SENSIBILISATION. FORMATION. EXPÉRIMENTATION.

JOURNÉE CYBERSÉCURITÉ

PLAN

- Introduction à la cybersécurité
- Atelier
- CTF

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 acteurs sont impliqués
  - Individus
  - Logiciel
  - Matériel
  - Télécommunications
- **La robustesse d'un système est définie par son maillon le plus faible!**

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

- En tant que développeur, vous avez un rôle primordial à jouer dans la mise en oeuvre de la sécurité dans les applications
- Votre code effectue divers traitements sur les données et peut constituer la porte d'entrée vers une utilisation non-autorisée
- Vous devez exploiter le principe de **programmation défensive** pour 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*
- **Être conscient des enjeux inhérents à la sécurité vous rends 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
- Un fois un défi résolu, un *flag* est remis et doit être validé pour obtenir des points

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 programme de *Bug Bounty*(Facebook, Google, etc.)
- Il existe également des plateformes qui servent d'intermédiaire entre les entreprises et les chercheurs de vulnérabilités

bugcrowd

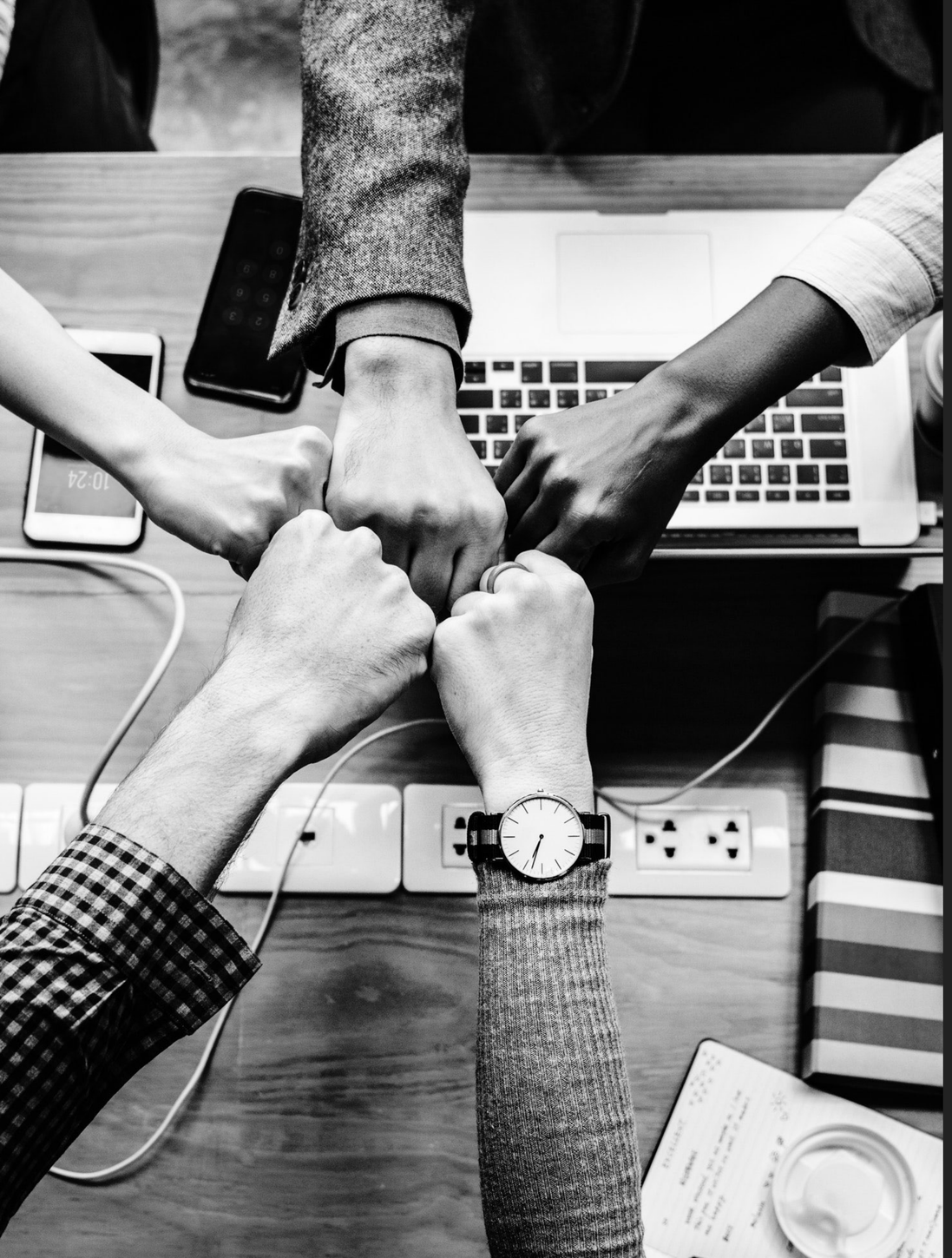
hackerone

RESSOURCES

- https://www.hacksplaining.com/lessons
- https://www.hacker101.com/
- https://www.owasp.org/index.php/Main_Page
- https://www.peerlyst.com/posts/how-to-create-a-degree-in-cybersecurity-and-open-source-free-gabrielleb

- https://leanpub.com/web-hacking-101
- https://leanpub.com/ltr101-breaking-into-infosec
- https://www.amazon.ca/Web-Application-Hackers-Handbook-Exploiting/dp/1118026470
- https://www.packtpub.com/networking-and-servers/mastering-modern-web-penetration-testing
- https://www.amazon.ca/Penetration-Testing-Hands-Introduction-Hacking/dp/1593275641/

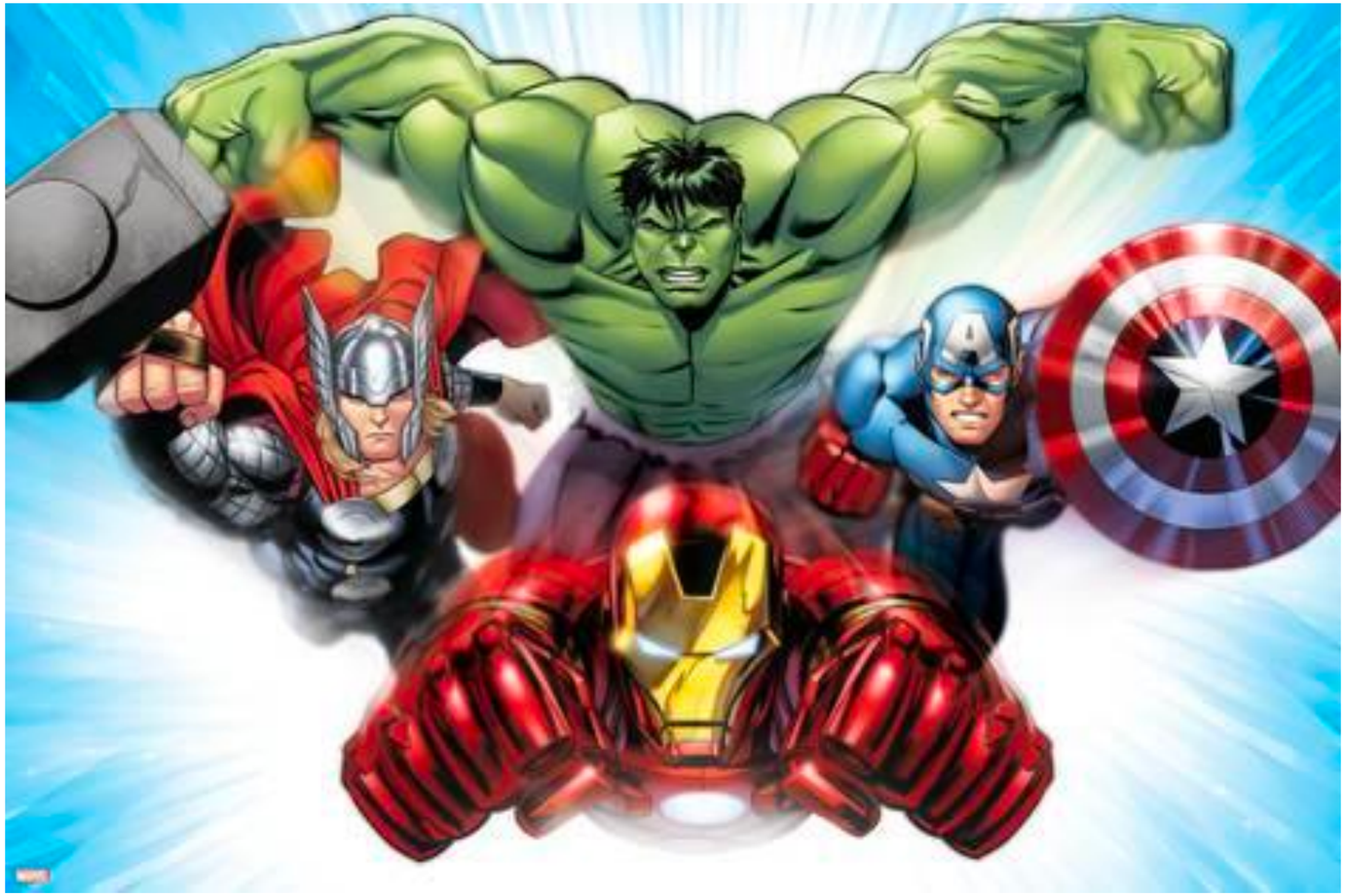
QUESTIONS? 



ATELIER

ATELIER

- Dirigé
- Collaboratif
- Interactif
- Appliqué



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 privilégiées

DEFENCE SPACE

- Fichiers
  ftp://fichiers.local.shawinigan.info/
- https://download.vulnhub.com/defencectf2017/DEFENCESPACECTF-2017.ova
- VirtualBox
  https://www.virtualbox.org/wiki/Downloads
- Validation des *flags*
  http://ctflocal.shawinigan.info/

VIRTUAL BOX

- https://www.virtualbox.org/
- Outil de virtualisation *open source*
- Permets de créer des **machines virtuelles**
  - La simulation d'un ordinateur complet à partir d'un autre ordinateur
  - Sécurité grâce à un environnement isolé
  - Plusieurs environnements sur une même machine physique
  - Gestion des environnements simplifiée, un clone d'une VM est simple à restaurer en cas de problème

KALI LINUX

- https://www.kali.org/
- Distribution Linux basée sur Debian regroupant un ensemble d'outils(*600*+) utiles en test de vulnérabilité et sécurité informatique

NMAP

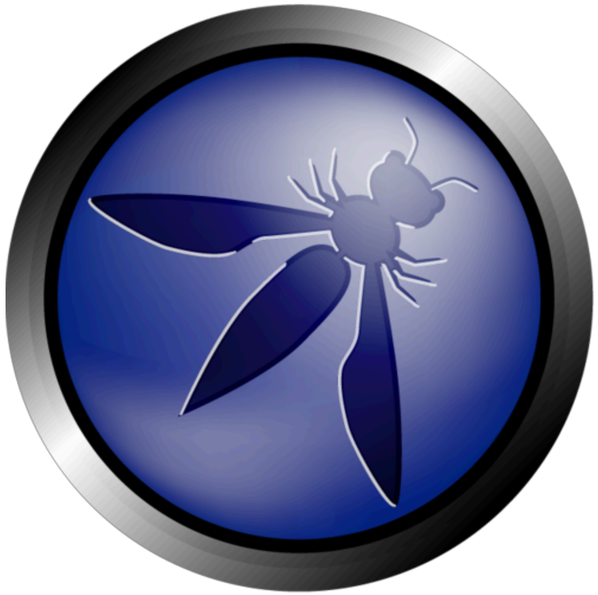
- https://nmap.org/
- *Network Mapper* analyse les hôtes présents sur un réseau et les services qu'ils exposent
  - Qui est présent sur le réseau?
  - Quels sont les ports ouverts? Par quels services?
- https://bencane.com/2013/02/25/10-nmap-commands-every-sysadmin-should-know/

OUTILS DE CONVERSION

- Base64: Encodage des données au format ASCII
  http://www.utilities-online.info/base64/
  - **Attention** Encodage != Encryption
- HEX: Représentation hexadécimale des caractères
  https://cryptii.com/pipes/hex-to-text
- MD5: Méthode de **hachage**
  https://www.md5online.org/
  - **Attention** Le hachage est unidirectionnel

DIRBUSTER

- https://www.owasp.org/index.php/Category:OWASP_DirBuster_Project
- Découverte des applications web utilisées par un serveur web par force brute
- **OWASP**: Votre nouveau meilleur ami 🤯
  https://www.owasp.org



SSLSCAN

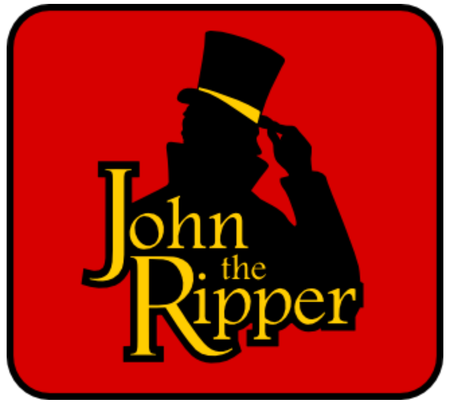
- https://github.com/rbsec/sslscan
- Expose les données des certificats SSL et les méthodes d'encryptions supportées

NETCAT

- http://netcat.sourceforge.net/
- Couteau suisse de la réseautique, il permets d'établir une communication TCP ou UPD autant en lecture qu'en écriture sur n'importe quel port.

JOHN THE RIPPER

- https://www.openwall.com/john/
- Utilitaire de résolution de mots de passe supportant plusieurs méthodes d'encryption et hachage.

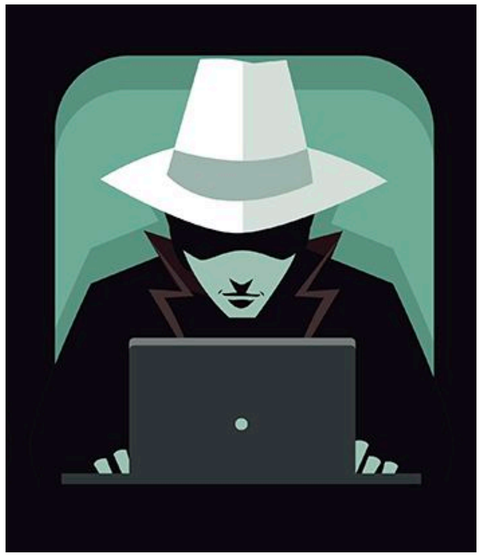


STEGHIDE

- http://steghide.sourceforge.net/
- Utilitaire de stéganographie qui permets de dissimuler de l'information via la compression et l'encryption de données dans plusieurs formats multimédias(JPEG, BMP, WAV)

RÉCAPITULATIF

- Reconnaissance → Récolte → Exploitation
- Les CTF sont des jeux 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...



PLUS DE CTF!

- En ligne
  - Backdoor
  - https://ctf.hacker101.com/
  - Hack the box
  - Pwnable
  - RingZer0
- Machines virtuelles téléchargeables
  - Exploit Exercices
  - Vulnhub
- OWASP
  - WebGoat
  - NodeGoat
  - Security Shepherd
- Listes
  - Black.Room Security
  - CAPTF
  - Penetration testing lab mind map

CTF

CTF

- https://sourceforge.net/projects/lampsecurity/files/CaptureTheFlag/CTF8/
- Autres défis de http://ctflocal.shawinigan.info/