INTRODUCTION

PYTHON POUR LA CYBERSECURITÉ

NOUS SOMMES

- **Juline Michel**
- Doctorant au laboratoire ICube et au Laboratoire de recherche de l'EPITA (LRE) dans l'équipe sécurité et système(SECUSYS).
- Thèse: sur la détection robuste des attaques dans les grands réseaux,
  plus particulièrement l'exploitation de la structure des données comme moyen de parvenir à la création de vecteur de caractéristiques stables et qualitatifs par rapport aux objectifs de détection.

- **Nadim Henoud**
- Directeur d'ingénierie à Potech
- 15 ans de génie logicielle et de cybersécurité
- Master en Sécurité des Réseaux

- Et je donne ce cours! 😁

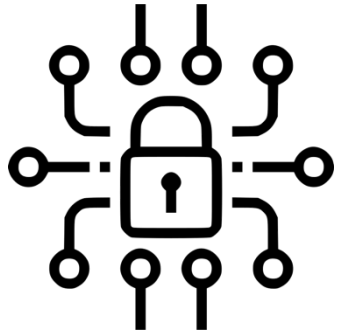
Rien n'est impossible…
Il faut juste du temps (et de l'argent ;)

VOUS ETES

- Occupation principale dans la vie
- Un hobby non relié à l'informatique

- Pourquoi vous êtes la?

ILS SONT



- **Python** est un langage de programmation interprété, multiparadigme et multiplateformes. Il favorise la programmation impérative structurée, fonctionnelle et orientée objet. Il est doté d'un typage dynamique fort, d'une gestion automatique de la mémoire par ramasse-miettes et d'un système de gestion d'exceptions ; il est ainsi similaire à Perl, Ruby, Scheme, Smalltalk et Tcl.

ILS SONT

- **Les Pentesters** sont des professionnels qui mène un test d'intrusion (« penetration test » ou « pentest », en anglais) qui est une méthode d'évaluation (« audit », en anglais) de la sécurité d'un système d'information ou d'un réseau informatique ; il est réalisé par un testeur (« pentester », en anglais).

EVALUATION DES VULNÉRABILITÉS ET TESTS D'INTRUSION

- Une évaluation des vulnérabilités
  - Identifier des vulnérabilités existantes sur une ou plusieurs machines
  - Scan simple et rapide
  - Purement technique
- Un test d'intrusion
  - Exploiter une et/ou des vulnérabilité(s)
  - Prend en compte tous les vecteurs d'attaques
  - le but contrôler un SI

EVALUATION DES VULNÉRABILITÉS ET TESTS D'INTRUSION

- C'est le processus par lequel un hacker ethique se met à la place d'un attaqueur malveillant et utilise toutes les moyens possibles pour atteindre son but
- Un test d'intrusion requiert ainsi la capacité de créer ses propres outils adaptés à l'environnement
- C'est surtout être vif d'esprit et avoir une pensée critique

To me, the extraordinary aspect of martial arts lies in its simplicity. The easy way is also the right way, and martial arts is nothing at all special; the closer to the true way of martial arts, the less wastage of expression there is.

– Master Bruce Lee, Founder, Jeet Kune Do

POURQUOI PYTHON

- Facile, lisible, rapide, évolutif
- Accessible et modifiable
- Documentation excellente, communauté très large
- Gratuit et Open-Source

- **Permet la création d'attaque qui n'ont pas de signature reconnue**

- **C'est fun**… au début… 🙄

LE BUT

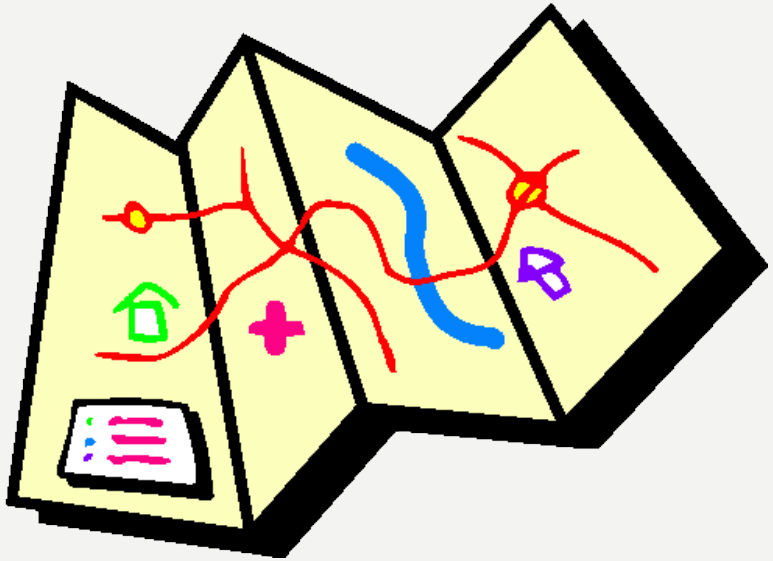
- Apprendre à utiliser python dans le cadre des tests d'intrusions

LES OBJECTIFS

- Appréhender les notions de bases nécessaires en Python pour l'exploiter dans une approche de sécurité offensive
- Exploiter le langage Python pour le pentest
- Automatiser le traitement des tâches relatives au pentest

CONTENU DU COURS

- Le scan des ports, les renifleurs de paquets et l'injection
- La manipulation des pages web: HTML scraping & parsing, screen scraping, automatisation des formulaires
- Recherche d'exploit et analyse de malware
- La force brute dans le craquage de mots de passe
- Automatisation des attaques
- L'évasion des A/V lors des attaques



CADRE JURIDIQUE

- Le fait **d'accéder** ou de se **maintenir**, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de **trois ans d'emprisonnement et de 100 000 € d'amende**.
- Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de cinq ans d'emprisonnement et de 150 000 € d'amende.
- Lorsque les infractions prévues aux deux premiers alinéas ont été commises à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à sept ans d'emprisonnement et à 300 000 € d'amende

Code pénal – Article 323-1

CADRE JURIDIQUE

- Le fait **d'accéder** ou de se **maintenir**, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de **trois ans d'emprisonnement et de 100 000 € d'amende**.
- Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de cinq ans d'emprisonnement et de 150 000 € d'amende.
- Lorsque les infractions prévues aux deux premiers alinéas ont été commises à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à sept ans d'emprisonnement et à 300 000 € d'amende

Code pénal – Article 323-1

ANATOMIE D'UNE CYBER-ATTAQUE

Reconnaissance:
Rechercher une faiblesse y inclut la collecte d'information d'identification à travers le phishing, les scans de réseaux, les scans de vulnérabilités, etc.

Armement:
Créer un malware adapté aux contraintes de la faiblesse découvert lors de la reconnaissance.

Exploitation:
Installer et exploiter le malware livrer pour élever les privilèges.

Livraison:
Livrer le malware à la victime via l'exploit ou le backdoor découvert lors de la reconnaissance.

Maintenir l'accès:
Echapper aux mesures défensives, découvrir le réseau et infecter d'autres machines

Controle et évasion:
Contacter le server C&C, exfiltrer les données, effacer ses traces