Voici un exemple complet de **contrôle type QCM et questions ouvertes**, similaire à celui que tu m'as envoyé, basé sur les chapitres de sécurité informatique, AAA, menaces, vulnérabilités, protocoles (comme RADIUS), et attaques :

Contrôle de Révision – Sécurité des Systèmes et Réseaux

Durée : 30 minutes – **Total : 6 points**

Questions de cours (6 points)

---

1. Définir le rôle de la confidentialité des données. *(1 pt)*

.....
.....

Correction : La confidentialité vise à empêcher l'accès non autorisé aux données. Seules les personnes autorisées peuvent consulter l'information.

---

2. Parmi les affirmations suivantes, lesquelles sont vraies ? *(1 pt)*

- a. Une attaque par force brute consiste à deviner les mots de passe en testant toutes les combinaisons possibles.
- b. Une vulnérabilité est une attaque directe contre un système.
- c. Le spoofing est une méthode d'usurpation d'identité.
- d. Une menace est toujours liée à un pirate informatique.

Réponses correctes : a et c
b est faux (vulnérabilité = faille),
d est faux (les menaces peuvent être naturelles ou humaines).

---

3. Donner trois fonctions principales du protocole RADIUS. *(1 pt)*

.....
.....
.....

Correction :

1. Authentification des utilisateurs
2. Autorisation des accès
3. Comptabilité (suivi de la connexion)

---

4. Qu’est-ce qu’un malware de type ransomware ? *(1 pt)*

.....
.....

Correction : C’est un logiciel malveillant qui chiffre les fichiers d’un utilisateur et demande une rançon pour les déchiffrer.

---

5. Parmi les attaques suivantes, lesquelles sont des attaques de type "spoofing" ? *(1 pt)*

a. ARP spoofing
b. DDoS
c. DNS spoofing
d. Ping flood

Réponses correctes : a et c

---

6. Quelle est l’utilité du mot-clé `local` dans une configuration AAA ? *(1 pt)*

a. Permet d’utiliser une base d’utilisateurs stockée localement sur le routeur
b. Désactive le protocole RADIUS
c. Limite les utilisateurs aux ports console uniquement
d. Active le chiffrement MD5

Réponse correcte : a

Si tu veux, je peux aussi te faire un autre exemple orienté uniquement sur les **protocoles AAA (RADIUS, TACACS+), les types de menaces, ou les attaques DoS**. Tu veux un autre exemple ?

Parfait ! Voici un **deuxième exemple de contrôle**, cette fois axé sur les **protocoles AAA, types d’attaques, menaces, vulnérabilités et spoofing**, toujours dans le même format, avec les **réponses corrigées à la fin**.

Contrôle – Sécurité Réseau et Authentification AAA

Durée : 30 minutes – **Total : 6 points**

Questions de cours (6 points)

---

1. Citer les trois étapes du mécanisme AAA. *(1 pt)*

.....
.....

Correction :

1. Authentification
2. Autorisation
3. Comptabilité

---

2. Parmi les propositions suivantes, lesquelles sont vraies ? *(1 pt)*

- a. Le protocole RADIUS chiffre l'intégralité du message.
- b. TACACS+ chiffre uniquement le mot de passe.
- c. RADIUS utilise le protocole UDP.
- d. TACACS+ est souvent utilisé pour les équipements Cisco.

Réponses correctes : c et d
a est faux (RADIUS ne chiffre que le mot de passe),
b est faux (TACACS+ chiffre tout le message)

---

3. Qu'est-ce qu'une attaque "man-in-the-middle" ? *(1 pt)*

.....
.....

Correction :
Une attaque où un pirate intercepte et éventuellement modifie la communication entre deux parties sans qu'elles ne s'en rendent compte.

---

4. Citer deux différences entre RADIUS et TACACS+. *(1 pt)*

.....
.....

Correction :

- RADIUS utilise UDP, TACACS+ utilise TCP
- RADIUS chiffre uniquement le mot de passe, TACACS+ chiffre tout le message

---

5. Lequel des éléments suivants est une vulnérabilité ? *(1 pt)*

a. Un mot de passe par défaut laissé sur un serveur
b. Un employé mécontent
c. Une panne électrique
d. Une inondation

Réponse correcte : a

---

6. Quelle(s) attaque(s) correspond(ent) à une usurpation d'identité ? *(1 pt)*

a. IP Spoofing
b. MAC Spoofing
c. SYN Flooding
d. Brute Force

Réponses correctes : a et b

Souhaites-tu un **troisième exemple** encore plus orienté "DoS/DDoS", "réseaux sécurisés" ou plutôt un **QCM pur 100% sans question ouverte** ?