

# 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 :

```
dst='192.168.1.1-15'
```

Exemple de code dans un script python

file `scanlp.py`

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

rang = '192.168.1.1-15'
ping = IP(dst=rang) / ICMP()
rep,non_rep = sr(ping, timeout=0.5)
for element in rep: # element représente un couple (paquet émis, paquet reçu)
    if element[1].type == 0: # 0 <=> echo-reply voir page de Wikipedia
        print( element[1].src + ' a renvoyé un 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

From:  
[/ - Les cours du BTS SIO](#)

Permanent link:  
[/doku.php/dev/python/scapy/scapyscript-1?rev=1509809370](https://doku.php/dev/python/scapy/scapyscript-1?rev=1509809370)

Last update: **2017/11/04 16:29**

