**TP 1 - Réalisation d’une intrusion**

**Objectifs**

* Commencer à automatiser l’exploitation des machines victimes.
* Création d’un fichier de ressources capable de faire appel à un scanner.

**Travail demandé**

1. Identifier les options requises pour lancer un scan *ssh\_login :*

* Donnez les commandes nécessaires pour répondre à cette question :

set RHOSTS (ip adresse)…………………………………………..

set PORTS (n°port ici 22) …………………………………………..

set USERPASS\_FILE (pass)………………………………………..

* Donnez les paramètres requis et expliquez leur utilité pour lancer un scan

set RHOSTS (192.168.21.25) sauvegarder adresse ip cible

set PORTS (22) sauvegarder port de la machine cible a scanner

set USERPASS\_FILE (chemin) préciser chemin vers un fichier de login et mot de passe a utiliser………

1. Créer une fonction *get\_networks* qui retourne :
   * L'adresse MAC
   * L’adresse broadcast
   * L’adresse de la passerelle par défaut
   * L’adresse IP

d’une machine cible

**Indications :** Utiliser les fonctions de la librairie *netifaces (voir support de cours)*

1. Créer une fonction *resource\_file\_buider* qui permet de générer un fichier contenant les commandes requises pour lancer un scanner *ssh\_login* :

use auxiliary/scanner/ssh/ssh\_login

set RHOST *argument1*

set RPORT *argument2*

set USERNAME *argument3*

set PASSWORD *argument4*

run

*argument1, argument2, etc.* représentent les arguments de la fonction.

**Indications :** Utiliser les fonctions de gestion de fichiers : *open, write et closed.*

1. Créer le programme qui permettra de générer le script de lancement de scanner et tentative de brute force sur le port 22 correspondant à une adresse IP dont le port 22 est ouvert.

**Indications :** Utiliser les étapes de création d’un script classique : 1) importation des librairies 2) validation des arguments 3) algorithme (voir exemple dans le support de cours)

**Le programme ainsi que les réponses aux questions doivent être envoyées par email à l’adresse suivante : monia.benmlouka@alyfpro.fr**