1. **Les adwares :** Un adware, ou en français publiciel, est un logiciel qui affiche de la publicité sur votre ordinateur. Il existe des logiciels permettant de détecter et supprimer ces adwares, comme **Ad-Aware** (qui ne fait pas que ça, d'ailleurs).
2. **Les keyloggers :** Un keylogger, ou enregistreur de frappes, est un logiciel qui enregistre ce que l'utilisateur tape au clavier et le sauvegarde dans un fichier, ou l'envoie par Internet sur un serveur. Ces logiciels sont généralement discrets et ont pour objectif d'intercepter des mots de passe, des numéros de carte de crédit, et d'autres données confidentielles. Les logiciels anti-espions comme **Spybot** peuvent les déceler.
3. **Les backdoors :** Une backdoor, ou porte dérobée, est un programme qui ouvre un accès sur votre ordinateur. Si une porte dérobée est ouverte sur votre ordinateur, on peut s'y connecter via le réseau et effectuer différentes actions définies par le développeur du programme. Pour s'en protéger, on peut utiliser un pare-feucomme OpenOffice comme Netfilter sous Linux, ou Zone Alarm sous Windows.
4. **Les espions :** Les spywares, ou logiciels espions, sont des programmes qui espionnent la machine. Ils peuvent espionner votre historique de navigation, vos fichiers personnels, dérober vos mots de passe, etc. On peut les contrer avec des anti-spywares (anti-espions) comme **Spybot**.
5. **Les trojans :** Un trojan, ou cheval de Troie, est un logiciel en apparence légitime (utilitaire, jeu, ...) mais qui inclut une fonction d'infiltration qui permet d'installer des espions ou autres en tous genres sur l'ordinateur.Les trojans peuvent être détectés par les logiciels antivirus comme **Antivir, BitDefender, Kaspersky, ...**

À propos d'antivirus, tous ces programmes malveillants ne sont pas tous des virus. En effet, un virus se réplique. Mais ce n'est pas le seul, voyons cela dans la sous-partie suivante !

1. **Le ver :** il se duplique pour ne pas être solitaire
2. **Le virus** **:** il se cache pour ne pas se faire virer. Il existe un autre type de programme, très difficile à déloger et qui est potentiellement encore plus dangereux que les autres : le **rootkit**.
3. Logiciels :
   1. **nemesis**, sous Linux, permet de forger des requêtes ARP, entre autres ;
   2. **scapy**, sous Linux également, est un outil très pratique en réseau, il permet de faire beaucoup de choses comme forger des requêtes ou faire de l'analyse réseau par exemple ;
   3. **Wireshark**, sous Linux et Windows, permet d'analyser les requêtes qui passent par votre carte réseau ;
   4. **Cain&Abel**, pour Windows, est un outil très puissant et potentiellement très dangereux, car il permet en quelques clics de notamment casser des mots de passe, de cracker des réseaux Wi-Fi et (c'est ce qui nous intéresse ici) de mettre en œuvre une attaque MITM très facilement ! Ce logiciel est génial car il est redoutable et facile d'utilisation, mais il peut être détecté comme dangereux par les antivirus. Et pour cause ! Il permet même de prendre discrètement le contrôle d'une machine à distance !
4. Se prémunir contre les intrusions
   1. Modifier mot de passe de root : passwd root
   2. Configurer firewall. Voir <http://www.alsacreations.com/tuto/lire/622-Securite-firewall-iptables.html>. <http://fr.openclassrooms.com/informatique/cours/securiser-son-serveur-linux/filtrer-le-trafic-via-le-firewall> (fichier firewall dans le disque)
      1. Le rendre exécutable : chmod +x /etc/init.d/firewall
      2. Afin de l'ajouter aux scripts appelés au démarrage : update-rc.d firewall defaults
      3. Pour le retirer, vous pouvez utiliser la commande suivante : update-rc.d -f firewall remove
   3. Configuration ssh : modifier le fichier /etc/ssh/sshd\_config
      1. Port 2222 # Changer le port par défaut (à retenir!). supérieur à 1024
      2. PermitRootLogin no # Ne pas permettre de login en root
      3. AllowUsers dew # N'autoriser qu'un utilisateur précis
   4. Autorisations diverses : N'autorisons les compilateurs et installeurs que pour root (le numéro de version est à adapter selon la fraîcheur de votre installation) :
      1. chmod o-x /usr/bin/gcc-4.1
      2. chmod o-x /usr/bin/make
      3. chmod o-x /usr/bin/apt-get
      4. chmod o-x /usr/bin/aptitude
      5. chmod o-x /usr/bin/dpkg
   5. avoir un système à jour : créer un fichier auto-update ( et le rendre executable : chmod +x /etc/cron.weekly/auto-update) dans /etc/cron.weekly/ et lui rajouter ces lignes (<http://shakup.net/quelques-astuces-pour-securiser-votre-serveur-web-sous-linux/>) :

!/bin/sh

# Cron d'automatisation des mises à jour

apt-get update && apt-get -y upgrade

* 1. **Portsentry** (scan de ports) : Cet utilitaire permet de bloquer en temps réel la plupart des scans de port connus (même très discrets et échappant aux règles de filtrage du firewall basiques). Voir <https://www.noobunbox.net/securiser-un-serveur-avec-portsentry/> (dans dique dur portsentry tuto.pdf)
  2. Fail2ban (brute-force, dictionnaire, déni de service) : Fail2banest un petit utilitaire qui se base sur les logsde la machine pour chercher des actions suspectes répétées (par exemple, des erreurs de mots de passe) dans un laps de temps donné. S’il en trouve, il bannira l’IP de l’attaquant via iptables. Voir <https://www.noobunbox.net/securiser-un-serveur-avec-fail2ban/> (dans disque dur dossier Linux/fail2ban tuto.pdf)
  3. Rkhunter (rootkit et backdoors) / Rkhunter est un utilitaire qui est chargé de détecter d’éventuels rootkits sur votre serveur. Il est relativement léger (s’exécute une fois par jour par défaut) donc on aurait tort de se priver. Voir <http://doc.ubuntu-fr.org/rkhunter> (dans disque dur dossier linux/rkhunter tuto.pdf)
  4. Recevoir un email lors d’une connexion ssh : Cette fois-ci c’est plus une astuce qu’un logiciel. Si vous souhaitez recevoir un email dés que quelqu’un se connecte sur un compte d’un utilisateurs système, vous pouvez modifier son fichier ~user/.bashrc et ajouter la ligne suivante : echo ‘Acces SheLL Root’ `who` `date` | mail -s `hostname` Shell Root [email@domaine.tld](mailto:email@domaine.tld). Voir : <http://www.alsacreations.com/tuto/lire/622-Securite-firewall-iptables.html>.

1. **Surveiller les logs**: La plupart des logiciels cités plus haut vous enverront des notifications par mail en cas d’alerte. Cependant, surveiller les *logs*est important, car ils reflètent la « vie » de votre serveur. Les *logs*les plus intéressants sont notamment :
   1. /var/log/auth.log qui contient toutes les tentatives d’accès au serveur. Il peut être utile de filtrer le contenu, par exemple : *cat /var/log/auth.log | grep authentication failure* ;
   2. /var/log/message et /var/log/syslog contient un peu de tout (erreurs, bugs, informations, etc) ;
   3. /var/log/fail2ban est le log d’alerte de fail2ban. Cherchez notamment : cat /var/log/fail2ban | grep ban ;
   4. /var/log/snort/alert vous indiquera les logs d’alertes de Snort ;
   5. /var/log/rkhunter pour voir les rapports quotidien de Rkhunter. Faites attention aux erreurs trouvées, ce n’est pas bon signe (même si le risque de faux positifs existe ici).
   6. **Logwatch :** Il est aussi possible d’utiliser des utilitaires qui vous simplifient un peu ce travail de lecture des logs. Logwatch notamment permet de résumer plusieurs logs afin de ne vous retourner que des anomalies si possible. Cela évite un long et fastidieux travail de recherche. (installer : apt-get install logwatch)
      1. Spécifiez l’option « MailTo » car logwatch envoie ses résumés de logs par mail.
      2. Il va normalement s’exécuter tous les jours (ls -l /etc/cron.daily/ | grep logwatch pour s’en assurer).