Master INFO
RT0706

UNIVERSITÉ DE REIMS CHAMPAGNE-ARDENNE

TP1: Reconnaissance and Mapping

Un compte rendu de TP doit être rédigé, nommé sous la forme **TP1_NOM1_NOM2.pdf** et envoyé dans la section dédiée sur le Moodle.

Un retard de livraison de compte rendu entrainera une perte de points.

Chaque réponse doit-être accompagnée d'une preuve sous forme d'une ou plusieurs captures d'écran démontrant votre démarche et votre compréhension de l'exercice.

1. DNS (2 points)

a. Donnez l'adresse IPv4 associée au domaine « piosky.fr ». (0.5 point)
b. Donnez l'adresse IPv6 associée au domaine « google.fr ». (0.5 point)
c. Quel est le registrar du domaine « piosky.fr » ? (0.5 point)
d. Quel est l'hébergeur du domaine « piosky.fr » ? (0.5 point)

2. OSINT (7 points)

a. Quelle est l'autorité qui a généré le certificat du site https://piosky.fr ? (0.5 point)
b. Avez-vous des vulnérabilités avérées à remonter concernant ce certificat ? (1 point)
c. Retrouvez le framework web, le générateur du site et la version de la librairie JavaScript du site https://cve.piosky.fr/ (1 point)
d. Listez les sous-domaines du domaine « piosky.fr ». Montrez votre démarche. (1.5 points)
e. Donnez votre recherche Google permettant de lister les PDF exposés par le site excellium-services.com (1 point)
f. De manière passive, retrouvez l'adresse mail professionnelle d'Anthony Maia. Expliquez votre démarche. Aucun mail ne doit-être envoyé à cette adresse. (2 points)

3. Mapping (3 points)

a. Quels sont les services exposés par le domaine piosky.fr ? (1 point)
b. Quel est la technologie du serveur web qui supporte le site https://piosky.fr ? (1 point)
c. Quel est le système d'exploitation derrière le site https://piosky.fr ? (1 point)

4. Root-me.org (8 points)

a. Faire le challenge suivant:
   - https://www.root-me.org/fr/Challenges/Web-Serveur/Mot-de-passe-faible (0.5 point)

b. Faire le challenge suivant:
   - https://www.root-me.org/fr/Challenges/Web-Serveur/Install-files (1 point)

c. Faire le challenge suivant **en utilisant un proxy** :
   - https://www.root-me.org/fr/Challenges/Realiste/Eh-oui-parfois (2 points)

d. Faire le challenge suivant :
   - https://www.root-me.org/fr/Challenges/Web-Serveur/Insecure-Code-Management (2 points)

e. Faire le challenge suivant :
   - https://www.root-me.org/fr/Challenges/Web-Serveur/JSON-Web-Token-JWT-Introduction (2.5 points)