INSA

Exercices d'examen
Décembre 2013

Détection d'intrusion

Exercices proposés avec corrigé

Exercice 1 *(1 points)*

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

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

Exercice 2 *(3 points)*

Voici une signature de détection d'intrusion réseau extraite de la base des signatures utilisée par le logiciel Snort pour détecter des messages électroniques présentant des caractéristiques spécifiques :

```
alert tcp $EXTERNAL_NET any -> $SMTP_SERVERS 25 (msg:"SMTP Microsoft Outlook VEVENT
non-TZID overflow attempt"; flow:to_server, established; content:"DTSTART|3B|";
nocase; content:!"value"; within:5; nocase; content:!"TZID"; within:4; nocase;
reference:bugtraq,21931; reference:cve,2007-0033;
reference:url,www.microsoft.com/technet/security/Bulletin/MS07-003.mspx;
classtype:attempted-user; sid:10012; rev:1;)
```

Question 1 *(1 point)* : Expliquez sur quels critères Snort détecte un message électronique particulier (type de flux réseau, caractéristiques des données) ?
Question 2 *(1 point)* : Proposez une évolution de cette signature permettant de détecter les messages électroniques contenant les mots-clefs consécutifs suivants : « terroriste », « nazi », « pedophile ».
Question 3 *(1 point)* : Donnez quelques avantages/inconvénients[1] de l'utilisation de cette approche pour la sélection de messages à analyser.

Corrigé

1. *Les critères de détection sont : d'abord d'un point de vue réseau, il s'agit d'une connexion TCP à destination du port (serveur) n°25 (port standard des serveurs de messagerie SMTP). Ensuite, la sonde recherche dans la transmission entre le serveur et son client un flux contenant la chaîne de caractère « DSTART » suivie du caractère codé 3B en hexadécimal. Toutefois, les contraintes additionnelles suivantes doivent également être remplies : les chaines « value » (à une distance de 5 caractères) puis « TZID » (à une distance de 4 caractères de la précédente) ne doivent pas apparaître consécutivement à « DSTART ». (Rq : Aucune des recherches de chaîne de caractère ne tient compte de la casse.)*

[1] Vous êtes dispensé de préciser si vous trouvez que c'est un avantage ou un inconvénient.

2. `alert tcp $EXTERNAL_NET any -> $SMTP_SERVERS 25 (msg:"LENS cyber-inspektor"; flow:to_server, established; content:"terroriste"; nocase; content:"nazi"; within:20; nocase; content:"pedophile"; within:20; nocase; reference:nsa,654321; classtype:string-detect; rev:1;)`
3. *La signature ne détecte que les messages où les mots-clefs apparaissent dans l'ordre et pas ceux où ils sont dans le désordre. (On peut bien sûr multiplier les signatures pour compenser et faire du nombre.)*
   L'approche est probablement plus efficace en terme d'espace de stockage que d'enregistrer tout le trafic de messagerie des utilisateurs.
   On ne peut pas vérifier le contenu du message pour savoir ce qu'il signifie ; on sait juste qu'il correspondait à la définition de la signature.
   Le stockage du flux d'alerte peut probablement être considéré comme (relativement) légal, puisqu'il ne contient pas vraiment de données personnelles (juste des méta-données).
   L'auteur de ces lignes et tous les enseignants participants, ayant imprudemment envoyé le sujet d'examen par courriel, vont certainement se retrouver soupçonner. Et même soupçonnés à nouveau avec l'envoi du présent corrigé ; sans parler de tous les autres...

Exercice 3 *(4 points)*

On imagine un logiciel permettant de vérifier le contenu du système de fichiers d'une machine (prise isolément) en utilisant une fonction de hachage cryptographique. Ce logiciel est utilisé à l'installation initiale de la machine afin de constituer une liste rassemblant toutes les empreintes des fichiers exécutables de la machine. Cette liste est stockée dans un fichier lui-même placé à un endroit protégé de la machine (avec des droits d'accès limités, notamment aux seuls administrateurs). Ce fichier d'empreintes est signé à l'aide d'un outil de signature utilisant un algorithme cryptographique à clef publique. (type RSA) Les calculs cryptographiques et le stockage de la clef privée de signature sont effectués à l'aide d'une carte à puce *séparée*.

Supposons qu'un attaquant arrive à modifier un fichier exécutable sur la machine ainsi protégée et qu'il modifie *également* le fichier des empreintes afin d'ajuster l'empreinte enregistrée pour l'exécutable qu'il a altéré afin qu'elle soit correcte.

Suite à une suspicion d'intrusion, un administrateur légitime arrive sur la machine afin d'effectuer un contrôle.
Question 1 *(1 point)* : Est-il possible de détecter le fait que la machine a été globalement corrompue ? Justifier.
Question 2 *(1 point)* : Est-il possible de savoir quel fichier exécutable a été modifié ?
Question 3 *(1 point)* : Quel programme en particulier devrait viser l'attaquant sur la machine afin d'essayer d'éviter toute détection lors de la vérification des empreintes ? Pourquoi ?
Question 4 *(1 point)* : Comment doit-on effectuer le contrôle pour garantir la détection ?

Corrigé

1. *Oui, car lors de la vérification, c'est la signature cryptographique du fichier d'empreinte lui-même, effectuée par la carte à puce, qui sera erronée. Ceci permettra de détecter globalement que les empreintes ont été corrompues.*
2. *Non, l'empreinte originelle n'étant plus disponible et toutes les empreintes étant valides, on ne pourra pas savoir quel fichier en particulier a été altéré (en dehors de la liste des empreintes elle-même).*
3. *Pour réussir son attaque, l'intrus doit viser spécifiquement le programme utilisé pour communiquer avec la carte à puce ou pour effectuer la vérification des empreintes. En effet, en modifiant cet exécutable, il peut envisager de cacher à l'administrateur (qui va justement le lancer) que le fichier des empreintes est corrompu. Il peut même éventuellement en profiter pour faire recalculer la bonne signature à la carte à puce (au lieu de lui faire effectuer une vérification).*
   On peut envisager des variantes de cette méthode : une action malveillante visant le système de connexion (login) sur le principe d'un cheval de Troie ou – nettement plus sophistiquée – visant le remplacement du noyau du système d'exploitation par une version corrompue incluant des fonctions de dissimulation.
4. *Pour éviter ce type d'attaque, l'administrateur doit exécuter un programme qu'il amène lui-même pour faire la vérification. De manière générale, en cas de suspicion d'intrusion, il ne devrait faire confiance à aucun des logiciels installés sur la machine qu'il vérifie. Il serait même nécessaire (en particulier par rapport à une intrusion ciblant le noyau) de redémarrer la machine sur un système sain (par exemple sur CDROM) pour effectuer la vérification.*