SENSIBILISATION. FORMATION. EXPÉRIMENTATION.

JOURNÉE CYBERSÉCURITÉ 0X02

PLAN

- Introduction à la cybersécurité
- Atelier

INTRODUCTION À LA CYBERSÉCURITÉ

LA CYBERSÉCURITÉ

- La sécurité informatique, ou cybersécurité, représente l'ensemble des mécanismes mis en place visant à empêcher l'utilisation détournée d'un système ou de ses données.
- Plusieurs facteurs sont impliqués
  - Individus
  - Logiciels
  - Matériel
  - Télécommunications
- **La robustesse d'un système est définie par son maillon le plus faible!**

...🤔


DoorCode: 63526
DoorCode: 63526

ATTRIBUTS DE LA CYBERSÉCURITÉ

https://www.researchgate.net/profile/Ali_Aldallal2/post/What_is_information_security/attachment/59d640f979197b807799d189/AS%3A433099327709184%401480270334665/download/opentext-graphic-for-web-information-security-en.jpg

RESPONSABILITÉS D'UN DÉVELOPPEUR

- Les développeurs ont un rôle primordial à jouer dans la mise en oeuvre de la sécurité logicielle
- Le code effectue divers traitements sur les données et peut constituer la porte d'entrée vers une utilisation non autorisée
- Le principe de **programmation défensive** permet de corriger les failles potentielles au fur et à mesure de la rédaction du code
- Ainsi, connaître les techniques de contournement devient un atout pour mieux se sécuriser:
  Hacker Mindset → Penser en dehors de la boîte et ne rien prendre pour acquis.
- **Être conscient des enjeux inhérents à la sécurité vous rend plus complet**

CTF

- *Capture the Flag:* https://youtu.be/8ev9ZX9J45A
- Jeu d'habileté qui simule un environnement présentant des vulnérabilités pouvant être exploitées par les participants
- Il existe différents types d'épreuves demandant des aptitudes variées
  - Rétro-ingénierie
  - Analyse du trafic réseau
  - Programmation
  - Logique applicative
  - Encryption
  - Attaque/Défense
  - Électronique
- Une fois un défi résolu, un *flag* est remis et doit être validé pour obtenir des points

MÉTHODOLOGIE

- **Reconnaissance**
  Identifier la cible, les adresses IP, les noms de domaines

- **Récolte d'information**
  Ports utilisés, librairies, frameworks
  Explorer le contenu des répertoires standards, des identifiants par défaut

- **Exploitation**
  À partir des informations recueillies, manipuler le système pour obtenir les données/accès privilégiés

CONSIDÉRATIONS LÉGALES

ATTENTION

Réservez vos séances d'exploration de vulnérabilités pour un contexte autorisé.

Vous ne pouvez pas exploiter une application web, un réseau, ou tout autre système, sans avoir le consentement explicite de son propriétaire.

BUG BOUNTY

- Mécanisme permettant de dévoiler de façon responsable la présence de failles dans un système. Le chercheur de vulnérabilités peut même être rémunéré pour ses trouvailles.
- Certaines entreprises proposent leurs propres programmes de *Bug Bounty*(Facebook, Google, etc.)
- Il existe également des plateformes qui servent d'intermédiaire entre les entreprises et les chercheurs de vulnérabilités

bugcrowd

hackerone

RESSOURCES

- https://www.hacksplaining.com/lessons
- https://www.hacker101.com/
- Classé par catégories: https://www.peerlyst.com/posts/how-to-create-an-open-education-degree-in-cybersecurity-free-gabrielleb

- Consommer l'information de façon passive ne suffit pas, pour intégrer les concepts, il faut passer à l'action par la pratique!
- https://ctf.hacker101.com/
- https://ringzer0ctf.com/
- https://www.vulnhub.com/

- **Répertoire ShawiSec:** https://ressources.shawisec.ca/

QUESTIONS? 

ATELIER

CTF

MINI-CTF OWASP DU HACKFEST 2018

- Validation des *flags*
  0x02.shawisec.ca
- Canal de discussion Discord
  https://discord.gg/CPV6Yn2
- Démarche de résolution
  https://ressources.shawisec.ca/writeups/01-02-2019-journee-cybersecurite-0x02/
- Vous en voulez plus?
  https://ctf.hacker101.com/

ATELIER

RÉCAPITULATIF

- Reconnaissance → Récolte → Exploitation
- Un CTF est un *jeu* dans un contexte particulier.
- Le but est d'**apprendre en s'amusant,** on peut manipuler les outils pour en découvrir le fonctionnement, mais une situation réelle de recherche de vulnérabilités demande beaucoup de réflexion car **le chemin est rarement aussi bien tracé**...

MERCI! ✌️