contraseñas, password

Contraseñas

Ataques por fuerza bruta

- Utilizando las tarjetas gráficas oclHashcat

Listas de contraseñas por defecto

- http://www.phenoelit.org/dpl/dpl.html

Recuperación de contraseñas

- Hydra crackeador multihilo por fuerza bruta en base a diccionarios
- http://www.elcomsoft.com/download.html
- Cain y Abel http://www.oxid.it/cain.html
- THC Hydra http://www.thc.org/thc-hydra/
- Brutus http://www.hoobie.net/brutus/
- Bruter para probar la seguridad de las contraseñas por fuerza bruta (ftp, sql, imap, ….) http://sourceforge.net/projects/worawita/
- http://www.dragonjar.org/rsmangler-multiplica-tus-diccionarios-para-hacer-bruteforce.xhtml
- http://www.dragonjar.org/diccionarios-para-realizar-ataques-de-fuerza-bruta.xhtml
- recuperar contraseñas ficheros rar mediante la GPU http://www.golubev.com/rargpu.htm
- BarsWF cracker para MD5 http://3.14.by/en/md5
- L0phtcrack Aplicación de recuperación y auditoría de passwords

Recuperar contraseñas pdf

- pdfcrack http://pdfcrack.sourceforge.net/

Contraseñas LM

- John the Ripper http://www.openwall.com/john/
- Ophcrack http://ophcrack.sourceforge.net/
- Raimbow Crack http://www.antsight.com/zsl/rainbowcrack/
  Es un cracker de hashes que precomputa todo 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

Wifi

- Aircrack http://www.aircrack-ng.org/
- Airsnort http://airsnort.shmoo.com/

Referencias

- http://securityxploded.com/pdfunlocker.php