RAPPORT TP 3 ET TP4

TP4

# Manipulation de paquets avec Scapy

## Demarrage d’un réseau virtuel

### Lancez tcpdump -i eth0 sur la passerelle immortal afin d'espionner le trafic échangé entre les autres machines. Lancez netstat -tupl pour voir quels services (et donc quels ports) sont ouverts sur opeth (ou syl).

Text

Description automatically generated

A picture containing text

Description automatically generated

## Prise en main de Scapy

### Lancez scapy3 sur la machine grave en tant que root (ou sudoer)

Text

Description automatically generated

### Il est également possible d'écrire des programmes Scapy sous forme d'un script Python, qu'il faut enregistrer avec un éditeur de texte, comme nano ou emacs

A screenshot of a computer

Description automatically generated with medium confidence

Text

Description automatically generated

## Ping

### Regardez dans le fichier ping.py un exemple d'utilisation de Scapy qui envoie un ping (ICMP) puis récupère la réponse. Essayez-le en recopiant le programme ligne par ligne, ou en faisant un copier/coller.

Text

Description automatically generated

## ARP

### Rappelez le fonctionnement du protocole ARP. Notez que le protocole ARP ne dispose que de deux opérations : la requête (Who Has) et la réponse. On peut alors utiliser ce protocole pour effectuer un ping dans le réseau local Ethernet. Il s'agit d'envoyer une requête ARP. Si la machine répond, c'est bien qu'elle est en vie !

FLEMME ALED

### Commencez par construire une trame Ethernet avec Ether() vers l’adresse de broadcast FF:FF:FF:FF:FF:FF et encapsulez le datagramme ARP() à destination de l'adresse IP visée. Pour envoyer et recevoir une trame Ethernet, il faut utiliser la fonction srp1() (à la place de la fonction sr1() réservé aux paquets IP). On peut aussi utiliser dans cette fonction l'option timeout=1 pour limiter le temps d'attente à 1 seconde, dans le cas où il n'y a pas de réponse.

REGARDER LE SITE DE SCAPY POUR CA