Exercice N°1 : répondre aux questions suivantes d'une manière précise et concise :

1. Quels sont les moyens de sécurité permettant de satisfaire les critères de sécurité suivants :
   - La disponibilité.
   - La confidentialité.
   - L'intégrité.
2. Quels sont les objectifs de sécurité violés par les attaques suivantes :
   - Attaque par synflood.
   - Attaque par injection SQL.
   - Attaque de type TCP/IP spoofing.
3. Pourquoi l'ouverture des systèmes d'information des organisations par les réseaux de télécommunication pose-t-elle des problèmes de sécurité ?
4. Pourquoi l'usage du chiffrement asymétrique est-il préféré au chiffrement symétrique dans des transactions sur internet ? dans quelles circonstances le chiffrement symétrique peut-il être utilisé ?
5. A quel besoin répond une infrastructure de gestion de clés (Public Key Infrastructure, PKI) ?
6. les programmes CGI traitent les données envoyées par les utilisateurs au serveur web. Donner un exemple de vulnérabilité de ces programmes. Comment peut être utilisée par les pirates pour contourner les mesures de sécurité.

Exercice2 : On rappelle que l`IP spoofing consiste pour un pirate à se faire passer pour une machine B auprès d`une machine A (au niveau de l'adressage IP). L'attaque se compose généralement de trois étapes : Le pirate paralyse la machine B, Le pirate devine le procédé utilisé par A pour générer ses numéros de séquence initiaux (ISN). Le pirate se fait passer pour B auprès de A.

1. Le pirate profite de quelle faille du système d'exploitation pour paralyser la machine B ? Proposer une solution pour remédier à ce problème.
2. Dans quel cas le pirate peut deviner le procédé de génération des numéros de séquence ?
   Proposer une solution pour empêcher le pirate de déduire ce procédé.

Exercice3 : Pour attaquer un réseau d'entreprise, l'attaquant envoie un message, à un utilisateur de ce réseau d'entreprise, grâce à des fichiers attachés contenant des programmes permettant de récupérer l'ensemble des adresses de courrier contenues dans le carnet d'adresse et en envoyant des copies d'eux-mêmes chaque seconde à tous ces destinataires. Ce message reproduisait trop vite sur le réseau. De plus, tous ces messages ont créé une saturation au niveau de la bande passante, ce qui a obligé l'entreprise à arrêter les connexions réseaux pendant une journée.

1. De quel type d'attaque s'agit-t-il ?
2. Quel est l'objectif de l'attaquant ?
3. Quel type de programme d'infection s'agit-t-il ?
4. Quel est la solution utilisée pour se protéger contre ce type de programme ?

Correction :

Exercice1 :

1. Les moyens de sécurité satisfaisant :
   - La disponibilité sont la redondance et la sauvegarde périodique.
   - La confidentialité sont le contrôle d'accès, l'authentification et le chiffrement.
   - L'intégrité sont le contrôle d'erreur, le chiffrement et la détection des virus et d'intrusion.
2. les objectifs violés sont :
   - synflood : la disponibilité.
   - Injection SQL : confidentialité.
   - TCP/IP spoofing : confidentialité.
3. L'ouverture des systèmes d'information via les réseaux de télécommunication étend les frontières des systèmes d'information, cela accroit leur exposition aux risques (risque d'intrusion, risque de prise de contrôle à distance, risque d'infection…) et augmente le nombre de vulnérabilités et de menaces .
4. Le chiffrement asymétrique est préféré du fait qu'il résout le problème de distribution des clés, via l'usage de certificats numériques.
   Le chiffrement symétrique peut être combiné avec le chiffrement asymétrique pour des raisons de rapidité de chiffrement de gros volume de données.
5. Une infrastructure de gestion de clés répond au besoin de distribution de clés de chiffrement (asymétrique) entre acteurs qui à priori ne se connaissent pas.
6. Une vulnérabilité des programmes CGI est l'absence du contrôle des données saisies par les utilisateurs.
   Les pirates peuvent injecter du code malicieux.

Exercice2 :

1. Le pirate profite de la gestion de la pile TCP/IP pour traiter les demandes de connexion.
   Solution : éliminer les connexions les plus anciennes quand la pile est pleine.
2. Dans le cas où les numéros de séquence sont générés par une méthode déterministe.
   Solution : générer les numéros de séquence aléatoirement.

Exercice3 :

1. L'attaque est dénis de service.
2. L'objectif de l'attaquant est de paralyser le réseaux local de l'entreprise et donc elle va perdre de l'argent, des clients, l'image de marque.
3. Il s'agit d'un ver.
4. Sensibiliser les employés et utiliser des antivirus.