2023/2024

Travaux Pratiques 3 : Découverte de la topologie réseau

L'objectif des exercices qui suivent est de vous familialiser avec les outils et démarche de découverte de la topologie réseau.

1. Introduction

Quelques commandes utiles pour le TP

`nslookup` <nom_domaine>

`ping` <adresse ip>

`traceroute` <nom domaine ou adresse ip>

`whois` <nom domaine>

Sites

https://www.iana.org/numbers - Internet Assign Numbers Authority

https://who.is – WHOIS Search

Outils

https://nmap.org - The network mapper

https://www.fing.com – Network Scanner App

Exercice 1 – Reconnaissance de l'environnement

Trouver toutes les informations possibles relatives au nom de domaine **univ-toulouse.fr** :

- plages d'adresses IP utilisées,
- éventuels serveurs (mél, DNS, web, …),
- localisation physique,
- noms et téléphone des membres de l'université, etc.

Détaillez votre démarche et les outils utilisés.

Exercice 2 – Scan et Enumération

Dans l'environnement déployé en salle de TP (si cela a pu être effectué), scanner :

- les postes présents dans l'environnement et trouver les systèmes d'exploitation utilisés
- les services proposés (« *ouverts* ») sur chacune des machines
- et les systèmes d'exploitation des machines identifiées

Sélectionner des services qui vous semblent « **intéressants** » pour une attaque : pourquoi les avez-vous choisi ?
Où chercheriez-vous de l'information ? Quels seraient les critères qui guideraient vos choix ?

Essayez d'en savoir plus sur leur version de protocole utilisé et la manière dont vous pourriez entrer dans le système : où vous procurez-vous l'information et qu'aller vous utiliser pour tenter une intrusion ?