Université Bordeaux — année 2025-2026

Master Informatique/Master CSI — Admin. des Réseaux

TD - Forger des paquets ...

Le but de ce TP est d'étudier l'encapsulation ainsi que des outils de diagnostic simples.

La topologie réseau à être utilisée peut être obtenue en lançant le script de démarrage `/net/stockage/-aguermou/AR/TP/3/qemunet.sh` en lui fournissant la description de la topologie réseau à l'aide de l'option `-t` ainsi que l'archive contenant la configuration initialte des machines à l'aide de l'option `-a`. Ceci revient à lancer les commandes suivantes :

— au cremi :
```
# cd /net/stockage/aguermou/AR/TP/3/; ./qemunet.sh -x -t topology -a archive_tp3.tgz
```
— à distance :
```
# cd /net/stockage/aguermou/AR/TP/3/; ./qemunet.sh -d tmux -b -t topology -a archive_tp3.tgz
# tmux a
```

Vous pouvez consulter le contenu `/net/stockage/aguermou/AR/TP/3/topology` pour voir la topologie du réseau.

1 Forger soi-même ses paquets : `scapy`

Nous allons nous intéresser à l'outil `scapy`. Il s'agit d'un environnement permettant de forger soi-même ses propres paquets. Nous allons donc illustrer l'encapsulation des protocoles à l'aide de `scapy`.

1. Tout d'abord, il est important de se documenter. Tout ce dont nous aurons besoin se trouve sur la page suivante :

   https://scapy.readthedocs.io/en/latest/usage.html#interactive-tutorial

2. À l'aide de la commande `scapy` `sr(...)` (ou `sr1(...)`) forger un paquet ICMP (protocole de `ping`) qui devra être envoyé à partir de syl vers immortal. Qu'en est-il de l'encapsulation dans ce cas ? Quel est le type de la réponse ?
3. Lancer la commande `ping` sur immortal en direction de syl. Utiliser maintenant la commande `scapy` `sniff` pour afficher le contenu des paquets à destination de `syl` (un exemple est fourni dans la documentation).
4. Toujours avec la commande `scapy` `sr` forger un paquet TCP d'ouverture de connexion sur le port 22 à partir de syl vers immortal. De quelle nature est la réponse obtenue ? Compléter l'échange pour finaliser la poignée de main TCP.
5. À l'aide de `scapy` et de `python` implémenter un équivalent à `traceroute`.

2 Protocol ARP : Une attaque simple

1. Un utilisateur se connecte périodiquement en utilisant `telnet` depuis `dt` sur `opeth`. Il vous est demandé d'écouter et d'analyser le trafic correspondant depuis `immortal` pour trouver les identifiants de l'utilisateur.
2. Nous allons nous intéresser maintenant à une attaque simple dans un réseau local : l'*ARP cache poisonning*. Il s'agit d'usurper les adresses MAC de certaines machines pour mettre en place une attaque de type *man in the middle*.

(a) Mettre en place l'attaque à l'aide d'arpspoof de telle sorte que `syl` s'interpose entre `opeth` et `immortal`. Quel est le mécanisme utilisé ? (je vous laisse chercher de la documentation :-)).

(b) Reproduire l'écoute effectuer précédemment depuis `syl` (vous devriez être en mesure de retrouver les même informations).