

Travaux Pratiques 3 : Découverte de la topologie réseau

L'objectif des exercices qui suivent est de vous familiariser 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://www.ripe.net> - Réseaux IP Européens

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

Détaillez votre démarche.

Exercice 2 – Scan et Enumération

Dans l'environnement déployé en salle de TP, scanner

- les postes présents dans l'environnement,
- les services 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 ?

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 ?