docker-compose build

docker-compose up -d

Firefox est disponible depuis votre propre navigateur internet via l'adresse http://localhost:5801

Dans firefox taper l'adresse du Site Web en question : http://Tourisme_Scranton/

docker exec -it ubuntu /bin/bash Pour accéder au terminal de l'attaquant

dirb http://Tourisme_Scranton/ Pour analyser 1ere fois le site web

Ce qui se trouve à l'adresse http…/robots.txt est une fausse piste qui ne mène à rien

wget http://Tourisme_Scranton/ Va récupérer la page index.html du site.

Ensuite :

html2dic http://Tourisme_Scranton/ > mydic.txt Pour créer son propre dictionnaire de mot avec ceux présent sur la page html du site.

dirb http://Tourisme_Scranton/ mydic.txt Permet de trouver le répertoire Schrute non visible sans cette recherche.

dirb http://Tourisme_Scranton/Schrute/ -X .txt Va alors rechercher les fichiers dont l'extension est .txt

Après avoir récupéré le flag,
wget htt…/Schrute/flag.txt (ou depuis le firefox à disposition)

utiliser cyberchef pour retrouver le flag en clair.

Pour cela lui indiquer s’il ne le propose pas automatiquement de lui meme. From hexa puis from base64.

FIN