# Virtualisation

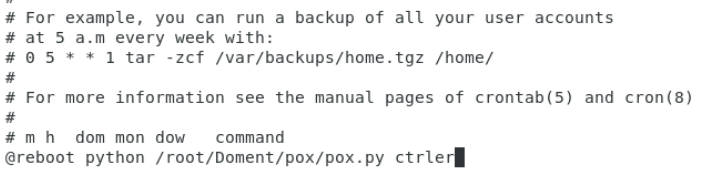
## Automatisation démarrage des machines

Pour le démarrage des machines, un simple script bash a été réalisé. L’exécution du script se fait sur la machine hôte, avec le compte root, à l’aide de virsh.



## Démarrage automatique des services

Pour démarrer sur les machines virtuelles les services associés (Pox et Mininet), j’ai utilisé les crontable de ces machines afin de lancer les scripts pythons réalisés, dès le démarrage de la machine, comme suit :

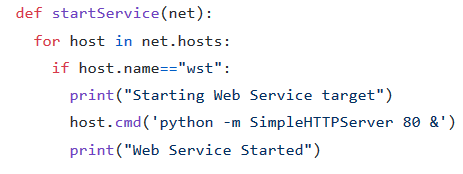


## Partie Mininet

Le réseau donné en consigne a été réalisé avec un script python :

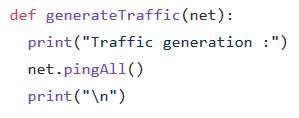


La suite du TP est l’attaque d’un service web que nous démarrons de la manière suivante :



Dans ce script python a été ajouté deux parties : la génération d’un traffic réseau « normal » et la génération d’une attaque. Chaque partie est faite pour mettre à l’épreuve la partie suivante qui concernera Pox.

Pour la génération de traffic un simple ping sera utilisé comme suit :



La partie attaque consiste à faire des requêtes HTTP sur la chaine vers la machine cible :



## Partie Pox

Pox est le controller mis en place, il servira à la détection d’attaque de type déni de service sur le réseau.

Voici comment est géré la détection :

Pour chaque paquet qui transite dans le réseau, on stock le couple source+destination ainsi que l’heure de transmission. La façon dont sont stocké les informations est la suivante :

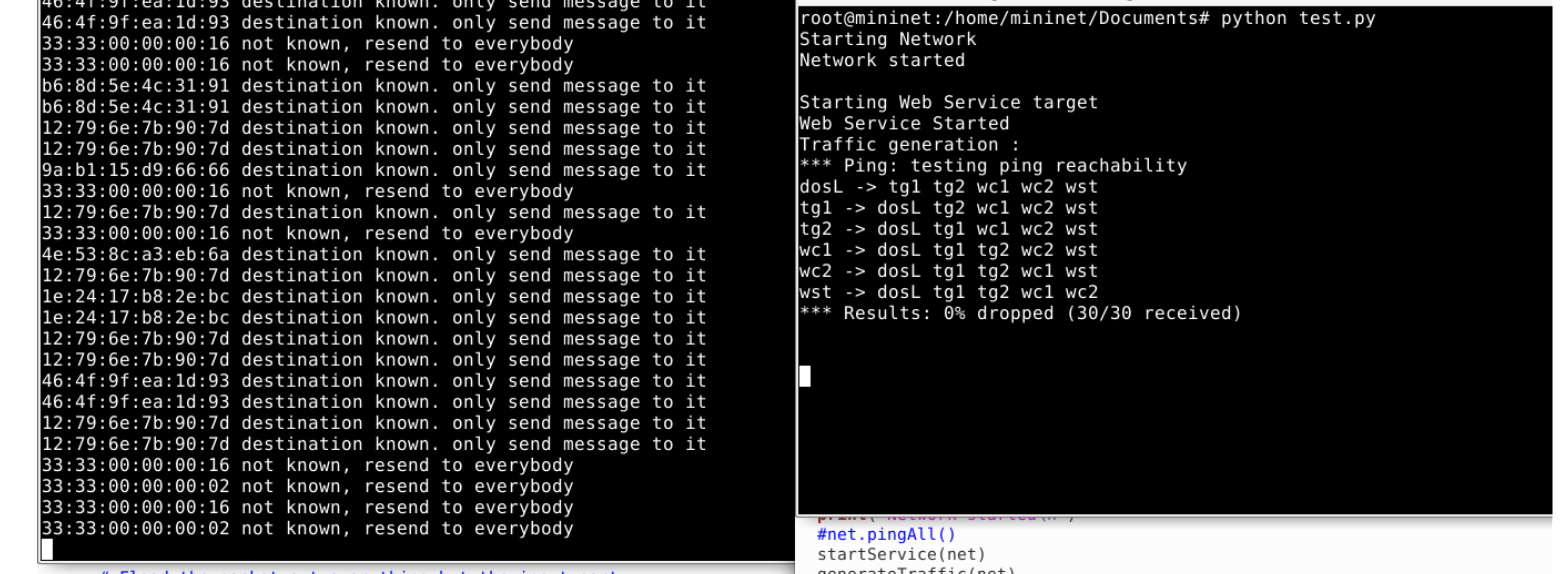
Un dictionnaire ayant pour clé le couple source+destination et pour valeur un tableau stockant les heures

Pour l’exercice, j’ai arbitrairement choisi une tolérance à 10 requêtes par seconde.

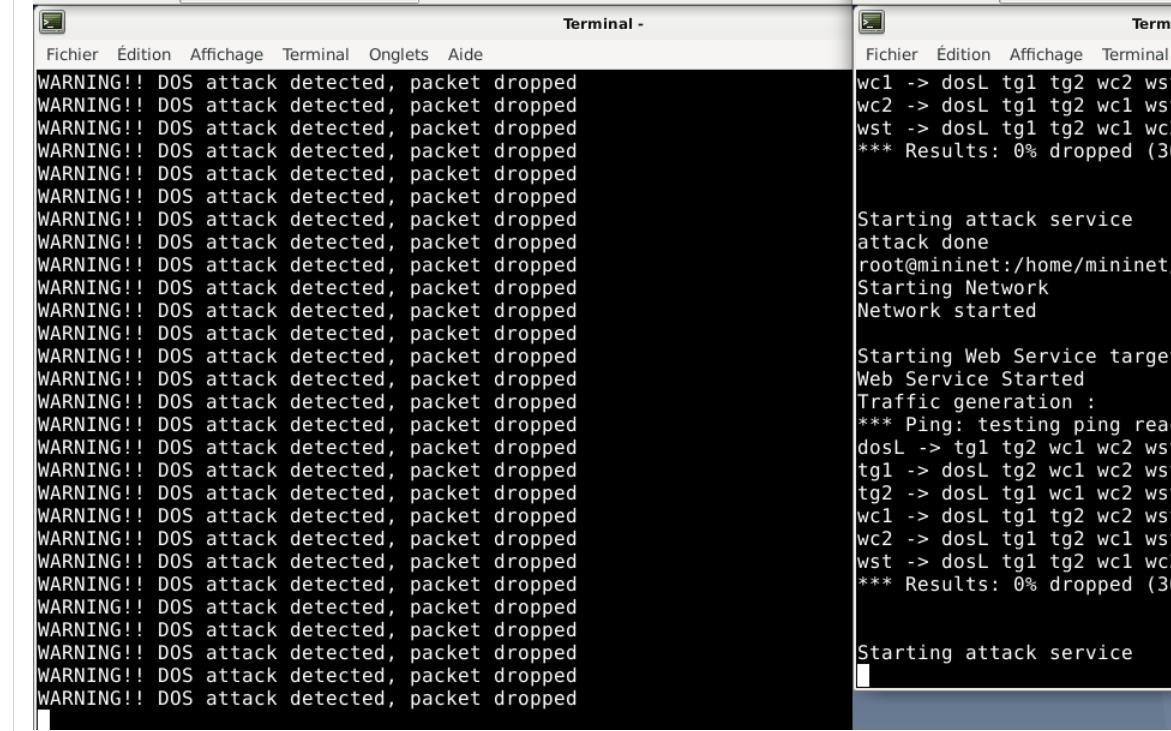
Pour chaque paquet émis, on vérifie si les 10 derniers paquets ont été envoyé dans la seconde.  
Si non : le paquet est transmis et les informations sauvegardées.   
Si oui : le paquet est « droppé » mais les informations le concernant sont malgré tout stocké afin de suivre la continuité de l’attaque.

Afin d’éviter les problèmes que pourrai engendrer le stockage des logs, seul une quantité nécessaire à l’analyse de donnée est gardée (10 logs par couple).

Activité avec traffic avant l’attaque :



Activité pendant l’attaque :



Activité normale après l’attaque :

