TD - Forger des paquets ...

Le but de ce TP est d'étudier des outils de diagnostics ainsi que d'utiliser des techniques de scan de ports simples.

1. Lancez le script `/net/stockage/aguermou/AR/TP/3/start-qemu` en lui fournissant l'archive `/net/stockage/aguermou/AR/images/archive_tp3.tgz` en argument avec l'option `-a`.
2. Regardez le contenu `/net/stockage/aguermou/AR/TP/3/config` et observez la topologie de notre 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 `http://www.secdev.org/projects/scapy/demo.html`.
2. À l'aide de la commande `scapy sr(...)` 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. 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 ?
4. 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).
5. À l'aide de `scapy` et de `python` implémenter un équivalent à `traceroute`.

2 Protocol ARP : Une attaque simple

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*.

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