cybersecurity centre

GCHQ Academic Centre of Excellence EPSRC

CyberSecuritySoton.org [w]

@CybSecSoton [fb & tw]

UNIVERSITY OF Southampton

# COMP6224
# User Authentication – Passwords Cracking Part 1

Dr Federico Lombardi

f.lombardi@soton.ac.uk

# Lecture Outline

- Password Attacks
  - Online Attacks
  - Offline Attacks
- Countermeasures
- Hash Cracking
- Introduction to John The Ripper

# Online Dictionary Attack

- ONLINE = Intelligent search
  - Try passwords associated with the user
    - e.g name, name of friends, car brand
  - Try words in a dictionary
  - Try popular passwords

- Save attacker's time

- No guarantee the right password is found

# Possible Countermeasures

- **Password policies**
  - Set password length: minimal password length should be prescribed
  - Set Password format: mix upper and lower case symbols, numerical, and non-alphabetical symbols
  - Avoid obvious passwords:12345, Forever1, John3:16, Monster1, Chicken1, …
- **Changing passwords**
  - Force users to change password regularly
- **Machine-generated passwords**
  - Pronounceable passwords are generated for the user

# Password count

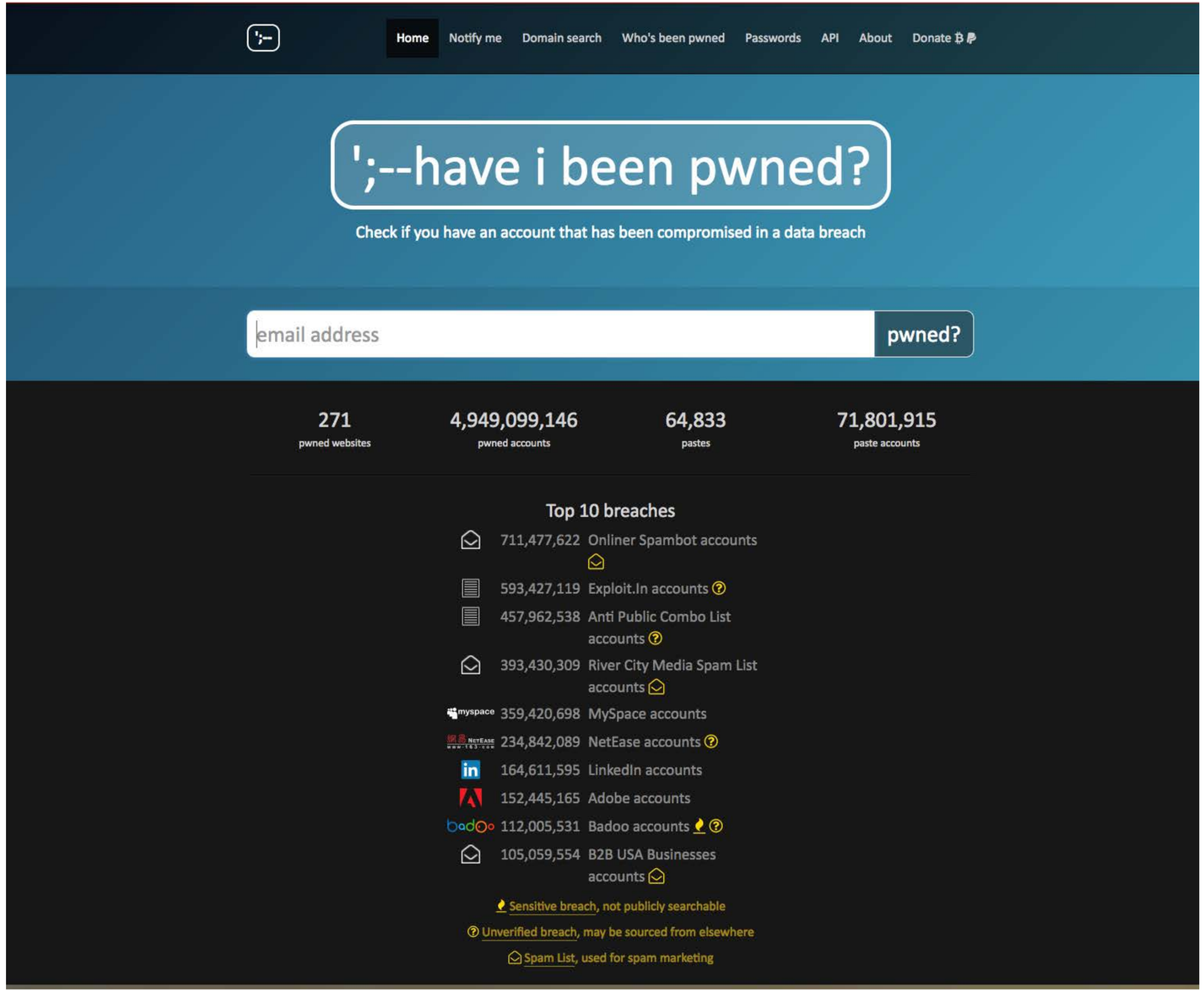
| | Count | Password | | Count | Password |
|---|---|---|---|---|---|
| 1 | 9218720 | 123456 | 21 | 370652 | 666666 |
| 2 | 3103503 | 123456789 | 22 | 354784 | 123 |
| 3 | 1651385 | qwerty | 23 | 347187 | monkey |
| 4 | 1313464 | password | 24 | 343864 | dragon |
| 5 | 1273179 | 111111 | 25 | 311371 | 1qaz2wsx |
| 6 | 1126222 | 12345678 | 26 | 300279 | 123qwe |
| 7 | 1085144 | abc123 | 27 | 299984 | 121212 |
| 8 | 969909 | 1234567 | 28 | 298938 | myspac |
| 9 | 952446 | password1 | 29 | 291132 | a123456 |
| 10 | 879924 | 1234567890 | 30 | 276473 | qwe123 |
| 11 | 866640 | 123123 | 31 | 270488 | 1q2w3e4r |
| 12 | 834468 | 12345 | 32 | 268121 | zxcvbnm |
| 13 | 621078 | homelesspa | 33 | 263605 | 7777777 |
| 14 | 564344 | iloveyou | 34 | 255079 | 123abc |
| 15 | 527158 | 1q2w3e4r5t | 35 | 250732 | qwerty123 |

# Further **Countermeasures**?

# Other Countermeasures (more effective)

- **Lockout mechanics**
  - Lock user account after several unsuccessful login attempts
- **Throttling**
  - Time delays are introduced between consecutive failed login attempts
- **Protective monitoring**
  - Monitoring login to detect unusual use
  - Notify the user with details of attempted login
- **Password blacklisting**
  - Check if an input password is in a list of common words

# Password blacklisting



# Offline Dictionary Attack

- OFFILINE = Attacker gains access to the password file
- Attacker obtains “encrypted password” or “ hashed password”
- Attacker tries passwords from a “dictionary” of commonly used passwords and compares with encrypted or hashed password
- This attacks with current processor speeds take hours or days or even less

UNIVERSITY OF Southampton

# Pastebin is an online service where hackers store breached password

New | Clone | Raw text | QR code

```
available databases [6]:
[*] information_schema
[*] Sql468241_1
[*] Sql468241_2
[*] Sql468241_3
[*] Sql468241_4
[*] Sql468241_5

+----+----------+-----------------------------------+------------+-------------------------+-------------+--------------+---------------+----------------
-----+---------------------+
| ID | user_url | user_pass                         | user_login | user_email              | user_status | display_name | user_nicename | user_registered
| user_activation_key |
+----+----------+-----------------------------------+------------+-------------------------+-------------+--------------+---------------+----------------
-----+---------------------+
| 1  | <blank>  | $P$Bzce[redacted]ijTM6dt5. | admin      | f[redacted]o@b[redacted]ia.it | 0           | admin        | admin         | 2012-04-17
14:28:00 | <blank>             |
+----+----------+-----------------------------------+------------+-------------------------+-------------+--------------+---------------+----------------
-----+---------------------+

+----+----------------+----------------------+
| id | username       | password             |
+----+----------------+----------------------+
| 1  | do[redacted]com | 14[redacted]014 |
+----+----------------+----------------------+
```

# Pepe (Post Exploitation Pastebin Emails)

UNIVERSITY OF Southampton

```
-----------------------Found email [redacted]@hotmail.com with password [redacted]-----------------------
---Have I Been Pwned---
Exactis
LinkedIn
YouveBeenScraped
---Pipl---
----------------------Found email [redacted]@live.com with password [redacted]1----------------------
---Have I Been Pwned---
LinkedIn
MyFitnessPal
OnlinerSpambot
YouveBeenScraped
---Pipl---
Name: Charlie [redacted]
Jobs:
Director - [redacted] at [redacted]
[redacted] Director at [redacted]
Co-Owner at [redacted]
Owner and Managing Director [redacted]
[redacted]
https://www.linkedin.com/in/[redacted]
http://[redacted].com/
```

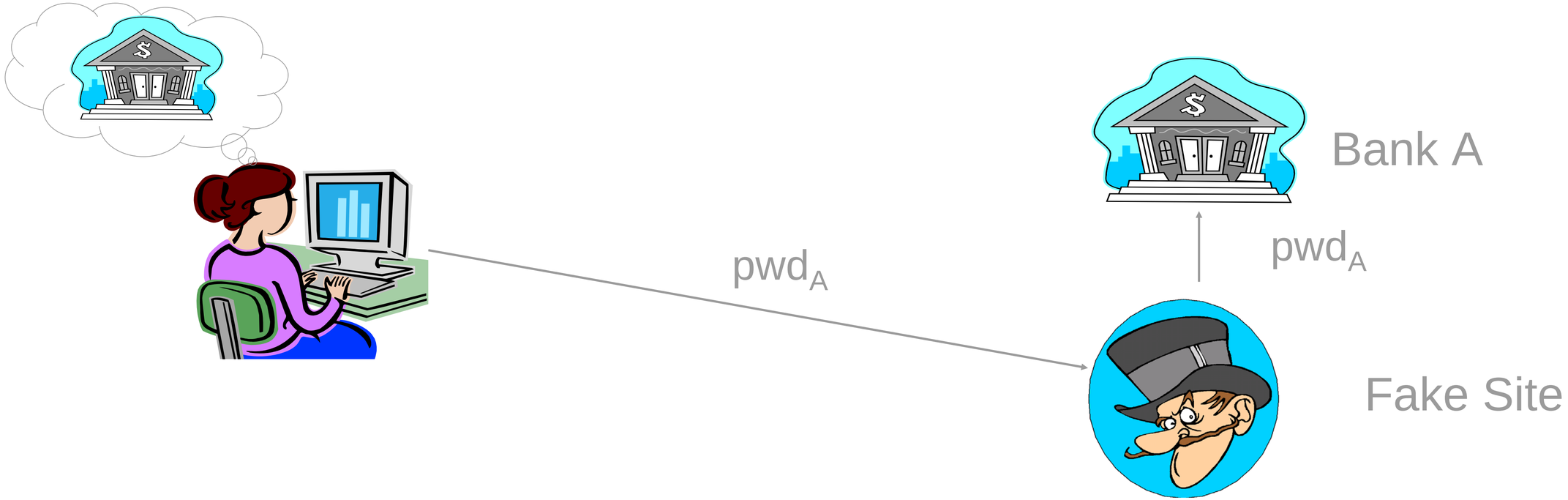
# Countermeasures

- **Password salting**
  - Append to the password a random number (salt)
  - If the salt is *b* bits, the number of possible passwords is increased of factor $2^b$

- **Password file access control**
  - Restrict access only to privileged users
  - Keep the hashed passwords separated from userIDs

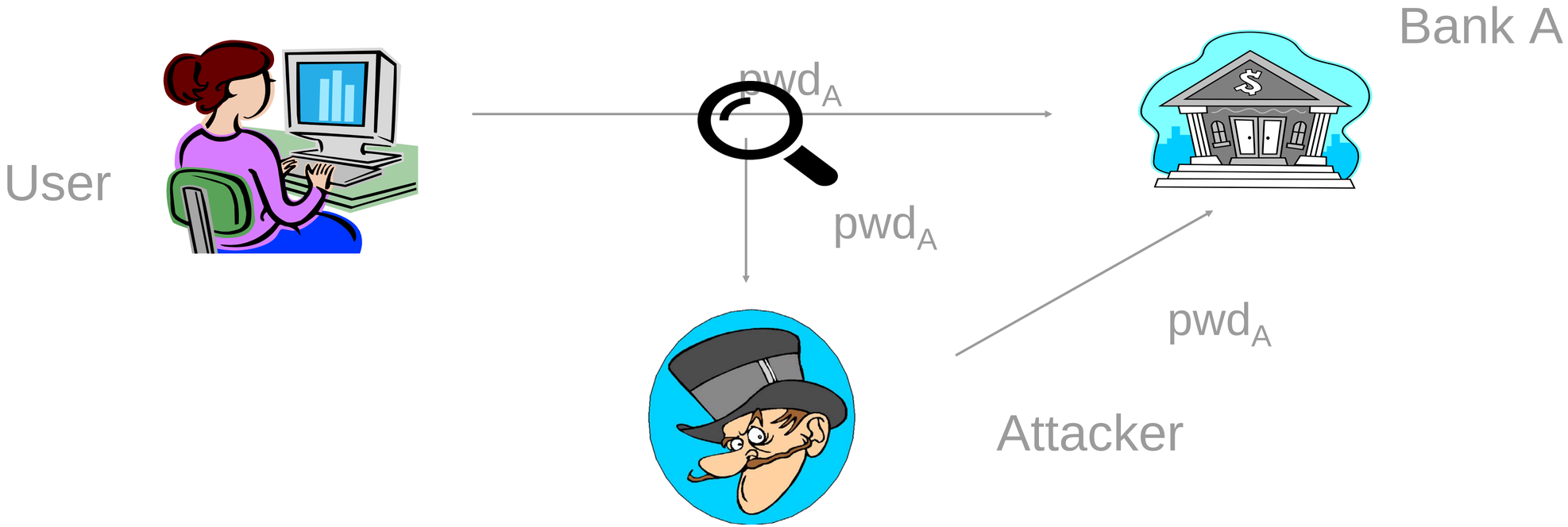
- **Fast reissuance of password**

# Social Engineering: Phishing




- Captured password can be used at target site
- **Countermeasure**: server-side authentication e.g SSL/TLS

# Interception




- Clear text password is intercepted by the attacker
- **Countermeasure:** Encrypt the communication among users and web site e.g SSL/TLS protocols

# Keylogger

- Small program that monitors each keystroke the user types on his keyboard
- Installed by attaching the program to an image or file and then send it via email
- Popular keyloggers
  - Refog
  - Revealer
  - KidLogger

# Other attacks

- **Shoulder-surfing**
  - Attacker gathers passwords by watching over a person's shoulder while he/she is logging in

- **Dumpster-diving**
  - Attacker look into the trash for piece of papers or documents with written passwords

- **Countermeasure**: User Awareness and Training

# Password Cracking in Practice

- **Windows stores the hashes of user passwords into the SAM database**
- **If you can steal the SAM database you can try to hack them… how?**

User SID HASHES

```
Administrator:500:e52cac67419a9a224a3b108f3fa6cb6d:8846f7eaee8fb117ad06bdd830b7586c:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1000:214c1f5d621f7dbbbc7b0f552c530719:c1c40b8b19e995748bba99667e3049d6:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:af01dfe386ba890a36e779f03a8f0a42:::
Fred:1003:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Fede:1004:bf6055b589337675e68aa26a841a86fa:ec8d06918467bb62e0ce0fb39444a33e:::
SUPPORT:1005:9c2a030f0b086b69aad3b435b51404ee:b23a90d0aad9da3615fafc27a1b8baeb:::
```

# Password Cracking Tools



## L0phtcrack

Extracts hashes from local or remote machines

Sniffs passwords from local network
(if used with an admin account)

## Pwdump

Command-line tool that can bypass SYSKEY encryption of the SAM (if you have admin rights)

Collects hashes and can store as text file

# We have the hashes… but we don’t have the passwords



We have to crack the hash to obtain the password

How to crack the hashes?

Let’s see some password cracking tools

# Password Cracking methods

UNIVERSITY OF Southampton

## Brute Force

- Uses combination of random numbers and characters
- Crack can take hours, years, or decades depending on password length and complexity
- 100% successful (eventually you will find the password)

## Dictionary

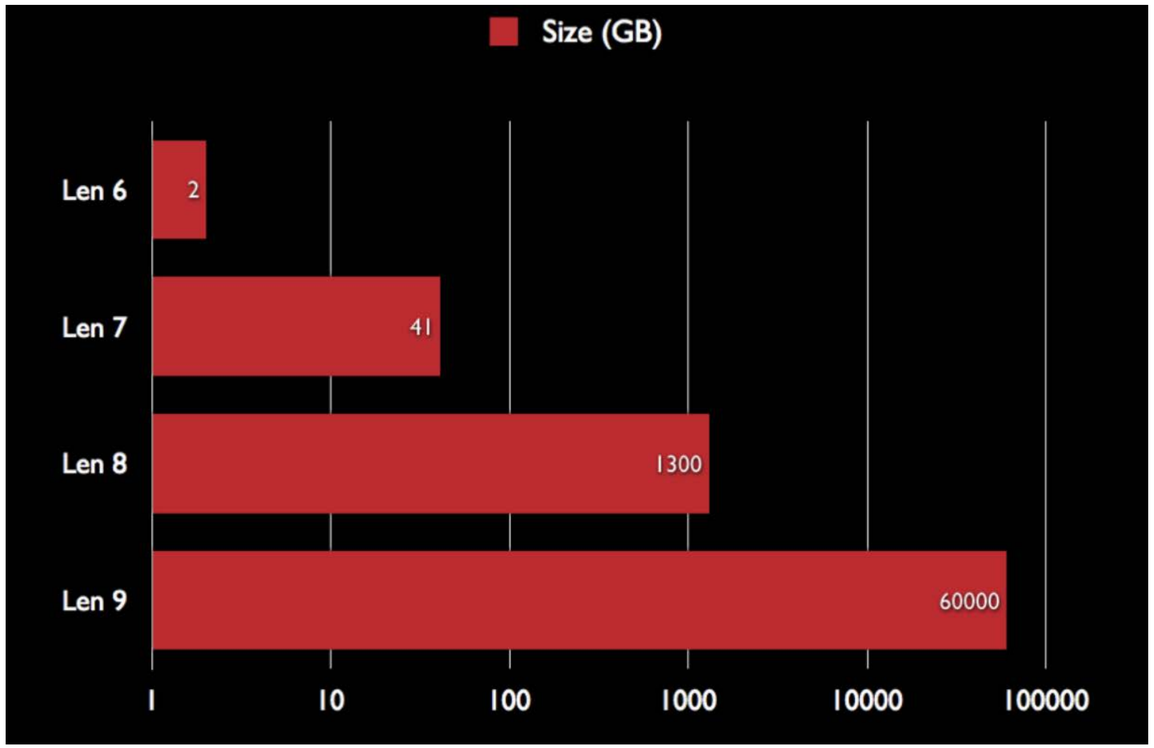
- Uses a dictionary or word list to crack password
- Quickest attack method
- Only as good as your dictionary
- Rainbow Tables (precomputed table for reversing cryptographic hash functions)

## Hybrid

- Combine dictionary or word list and prepends or appends characters and numbers to a base word
- More time than dictionary, less than brute force
- Example: password, 1password, password123, p@ssw0rd, …

# Dictonary Size

- A good dictionary may be huge
- According to the size of the password you may have hunderd of Terabytes of combination to try
- Reconnaissance phase can help to write down important keyword to start with



# John the Ripper (aka JTR or John)



- **John** is a fast brute-force/dictionary password cracker
- Its primary purpose is to detect weak passwords
- Support many password formats
  - crypt(3) password hash types (Unix)
  - LM hashes (Windows SAM database)
  - plus lots of other hashes and ciphers in the community-enhanced version
- **Limit**: Passwords cracked are not case-sensitive (Passwd = PASSWD)

# JTR example against a SAM database



Let's try to hack the SAM database we stolen

Put in a txt file the row of the user we are interested to crack

in our example it will be winpass.txt

Crack the hash:

```
$ john --format=LM --user=Fede Desktop/winpass.txt
```

See the result:

```
$ john --format=LM --user=Fede Desktop/winpass.txt --show
```