République algérienne démocratique et populaire
Ministère de l'enseignement supérieur et de la recherche scientifique
Université Kasdi Merbah Ouargla
Faculté des nouvelles technologies de l'information et de la communication
Département de l'informatique et des technologies de l'information

Examen du module : Sécurité 2 (M2 ASR) Durée : 1h30

Nom :
Prénoms :

Exercice 1 (06 pts): Veuillez répondre aux questions suivantes

1. Quelle propriété permet de garantir que seules les personnes habilitées doivent avoir accès aux données ? Confidentialité
2. Quelle propriété permet de garantir le bon fonctionnement du système et l'accès à un service et aux ressources à n'importe quel moment ? La disponibilité
3. Quelle propriété permet de garantir qu'une transaction ne peut être niée par aucun des correspondants ? La non répudiation
4. Quelle propriété permet de garantir l'intégralité des données, leur précision, l'authenticité et la validité ? L'intégrité
5. Quelle propriété permet d'assurer l'identité d'un utilisateur avant l'échange de données ? Authentification
6. Dans l'analyse des risques, que signifie l'exploitation d'une faiblesse de sécurité par un attaquant ? Menace
7. Dans l'analyse des risques, que signifie faiblesse de sécurité qui peut être de nature logique ou physique ? Vulnérabilité
8. Dans l'analyse des risques, que signifie l'impact sur l'entreprise de l'exploitation d'une faiblesse de sécurité ? Conséquence
9. Quelle attaque consiste à casser un mot de passe en testant tous les mots de passe possibles ? Attaque par force brute
10. Quelle attaque consiste à se faire passer pour un autre système en falsifiant son adresse IP ? IP Spoofing
11. Quelle attaque consiste à faire passer les échanges réseau entre deux systèmes par le biais d'un troisième, sous le contrôle du pirate ? Man In the Middle Attaque
12. Quel mécanisme offre la fonctionnalité « packet scrubbing », qui permet de contrôler la consistance des données en relation avec les protocoles qui les véhiculent ? N-IPS

Exercice 2 (04 pts): Dans une entreprise, le directeur dispose d'une clé publique (X) et d'une clé privée (Y), le comptable a une clé publique (A) et d'une clé privée (B) et un client a une clé publique (K) et d'une clé privée (L).

1. Quelle clé utilise le comptable pour signer un message à envoyer au client ? B
2. Quelle clé utilise le directeur pour signer un message à envoyer au comptable ? Y
3. Quelle clé utilise le comptable pour chiffrer un message à envoyer au directeur ? X
4. Quelle clé utilise le client pour déchiffrer un message reçu par le directeur ? L
5. Quelle clé utilise le comptable pour vérifier une signature reçue par le directeur ?Y
6. Quelle clé utilise le directeur pour chiffrer un message à envoyer au client ? K
7. Quelle clé utilise le client pour vérifier une signature reçue par le comptable? A
8. Quelle clé utilise le directeur pour déchiffrer un message reçu par le client? Y

Exercice 3 (10 pts): Veuillez indiquer si ces affirmations sont vraies ou fausses (V/F)

Affirmations	V/F
Les ACL sont généralement appliquées au trafic entrant (ingress) ou sortant (egress) de l'interface d'un équipement réseau.	V
Les hackers (black hats) ont comme ambition d'aider à la sécurisation du système	F
Une identification élémentaire est le mot de passe que vous entrez dans le système informatique	F
Les risques ayant une occurrence faible et une conséquence faible sur l'entreprise ne sont pas pris en compte.	V
Authentication Header est le protocole d'établissement d'une connexion SSL. Il permet d'authentifier les parties client-serveur et de négocier les paramètres cryptographiques.	F
Dans le filtrage dynamique, le pare-feu agit comme un filtre au niveau applicatif (niveau 7 du modèle OSI)	F
Les risques ayant une occurrence forte et une conséquence faible doivent être pris en compte	V
Dans une attaque par amplification l'attaquant demande au serveur d'utiliser une version d'un protocole plus ancienne afin d'exploiter les failles qu'elle comporte.	F
Encapsulating Security Payload permet d'échanger des messages prédéfinis sur les états d'une connexion SSL.	F
L'IP spoofing consiste à se faire passer pour un autre système en falsifiant son adresse IP.	V
Lors d'une attaque, les scanneurs de vulnérabilité permettent d'effacer les journaux d'activité.	F
Dans une attaque man-in-the-middle, une ou plusieurs machines inondent le réseau avec des paquets réseau afin de saturer la bande passante	F
Les risques ayant une occurrence faible et une conséquence forte doivent être pris en compte	V
L'authentification désigne l'ensemble des mécanismes garantissant que les ressources de l'entreprise sont accessibles	F
L'intégrité désigne l'ensemble de mécanisme permettant de garantir qu'un message a bien été envoyé par un émetteur et reçu par un destinataire.	F
Les attaques par rejeu (replay attaque) sont des attaques de type man in the middle consistant à intercepter des paquets de données et à les rejouer	V
Une authentification élémentaire est le nom d'utilisateur que l'on saisit dans un système informatique.	F
La confidentialité désigne l'ensemble des mécanismes garantissant qu'une information n'a pas été modifiée.	F
Les risques ayant une occurrence forte et une conséquence forte ne doivent pas exister	V
L'attaque par downgrade consiste à utiliser des serveurs dont la réponse à une requête renvoie bien plus de données que la requête originale.	F

Bon courage