Format du hash du password

- Les mots de passe sont hachés avec une variante de MD5 s'ils commencent par 1 (une variante du DES était utilisée avant, avec deux caractères de sel).
- la simple récupération des fichiers `/etc/shadow` et `/etc/passwd` suffit
- Fusion des deux fichiers par `unshadow` pour une utilisation par « `John The Ripper` »
  - `john -s ~/unshadow.txt`

Elevation de privilèges

- CVE-2008-(0600|0009|0010) : vmsplice
  - Permet d'exécuter du code sous l'UID 0
    - Versions 2.6.17 à 2.6.24
- CVE-2009-1185 : udev
- CVE-2010-3847 : The GNU C library dynamic linker expands $ORIGIN in setuid library search path
- CVE-2010-3904 : RDS privilege escalation exploit
  - Linux Kernel <= 2.6.36-rc8
- CVE-2013-2094 : Linux kernel perf_swevent_init
  - Linux Kernel < 3.8.9