Premiers scripts Python avec Scapy

Scan d'adresse IP d'un sous-réseau

Quelques compléments

- pour indiquer une plage d'adresses IP utiliser la syntaxe suivante pour l'attribut **dst** du paquet **IP** :

```
dsp='192.168.1.1-15'
```

Exemple de code dans un script python

file scanIp.py

```
#! /usr/bin/python
from scapy.all import *

plage = '192.168.1.1-15'
paquet = Ether() / IP(dst=plage) / ICMP()
rep,non_rep = srp(paquet, timeout=0.5 )
for element in rep : # element représente un couple (paquet émis, paquet reçu)
    if element[1][ICMP].type == 0 : # 0 <=> echo-reply voir page de Wikipedia
        print( element[0][IP].dst + ' a renvoye un echo-reply ')
for element in non_rep : # element représente un couple (paquet émis, paquet reçu)
    if element[1][ICMP].type == 8 : # 8 <=> echo-request voir page de Wikipedia
        print( element[0][IP].dst + ' : aucun echo-reply ')
```

A faire

- Q1 : **Ecrire** un script python **scanIpHote.py** qui indique si un hôte passé en paramètre répond au ping.

- Q2 : **Ecrire** un script python **scanIpPlage.py** qui :
  - **scanne** les 50 premières adresses IP du **sous-réseau du BTS SIO**,
  - indique les hôtes qui **répondent** au ping,
  - indique les hôtes qui **ne répondent pas** au ping.

Retour à Python : la bibliothèque Scapy ...

- Python : la bibliothèque Scapy pour manipuler les paquets réseau