Département de Réseaux & Télécommunications
2ème année Master
Année 2025 – 2026
Matière : Sécurité des réseaux de communication

Enoncé + corrigé-type de l'examen final

Chargé de la matière : Pr. Laboudi Zakaria

Exercice 01 (5pts) : pour chaque question, entourer **la ou les bonnes réponses.**

Q1) Une attaque par déni de service (DoS) vise principalement:

A. La confidentialité **B.** L'intégrité

C. La disponibilité **D.** L'authenticité

Q2) Le service de non-répudiation garantit que:

A. Les données sont chiffrées

B. L'émetteur ne peut nier l'envoi d'un message

C. Le réseau reste disponible **D. Le récepteur ne peut nier la réception**

Q3) Un pare-feu permet:

A. Le filtrage entrant et sortant

B. La protection contre les attaques internes

C. L'application d'une politique de sécurité

D. Le contrôle des communications réseau

Q4) Un système IDS:

A. Empêche automatiquement les intrusions

B. Détecte des comportements anormaux

C. Peut produire des faux positifs **D. Analyse le trafic réseau**

Q5) Les mécanismes assurant la confidentialité incluent:

A. Le chiffrement **B. Le contrôle d'accès**

C. La journalisation **D. Le bourrage de trafic**

Exercice 02 (3pts) : questions de réflexion

Pour chacun des scénarios donnés ci-dessous, il est demandé de proposer une solution simple, concise et argumentée en quelques lignes.

Scénario 1 : dans une entreprise, plusieurs postes de travail sont ralentis et communiquent avec des serveurs externes inconnus sans action de l'utilisateur.

Question : quel type de menace est suspecté et quelle mesure recommandez-vous ?

Réponse

Malware / botnet, antivirus, pare-feu, isolation du poste.

Scénario 2 : un administrateur découvre qu'un serveur utilise une version logicielle contenant une vulnérabilité récemment publiée.

Question : quelle action prioritaire doit-il entreprendre pour réduire le risque ?

Réponse

Mise à jour, correctif de sécurité, gestion des vulnérabilités.

Scénario 3 : un utilisateur affirme avoir reçu des messages provenant d'un collègue, mais le contenu semble inhabituel et suspect.

Question : quel type d'attaque est probable et quel mécanisme permet de s'en protéger?

Réponse

Mascarade / usurpation d'identité, authentification, signature numérique.

Scénario 4 : le site web d'une entreprise devient inaccessible après la réception d'un grand nombre de requêtes SYN incomplètes.

Question : quel type d'attaque est probablement en cours et quelle solution simple peut être mise en place ?

Réponse

Attaque SYN Flood (DoS), pare-feu stateful, limitation des connexions.

Scénario 5 : suite à une panne ou une attaque, une entreprise ne peut plus accéder à ses données pendant plusieurs heures.

Question : quel service de sécurité est concerné et quelle solution simple permet de limiter l'impact ?

Réponse

Disponibilité, sauvegardes, réplication des données.

Scénario 6 : un ordinateur personnel est connecté au réseau interne de l'entreprise sans validation préalable.

Question : quel mécanisme de sécurité permet de contrôler ce type d'accès ?
Réponse

Contrôle d'accès réseau, authentification réseau.

Exercice 03 (10pts) : cryptographie et signature numérique par RSA

Alice et Bob utilisent chacun un système RSA en utilisant les paramètres suivants : Alice : (p = 17, q = 3 et e = 3) et Bob : (p = 3, q = 11 et e = 3).

1) Quelles les valeurs du module RSA et de l'indicatrice d'Euler pour chacun des deux systèmes (d'Alice et Bob) ?

- Pour Alice :

  Le module RSA $n = p \times q = 51$

  L'indicatrice d'Euler $\phi(n) = (n-1) \times (q-1) = 32$

- Pour Bob :

  Le module RSA $n = p \times q = 33$

  L'indicatrice d'Euler $\phi(n) = (n-1) \times (q-1) = 22$

2) Quelles sont les valeurs de la clé publique et la clé privée d'Alice et de Bob ?

- Pour Alice :

  La clé publique (n, e) = (51, 3)

  La clé privée (n, d) = (51, 11) (d est obtenu en appliquant l'algorithme d'Euclide étendu)

- Pour Bob :

  La clé publique (n, e) = (33, 3)

  La clé privée (n, d) = (33, 7) (d est obtenu en appliquant l'algorithme d'Euclide étendu)

3) Alice veut envoyer un message m = 2 à Bob.

3.1) Calculer la valeur du message chiffré C (m) ?

$C(m) = m^e \bmod n = 2^3 \bmod 33 = 8$

3.2) Lors de réception du message, comment Bob peut-il déchiffrer le message reçu ?

$m = C(m)^d \bmod n = 8^7 \bmod 33 = 2$

4) On considère maintenant qu'Alice veut envoyer le message m = 2 à Bob en rajoutant une signature numérique.

4.1) Calculer la valeur de la signature numérique liée au message chiffré C (m) ?

$S(C(m)) = C(m)^d \bmod n = 8^{11} \bmod 51 = 2$

4.2) Lors de réception du message, comment Bob peut-il s'assurer que le message reçu est effectivement de la part d'Alice ?

$V(S(C(m))) = S(C(m))^e \bmod n = 2^3 \bmod 51 = 8 = C(m)$

5) On considère maintenant qu'Alice veut envoyer le message m = 2 à Bob en rajoutant une signature numérique que seul Bob peut la vérifier.

5.1) Calculer la valeur de la signature numérique liée au message chiffré C (m) ?

$C(S(C(m))) = S(C(m))^e \bmod n = 2^3 \bmod 33 = 8$

5.2) Lors de réception du message, comment Bob peut-il s'assurer que le message reçu est effectivement de la part d'Alice ?

$S(C(m)) = S(C(m))^d \bmod n = 8^7 \bmod 33 = 2$

6) Refaire les questions 3 et 4 en considérant le message m = (2, 3).

6.1) Calculer la valeur du message chiffré C (m = 3) ?

$C(m) = m^e \bmod n = 3^3 \bmod 33 = 27$

6.2) Lors de réception du message, comment Bob peut-il déchiffrer le message reçu ?

$m = C(m)^d \bmod n = 27^7 \bmod 33 = 3$

6.3) Calculer la valeur de la signature numérique liée au message chiffré C (m = 3) ?

$S(C(m)) = C(m)^d \bmod n = 27^{11} \bmod 51 = 3$

6.4) Lors de réception du message, comment Bob peut-il s'assurer que le message reçu est effectivement de la part d'Alice ?

$V(S(C(m))) = S(C(m))^e \bmod n = 3^3 \bmod 51 = 27 = C(m)$