Examen de SSI Ch 3-4-5

02/12/2025

Test de compréhension de cours de 15 min valant pour 20% de la note d'UE. Répondez aux questions sur la feuille.

NOM et prénom : _____ /20

1. (2 points) À quoi sert une zone démilitarisée dans un réseau ?

   Solution: À isoler toutes les connexions à l'interface avec internet : ces connexions sont des points d'entrée/sortie fortement exposés à des attaques. La DMZ permet alors d'avoir une ligne de défense supplémentaire en coupure avec internet pour filtrer les connexions, détecter des virus, éventuellement gérer un VPN...

2. (2½ points) Quel est le rôle d'un pare-feu ?
   - √ ◯ **de bloquer des connexions malveillantes.**
   - √ ◯ **de faire du contrôle d'accès réseau.**
   - ◯ √ de garantir la vie privée.
   - √ ◯ **de permettre à deux VLAN du réseau interne de communiquer en réduisant les risques.**
   - √ ◯ **d'être la première ligne de défense par rapport à internet.**

   Vrai Faux

3. (2½ points) Être connecté à un VPN...
   - ◯ √ garantit que je ne peux pas recevoir de virus.
   - √ ◯ **crée un canal sécurisé cryptographique.**
   - √ ◯ **peut servir à accéder à distance au réseau interne de mon entreprise.**
   - ◯ √ garantit un bon niveau de sécurité si ce VPN est basé sur TLS 1.1.
   - √ ◯ **peut se faire avec seulement de la cryptographie symétrique si je fais confiance à la machine à laquelle je me connecte.**

   Vrai Faux

4. (2½ points) Une attaquante qui intercepte ma connexion HTTP/HTTPS...
   - ◯ √ peut introduire un virus dans le paquet si ma connexion est en HTTPS.
   - ◯ √ n'obtient aucune information sur ma connexion HTTPS.
   - √ ◯ **peut usurper mon identité dans la connexion HTTP.**
   - √ ◯ **peut empêcher ma connexion d'arriver à destination.**
   - ◯ √ peut usurper mon identité si HTTPS utilise AES128-GCM avec SHA2.

   Vrai Faux

5. (3 points) Parmi les standards ci-dessous, lesquels permettent de l'intégrité à sécurité acceptable ?
   - √ ◯ **une signature RSA avec une clef de 2048 bits et SHA384.**
   - ◯ √ AES.
   - ◯ √ DES en mode CBC-MAC.
   - √ ◯ **AES en mode GCM.**
   - √ ◯ **SHA256**
   - ◯ √ Diffie-Hellman.

   Vrai Faux

6. (2 points) Pourquoi faut-il protéger le partage d'une clef publique ?
   - √ ◯ **Parce que sinon, un attaquant peut espionner toute la communication réseau en étant indétectable.**
   - ◯ √ Parce que cette clef est secrète.
   - √ ◯ **Parce qu'il faut garantir l'intégrité de cette clef.**
   - √ ◯ **Pour faire fonctionner TLS.**

   Vrai Faux

7. (2½ points) Une fonction de hachage cryptographique est :
   - ◯ √ un cryptosystème à clef secrète.
   - ◯ √ un cryptosystème à clef publique.
   - ◯ √ un cryptosystème qui permet de garantir l'authentification.
   - √ ◯ **nécessaire pour faire une signature électronique.**
   - ◯ √ résistante aux collisions avec moins de 2^n essais, avec n le nombre de bits du haché.

   Vrai Faux

8. (1½ points) Il est possible de prouver que le résultat d'un vote électronique est correct sans révéler qui a voté quoi.
   - √ **Vrai.**
   - ◯ Faux.

9. (1½ points) Pour résister à un ordinateur quantique, il suffit de doubler la taille des clefs cryptographiques.
   - ◯ Vrai.
   - √ **Faux.**