Mag. iur. Dr. techn. Michael Sonntag

Password retrieval

Institute for Information Processing and
Microprocessor Technology (FIM)
Johannes Kepler University Linz, Austria

E-Mail: sonntag@fim.uni-linz.ac.at
http://www.fim.uni-linz.ac.at/staff/sonntag.htm

Source data

- Source files
  - → shadow1, shadow2, shadow3
    - » Linux password files
  - → passwords.txt
    - » A file with passwords extracted from Windows
  - → VNC.reg
    - » Registry extract with encrypted VNC password
- Requirements:
  - → Administrative rights
    - » For installing software
  - → Installed software (see CD)
- Software:
  - → John the Ripper
  - → Cain&Abel
  - → Ophcrack

Please note!

- We are not going to attack anyone here!
- We are trying to indentify problems for later fixing it

- Permission is **always** required for trying to break passwords
  - → Which system(s) (source of encrypted files/passwords)
  - → At what time
  - → What passwords

John the Ripper

- Password cracking tool
  - → Uses word lists as well as brute-force
    - » Word "multiplication" by mangling rules (reverse, l33t…)
      - – Note: Long lists take longer, but provide better chances!
    - » Brute force: Define character set and set password length limit
  - → Can also be used as a password-strength checking module
  - → "Reconstructs" the password from its hash
    - » Therefore requires access to the password file!
  - → Can be interrupted and restarted (may take a long time!)
- Supported are the following password hash types
  - → crypt(3) hash types: traditional & double-length DES-based, BSDI extended DES-based, FreeBSD MD5-based (also used on Linux, Cisco IOS), OpenBSD Blowfish-based (also used on some Linux distr.), Kerberos/AFS, Windows NT/2000/XP LM DES-based
    - » More with additional patches!

John the Ripper

- Your tasks:
  - → Run John the Ripper against the provided shadow files
    - » "Scenarios/shadow1": Try wordlist
    - » "Scenarios/shadow2":
      - – Try wordlist
      - – Try incremental (=brute force) search, profile "alpha"
    - » "Scenarios/shadow3": Try in your spare time!
  - → Press “space” to get statistics
  - → Interpret the results/success probabilities

- Note: Several other programs for the Windows OS exist too, but these do not recover the password, they merely reset it
  - → You can get access to the computer, but the password itself remains secret!

Expected result: John the Ripper

- shadow1: The password is in the wordlist: "network“
  - » “john shadow1”

  → Will be found very fast
- shadow2: The password is not in the wordlist
  - » “john shadow2”

  → Will not be found at all!

  → Try the brute-force search: Takes considerably longer
  - » But also finds words not in a list/created by mangle rules!
  - » “john –i=Custom shadow2”; and modify (=add) john.local.conf:
    - –
      ```
      [Incremental:Custom]
      File = $JOHN/alpha.chr
      MinLen = 4
      MaxLen = 4
      CharCount = 26
      ```
    - – Note: Length is here set to 4 because we know this and that only lowercase letters are used (CharCount 26)!

Expected result: John the Ripper

- shadow3: Has a very complex and long password
  - → It is not in the word list
  - → It cannot be found by brute force
    - » Unless you have very powerful hardware and much time!
    - » Note: John the Ripper does not support parallelization!
      - – Other such tools do (10 characters MIGHT be possible!)…

Cain & Abel

- Password cracking tool for Windows
  - → Has lots of other functions as well, e.g.
    - » Unmasking password entry boxes (pre-filled old passwords!)
    - » Network sniffer
    - » Base64 decoder
  - → Supports a large number of different passwords
- Contains a program for creating rainbow tables
- Your task: Install and start Cain&Abel
  - → Decrypt the VNC server password as stored in the registry extract “Scenarios/VNC.reg”
    - » This is trivial … once you have found how/where to enter it!
    - » Give an estimate on the quality of this password based on …
      - – How/where it is stored
      - – How long cracking it takes
  - → Other locations (e.g. UltraVNC): INI file in program directory

Ophcrack

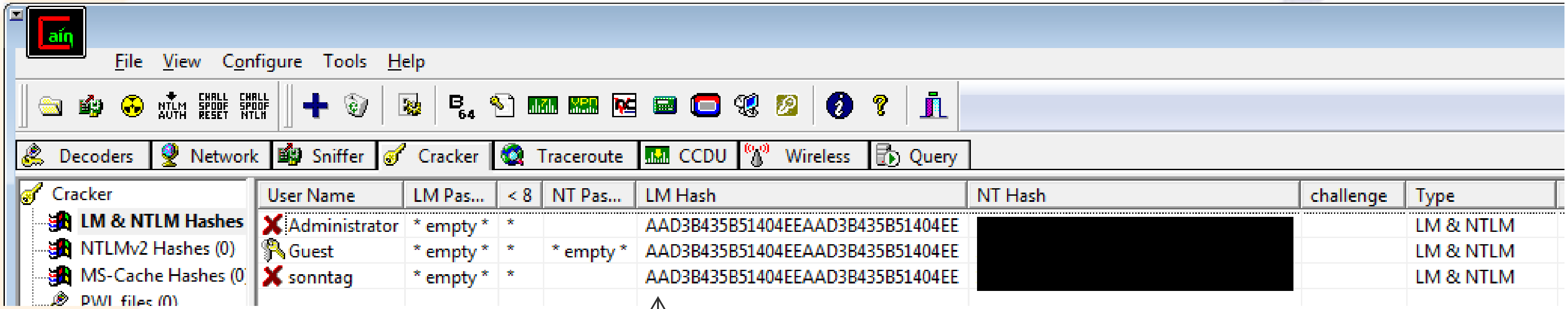
- Password cracking tool for Windows
  - → LAN Manager/NT LAN Manager hashes (i.e. Win passwords)
    - » LM / NTLM hashes (not stored in cleartext, but as hash only)
    - » Windows Vista has the (easier) LM hashes disabled by default
      - – Older versions still store the weak LM for backwards compatibility
  - → Can import the hashes from various formats or read it directly
- Based on Rainbow tables and brute force
  - → Some are freely available, others cost money
    - » You could theoretically create them yourself, but this is an extremely time- and resource-intensive activity!
  - → Free tables: About 99.9 % coverage for alphanumeric passwords of up to 14 characters (LM), 99% for NTLM
    - » All printable chars/symbols/space (NT/Vista); German →á US$ 99

Sidenote: Extracting the LM Hashes

- They are stored in the SAM registry part
  - → C:\WINDOWS\System32\config\SAM
    - » Encrypted and locked when Windows is running
    - » Shutdown, decrypt, read
- Easier: Special tools also work when WIN is running
  - → Difficulty: Needs high permissions (SYSTEM account, …)
- Exemplary software: PWDump/fgdump
  - → Needs Administrator privileges
    - » Why then the need for password cracking? You can get access to everything if you're Administrator?!?
      - – Passwords might be reused somewhere else, …
  - → Numerous versions exist, which use different approaches (e.g. DLL injection, work over network, …)
  - → >= Win 7? Some tools don't even work with "Run as Admin"!
    - » Must be the real Administrator account (this is different!)

Sidenote: Extracting the LM Hashes

- Other approach to retrieve passwords (e.g. Windows 7):
  - → Start Cain & Abel (as Administrator/confirm privileges)
  - → Select "Cracker" and "LM & NTLM Hashes"
  - → Right-click in window to right and select "Add to list"
  - → Select to import hashes from the local system
  - → Wait a short time and see them appear!
  - → Write down, copy, … hash values for cracking
    - » Or crack them directly in there if the additional tools/databases have been installed!



User Name	LM Pas...	< 8	NT Pas...	LM Hash	NT Hash	challenge	Type
Administrator	* empty *	*		AAD3B435B51404EEAAD3B435B51404EE	[redacted]		LM & NTLM
Guest	* empty *	*	* empty *	AAD3B435B51404EEAAD3B435B51404EE	[redacted]		LM & NTLM
sonntag	* empty *	*		AAD3B435B51404EEAAD3B435B51404EE	[redacted]		LM & NTLM

↑ Always the same because disabled by default in Win7!

Rainbow tables

- Reducing time by investing memory
  - → "Pre-computed passwords"
- Simplest form: Generate all passwords + their hashes and store them for later lookup (immediate cracking!)
  - → Drawback: Gigantic table!
- Rainbow tables: Compute all passwords, but store only a small part of them → After finding the hash, some time is required to obtain the actual password
  - → Time is reduced by the square of the available memory
- Countermeasure: Use "salting"
  - → A random value is generated, prepended to the password, and stored
  - → Rainbow table would have to be enlarged for the salt
    - » 4 char salt + 14 char password → 18 char rainbow table!
      - – Plus: Salt is typically binary, so 256^4 instead of $\approx 70^4$!

Philippe Oechslin: Ophcrack http://lasecwww.epfl.ch/~oechslin/projects/ophcrack/

Ophcrack

- Your tasks:
  - → Run Ophcrack against the provided passwords
    - » File: “Scenarios/Passwords.txt”
  - → Discuss the results:
    - » Why are some found quickly, but the same password takes much longer in another instance?
    - » Why is this working in Windows, but not for other systems?

Expected result: Ophcrack

- JDoe: Can be found very fast with the XP free tables
- JDoe2: Can be found with the Vista free tables
- JDoe3:
  - → Cannot be found with the XP free tables
    - » These work only for LM hashes; this account only has NTLM!
  - → Cannot be found with the Vista free tables
    - » This seems to be one of the "missing" passwords!
    - » Based on a dictionary with variations; Success rate 99%
      - – Better: Commercial; 8GB instead of 461 MB

- Note: The second account takes much longer
  - → NTLM hashes are much stronger than the NT hashes
  - → As both are the same word, once the NT hash is known, only the capitalization must be tried out!

Expected result: Ophcrack

- Windows password hashes have several problems
  - → LM are effectively 2 passwords of 7 characters
  - → LM passwords are converted to uppercase
    - » NTLM doesn’t do this: Upper- and lowercase are important!
  - → LM and NTLM do not employ any "salting"
    - » This is why rainbow tables are feasible here!
- How to disable at least the especially weak LM hashes:
    - » Attention: Will not allow connecting from Windows ME/98/… computers any more!
    - » Disabled by default from Windows Vista onwards
  - → Set the registry key HKLM\SYSTEM\CurrentControlSet\Lsa\NoLMHash to 1

Questions?

Thank you for your attention!