- Si certaines commandes ne sont pas disponibles depuis votre poste, installez-les.
- Si ce n'est pas déjà le cas, installez sur votre poste les logiciels Firefox, Wireshark, …
- certaines commandes requièrent des privilèges administrateurs (root) pour être exécutées. Le compte *root* a *licpro* comme mot de passe.

ATTENTION !!! Certaines commandes (nmap, tcpdump, wireshark et AutoScan) ne doivent être utilisées qu'avec l'accord de l'administrateur du réseau et des utilisateurs.

Exercice 1 – Commandes réseau

Pour vous aider, il y a la commande *man.* Vous pouvez également consulter:
http://www.misfu.com/commandes-outils-reseaux-linux.html

1. Quelles sont les adresses IP, réseau et MAC de votre poste ?
2. Vérifiez que http://www.google.fr répond (aux ICMP_ECHO_REQUEST).
3. Pour la même adresse, déterminez le chemin emprunté.
4. Quelle est la passerelle de votre réseau ? Quelle est son IP publique ? Son nom ?
5. Quelle est l'adresse du DNS de votre réseau ? Qu'en concluez-vous ?
6. Demandez l'adresse IP du poste d'un autre étudiant et déterminez son adresse MAC.
7. Quelles sont les adresses IP actives sur votre réseau ?
8. Quels sont les serveurs actifs sur votre poste ?
9. Quels sont les ports ouverts sur la passerelle de votre réseau ? Sur le poste du voisin ?
10. Effacez la table de routage de votre machine et essayer de faire de votre voisin votre nouvelle passerelle.
11. Ajoutez une règle *iptables* afin de vous bloquer l'accès à un site Web et testez.
12. Remettre tout en ordre (plus de filtrage et passerelle obtenue par DHCP).

Exercice 2 – Écoute

Nous allons utiliser 2 applications: *tcpdump* (un *packet sniffer* en ligne de commande) et *Wireshark* (idem mais avec une interface graphique).

1. Écoutez votre interface Ethernet à l'aide de *tcpdump*. Vous allez voir s'afficher des paquets. Observez ce qu'il se passe lors du chargement d'une page Internet.

La ligne de commande sous GNU/Linux est très puissante et dépasse largement le cadre de ce TP. On pourra simplement imaginer la puissance de *tcpdump* lorsque cette commande est combiner avec d'autres... Maintenant, nous allons utiliser *Wireshark,* qui possède une interface graphique pratique et assez complète.

2. Écoutez votre interface Ethernet à l'aide de *Wireshark*. Vous allez voir ici aussi s'afficher des paquets.
    - Observez ce qu'il se passe lors du chargement d'une page Internet.

- Regardez dans les paquets et remarquez comment il est possible de voir l'encapsulation dans les différentes couches du modèle TCP/IP.
- Observez les échanges TCP nécessaires (SYN, ACK et FIN)
- Observez les échanges HTTP et comparez avec les statuts du protocole.

3. Observez différents types de paquets: DHCP, ICMP, HTTP, …
4. Essayez de vous identifiez sur un site non protégé (par ex:http://www.formulawan.fr/) et capturé les identifiants. PS: pas besoin de vous inscrire.
5. Essayez de vous identifiez sur un site sécurisé en https (par exemple l'ENT) et comparer les échanges.
   - Peut-on voir les informations échangées ?
   - Avez-vous remarquez les échanges de clés à l'aide du protocole SSL/TLS ?

Commandes à utiliser pour l'exercice 1:

1. *ifconfig*
2. *ping*
3. *traceroute*
4. Plusieurs possibilités: *ifconfig, route,...*
   Pour connaître l'IP publique : http://www.showmyip.com/
   Pour avoir le nom de la passerelle, par exemple *nslookup*
5. regardez dans le fichier /etc/resolv.conf
6. ping + arp
7. utilisez AutoScan par exemple et explorez l'outil.
8. *netstat*
9. utilisez *nmap* (ligne de commande) ou *nmapfe* (interface graphique)
10. *route*
11. *iptables*
12. plusieurs façons, dont l'utilisation de *route* et *iptables*. Il est possible aussi de redémarrer les services réseaux (*/etc/init.d/networking restart*). On peut aussi faire une demande DHCP à l'aide de *dhclient...*