

Contrôle Continu Module Sécurité Informatique L3, **1h20** (Documents et Téléphone non autorisés)

**Exercice 1** (QCM, **11** points)

Pour chacune des questions suivantes, entourez la ou les bonnes réponses.

**Attention** si vous cochez Autre (il s'agira donc de l'unique bonne réponse), vous devriez donner la bonne réponse

**Q1-** Une vulnérabilité

- 1) n'a un réel impact que si un exploit existe (0.5)
- 2) peut toujours être utile même si un correctif de sécurité la concernant existe (0.5)

**Q2-** Une vulnérabilité dont l'existence n'a pas été connue auparavant est appelée

- 4) Aucune des réponses précédentes (1)

**Q3-** L'impact d'une vulnérabilité pour laquelle un exploit existe diminue avec

- 1) le temps (0.5)
- 2) la publication du correctif (0.5)

**Q4-** Le vers Stuxnet a pu s'introduire au réseau informatique de la centrale nucléaire Boushaher via :

- 4) Autre : Clé USB (1)

**Q5-** un logiciel malveillant polymorphe est un logiciel malveillant

- 4) Autre: qui est capable de modifier son code (1)

**Q6-** La base virale désigne

- 1) Autre : une base de données contenant la signature des logiciels malveillants (1)

**Q7-** Une Attaque de type DDoS

- 4) Aucune des réponses précédentes (1)

**Q8-** Un utilisateur reçoit un email avec une pièce jointe (pj) venant d'une personne qu'il connaît (@ email expéditeur), mais l'email lui paraît suspect. La meilleure démarche à suivre est de :

- 2) Téléphoner à l'expéditeur pour s'assurer de l'envoi de la pj (0.5)

**Q9-** Un utilisateur utilise le navigateur Firefox, puis apprend que la version qu'il utilise est affectée d'une nouvelle vulnérabilité pour laquelle un exploit existe mais le correctif n'est pas encore disponible. La meilleure démarche à suivre dans cette situation est de :

- 1) Changer de navigateur le temps que le correctif soit disponible (1)

**Q10-** Un logiciel malveillant dont l'unique tâche est d'enregistrer les frappes claviers est connu sous le nom

- 4) Autre : key logger (enregistreur de frappes) (1)

**Q11-** Depuis Internet, lorsqu'un attaquant réussit à contourner les mécanismes d'authentification et à interroger directement la base de données par écriture de commandes spécifiques, on parle de :

- 4) Autre : attaque de type injection SQL (1)

**Q12-** Une Attaque de type élévation de privilèges désigne le moyen par lequel un attaquant arrive à

- 1) Aucune des réponses précédentes (0.5)

## Exercice 2 (3 pts)

Pour chaque question, donnez une réponse (un petit paragraphe)

- Pourquoi est-il recommandé de se connecter à sa machine avec un compte à moindre privilèges (ex. session invité sous Linux) ?

**R :** Car ainsi un attaquant (utilisateur, logiciel malveillant, etc.) aura des droits restreints et non pas administrateur, ne lui permettant pas de mener au bout son attaque (installation de logiciels, ouverture de connexion, modification de paramètres, etc.) (1)

- Pourquoi est-il déconseillé de se connecter à son compte email, facebook, etc., depuis une machine sur laquelle on n'a pas un contrôle (ex : cyber-café, PC d'un ami, etc.)

**R :** Car on risque de se faire voler des informations confidentiels (mot de passes, emails, etc.) vu qu'on ne peut pas savoir si la machine en question n'est pas infecté par un logiciel malveillant, qui peut être même installé par le propriétaire de la machine afin d'espionner les autres utilisateurs (1)

- Pourquoi une fonction de hachage seule ne protège pas l'intégrité des données contre un attaquant ?

**R :** car un attaquant est en mesure de modifier les données puis recalculer le nouveau hash sur les données modifiées, ainsi le récepteur des données n'est pas en mesure de détecter la modification illicite (1)

## Exercice 3 (3 points)

Votre machine dispose d'un fichier système nommé trace.log qui contient les événements suivants :

- Historique des ouvertures/fermetures de sessions sur la machine (identifiant utilisateur, heure, @IP si ouverture distante)
- Les logiciels installés/désinstallés ainsi que les mises à jour logiciels
- Historique des connexions réseaux entrantes/sortantes de la machine

Un logiciel malveillant infectant votre machine, a apporté des modifications à ce fichier (suppression/modification).

**Q1)** selon vous quel(s) besoin(s) en sécurité a (ont) été affecté ?

**R :** Les besoins d'intégrité et Preuve (Traçabilité). (0.5 + 0.5)

Dans quel but a été modifié le fichier ?

**R :** Cacher la présence d'une activité malveillante (logiciel malveillant, compte caché, attaquant se connectant à distance à la machine, ou depuis la machine) (1)

On suppose maintenant que ce fichier est protégé en intégrité, où toute modification illicite est détectée par le système et par l'administrateur de la machine

**Q2)** En quoi ce fichier pourrait être utile à l'administrateur de la machine (Expliquez) ?

**R :** Il sert à détecter la présence d'une activité malveillante sur la machine. Si l'intégrité du fichier est préservée, toute action malveillante sera enregistrée dans trace.log. Si l'intégrité du fichier n'est pas préservé (le fichier est illicitement modifié), ceci peut aussi alerter sur l'existence d'une activité malveillante sur la machine (1)

#### Exercice 4 (3 points)

On s'intéresse à l'étude de l'interface utilisée par la BNA (Banque Nationale d'Algérie, Figure 1) et permettant à un client de la banque de gérer son compte à distance en se connectant au lien <https://ebanking.bna.dz/ptcl/fr/idehom.html>

https://ebanking.bna.dz/ptcl/fr/idehom.html

**IDENTIFICATION**

Accéder à vos comptes

1. Entrez votre Identifiant :

2. Tapez votre mot de passe :  X effacer

3. Valider en cliquant sur le bouton ci-dessous

Valider

**Nota**

Après avoir e-Banking, vous serez redirigé vers le serveur BNA e-Banking.

Le cas échéant, le filtrage des données sera effectué.

Figure 1 Interface de connexion à la gestion de compte en ligne BNA

**Q1)** Quelle est l'utilité du mot de passe ?

**R :** permet d'authentifier l'utilisateur (possédant l'identifiant) à la BNA (service de gestion de compte BNA) (0.5)

**Q2)** Quelles sont les indications permettant au client d'avoir une assurance qu'il est connecté au bon site ?

**R :** existence d'une connexion sécurisée (https ou le cadenas fermé), ainsi que le nom de domaine sur la barre de saisie url identique au nom domaine tapé (1)

**Q3)** Selon vous, pourquoi la BNA a opté pour la saisie du mot de passe via un clavier virtuel, alors que la saisie de l'identifiant se fait via le clavier du PC (Justifiez) ?

**R :** pour se protéger contre des logiciels malveillants de type keylogger. En effet, en utilisant le clavier virtuel, le mot de passe saisi par l'utilisateur ne peut pas être capté/enregistré, alors que l'identifiant lui peut l'être. Ainsi, un attaquant ne peut pas voler le mot de passe du client et se connecter à sa place (1.5)

**Question Bonus (1 pt)** Le clavier virtuel contient des cases vides, et l'agencement des chiffres sur la grille change d'une connexion à l'autre, Pourquoi (Justifiez) ?

**R :** Certes un attaquant ne peut pas enregistrer directement le mot de passe saisi via le clavier virtuel, mais il peut être en mesure de capter les coordonnées (X,Y) d'un clic souris (souvenez-vous de l'implémentation de l'interface Mouselistener). Si la position des chiffres ne change pas un attaquant peut trouver la correspondance coordonnées-clic souris chiffre tapé. En changeant aléatoirement l'emplacement des chiffres (peut-être de type Bouton) un attaquant ne peut pas trouver la correspondance coordonnées-clic souris chiffre tapé