Aubrée Romain **Beauvallet**
22/01/2026
SLAM

Groupe 1

Bloc 3 CH 4 TH 3 TD 3

Contexte 2
Exercice 1.1 2
Exercice 1.2 2
Exercice 1.3 2
Exercice 1.4 2
Exercice 1.5 2
Exercice 2.1 3
Exercice 2.2 3
Exercice 2.3 3
Exercice 2.4 3
Exercice 2.5 4
Exercice 2.6 4
Exercice 3.1-4 5

Contexte

Sécurisation des équipements et des usages des utilisateurs.

Exercice 1.1

Il faudrait un serveur proxy (ou un pare-feu disposant de fonctionnalités de filtrage d'URL/applicatif)

Exercice 1.2

Le demande de requête est envoyée à l'outil qui est entre le LAN et le WAN, elle est comparée ensuite avec une base de données pour voir si elle est blacklisté, puis selon le résultat, la requête est bloquée ou non.

Exercice 1.3

Windows update va regarder régulièrement et installer les dernière mise à jour Windows, ça fréquence de scan et l'installation automatique des mise a jours peuvent être configuré.

Exercice 1.4

Les mises à jour ont pour but de fixer les failles de sécurité, c'est pour cette raison qu'il est déconseillé d'utiliser d'OS trop anciens.

Exercice 1.5

Il serait judicieux d'installer un antivirus pour empêcher les utilisateurs de télécharger des virus sur les nom qui n'ont pas été blacklisté par le proxy.

Exercice 2.1

Les mots de passes doivent être construit comme ceci :

- Pas de mot entier existant
- Avoir des chiffres
- Avoir des lettres
- Mélanger le minuscule et majuscule
- Avoir des symbole spéciaux
- Ne pas y inclure d'information personnel (date de naissance etc)
- Doivent être suffisamment long (8 caractère strict minimum)

Exercice 2.2

Pour bien gérés ces mot de passe il faut :

- Ne pas utiliser les mêmes mot de passe entre chaque site/appareil
- Les changer en cas de suspicion
- Ne pas les communiquer ou les partager
- Ne pas les écrires sur un post-it ou autre forme physique

Exercice 2.3

Utiliser une phrase, citation ou chanson, puis le crypter, avec des chiffres, n'utiliser que les premières lettres, etc… Ou, utiliser la phonétique du mot (**J'ai acheter du pain -> GHchTdP1**) Le but est de pouvoir retenir de long mot de passe avec des momento technique personnel.

Exercice 2.4

Il faut bien penser à se déconnecter une fois la session terminée, et de ne pas enregistrer les mot de passe sinon d'autres utilisateurs qui suivront notre place pourront utiliser nos comptes…

Exercice 2.5

Les options ont pour but de :

- Afficher l'historique des mot de passes au cas ou
- Afficher la durée de vie max d'un mot de passe
- Afficher la durée minimum
- Enregistré les mot de passe avec un chiffrement
- Montre si le mot de passe respecte les règles de complexité (**1.2**)
- Affiche la longueur minimum d'un mot de passe

Exercice 2.6

(J'aime les pommes de terre et William Saurin -> **JmléP0m2Ta1réOu1lamS0r1**).

Exercice 3.1-4

Avantage	Inconvénients
Sécurité : Chiffrement fort et stockage local (le fichier reste chez nous, pas sur un cloud tiers)	Risque de perte : Si on perd le mot de passe principale, impossible de récupérer les accès (pas de "mot de passe oublié")
Gratuit et Open Source : Pas de coût, code vérifiable et transparent	Pas de synchro automatique : C'est à nous de déplacer le fichier de base de données si on veut l'utiliser sur plusieurs appareils
Portabilité : Peut s'installer sur une clé USB (version portable) pour l'utiliser où on veut	Interface : Complexe et moins facile à prendre en main que les outils payants

Conclusion

Initialisation à la gestion de mot de passe et les manières de les sécuriser.