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 des 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 ?