Contrôle : Promouvoir les bonnes pratiques

**Dans votre lycée, quotidiennement, les étudiants utilisent des ressources du réseau informatique de l'établissement. Votre enseignant en BTS SIO, souhaite rédiger un guide de bonnes pratiques, afin d'encadrer les usages des étudiants et, ainsi, les responsabiliser.**

**Principes de l’authentification**

1. En vous appuyant sur les informations données par l’ANSSI, indiquez les spécifications qui doivent être mentionnées dans le guide au sujet de la création des mots de passe utilisés par les étudiants pour leurs connexions au réseau local.
2. Précisez les recommandations à suivre pour la gestion de ces mots de passe durant les deux années du BTS.

1. Expliquez les deux méthodes utilisées pour définir un mot de passe par passphrase (passe de phrase ou phrase secrète).

Les utilisateurs seront souvent amenés à utiliser des identifiants de connexion sur des navigateurs Internet ou des logiciels spécifiques lors de leurs différents travaux.

1. Indiquez quelles manipulations ne sont pas souhaitables, et expliquez pourquoi.

**En vous aidant de vos connaissances sur les sites gouvernementaux**

1. Les attaques directes permettent de récupérer les identifiants et mot de passe d’un utilisateur pour se connecter à sa place.
2. Citer une exemple d'attaques directes
3. Quelles mesures complémentaires vous semblent efficaces pour renforcer l’authentification par mot de passe ? (Plusieurs réponses possibles)

* Question secrète du type « Quel est le nom de jeune fille de votre mère ? »
* SMS : envoi d’un SMS avec un code de confirmation
* Notification de connexion par courriel
* Saisie de votre date de naissance à chaque connexion

1. Citer une exemple d'attaques indirectes
2. L'authentification consiste à apporter :

* **la preuve de son identité**
* des droits d’accès
* des habilitations

1. Quels sont les facteurs de d’authentification

* Facteur de possession
* Facteur d’habilitation
* Facteur d’authentification
* Facteur de connaissance
* Facteur biométrique

1. **Associez chaque moyen à son facteur d’authentification**

|  |  |  |  |
| --- | --- | --- | --- |
| 1 | Mot de passe | 1 | Facteur de possession |
| 2 | clé | 2 | Facteur de connaissance |
| 3 | Empreinte digitale | 3 | Caractéristique biométrique |

1. En Belgique, certains employés ont accepté de se faire implanter des puces sous la peau.

Est-ce possible en France ? (vous argumenterez votre réponse)

1. **Quels sont les solutions pour gérer ses multiples mots de passe**

**Authentification et habilitation**

1. **Définir le principe de l’authentification**
2. **Définir le principe de l’habilitation**
3. **Associez les éléments suivants**

|  |  |  |  |
| --- | --- | --- | --- |
| 1 | Comptes locaux Linux | 1 | Annuaire LDAP |
| 2 | Comptes itinérants Windows | 2 | Base SAM |
| 3 | Comptes locaux Windows | 3 | Fichier passwd |
| 4 | Mots de passe Linux |  | Fichier shadow |

**Attribution de privilèges : grands principes**

1. **« Moindre privilège consiste à »**

* n’attribuer aux utilisateurs que les droits dont ils ont besoin pour effectuer les taches
* donner accès aux disques et aux applications
* donner accès seulement aux données nécessaires aux utilisateurs

1. **« Besoin d’en connaitre consiste à »**

* donner les accès et les privilèges appropriés aux utilisateurs
* donner accès aux disques et aux applications
* n’attribuer aux utilisateurs que les droits dont ils ont besoin pour effectuer les taches
* attribuer les comptes aux utilisateurs de manière nominative

1. **Quelle est la différence entre « partage » et « sécurité » lorsque vous accéder aux propriétés d’un dossier sur Windows.**

**Sensibilisation des utilisateurs**

1. **Quels conseils donneriez-vous aux utilisateurs pour éviter le piratage de ces données personnelles »**
   * **Sur la boite mail :**

* Se tenir informé de l’actualité liée à la sécurité
* Faire attention aux pièces jointes (même pour les expéditeurs connus)
* Déconnecter son poste lors qu’il n’est pas utilisé
* Désactiver l’exécution des liens hypertextes et l’affichage des images dans les mails
  + **Sur le navigateur :**
* Dans la mesure du possible, naviguer toujours en « https » (protocole SSL/TLS)
* Effacer régulièrement l’historique de navigation, les fichiers temporaires, les cookies votre navigateur Web
* Traiter le spam
* Limiter les informations que vous partagez par les réseaux sociaux ou mail