cybersecurity centre

GCHQ Academic Centre of Excellence EPSRC

CyberSecuritySoton.org [w]

@CybSecSoton [fb & tw]

UNIVERSITY OF Southampton

COMP6224
User Authentication – Passwords Cracking
Part 2

Dr Federico Lombardi

f.lombardi@soton.ac.uk

Lecture Outline

- Dictionary Attacks
- Rainbow Table
- How to securely store passwords

Exercise 1

- Assume that you are only allowed to use the 26 letters of the alphabet to construct passwords
  - How many passwords are possible if a password is at most n = 4, 6, 8 characters long and there is no distinction between upper case and lower case characters?
  - How many different passwords are possible if a password is at most n= 4, 6, 8 characters long and passwords are case sensitive?
  - How can you compute the entropy of the following password: hellocomputer
  - If we replace the char ‘e’ with ‘3’ and the char ‘o’ with ‘0’, are we increasing the security of the passwords?
  - Time: 10 min

Problem for the attacker

If we have a domain of password big enough, **brute force** takes too time.

So, the attacker can use a **dictionary attack**, to save time… Is it enough for the attacker?

A dictionary should be different for the user to target

Exercise 2

Custom Dictionary for a target user.

Think about how to design a software that is able to create a dictonary for a target user.

Time 5 min

UNIVERSITY OF Southampton

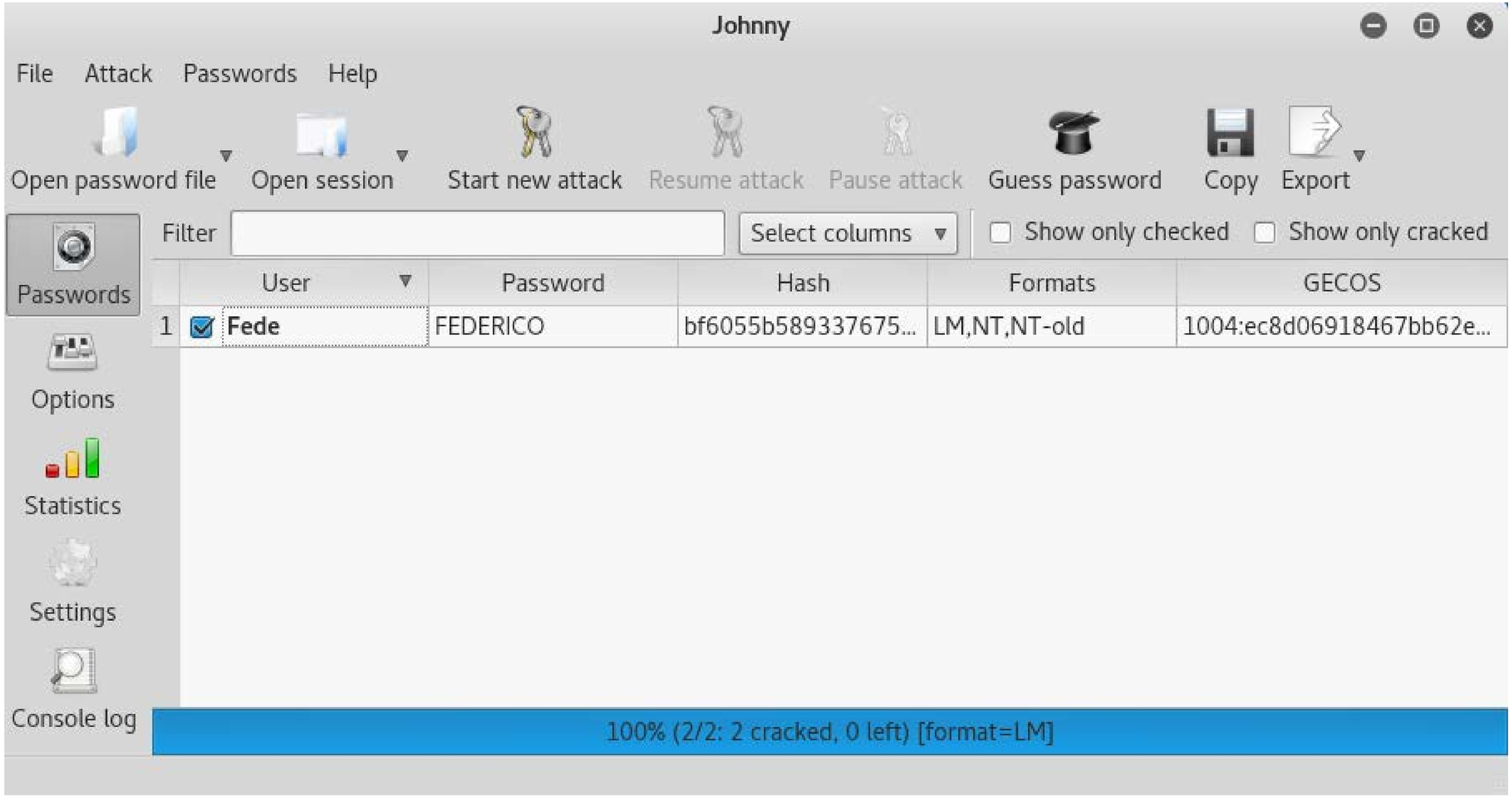
The Mentalist

Tool for custom wordlist generation

It utilizes common human paradigms for constructing passwords

Can output the full wordlist as well as rules compatible with Hashcat and JTR.

Johnny: GUI-based version of John the Ripper



Online cracking tool: Crackstation

UNIVERSITY OF Southampton

crackstation.net

Online tool containing over 100 TB of precomputed hashes

The word list is downloadable

CrackStation

Defuse.ca ·

CrackStation » Password Hashing Security » Defuse Security »

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

```
ec8d06918467bb62e0ce0fb39444a33e
```

I'm not a robot

reCAPTCHA
Privacy - Terms

Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
ec8d06918467bb62e0ce0fb39444a33e	NTLM	federico

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

Hashcat

Hashcat is the (self-proclaimed) world's fastest password recovery tool

It takes as input a list of hashes and some rules to find the password that generates that hash

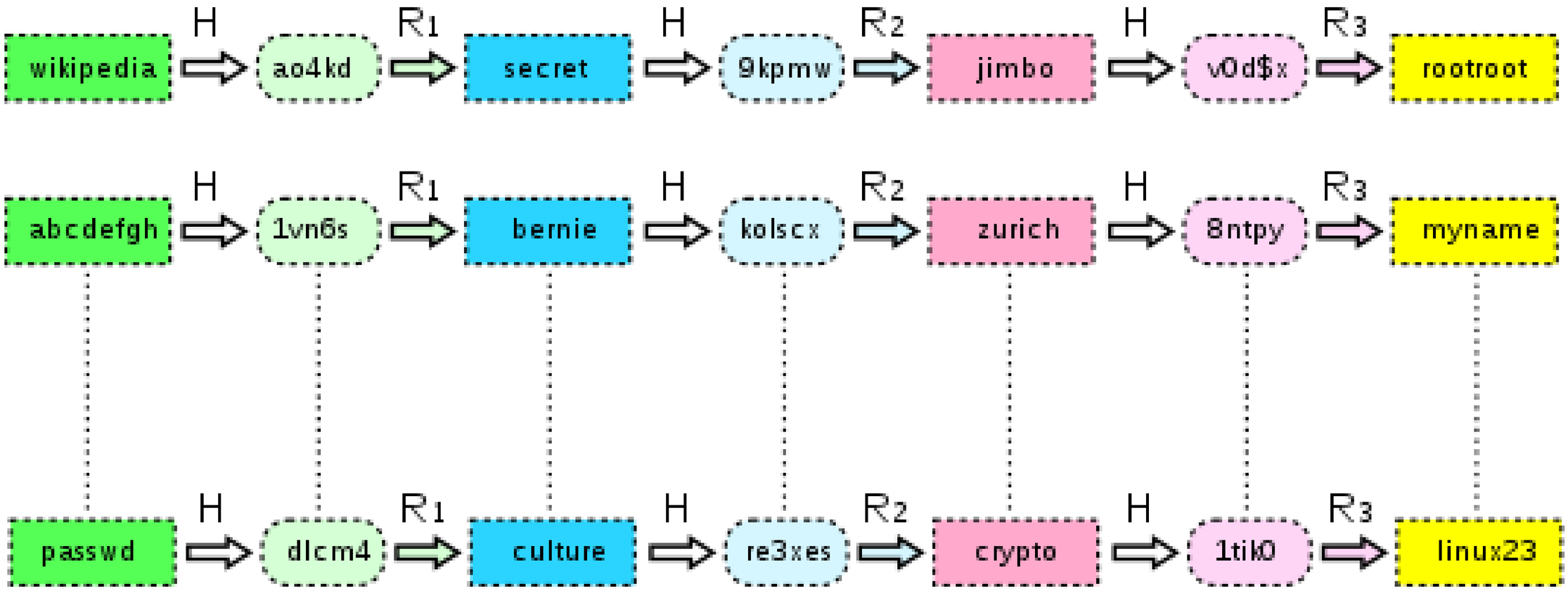
./hashcat -a <mode> file.hash

Usually executed with GPU-based servers to speed up the cracking process

How to revert a hash? Rainbow Table

Rainbow Table: Precompited table with the association <password, hash>

- H: hash function
- R: reduction functions: generate a new password to be hashed



Rainbow Table:

0) precompute the rainbow table and store only first and last plaintext

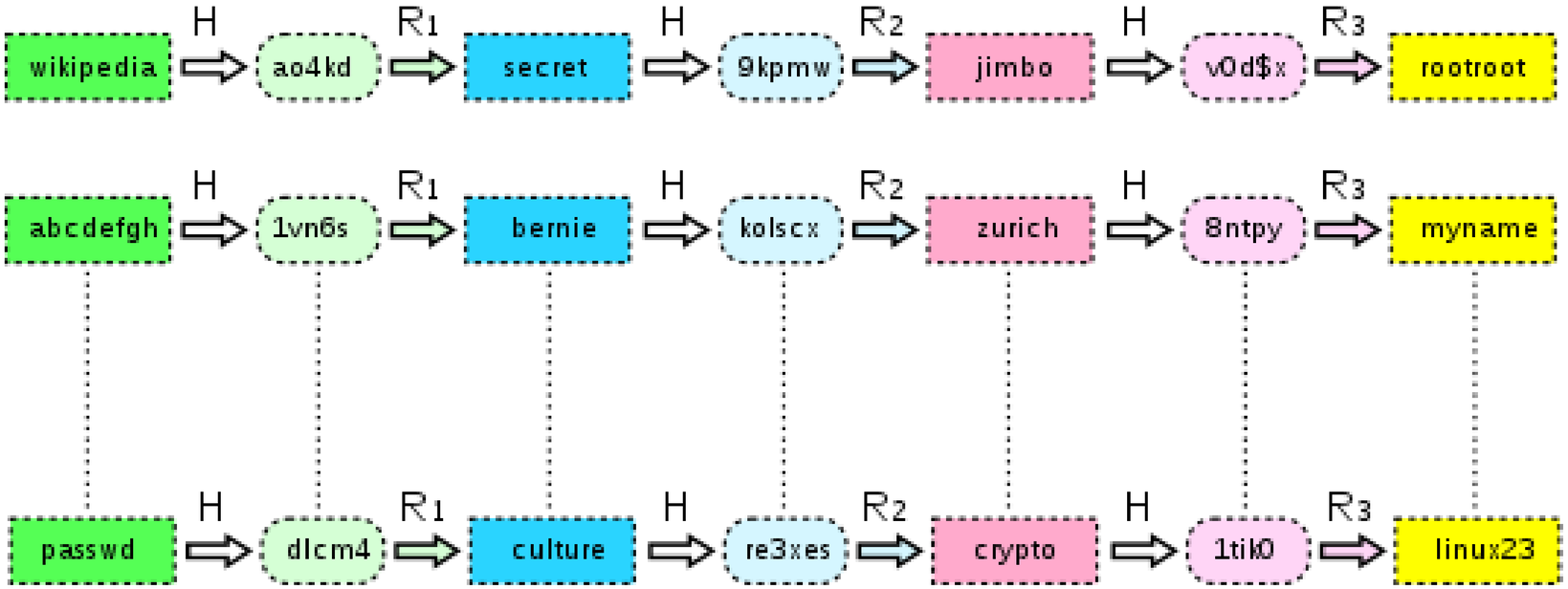
1) From an hash (re3xes) compute R3. Is the plaintext generated (rambo) in the stored table? No!

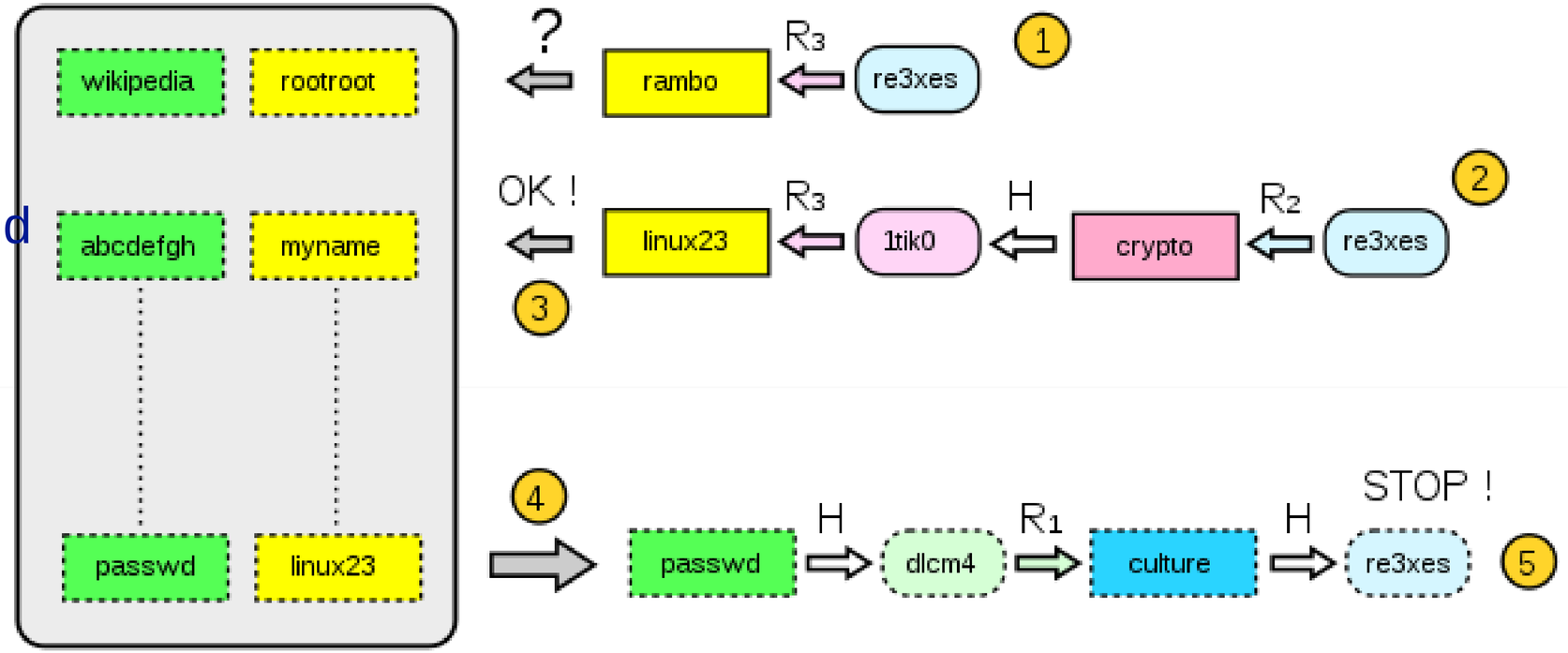
2) Redo step 1 with R2 & R3: R2->crypto->R3->linux23.

3) Is linux23 in the table? YES

4) Get the chain where linux23 is and start computing the hashes from «password»

5) Stop when you find the plaintext that hashed give you re3xes





Motivation

UNIVERSITY OF Southampton

Why Rainbow Table?

Because is a good tradeoff between space and time!

Storing all possible couple <password, hash> requires too space

Brute forcing all possible hashes requires too many time

With rainbow table you store only 2 plaintext for each row and compute few hashes for iteration

RainbowCrack

RainbowCrack is a software to crack hashes through **Rainbow Table.**

A brute force hash cracker generate all possible plaintexts.

Then computes the corresponding hashes on the fly.

Then compare the hashes with the hash to be cracked.

Once a match is found, the plaintext is found.

If all possible plaintexts are tested and no match is found, the plaintext is not found.

With this type of hash cracking, all intermediate computation results are discarded.

Download RainbowCrack

RainbowCrack 1.6.1 is released on April 25, 2015.

We strongly recommend 64-bit version of the software. As no more than 2 GB memory can be used by 32-bit application.

Version		Software	Operating System	GPU Acceleration
1.6.1		rainbowcrack-1.6.1-win32.zip	Windows 7/8 32-bit	NVIDIA AMD
		rainbowcrack-1.6.1-win64.zip	Windows 7/8 64-bit	
		rainbowcrack-1.6.1-linux32.zip	Linux 32-bit (x86)	No
		rainbowcrack-1.6.1-linux64.zip	Linux 64-bit (x86_64)	
1.6		rainbowcrack-1.6-win32.zip	Windows XP/Vista/7/8 32-bit	NVIDIA AMD
		rainbowcrack-1.6-win64.zip	Windows XP/Vista/7/8 64-bit	
		rainbowcrack-1.6-linux32.zip	Linux 32-bit (x86)	No
		rainbowcrack-1.6-linux64.zip	Linux 64-bit (x86_64)	
1.5		rainbowcrack-1.5-win32.zip	Windows XP/Vista/7/8 32-bit	No
		rainbowcrack-1.5-win64.zip	Windows XP/Vista/7/8 64-bit	
		rainbowcrack-1.5-linux32.zip	Linux 32-bit (x86)	No
		rainbowcrack-1.5-linux64.zip	Linux 64-bit (x86_64)	

How to store a password?

UNIVERSITY OF Southampton

Is this approach secure?

```sql
SELECT Username, U.PasswordHash, R.PasswordText
FROM dbo.[User] U
  JOIN dbo.Result R ON U.PasswordHash = R.PasswordHash
```

Results | Messages

	Username	PasswordHash	PasswordText
1	User3	bf787577ff656cde5b5d1f8236a75d2a	rootkit
2	User5	25d55ad283aa400af464c76d713c07ad	12345678
3	User9	22d7fe8c185003c98f97e5d6ced420c7	qwertyui
4	User13	e99a18c428cb38d5f260853678922e03	abc123
5	User16	5aca695374f4ee2032155a565ad78462	r00tk1t
6	User21	596a96cc7bf9108cd896f33c44aedc8a	fuckyou
7	User22	1bbd886460827015e5d605ed44252251	11111111
8	User24	0b4e7a0e5fe84ad35fb5f95b9ceeac79	aaaaaa

How to store a password?

UNIVERSITY OF Southampton

Is this approach secure? **NO!!! Never put the password in plaintext**

```sql
SELECT Username, U.PasswordHash, R.PasswordText
FROM dbo.[User] U
  JOIN dbo.Result R ON U.PasswordHash = R.PasswordHash
```

Results | Messages

	Username	PasswordHash	PasswordText
1	User3	bf787577ff656cde5b5d1f8236a75d2a	rootkit
2	User5	25d55ad283aa400af464c76d713c07ad	12345678
3	User9	22d7fe8c185003c98f97e5d6ced420c7	qwertyui
4	User13	e99a18c428cb38d5f260853678922e03	abc123
5	User16	5aca695374f4ee2032155a565ad78462	r00tk1t
6	User21	596a96cc7bf9108cd896f33c44aedc8a	fuckyou
7	User22	1bbd886460827015e5d605ed44252251	11111111
8	User24	0b4e7a0e5fe84ad35fb5f95b9ceeac79	aaaaaa

How to store a password?

UNIVERSITY OF Southampton

Ok.. Is this better?

```sql
SELECT Username, U.PasswordHash,
FROM dbo.[User] U
  JOIN dbo.Result R ON U.PasswordHash = R.PasswordHash
```

Results | Messages

	Username	PasswordHash
1	User3	bf787577ff656cde5b5d1f8236a75d2a
2	User5	25d55ad283aa400af464c76d713c07ad
3	User9	22d7fe8c185003c98f97e5d6ced420c7
4	User13	e99a18c428cb38d5f260853678922e03
5	User16	5aca695374f4ee2032155a565ad78462
6	User21	596a96cc7bf9108cd896f33c44aedc8a
7	User22	1bbd886460827015e5d605ed44252251
8	User24	0b4e7a0e5fe84ad35fb5f95b9ceeac79

How to store a password?

UNIVERSITY OF Southampton

Is this better? **Yes, but still not secure, the attacker may reverse the hash!**

```sql
SELECT Username, U.PasswordHash,
FROM dbo.[User] U
  JOIN dbo.Result R ON U.PasswordHash = R.PasswordHash
```

Results | Messages

	Username	PasswordHash
1	User3	bf787577ff656cde5b5d1f8236a75d2a
2	User5	25d55ad283aa400af464c76d713c07ad
3	User9	22d7fe8c185003c98f97e5d6ced420c7
4	User13	e99a18c428cb38d5f260853678922e03
5	User16	5aca695374f4ee2032155a565ad78462
6	User21	596a96cc7bf9108cd896f33c44aedc8a
7	User22	1bbd886460827015e5d605ed44252251
8	User24	0b4e7a0e5fe84ad35fb5f95b9ceeac79

How to avoid or mitigate a reverse password attack?

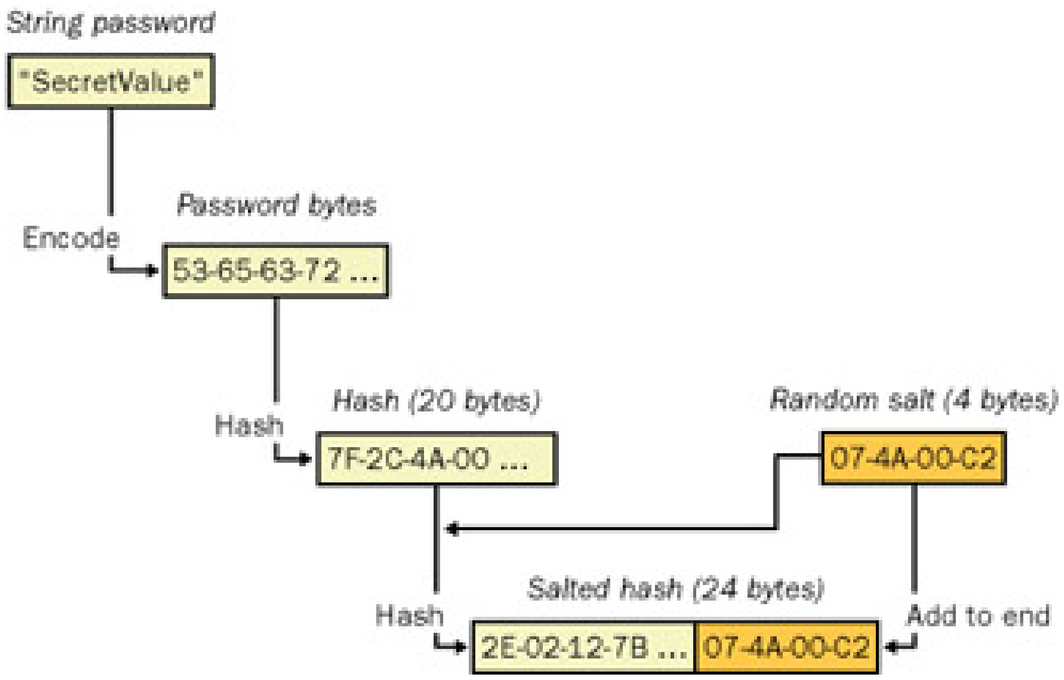
Password Hash + Salt

1) Compute the hash of the password

2) Add the random salt

3) Compute the hash of hashed passowrd + salt

4) Store the salted hash and the salt



What to store then?

```
SELECT Username, PasswordHash, Salt FROM dbo.[User]
WHERE Username LIKE 'Same%'
```

Results | Messages

	Username	PasswordHash	Salt
1	Same1	13b328b74183e310cafab8781184a367	08aVO318gCM=
2	Same2	cefcd39c0a019b7a04d9a63951d8981b	YdIa0VAQPLs=

Other alternative cracking tools

Cane and Able

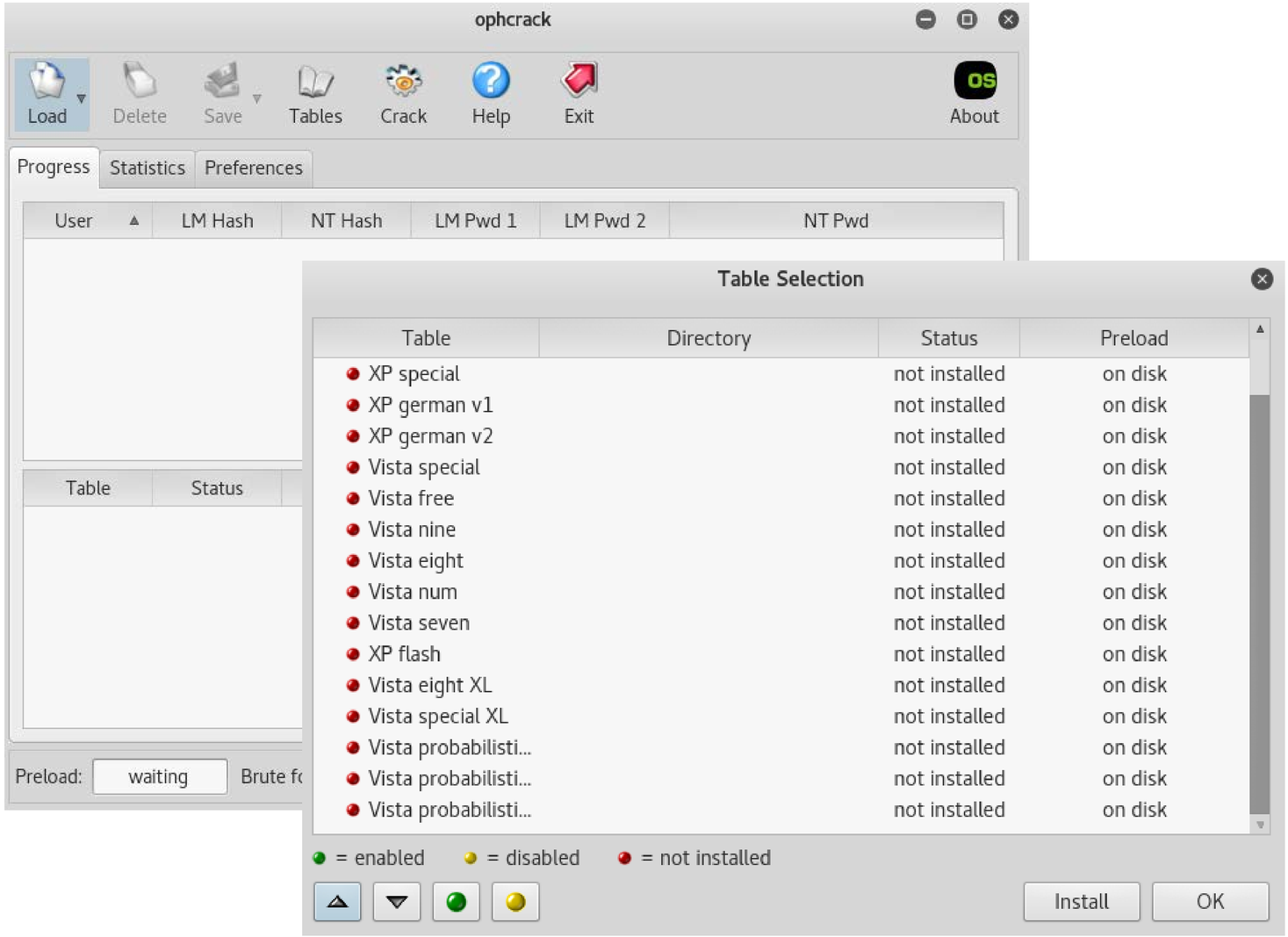
Multipurpose tool for password cracking, Windows enumeration, and VOIP sniffing in three ways:

- Dictionary
- Brute Force
- Rainbow Tables

Ophcrack

Uses rainbow tables for very fast password cracking

Ophcrack



- Rainbow Tables available to download from internet
- Different tables for each operativ system

Offline Cracking vs Online Cracking

UNIVERSITY OF Southampton

Offline Cracking:

We have a passowrd of a program to crack (like zip file)

Tools just described are excellent for that!

Online Cracking:

We have an online service to crack (like an ssh connection)

Hydra

A brute-forcing/dictionary tool for online services

Useful for services like ssh, ftp, etc…

Summary

- Password based authentication systems are not secure
  - Users use ease to guess passwords
  - Users reuse passwords across multiple web sites
- Password based authentication systems are vulnerable to various attacks
  - Social engineering and data breaches are on top of the list
- Effective countermeasures are
  - Account lockout and throttling
  - Predictive monitoring
  - Password blacklisting

Recommended Readings

- NCSC. Password Guidance: Symplifying your approach. Available at: https://www.ncsc.gov.uk/guidance/password-guidance-simplifying-your-approach
- NIST. New Digital Identity Guidelines. Available at: https://pages.nist.gov/800-63-3/
- Chapter 2. Goodric, Tamassia. Introduction to Computer Security.
- B.Stock, M. Johns. Protecting Users Against XSS-based Password Manager Abuse. ASIACCS 2014.
- Smart Cards and Mobile Device Authentication: An Overview and Implementation. NISTIR 7206, 2005.