from scapy.all import \*

common = [80, 443, 67, 68, 20, 21, 23, 22, 53, 8080, 123, 25, 3389, 110, 554, 445, 587, 993, 137, 139, 8008, 500, 143, 161, 162, 389, 1434, 5900]

# liste des 28 ports les plus utilisés

for i in range(len(common)):

    x=common[i]

    paquet = IP(dst="192.168.56.1") / TCP(dport=x, flags='S')

    send(paquet)

# envoi une trame a tout les ports de la liste common

Envoi une trame de type syn, réponse de type rst ack

p=input(f"entrez les 3 premiers octets de votre ip (x.x.x):\n ")

for i in range(256):

    x=p+f".{i}"

    paquet = IP(dst=x) / TCP(dport=1, flags='S')

    print(x)

    send(paquet)

# envoi un paquet a tout les hotes entre 0 et 255

Envoi une trame a toutes les ip présent dans le réseau :

L’ip entrée par l’user est égale a x.x.x / on va ensuite faire loop dans 256 itérations afin de courvir toute les ip / On va ensuite ajouter le dernier octet de l’ip avec la variable temporaire x qui prendre la valeur de i, donc x sera égal a l’itération de i et donc prendra la valeur de l’itération actuelle.