Fiche TD N°1

Détection d'intrusion

Questions de cours :

1. Donnez un scénario pour lancer une attaque DoS en réseau.
2. Quelle est la différence entre un IDS et un IPS ?
3. Quelle est la différence entre un système de réponse active et un IPS ?
4. Quels sont les avantages d'un IDS qui inspecte les données au niveau de la couche Application ?
5. Quelles sont les caractéristiques les plus importantes pour la détection d'anomalies dans les journaux d'accès Web ?
6. Comment pourriez-vous gérer les faux positifs et les faux négatifs dans IDS ?

Exercice 2 :

Q1. Un IDS vous permet de :

a. Détecter les intrusions sans les prévenir.
b. Détecter les intrusions et les prévenir.
c. Bloquer un ping réseau vers l'extérieur.
d. Supprimer les virus d'une machine.

Q2. Une entreprise souhaite installer un système permettant de détecter et de prévenir les attaques sur son réseau, vous lui proposez :

a. NIDS.
b. NIPS.
c. HIDS.
d. HIPS.

Q3. Une entreprise souhaite se protéger contre les attaques de type smurf, vous lui proposez d'installer :

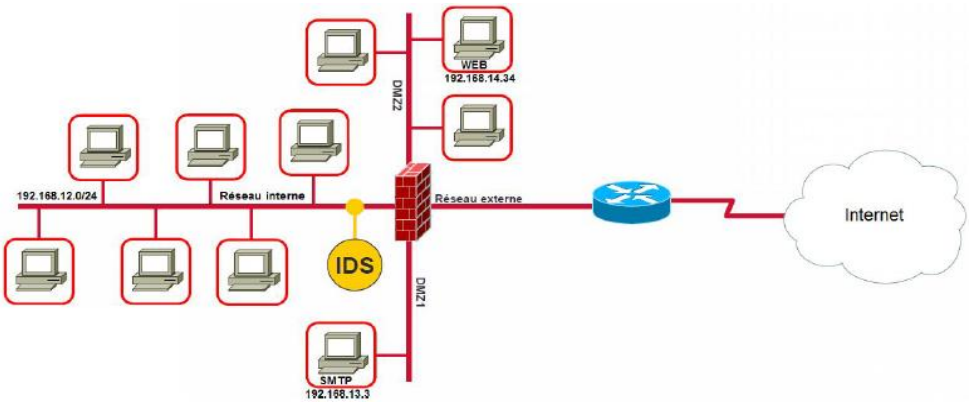
a. Un WAF (Web Application FW).
b. Un pare-feu de la couche réseau.
c. Un antivirus.
d. Un IDS/IPS.

Q4. A quoi correspond un "faux positif" :

a. Un message d'alerte qui ne devrait pas déclencher une alerte (émis à tort).
b. Un message d'alerte qui devrait déclencher une alerte.
c. Un message d'alerte pour un événement légitime.
d. Aucune réponse n'est correcte.

Exercice 3 :

Une entreprise dispose de l'architecture réseau montrée sur la figure suivante :



- Les administrateurs réseaux souhaitent construire :
  a) Une règle permettant un déclenchement d'alerte dès qu'un utilisateur du réseau local essaie de se connecter au serveur SMTP qui se trouve dans la DMZ 1 avec la protocole TCP.
  b) Une règle permettant un déclenchement d'alerte dès qu'un utilisateur du réseau local essaie de se connecter à un site malicieux en https (www.siteMalicieux.com) avec la protocole TCP.
  c) Une règle permettant un déclenchement d'alerte dès qu'un utilisateur du réseau local essaie de s'authentifier avec le login "ImHacker" sur le serveur Web en http qui se trouve dans la DMZ2.

- En utilisant la syntaxe des règles *Snort*, créez une règle pour chaque point ci-dessus permettant de respecter le besoin de votre client.

Exercice 4 :

Ci-dessous 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 overflow attempt"; flow:to_server, established; content:"DTSTART"; nocase; content:!"value"; within:5; nocase; content:!"ATTACK"; within:4; nocase; reference:cve,2007-0033;

1. Expliquez sur quels critères Snort détecte un message électronique particulier (type de flux réseau, caractéristiques des données) ?

2. Proposez une évolution de cette signature permettant de détecter les messages électroniques contenant les mots clefs consécutifs suivants : « hacker », « attack », « phishing », et affichant le message suivant : « Potential cyber attack ».