Parcours : DISCOVERY

Module : Naviguer en toute sécurité

Projet 1 - Un peu plus de sécurité, on n'en a jamais assez !

1/ Fonctionnalité de sécurité de votre navigateur

Objectif : identifier les éléments à observer pour naviguer sur le web en toute sécurité

1/ **Identifie les adresses internet qui te semblent provenir de sites web malveillants.**

Article 1 = ANSSI - Dix règles de base

Article 2 = Economie.gouv - Comment assurer votre sécurité numérique

Article 3 = Site W - Naviguez en toute sécurité sur Internet

Article bonus = wikiHow - Comment surfez en sécurité sur internet

3. Fonctionnalité de sécurité de votre navigateur

Objectif : identifier les éléments à observer pour naviguer sur le web en toute sécurité

1/ Identifie les adresses internet qui te semblent provenir de sites web malveillants.

Les sites web qui semblent être malveillants sont :

● www.morvel.com, un dérivé de www.marvel.com, le site web officiel de l'univers Marvel

● www.fessebook.com, un dérivé de www.facebook.com, le plus grand réseau social du monde

● www.instagam.com, un dérivé de www.instagram.com, un autre réseau social très utilisé

Les seuls sites qui semblaient être cohérents sont donc :

● www.dccomics.com, le site officiel de l'univers DC Comics

● www.ironman.com, le site officiel d’une compétition internationale de triathlon (et non du super-héros issu de l’univers Marvel)

9 - Que faire si votre ordinateur est infecté par un virus

Objectif :

1/ Proposer un ou plusieurs exercice(s) pour vérifier la sécurité en fonction de l’appareil utilisé ??????? Comment faire ???????

Pour vérifier la sécurité en fonction de l'appareil utilisé, vous pouvez mettre en place différents exercices et tests adaptés à chaque type d'appareil. Voici quelques suggestions :

1. Exercices pour les ordinateurs :
    - Testez la robustesse des mots de passe en lançant une attaque par force brute sur un compte utilisateur fictif.
    - Simulez une tentative de phishing en envoyant un e-mail contenant un lien suspect à des utilisateurs et observez combien d'entre eux tombent dans le piège.
    - Effectuez une analyse de vulnérabilités en utilisant des outils comme Nessus ou OpenVAS pour identifier les failles de sécurité potentielles sur les machines.
2. Exercices pour les smartphones :
    - Testez la réaction des utilisateurs face à des demandes d'autorisation suspectes en simulant des applications malveillantes.
    - Vérifiez la sécurité des connexions Wi-Fi en utilisant des outils comme Wireshark pour détecter les tentatives d'interception de données.
    - Testez la résistance des dispositifs aux attaques de force brute en tentant de contourner les verrouillages d'écran.
3. Exercices pour les appareils IoT (Internet des objets) :
    - Testez la sécurité des dispositifs en les exposant à des attaques par déni de service (DDoS) pour évaluer leur capacité à résister à ces types d'attaques.
    - Analysez le trafic réseau généré par les appareils IoT pour détecter toute activité suspecte ou non autorisée.
    - Vérifiez la robustesse des mécanismes d'authentification en tentant d'accéder aux appareils avec des identifiants incorrects ou falsifiés.
4. Exercices pour les systèmes embarqués :

- Testez la sécurité physique des dispositifs en essayant de les ouvrir ou de les manipuler pour accéder à des données sensibles.
- Évaluez la résistance des systèmes embarqués aux attaques par injection de code en tentant d'exécuter du code malveillant à distance.
- Vérifiez la sécurité des protocoles de communication utilisés par les systèmes embarqués en analysant le trafic réseau pour détecter d'éventuelles vulnérabilités.

9. proposer un exercice pour installer et utiliser un antivirus + antimalware en fonction de l'appareil utilisé.

Voici un exercice pour installer et utiliser un logiciel antivirus et antimalware en fonction de l'appareil utilisé :

Objectif de l'exercice :

Installer et configurer un logiciel antivirus et antimalware sur un appareil spécifique, puis effectuer une analyse de sécurité pour détecter et supprimer les menaces potentielles.

Matériel nécessaire :

- Un ordinateur (Windows, MacOS, Linux)
- Un smartphone (Android, iOS)
- Un appareil IoT ou un système embarqué (selon disponibilité)

Étapes de l'exercice :

1. Préparation :
    - Sélectionnez un logiciel antivirus et antimalware approprié pour l'appareil que vous utilisez. Assurez-vous de choisir un logiciel réputé et bien évalué.
2. Installation :
    - Sur l'ordinateur : Téléchargez et installez le logiciel antivirus/antimalware en suivant les instructions du fabricant.
    - Sur le smartphone : Accédez à la boutique d'applications (Google Play Store pour Android, App Store pour iOS) et installez le logiciel antivirus/antimalware.

- Sur l'appareil IoT ou le système embarqué : Si applicable, téléchargez et installez le logiciel recommandé par le fabricant ou le fournisseur.

3. Configuration :
    - Sur tous les appareils : Configurez le logiciel pour qu'il effectue des analyses régulières et mettez à jour les définitions de virus.
    - Sur l'ordinateur : Personnalisez les paramètres selon les besoins spécifiques de l'utilisateur, tels que les horaires d'analyse et les actions à prendre en cas de détection de menaces.
    - Sur le smartphone : Activez les fonctionnalités de sécurité supplémentaires telles que le blocage d'appels indésirables ou la protection contre le vol d'identité.
    - Sur l'appareil IoT ou le système embarqué : Suivez les instructions du fabricant pour configurer les paramètres de sécurité recommandés.
4. Analyse de sécurité :
    - Lancez une analyse complète du système à l'aide du logiciel antivirus/antimalware.
    - Surveillez attentivement les résultats de l'analyse pour identifier les éventuelles menaces détectées.
5. Actions correctives :
    - Sur la base des résultats de l'analyse, suivez les instructions du logiciel pour supprimer ou mettre en quarantaine les menaces détectées.
    - Effectuez les mises à jour nécessaires pour garantir la sécurité continue de l'appareil.
6. Évaluation :
    - Réfléchissez à l'efficacité du logiciel antivirus/antimalware dans la détection et la suppression des menaces.
    - Identifiez les éventuelles améliorations à apporter à la configuration ou au choix du logiciel.