Hacker Windows

Version 1.0 le 15/08/2017

Attention, vous n'avez pas le droit de vous introduire dans un appareil qui ne vous appartient pas ou sans l'accord du propriétaire.

Au cours des nombreuses interventions sur des ordinateurs, j'ai pu constater ceci :

- avec un smartphone qui devient de plus en plus omniprésent, un ordinateur qu'on délaisse, des personnes en arrivent à oublier leur code utilisateur et se retrouvent avec une machine dont ils ont besoin sans la capacité d'y accéder.
- On vous demande de réparer l'ordinateur sans vous avoir donné le code.

Il s'agit ici de profiter d'une faille de Windows pour créer un compte administrateur sur la machine en remplaçant le logiciel utilman.exe destiné aux personnes déficientes visuelles par la commande.

Pour se faire :

- accéder à la machine par le biais d'un Live Linux de votre choix.
- Renommer utilman.exe en utilman.bak
- Faire une copie du fichier cmd.exe
- Renommer cette copie en utilman.exe
- Redémarrer la machine
- En cliquant sur l'aide, une commande se lance dans laquelle il faut saisir : `net user nomduuser motdepasse /add` et `net localgroup Administrateurs nomduuser /add` où nomduuser est le nom du nouvel administrateur, motdepasse son mot de passe. Vous pouvez alors vous connecter à la machine et faire toutes les manipulations que vous désirez