

TP5 B3 Synthèse

Florentin Bracq- -Flabat, BTS SIO 1

Cybercafé

A white, torn-paper-like horizontal band runs across the bottom of the image, separating the dark background from the bottom edge. The band has a jagged, irregular top edge, suggesting it was torn from a sheet of paper. The background above the band is a solid, dark color.

Configurer dans le réseau local un pare feu pour filtrer les connexions internet

- Un pare feu peut protéger les machines connectées dans le réseau local en filtrant les requêtes entrantes et sortantes, il pourra par la même occasion bloquer l'accès à certains sites web.



Comment un pare feu autorise-t-il les connexions ou non à un site spécifique ?

- Un pare feu analyse les connexions entrantes et sortantes sur le réseau et bloque les connexions qui ne sont pas autorisées, qui peuvent être dans une liste prédéfinie



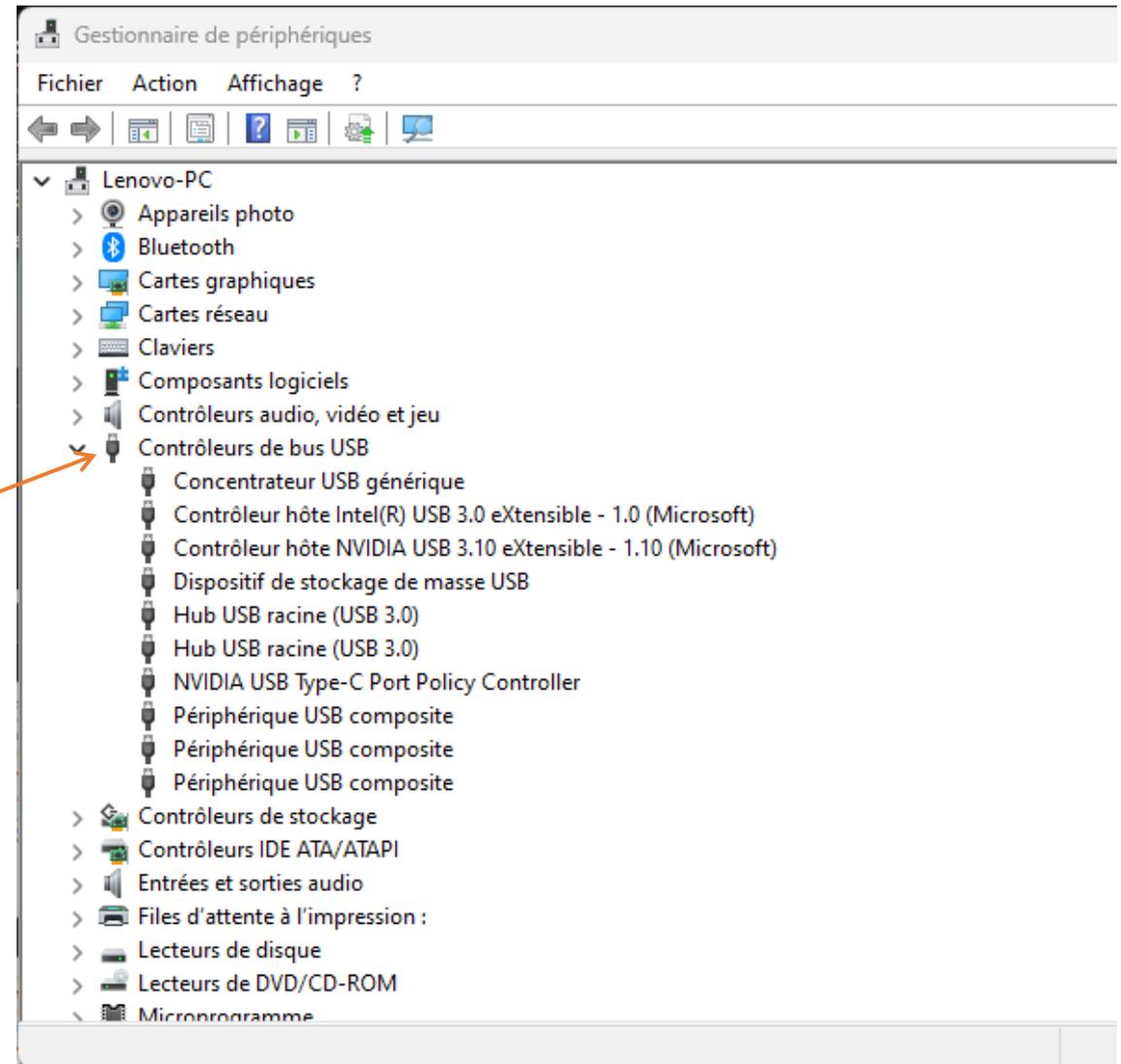


Blocage des sites de téléchargements illégaux

- Il existe une multitude de sites de téléchargements illégaux, il est donc plus simple de bloquer cette catégorie de sites, plutôt que de bloquer les sites un par un

Blocage des ports USB

- Afin de limiter le risque d'infection d'un système, il peut être possible de bloquer les ports USB d'un poste via le gestionnaire de périphériques en désactivant les périphériques USB



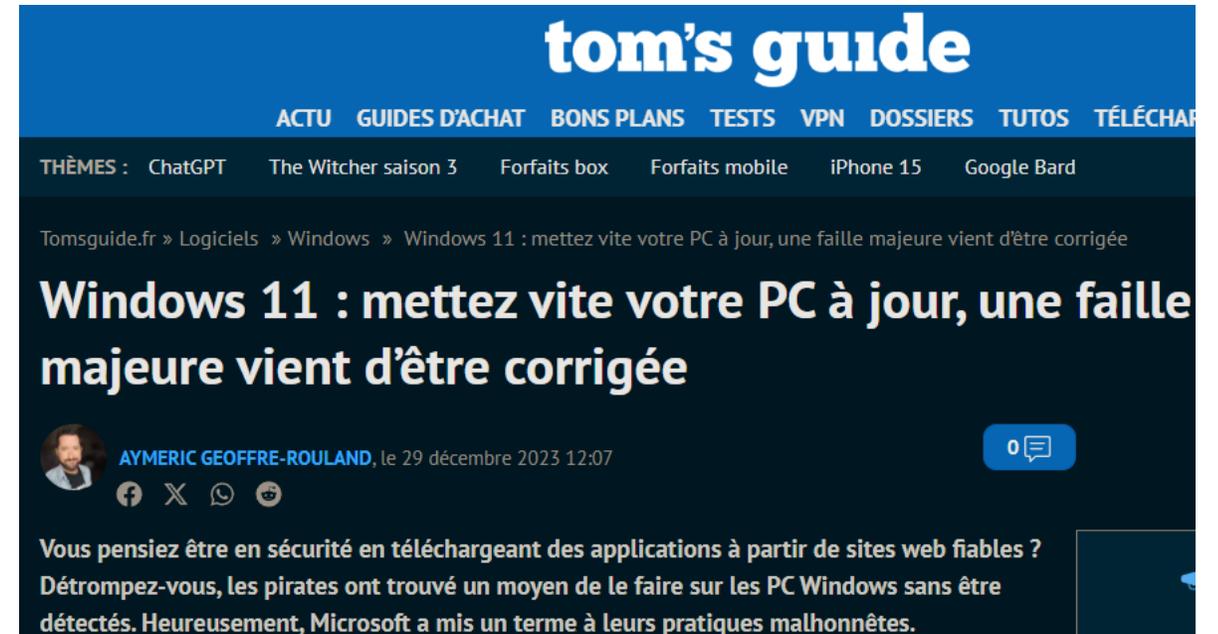
Faire les mises à jour avec Windows Update

- Pour garantir une sécurité minimale, une meilleure stabilité et une correction de bug, il est conseillé de faire les mises à jour de Windows, pour conserver un système à jour



Correction de failles de sécurité avec Windows Update

- Exemple avec un article du 29/12/2023 de tom's guide



Installation d'un antivirus

- Pour contrôler les ports USB d'un poste il peut être possible d'installer un antivirus pour analyser par exemple le contenu d'une clé USB et supprimer ou mettre en quarantaine les éventuelles menaces





Lycée

Création d'un mot de passe et recommandations

- Pour créer un mot de passe il faut qu'il soit composé de différents types de caractères :
- Majuscules
- Minuscules
- Caractères spéciaux (ex : #€\$*@)
- Chiffres
- La longueur du mot de passe conseillé est de 12 caractères, elle devrait passer bientôt à 16 caractères



Définir un mot de passe par passphrase

- Il est possible de définir un mot de passe par passphrase en utilisant une suite de mots (Ex : Ch€v@lp@tur€chi€n\$0uri\$)
- Il est également possible de définir un mot de passe par passphrase en utilisant une phrase qui a un réel sens (Ex : J€\$ui\$€tudi@nt€nbt\$\$i0)

Utiliser un mot de passe différent à chaque compte

- Il est très fortement déconseillé d'utiliser le même mot de passe pour chaque compte en ligne, si par exemple un pirate arrivait à accéder à l'un de vos comptes, il pourrait tester sur différents sites pour essayer de récupérer différents comptes

Le rôle des différentes stratégies de sécurité



Conserver l'historique des mots de passe : aucun mot de passe mémorisé



Durée de vie maximale du mot de passe : 42 jours



Durée de vie minimale du mot de passe : 0 jours



Enregistrer les mots de passe en utilisant un chiffrement : Désactivé

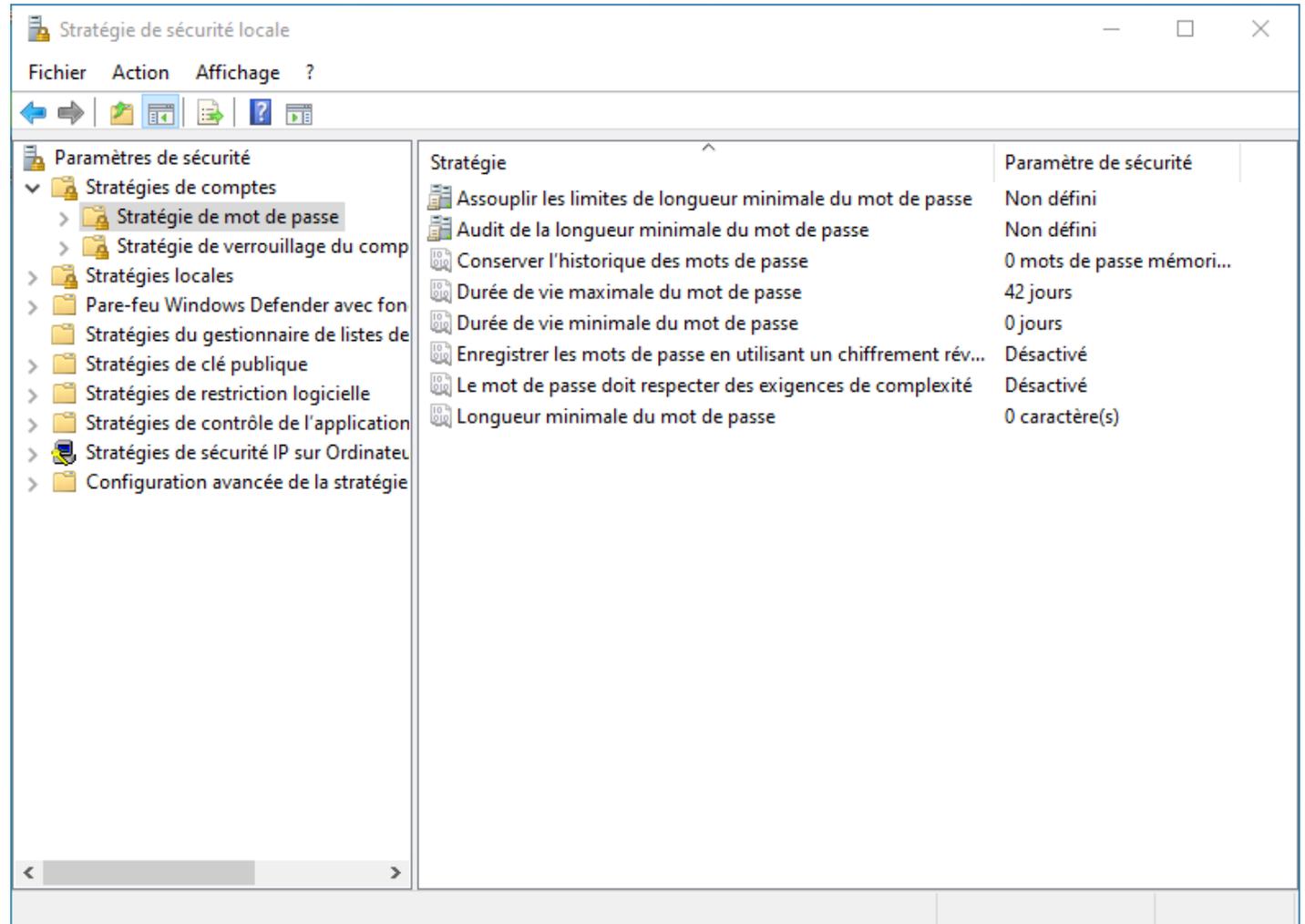


Le mot de passe doit respecter des exigences de complexité : Désactivé



Longueur minimale du mot de passe : 0 caractère(s)

Application de la stratégie sur une VM Windows 10



Gestion des mots de passe

Avantages et Inconvénients de KeePass

| Avantages | Inconvénients |
|---|---|
| Simple à utiliser | Perte des mots de passe si oubli du mot de passe principal |
| Un seul mot de passe à retenir | Risque de divulgation des mots de passe, si le fichier de base de données est perdu |
| Mots de passe différents et complexes à chaque compte | Le coffre-fort de mot de passe n'est pas accessible à tout moment |