

Question de cours :

1 .Objectif de l'intégrité des données

L'intégrité des données garantit que les informations ne sont **pas altérées** de manière non autorisée pendant leur stockage, transmission ou traitement. Elle vise à :

- Empêcher les modifications accidentelles ou malveillantes.
- Assurer l'exactitude et la cohérence des données.
- Utiliser des mécanismes comme les **hashs** (SHA-256) ou les **signatures numériques**.

2. Propositions vraies -- deepseek

Les affirmations correctes sont :

- ✓ **Un risque est une combinaison d'une menace et des pertes potentielles.**
- ✓ **Une vulnérabilité est tout point faible dans le système.**
- ✓ **L'inexpérience d'un programmeur est une menace** (erreur humaine).

Explications :

- Une *menace* provient de l'extérieur (ex: hacker), mais une *faille* = *vulnérabilité*.
- Le risque évalue l'impact (ex: perte financière due à une vulnérabilité exploitée).

2. Lesquelles des propositions suivantes sont vraies ? --ChatGPT

- **Une menace et une attaque possible par un actif de l'extérieur du Système : Vrai**
- **Un risque est une combinaison d'une menace et les pertes qui peuvent être causées par cette menace : Vrai**
- **Une vulnérabilité dans la sécurité informatique est tout point faible dans le Système : Faux** (c'est la définition d'une **faille**)
- **Une faille dans la sécurité informatique est tout point faible dans le Système : Vrai**
- **L'inexpérience d'un programmeur d'un logiciel de communication avec une BD est une menace pour le SI : Faux** (c'est une vulnérabilité, pas une menace)

Réponses vraies : 1, 2, 4

3. Caractéristiques de RADIUS --deepseek

1. **Protocole UDP** (ports 1812/1813) pour l'authentification/comptabilité.
2. **Chiffrement partiel** : Seul le mot de passe est encrypté.
3. **Combine authentification et autorisation** (contrairement à TACACS+).
4. **Standard ouvert** (RFC 2865), largement utilisé pour les accès réseau (WiFi, VPN).

3. Donner au moins trois caractéristiques principales du protocole RADIUS : ChatGPT

1. Il fournit une **authentification, autorisation et comptabilité (AAA)** pour les utilisateurs.
2. Il utilise le protocole **UDP** pour la communication.
3. Il chiffre uniquement le **mot de passe de l'utilisateur** dans la requête d'authentification.

4. Malware "Cheval de Troie" --deepseek

- **Définition** : Logiciel malveillant **masqué** dans un programme légitime (ex: faux antivirus).
- **Fonctionnement** :
 - Exécute des actions malveillantes après installation (ex: vol de données, backdoor).
 - **Non autorépliquant** (contrairement aux vers).
- **Exemples** : Emotet (cible les banques), Zeus (vol de mots de passe).

4. Décrire le malware « Cheval de Troie » :

Un **Cheval de Troie** est un logiciel malveillant qui se présente comme un programme légitime ou inoffensif pour tromper l'utilisateur. Une fois installé, il permet à un attaquant d'accéder à distance au système infecté.

5. Attaques par déni de service (DoS) --deepseek

Réponses : **a. SYN flooding** et **b. Ping of Death**.

- **SYN Flooding** : Surcharge le serveur avec des demi-connexions TCP.
- **Ping of Death** : Envoi de paquets ICMP surdimensionnés pour crasher la cible.
- *IP/DNS spoofing* : Usurpation d'identité, mais pas de DoS direct.

5. Parmi ces attaques, lesquelles réalisent un déni de service ?

- a. **SYN flooding** : **Oui**
- b. **Ping of Death** : **Oui**
- c. **IP spoofing** : **Non** (usurpation d'identité IP, utilisé pour d'autres types d'attaques)
- d. **DNS spoofing** : **Non** (redirige vers de faux sites)

Réponses correctes : **a, b**

6. Mot-clé `local-case` dans AAA --deepseek

Réponse : **b. Sensible à la casse.**

- **Explication** :
 - `local-case` différencie majuscules/minuscules dans les mots de passe.
 - Ex: Admin \neq admin.
- *Autres options incorrectes* :
 - `aaa new-model` active AAA globalement (option c).
 - Les lignes VTY sont configurées séparément (option a).

6. Qu'est-ce qui est indiqué par l'utilisation du mot-clé local-case dans une séquence de commandes de configuration d'authentification AAA locale ?

Réponse correcte : b. Que les mots de passe et les noms d'utilisateur sont sensibles à la casse (case-sensitive)

Exercice n°1 (8 points) --ChatGPT

Remplis les champs vides (1 point chacun)

1. Dans la sécurité informatique, **l'intégrité** signifie que les systèmes actifs informatiques ne peuvent être modifiés que par les personnes autorisées.
2. **Le ver (worm)** est un programme malveillant indépendant qui ne nécessite aucun autre programme.
3. **Le hacktiviste** est un individu qui commet des crimes et fait des choses sans doute contraires à l'éthique, mais pas pour un gain personnel ou pour causer des dommages.

Exercice n°1 (8 points) –Deepseek

Réponses aux Questions

1. **Intégrité**
Signifie que les systèmes ne peuvent être modifiés que par des personnes autorisées (ex : protection contre les altérations malveillantes).
2. **Ver (Worm)**
Programme malveillant indépendant qui se propage sans besoin d'un hôte (ex : WannaCry).
3. **Grey Hat Hacker**
Individu qui commet des actions contraires à l'éthique sans but lucratif (ex : divulgation de vulnérabilités sans autorisation).
4. **SYN Flood Attack**
Attaque par déni de service exploitant des connexions TCP semi-ouvertes pour saturer le serveur.
5. **Zero-Day Exploit**
Vulnérabilité exploitée avant qu'un correctif ne soit disponible (ex : CVE-2023-1234).

6. **Honeypot**

Système leurre conçu pour attirer et étudier les pirates (ex : serveur fictif avec de fausses données).

7. **Confidentialité**

Garantit que seules les personnes autorisées peuvent accéder aux données (ex : chiffrement AES-256).

8. **Serveur RADIUS/TACACS+**

Utilisé pour l'authentification dans le modèle AAA (ex : Cisco ISE, FreeRADIUS).

Exercice n°2 (6 points)

QCM / Réponses courtes (1 point chacun)

1. **Décrire le principe d'une authentification AAA basée sur un serveur ?**

L'utilisateur envoie ses identifiants au routeur qui les transmet au serveur AAA (comme un ACS). Ce dernier vérifie les informations et retourne une autorisation ou un refus.

2. **Donner un schéma explicatif en expliquant les principaux éléments de ce réseau**

(Résumé en texte si dessin non possible ici)

[Utilisateur] → [Routeur/Client NAS] → [Serveur AAA (RADIUS/TACACS+)]

- L'utilisateur se connecte au réseau.
- Le routeur (NAS) agit comme un relais.
- Le serveur AAA vérifie les identifiants (Authentification), attribue des droits (Autorisation) et consigne les actions (Accounting).

3. **Protocole utilisé entre un routeur 3COM et un serveur ACS**

☞ **RADIUS**

4. **Ce type d'attaque est appelé ...**

☞ **Attaque SYN Flood** (connu pour créer de nombreuses connexions semi-ouvertes)

5. **Décrit une vulnérabilité exploitée avant un patch :**

☞ **Zero-day (ou 0-day)**

6. **Spécifiquement conçu pour leurrer un pirate :**

☞ **Honeypot**

7. **Signifie que les infos ne sont accessibles qu'aux personnes autorisées :**

☞ **Confidentialité**

8. **Serveur appelé pour l'authentification AAA :**

☞ **Serveur ACS** (ou serveur AAA / RADIUS)

Exercice n°2 : Modèle AAA -- Deepseek

1. Principe de l'authentification AAA serveur-based

L'authentification AAA centralisée repose sur :

- **Un serveur dédié** (ex : Cisco ACS, FreeRADIUS) stockant les identifiants.
- **Protocoles** : TACACS+ (pour les admins) ou RADIUS (pour les utilisateurs).
- **Processus** :
 1. L'utilisateur saisit ses credentials.
 2. Le routeur transmet la demande au serveur AAA.
 3. Le serveur valide l'identité et renvoie une réponse (Accept/Reject).

2 . Schéma explicatif

[Client] → (Credentials) → [Routeur 3COM] → (TACACS+/RADIUS) → [Serveur ACS]

↑

(Accès réseau)

↓

[Base de données AAA]

- **Éléments clés :**

- **Client** : Initie la connexion (ex : employé en télétravail).
- **Routeur** : Authentifie via le serveur AAA.
- **Serveur ACS** : Centralise les politiques d'accès.

3. Protocole utilisé : RADIUS

- **Justification** :

- Les routeurs 3COM utilisent généralement **RADIUS** (standard ouvert, compatible multi-fournisseurs).
- RADIUS est optimisé pour la **facturation** (comptabilité détaillée des sessions).
- *Exception* : Si le routeur supporte TACACS+ (peu probable sur 3COM), mais RADIUS reste la norme pour les services facturables.

Exemple de configuration RADIUS sur 3COM

```
bash Copy Download  
radius-server host 192.168.1.100 key MySecretKey  
aaa authentication login default radius
```

3.