QCM – Sécurité Réseaux & Authentification AAA

---

1. Quel est l'objectif de l'intégrité des données ? *(1 pt)*

a. Protéger les données contre les accès non autorisés
b. Garantir que les données ne sont pas modifiées de manière non autorisée
c. Assurer la disponibilité des données
d. Empêcher toute attaque réseau

---

2. Parmi les éléments suivants, lesquels correspondent à une attaque de type DoS (Déni de Service) ? *(1 pt)*

a. Ping of Death
b. IP Spoofing
c. SYN Flooding
d. MAC Spoofing

---

3. Le protocole RADIUS est principalement utilisé pour : *(1 pt)*

a. L'attribution automatique d'IP
b. L'authentification centralisée des utilisateurs
c. Le chiffrement des données entre deux postes
d. Le routage dynamique

---

4. Le malware "Cheval de Troie" se distingue par : *(1 pt)*

a. Sa capacité à se répliquer automatiquement
b. Son apparence inoffensive pour tromper l'utilisateur
c. Sa propagation via des périphériques USB
d. Son ciblage des routeurs exclusivement

---

5. Parmi les types de spoofing, lequel consiste à falsifier l'adresse IP source ? *(1 pt)*

a. MAC Spoofing
b. DNS Spoofing
c. IP Spoofing
d. Email Spoofing

---

6. Quelle affirmation est vraie concernant le mot-clé `local-case` dans une configuration AAA ? *(1 pt)*

a. Il permet de rendre les identifiants sensibles à la casse
b. Il active l'authentification uniquement pour les lignes console
c. Il limite les utilisateurs aux lignes VTY uniquement
d. Il chiffre les mots de passe dans la base locale

QCM – Protocoles d'authentification et sécurité réseau

---

1. Le modèle AAA (Authentication, Authorization, Accounting) est utilisé pour : *(1 pt)*

a. Gérer les droits d'accès aux ressources réseau
b. Effectuer le routage des paquets
c. Enregistrer les actions des utilisateurs
d. Réaliser des sauvegardes automatiques

---

2. Le protocole RADIUS : *(1 pt)*

a. Utilise TCP pour ses communications
b. Chiffre uniquement le mot de passe utilisateur
c. Fournit un chiffrement complet de la session
d. Est souvent utilisé pour l'authentification réseau via Wi-Fi

---

3. Quelle différence majeure existe entre RADIUS et TACACS+ ? *(1 pt)*

a. RADIUS chiffre toute la session, TACACS+ seulement le mot de passe
b. RADIUS utilise TCP, TACACS+ utilise UDP
c. TACACS+ chiffre toute la session, RADIUS seulement le mot de passe
d. TACACS+ est open-source, RADIUS est propriétaire

---

4. Dans une configuration Cisco, que permet le mot-clé `login authentication default` ? *(1 pt)*

a. Appliquer l'authentification AAA par défaut
b. Restreindre l'accès aux utilisateurs locaux uniquement

c. Bypasser le serveur RADIUS
d. Appliquer une méthode d'authentification nommée "default"

---

5. Le protocole TACACS+ est préféré à RADIUS dans les environnements Cisco parce que : *(1 pt)*

a. Il est plus rapide
b. Il chiffre toutes les données de la session AAA
c. Il permet de séparer l'authentification, l'autorisation et l'audit
d. Il fonctionne uniquement en environnement Windows

---

6. Lequel des éléments suivants n'est pas une fonctionnalité du protocole AAA ? *(1 pt)*

a. Authentifier un utilisateur
b. Définir les permissions d'un utilisateur
c. Crypter le trafic réseau entre deux routeurs
d. Enregistrer les actions d'un utilisateur.

QCM – Attaques réseau & cybersécurité

---

1. Une attaque de type "brute force" consiste à : *(1 pt)*

a. Intercepter une session de connexion active
b. Tester toutes les combinaisons possibles de mot de passe
c. Tromper un utilisateur pour obtenir ses identifiants
d. Exploiter une faille d'un protocole de chiffrement

---

2. Une attaque Man-in-the-Middle (MITM) permet à l'attaquant de : *(1 pt)*

a. Lire et modifier les messages échangés entre deux parties
b. Accéder physiquement au serveur de l'entreprise
c. Se faire passer pour l'utilisateur auprès du serveur
d. Lire uniquement le contenu chiffré du message

---

3. Le phishing (hameçonnage) est une attaque qui : *(1 pt)*

a. Nécessite l’accès physique à la machine victime
b. Utilise des mails ou des sites falsifiés pour voler des données
c. Est souvent détectée par des antivirus
d. Implique toujours un cryptage des messages

---

4. Pour se protéger des attaques de type MITM, on peut utiliser : *(1 pt)*

a. HTTPS (TLS/SSL)
b. Le protocole FTP
c. Un pare-feu bien configuré
d. Des connexions VPN

---

5. Lequel de ces éléments est une bonne pratique de cybersécurité ? *(1 pt)*

a. Utiliser le même mot de passe pour tous les services
b. Activer l’authentification à double facteur (2FA)
c. Répondre aux mails inconnus rapidement
d. Mettre à jour régulièrement ses logiciels

---

6. L’attaque dite “replay” consiste à : *(1 pt)*

a. Réutiliser une ancienne transmission valide pour accéder à un service
b. Créer un faux site web pour tromper l’utilisateur
c. Deviner un mot de passe à l’aide de dictionnaires
d. Scanner un réseau pour trouver des vulnérabilités
