Approche technique de l'espace numérique

Chapitre 3

Quelques outils réseau

Pablo Rauzy <pr@up8.edu>
pablorauzy.fr/teaching/technum

Quelques outils réseau

ping

- Utilisation : `ping` *`host`*.
- Envoyer des *echo requests* ICMP à un hôte.
- Typiquement pour voir si il est en ligne.
- Version IPv6 : `ping6`.

traceroute

- Utilisation : `traceroute` *`host`*.
- Déterminer le chemin parcouru par les paquet jusqu'à un hôte.
- Version IPv6 : `traceroute6`.

nslookup

- Utilisation : `nslookup` *`name`* [*`server`*].
- Interroger les serveurs de noms.
- Par défaut on interroge le champs A, possibilité de spécifier un autre champs (AAAA, MX, TXT, ...) avec `-q=`.

whois

- Utilisation : `whois` *`name`*.
- Interroger la base de données “whois” qui donne les informations de contact du propriétaire d’un nom de domaine.

netstat

- Utilisation : `netstat [options]`.
- Affiche les connexions réseau (et d'autres informations).
- Beaucoup d'options selon ce qu'on veut afficher :
  - sockets UNIX, TCP, UDP, raw ;
  - IPv4 / IPv6 ;
  - connexions sortantes, sockets passives ;
  - etc.

iftop

- `top` pour le trafic réseau.

nc

- Utilisation `nc [options] [host port]`.
- Connexions et écoutes arbitraires TCP et UDP.
- Véritable couteau suisse réseau.

openssl s_client

- Utilisation : `openssl s_client -connect host:port`.
- Fonction client de netcat supportant TLS/SSL.

ssh

- Couteau suisse pour la connexion sécurisée :
  - session à distance,
  - création de tunnel,
  - redirection de port,
  - etc.
- Voir aussi :
  - `tsocks`.

`tcpdump` / Wireshark

- Capture et analyse du trafic réseau.

nmap

- Utilisation : `nmap [`*`options`*`] `*`cibles`*.
- Exploration réseau et scanneur de ports/sécurité.

iodine

- IP over DNS.
- Utile pour passer au travers des portails captifs.