (msg:"DNS zone transfer UDP";
content:"|00 00 FC|"; offset:14; reference:arachnids,212; reference:cve,1999-0532;
reference:nessus,10595; classtype:attempted-recon; sid:1948; rev:7;)
```

Question 3 *(1 point)* : Expliquez quel type de communication on détecte via cette signature. Pourquoi lever une alerte immédiatement dès que le flux apparaît (sans même regarder le contenu du message) ?

Corrigé

3. Cette troisième signature, qui ne teste que la présence de 3 octets bien précis dans un message UDP sur le port standard du DNS, est utilisée pour signaler par une alarme l'initiation d'un transfert de zone DNS. Ce signalement arrive dès le premier message visant à lancer l'opération de transfert.

En effet, un transfert de zone DNS correspond à la transmission, par le serveur principal d'un domaine DNS, de l'ensemble du contenu des informations concernant sa zone, à un autre serveur DNS secondaire de ce même domaine. Les données transmises[2] *vont remplacer les paramètres du serveur secondaire et ce sont celles-ci qui seront ensuite utilisées pour répondre aux requêtes que les clients soumettront au serveur DSN secondaire. C'est donc un flux technique à protéger tout particulièrement puisqu'il permettrait de modifier la correspondance (nom, adresse IP) perçue par tout un groupe de machines clientes et tout un sous-domaine DNS.*

---

[1] La publicité induite est tout à fait gratuite.

[2] Incluant toutes les associations (nom, adresse IP) pour toute la zone DNS concernée.

La raison pour laquelle une alerte est levée immédiatement par la signature, sans regarder plus avant si la zone transmise est légitime, vient des réseaux source et destination utilisés. Cette signature se déclenche quand un transfert de zone arrive d'Internet ($EXTERNAL_NET) à destination d'un serveur situé sur le réseau interne ($HOME_NET). Il s'agirait donc d'une situation où un serveur DNS soit-disant principal situé sur Internet voudrait remplacer les définitions des zones d'un serveur DNS secondaire interne à notre réseau. Il n'y quasiment aucune chance pour que le serveur DNS primaire soit situé à l'extérieur du réseau et les serveurs secondaires à l'intérieur ; c'est même généralement l'inverse pour des raisons de sécurité ! La signature présentée ici considère donc que tous les signalements de transferts de zones arrivant de l'extérieur sur UDP sont le signe d'une action anormale – cela peut dépendre de l'architecture du réseau mais c'est très probablement à juste titre.