IUT de Béziers	Travaux pratiques	R3C16
Réseaux et Télécoms		Pentesting
Université de Montpellier	Open Source Intelligence : OSINT	

Lors des séances de TD vous vous êtes familiarisés avec les démarches de renseignement de l'OSINT.

Si votre convention de pentest prévoit une phase de reconnaissance pour établir la surface du test, vous utiliserez cette méthodologie pour identifier et préciser votre cible.

Ce TP traite des méthodes de reconnaissance utilisables pour les système d'information et ne se limite donc pas au social engineering.

Ce n'est qu'une fois cette phase de reconnaissance achevée que le pentesteur pourra commencer à titiller (scan) le SI de son client puis d'en découvrir les vulnérabilités.

Attention, dans cet exercice on ne procède pas au balayage des cibles. Il est donc interdit de scanner les IP, les ports ou les vulnérabilités des cibles.

On se limitera exclusivement à des actions standards non intrusives et légitimes. On pourra consulter les sites web, les DNS, les routeurs, les bases de données publiques.

On pourra utiliser les utilitaires CLI ou les applications en ligne : whois, dig, traceroute+, theHarvester, netcraft, curl, … ainsi que les recherches sur le web.

Exercice 1 : Mise en route

Vous devez faire une cartographie en vue d'un pentest red team et rendre le rapport correspondant.

1. Une première cible est l'entreprise de Michael Jennings : EOT Consulting Group
2. Une seconde cible est l'IUT de Béziers.

Exercice 2 : Reconnaissance et cartographie d'une cible

Le livrable est un rapport de cartographie. Afin de vous évaluer, vous préciserez, par exemple en marge, la méthode employée pour collecter chaque type d'information présentée.

1. Choisir une entreprise ou une organisation cible suffisamment grande et collecter toutes les informations qui vous semblent utile pour un pentest en mode red team.
2. Débuter votre cartographie en vous appuyant sur des outils et des méthodes basiques.
3. Elargir votre travail en vous aidant d'outils intégrés, par exemple theHarvester
4. Prendre en main le logiciel Maltego pour finaliser votre cartographie.