**TP Scapy**

**Enoncé :**

On veut écrire un logiciel permettant de faire un « SYN Scan », permettant de déterminer l’ensemble des ports TCP ouverts, c-à-d permettant la connexion suivant le protocole TCP. Le principe du « SYN scan » est de tenter d’ouvrir une connexion vers une adresse IP et un port donnés en envoyant un segment de drapeau SYN, et d’attendre une réponse dans un laps de temps fixé : si la réponse est un segment TCP de drapeau RST alors la connexion est refusée et le port est considéré comme fermé; si une réponse n’est pas obtenu avant l’expiration du délai, alors on considère que le port est filtré par un firewall ; si la réponse est un segment de drapeaux SYN/ACK alors on considère le port comme ouvert.

a. Écrivez un programme Python réalisant un « SYN scan » pour la plage de ports 50 à 1024.

b. On veut maintenant réaliser une version améliorée : un « Stealth SYN scan », c-à-d. une version où lors de l’obtention d’un segment réponse SYN/ACK, le logiciel envoie un segment de drapeau RST pour mettre fin à la demande de connexion, et éviter de laisser une trace dans les journaux d’activités, log, de la cible. Donnez les modifications à apporter à votre code pour activer le mode « stealth », ou « furtif ».

**Amélioration :**

Les ports sont testés dans le désordre

Le temps entre les envois est différent

Le mac du pc source varie entre les envois