INSA – 5° R.T.

Proposition d'exercices d'examen
janvier 2011

Détection d'intrusion

Exercice proposé

Exercice 1 *(1 point)*

Certains systèmes de détection d'intrusion sont théoriquement en mesure de détecter des attaques inconnues. Il s'agit :

1. des sondes de détection d'intrusion réseau ;
2. des IDS utilisant une approche par signatures ;
3. des IDS utilisant une approche comportementale.

Exercice 2 *(1 point)*

Parmi les logiciels suivants, quels sont les logiciels d'utilisation continue et d'utilisation périodique (ou les 2) ?

1. une sonde de détection d'intrusion analysant les traces systèmes ;
2. un antivirus ;
3. un outil de vérification d'intégrité du système de fichier ;
4. une sonde de détection d'intrusion réseau.

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. Les calculs cryptographiques et le stockage de la clef de chiffrement 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 contenue 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 ?

Exercice 3 *(4 points)*

Voici une signature de détection d'intrusion réseau extraite de la base des signatures utilisée par le logiciel Snort pour détecter la présence d'une porte dérobée sur une machine M :

```
alert tcp $HOME_NET 5555 -> $EXTERNAL_NET any (msg:"BACKDOOR serveme
runtime detection"; flow:from_server,established; content:"ServeMe 1.x";
depth:11; nocase;
reference:url,www.megasecurity.org/trojans/s/serveme/Serveme.html;
reference:url,www3.ca.com/securityadvisor/pest/pest.aspx?id=453081036;
classtype:trojan-activity; sid:7091; rev:2;)
```

Question 1 *(1 point)* : Cette signature se déclenche t'elle face à des paquets réseaux issus de la machine de l'attaquant vers la machine M ou pour des paquets réseaux émis par M ?
Question 2 *(2 points)* : Expliquez sur quels critères Snort détecte la porte dérobée (type de flux réseau, signature recherchée) ?
Question 2 *(1 point)* : Présentez un moyen d'exploiter à votre avantage la connaissance de cette signature et de la présence de Snort sur le réseau.