

contraseñas, password

Recuperación de contraseñas

- <http://www.elcomsoft.com/download.html>
- Cain y Abel <http://www.oxid.it/cain.html>
- THC Hydra <http://www.thc.org/thc-hydra/>
- SolarWinds
- Brutus <http://www.hoobie.net/brutus/>
- Aircrack <http://www.aircrack-ng.org/>
- Aircrack-ng <http://aircrack-ng.org/>
- L0phtcrack Aplicación de recuperación y auditoría de passwords

Contraseñas LM

- John the Ripper <http://www.openwall.com/john/>
- Ophcrack <http://ophcrack.sourceforge.net/>
- Rainbow Crack <http://www.antsight.com/zsl/rainbowcrack/>
Es un cracker de hashes que precomputa todos los plaintext posibles uno por uno y los almacena en la "rainbow table". Aunque tome tiempo precomputar la tabla, puede ser más rápido que un cracker de fuerza bruta.
- <http://rainbowtables.it64.com>

Volcado de hash LM y NTLM

- pwdump <http://www.foofus.net/fizzgig/pwdump/>
- bkhive <http://www.irongeek.com/i.php?page=security/localsamcrack2>
- pwdump7 versión mejorada de pwdump http://www.tarasco.org/security/pwdump_7/
- gsecdump http://www.truesec.se/sakerhet/verktyg/saakerhet/gsecdump_v2.0b5



la sam se guarda en %systemroot%\system32\config\sam pero se guardan copias en %systemroot%\repair %systemroot%\system32\config\sam.bak. Una vez obtenida la sam se pueden volcar con samdump <http://blog.gentilkiwi.com/mimikatz/samdump>

BIOS

- cmospwd <http://www.cgsecurity.org/wiki/CmosPwd>

From:

<https://intrusos.info/> - LCWIKI

Permanent link:

<https://intrusos.info/doku.php?id=herramientas:contraseas&rev=1389129312>



Last update: **2023/01/18 13:54**