I - Questions de cours

1. La sécurité informatique est le domaine de l'informatique qui se concentre sur la protection des systèmes informatiques, des données et des réseaux contre les menaces, les attaques et les vulnérabilités.

2. Une politique de sécurité informatique est un ensemble de directives, de règles et de procédures définies par une organisation pour protéger ses actifs informatiques et garantir la sécurité de ses systèmes et données.

3. Avantages et limites des chiffrements symétrique et asymétrique :

- Chiffrement symétrique :

- Avantages : rapide, efficace pour le chiffrement de données en vrac.

- Limites : nécessite une gestion sécurisée de la clé de chiffrement, peu adapté aux communications sécurisées entre parties qui ne se font pas confiance.

- Chiffrement asymétrique :

- Avantages : permet l'échange sécurisé de clés, adapté aux communications entre parties non confidentes, offre une sécurité renforcée.

- Limites : plus lent que le chiffrement symétrique, nécessite davantage de ressources.

4. Les utilisateurs peuvent être pris en compte dans la mise en place d'une politique de sécurité informatique en sensibilisant, en formant et en impliquant les utilisateurs dans les pratiques de sécurité, en définissant des politiques d'accès et d'utilisation des ressources, et en mettant en place des mécanismes de contrôle et de suivi des activités des utilisateurs.

5. Les principales fonctions de sécurité d'un Firewall dans un réseau informatique sont de filtrer le trafic réseau en fonction de règles prédéfinies, de bloquer ou d'autoriser le trafic en fonction de critères de sécurité, de prévenir les accès non autorisés, de protéger contre les attaques par intrusion, de gérer les connexions entrantes et sortantes, et de surveiller le trafic pour détecter les activités suspectes.

6. Le principe de fonctionnement d'une clé de session est qu'elle est générée de manière aléatoire pour une communication spécifique, utilisée pour chiffrer et déchiffrer les données de cette session, et détruite après la fin de la session pour garantir la sécurité des échanges.

II - Questions de compréhension

1. Explication des lignes :

- `access-list 101 deny top any eq 21 host 195.83.80.5` : Cette ligne crée une règle dans une liste d'accès (ACL) numéro 101 qui interdit tout trafic de sortie (top) à partir de n'importe quelle source (any) vers le port 21, sauf s'il provient de l'hôte 195.83.80.5.

- `access-list 102 permit tep any any eq 25` : Cette ligne crée une règle dans une ACL numéro 102 qui autorise le trafic de sortie (tep) de n'importe quelle source vers n'importe quelle destination sur le port 25.

- `access-list 101 permit ip any any log` : Cette ligne crée une règle dans une ACL numéro 101 qui autorise tout trafic IP de n'importe quelle source vers n'importe quelle destination, et elle ajoute l'option "log" pour enregistrer les événements liés à cette règle.

2. La commande qui permet de générer une paire de clé (publique/privée) RSA de taille 2048 bits et stocker le résultat dans le fichier test.pem est :

- a) `Openssl genrsa -out test.pem 2048`

3. La commande qui permet d'extraire la partie publique de examen.pem et de la nommer ExamenPublique.pem est :

- b) `Openssl rsa -in examen.pem -pubout -out ExamenPublique.pem`

4. La commande qui permet de chiffrer le texte clair (essai.txt) à l'aide de votre clé publique (Publique.pem) et de mettre le résultat dans le fichier essaichiffre.txt est :

- (a) `Openssl rsautl -encrypt -pubin -inkey Publique.pem -in essai.txt -out essaichiffre.txt`

5. La commande qui permet de créer un certificat d'autorité de type X.509 (CA\_cert.pem) pour CA est :

- d) `openssl req -new -x509 -key CA\_cle.pem -out CA\_cert.pem`