L’Unique but de ce TP est de vous enseigner à vous protéger contre les Hackers et ne doit en aucun être utilisé pour faire du mal. Il peut contenir des techniques dangereuses.

SCANNER UN RESEAU AVEC NMAP

L’objectif de ce TP est de scanner votre réseau et de voir les appareils qui y sont connectés, les adresses IP et les ports et services utilisés.

1. Taper la commande ***nmap -- help***
2. Taper la commande ***ifconfig***

Quelle est votre adresse IP privée ? Quelle est votre adresse masque ?

3. Taper la commande : ***nmap adresse ip du réseau***
   a. Quelles sont les machines connectées à votre réseau ? Quel est le statut des ports ?
   b. Quelle est l’adresse MAC de la machine ?

4. Taper la commande ***nmap -0 adresse ip d’une machine***
   a. Quel est le système d’exploitation que cette machine utilise ?
   b. Quelle est son adresse MAC ?
   c. Quels sont les ports ouverts sur cette machine ?

5. Taper la commande ***nmap - -script default adresse ip d’une machine***
   a. Quel est le nom de la machine ?
   b. Quel est le nom de l’utilisateur ?
   c. Quelle est la version du système d’exploitation ?

6. Taper la commande ***nmap – v - -script vuln adresse ip d’une machine***
   a. Quelles sont les failles, faiblesses et vulnérabilités de cette machine ? (Ports, statut des ports, les services utilisés)

7. Taper la commande ***nmap – v - -script dos adresse ip d’une machine***
   a. Peut-on analyser, détecter et mener une attaque Dos ?

INTERFACE GRAPHIQUE ZENMAP

1. Faites un Quick scan de votre réseau
2. Faites également un scan intense
3. Essayer de trouver la topologie de ce réseau

L’Unique but de ce TP est de vous enseigner à vous protéger contre les Hackers et ne doit en aucun être utilisé pour faire du mal. Il peut contenir des techniques dangereuses.

Une fois le scan effectué avec les noms des machines, les adresses IP, les adresses MAC, les services qu’ils utilisent, les systèmes d’exploitation qu’ils utilisent, Qu’êtes-vous capable de pouvoir faire ?