Avantages de Kali Linux

1. Outils de test et pénétration avancés : Il y’a plus de 500 outils avancés de pénétration dans Kali Linux très utilisés dans différent domaine comme **l’analyse de vulnérabilité, le sniffing, la retro ingénierie, le forensic** etc. Quelques outils sont :

* Analyse de vulnérabilité : openvas, sqlmap
* Sniffiing : DNSChef
* Password attacks: John the Ripper
* Etc.

1. Les outils de Kali Linux sont totalement gratuits et libres d’utilisation, et le sera pour toujours.
2. Kali Linux est entièrement open source et facilement accessible par les utilisateurs. Il est disponible sur GitHub. Cela rend le système customisable et permet une évolution rapide car des personnes peuvent facilement contribuer et corriger les éventuels bugs.
3. Kali Linux utilise le système de fichier hiérarchique standard, permettant ainsi les utilisateurs linux de facilement retrouver les fichier binaire, librairie et autres
4. Kali Linux supporte plusieurs langues

Inconvénient de Kali Linux

1. L’un des inconvénients de Kali linux est que les utilisateurs sont souvent dupés dans de faux sentiment de sécurité et un faux sentiment de compétence. Ils ont tendance à croire que c’est tout ce dont ils ont besoin pour devenir un hacker : **Kali ≠ Hacking**
2. Il n’est pas très facile à prendre en main pour un débutant
3. Si l’on utilise Kali linux sur une machine virtuel, presque tous les **outils d’hacking sans fil** (wireless hacking tools) ne fonctionnent pas. Pour le faire, il faut l’installer en dual boot sur notre machine.
4. Il est conseillé d’installer Kali sur une machine virtuelle si c’est la première fois, afin d’apprendre à l’utiliser et savoir correctement le maitriser. Ainsi, il est facile de supprimer la VM, contrairement de refaire le système, car il est très facile de faire des gaffes sur le système Kali