Pour certains clients le pentesteur travaillera en boite fermée. Dans ce cas le pentest débute par une phase de reconnaissance. Le testeur va glaner autant d'informations que possible sur la cible auprès de sources publiques et privées pour éclairer la stratégie d'attaque à mettre en œuvre.
Les sources d'information incluent les recherches sur Internet, la récupération des informations d'enregistrement de domaine, l'ingénierie sociale, l'analyse non intrusive du réseau et parfois même la plongée dans les poubelles. Ces informations aident les testeurs à cartographier la surface d'attaque de la cible et les vulnérabilités possibles. La phase de reconnaissance peut varier en fonction de la portée et des objectifs du test d'intrusion.

L'open source intelligence : OSINT est une pratique du renseignement qui se base sur des sources de données publiques.

Pour apprendre et pratiquer la méthodologie de l'OSINT de nombreux sites existent. Certains proposent des formations d'autres des challenges.

Initiation à l'Open Source Intelligence

Pour cet exercice on va s'intéresser au site https://ozint.eu
Vous pouvez vous y créer un compte. Vous pouvez créer 2 ou 3 équipes pour vous mesurer les uns aux autres.

1. Pour tous

Tout d'abord vous devez tous lire les articles :
- Généralités / Introduction
- Généralités / Méthodologie générale

Les articles :
- Généralités / Les réseaux sociaux (introduction)
- Généralités / Installation machine virtuelle

ne nous intéressent pas.

Travail à la scie sauteuse : JigSaw

On a quatre thèmes à travailler : le web, les personnes, les photos et les lieux.

Dans un premier temps on forme quatre équipes de base de 4 personnes : team A, B, C, D.

Et on définit 4 sujets à étudier :
Sujet White : le web
- Généralités / Les moteurs de recherche
- Internet-Web / Les archives du Web
- Entreprises et documents officiels / Informations sur les sociétés

Sujet Red : les personnes
- Recherche sur les personnes / Les recherches sur l'état civil

- Recherche sur les personnes / Les recherches foncières
- Recherche sur les personnes / Recherche de profils
- Recherche sur les personnes / LinkedIn et Twitter

Sujet Purple : les images

- Recherches photos / Recherche par image
- Recherches photos / Les données d'une image (Exif)

Sujet Blue : les lieux

- Recherches géographiques / Géoportail
- Outils avancés / Introduction à Overpass

2. Travail individuel : « éparpiller par petits bouts façon puzzle »

Dans chaque équipe un étudiant choisit d'étudier un des quatre sujets : white, red, purple ou blue. Il va donc lire les articles correspondant puis peaufiner son apprentissage sur l'internet notamment ici : https://osinttraining.net/introduction-aux-renseignements-de-sources-ouvertes/

Il s'agit d'un travail individuel. L'étudiant source les documents glanés sur l'internet. Il peut illustrer le sujet par des exemples, notamment à travers les défis proposés par ozint.eu, et tout ce qui lui semble intéressant. Il produit un « brouillon » de document avec au moins un exemple.

3. Du travail d'expert

On réunit maintenant les experts de chaque sujet : white, red, purple, blue.
Ensemble ils échangent sur leur connaissance du sujet et produisent un document de synthèse consolidés.

4. Retour dans sa team

Les quatre teams de départ se reconstituent et chaque expert forme son équipe sur son sujet.
A l'issue de l'exercice tout le monde est opérationnel sur tous les sujets, les experts le sont un peu plus.

5. Debrief en plénière