Master 2 SeCReTS 2017-2018
Module Surveillance et gestion d'incidents
Examen

Merci de bien lire les consignes :
- une seule feuille A4 manuscrite autorisée ;
- aucune communication ;
- aucun accès à un ordinateur, une station de travail, un téléphone portable, une calculatrice, un PDA ou tout autre dispositif électronique, connectable ou non ;
- sujet à remettre en fin d'examen ;
- n'oubliez pas d'**indiquer nom et prénom sur la copie**.

Un point est attribué au soin apporté à la rédaction des réponses.

Première partie
Généralités (6pts)

1. Sur le déroulement d'une intrusion :
   - — *(1pt)* Rappelez quelle est la première phase d'une intrusion.
   - — *(1pt)* Comment un attaquant peut réussir à introduire du code malveillant sur une station utilisateur ? Citez une technique.
   - — *(1pt)* Comment un attaquant peut contrôler une machine derrière un pare-feu correctement configuré ?
2. Sur l'organisation de la surveillance :
   - — *(2pts)* Le Security Operations Center (SOC) est la partie du système d'information où remontent les informations de sécurité. Comment peut-on connecter le SOC au reste du SI sans le mettre en danger ? Citez 2 types d'équipements réseau permettant de faire cette interconnection.
   - — *(1pt)* Quand on parle de détection d'intrusion, qu'est-ce qu'un faux négatif ?

Deuxième partie
Evaluation de la sécurité (4pts)

1. *(1pt)* Comment un outil d'audit peut détecter si une vulnérabilité est exploitable sur un système, sans mettre ce système en danger ?
2. *(1pt)* Citez deux types de faiblesses qui peuvent apparaître à l'utilisation d'une configuration par défaut.
3. *(2pts)* On cherche à mettre en place un outil de vérification d'intégrité sur un système. D'après vous, quels types de test peuvent être mis en place :
   - — pour surveiller l'intégrité d'un binaire comme `/bin/bash` ?
   - — pour surveiller l'intégrité d'un fichier de log comme `/var/log/messages` ?

Troisième partie

Surveillance et gestion des incidents (10pts)

1. (5 pts) Donnez la configuration Logstash complète permettant de :
   — récupérer les logs envoyés par rsyslog sur le port 10514 en TCP ;
   — parser les logs suivant :

```
Mon 1 10:15:19 station004.uvsq.fr dhcpcd[1723]: eth0: offered 192.168.101.93 from
    192.168.101.254
```

   pour lequel il faut récupérer :
   — le timestamp ;
   — le nom de la machine ;
   — le nom du programme ayant généré le log ;
   — l'interface ;
   — l'ip offerte ;
   — l'ip du serveur DHCP.

```
Mon 1 10:15:00 station004.uvsq.fr sudo[1331]: pam_unix(sudo:session): session opened
    for user root by william(uid=0)
```

   pour lequel il faut récupérer :
   — le timestamp ;
   — le nom de la machine ;
   — le nom du programme ayant généré le log ;
   — le nom de l'utilisateur cible ;
   — le nom de l'utilisateur à l'origine de l'action ;
   — le status de la session.

```
Mon 1 10:35:24 station004.uvsq.fr sudo[3724]: pam_unix(sudo:session): session closed
    for user root
```

   pour lequel il faut récupérer :
   — le timestamp ;
   — le nom de la machine ;
   — le nom de l'utilisateur cible ;
   — le status de la session.
   — le nom du programme ayant généré le log ;
   — envoyer les logs vers une instance locale de Elasticsearch.
2. (1 pt) Pour effectuer la collecte des logs, quelles raisons sont en faveur de l'utilisation du TCP ?
3. (1 pt) Comment et pourquoi peut-on utiliser du chiffrement lors de la collecte de logs ?
4. (1 pt) Expliquez en quoi il est important de bien déterminer le périmètre d'impact d'un incident.
5. (1 pt) Quels conseils donneriez-vous à une entreprise souhaitant utiliser une solution comme MIPS ?
6. (1 pt) Une entreprise dispose des données suivantes sur son parc informatique :
   — les logs systèmes des serveurs et stations Windows ;
   — les flux réseau en certains points ;
   — les logs du proxy web ;
   — les logs de flux bloqués par le pare-feu.

   Donnez un exemple d'attaque que l'on peut détecter avec ces données, et une mesure de protection associée.

Quatrième partie

Architecture, capture et analyse réseau

1. (1 point) Citez deux dispositifs / technologies permettant de dupliquer du trafic réseau.
2. (1 point) Quel est l'intérêt de mettre en place du filtrage en interne d'un réseau ?
3. (2 point) Quelle attaque peut être détectée en faisant de la surveillance ARP ?
4. (1 point) Pourquoi est-il intéressant de séparer la capture de l'analyse réseau ?
5. (2 points) Quelles sont les deux grandes méthodes de détection d'intrusion ? Donnez un exemple d'attaque détectée pour chaque méthode de détection.
6. (2 points) Donnez 2 exemples d'analyse réseau que l'on peut faire en vue de faire de la détection d'intrusion.
7. (1 point) La règle suivante est chargée dans Snort :

```
alert tcp any any -> $HOME_NET any (msg:"TCP Port Scanning";
  detection_filter:track by_src, count 10,
  seconds 10; sid:1000003; rev:2;)
```

   Que permet de détecter la règle Snort précédente ? Comment un attaquant peut-il contourner cette règle ?

Fin de l'examen.
