Syllabus projet

Année : **2022-2023**

Enseignant(s)	Email(s)
GEORGES Louis	ttemporaire12078@myges.fr

TP2 - OSINT Automation - Copie

1 Matières, formations et groupes

Matière liée au projet : **S1 - Scripting en python**

Formations : -

Nombre d'étudiant par groupe : **1 à 3**

Règles de constitution des groupes: **Libre**

Charge de travail estimée par étudiant : **0,00 h**

2 Sujet(s) du projet

Type de sujet : **Imposé**

TP2 - OSINT Automation

Dans ce TP, vous allez devoir réaliser un outil en ligne de commande permettant d'automatiser l'utilisation de quelques outils connu servant à la reconnaissance de d'informations publiques (OSINT). Le but étant d'arriver à un outil exploitable en condition réel de test d'intrusion.

Vous aurez donc à automatiser ces 4 outils :

* Dnsscan - récupération passive d'informations liées au DNS

* Shodan - récupère en fonction de l'ip ou du nom de domaine des informations sur la cible (utilisable via l'api ou l'outil en ligne de commande)

* TheHarvester - Récupère des informations sur des adresses mails, noms de domaine etc.

* [Urlscan.io](https://urlscan.io/docs/api/) - réalise un scan d'une cible et récupère des informations.

Vous pouvez également implémenter d'autres outils à la place, tant qu'aucun d'entre eux ne réalise de test actif sur votre cible.

___

Consignes

Votre script python doit être le plus modulable possible. Il peut prendre des arguments (bilbliothèque Sys comme vue en cours ou argparse). À vous de choisir le format d'utilisation :

- Passage de toutes les informations d'exécution dans les arguments

- Configuration dans des fichiers de conf (yml ou txt) - permet d'activer ou désactiver les outils qui seront utilisés par le script.

ou

- construisez votre application en mode menu interactif, l'utilisateur pourra alors choisir à la carte les applications qu'il souhaite exécuter etc.

Une fois l'exécution terminée, tous les résultats sont logués dans un dossier créé portant le nom du domaine ou de l'adresse email recherché. Il y aura alors, un fichier de résultat par outil.

Vous devrez également réaliser un fichier Readme.md expliquant le fonctionnement et l'installation de votre outil + un fichier Requirements.txt détaillant les librairies à installer et leurs versions.

Vous travaillerez en groupe de 2 ou 3 ou seul pour ce TP. Utilisation de Git **obligatoire** (même pour ceux qui font le TP seul - permet de suivre les différents commit ou l'utilisation de branch).

En extension (sur 5 point) :

- Aujouter la recherche de Google Dorks à votre script. (2,5 points)

- Contenerisez votre application dans un Docker. (2,5 points)

Rendu

Le rendu se fera sur MyGes avec au choix :

- Une archive au format NOM1_NOM2_NOM3.zip contenant le code et les fichiers demandés (Readme et Requirements + .git)

- Un fichier txt, md ou pdf avec les noms de l'équipe et un lien vers le répo Git. (Il faudra au préalable m'ajouter comme collaborateur au projet : ls_grge@protonmail.com)

Sur ce TP, vous serez noté sur l'ergonomie de votre code, son fonctionnement et l'implémentation des différents éléments demandés.

3 Détails du projet

Objectif du projet (à la fin du projet les étudiants sauront réaliser un...)

> Dans ce TP, vous allez devoir réaliser un outil en ligne de commande permettant d'automatiser l'utilisation de quelques outils connu servant à la reconnaissance de d'informations publiques (OSINT). Le but étant d'arriver à un outil exploitable en condition réel de test d'intrusion.

Descriptif détaillé

Ouvrages de référence (livres, articles, revues, sites web...)

Outils informatiques à installer

4 Livrables et étapes de suivi

1	Rendu final	Rendu TP	**dimanche 12/02/2023 23h55**

5 Soutenance

Durée de présentation par groupe : **0 min**

Audience :

Type de présentation :

Précisions :