We will rockyou2009, rockyou2021, rockyou2024

Tom Gries (TOMO) | September 2024

@tomo@chaos.social

2024-09-18

Legal Disclaimer - Hackerparagraf

Die hier vorgestellten Methoden und Tools dienen zum Schutz der eigenen Systeme. Das Knacken fremder Passwörter ebenso wie das Eindringen in Systeme kann eine Straftat darstellen. Die vorgestellten Tools können unter den Hackerparagrafen **202c StGB** fallen. Entsprechend dürfen Sie nur auf eigene Kennwörter oder Testsysteme losgehen, beziehungsweise sich schriftlich die Erlaubnis des Systembesitzers einholen.

Zudem können Cracking-Tools die getesteten Systeme stark beeinträchtigen oder außer Funktion setzen. Entsprechend vorsichtig sollten Sie bei Produktivsystemen sein.

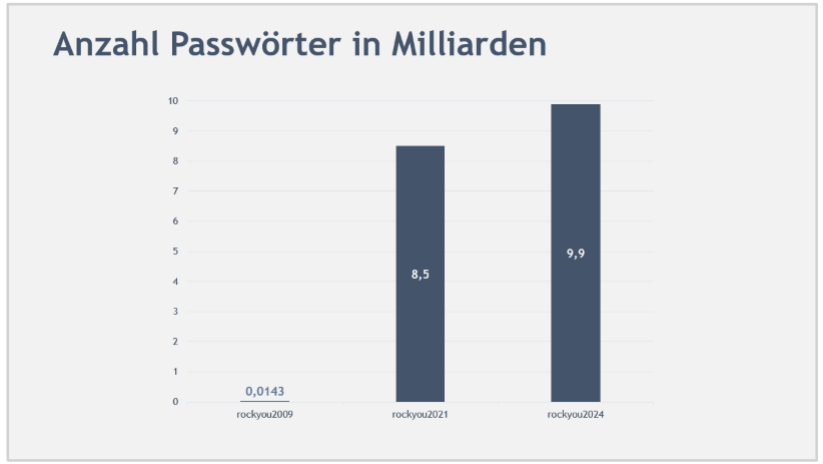
Die rockyou Wörterbücher

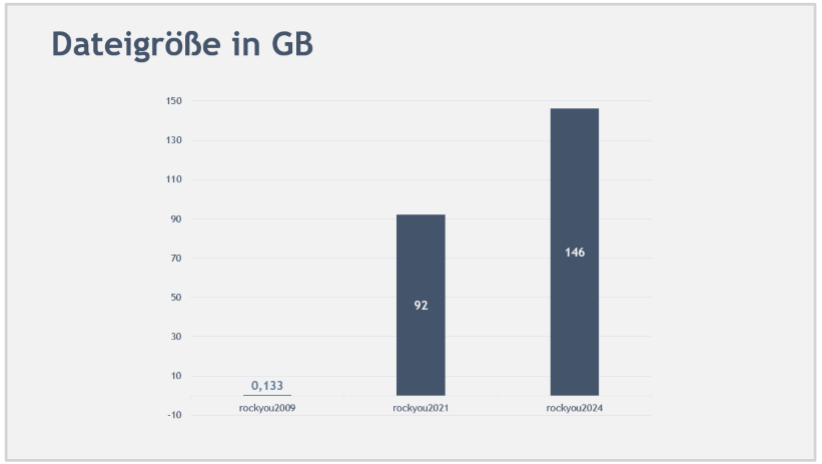
Ein erster Vergleich

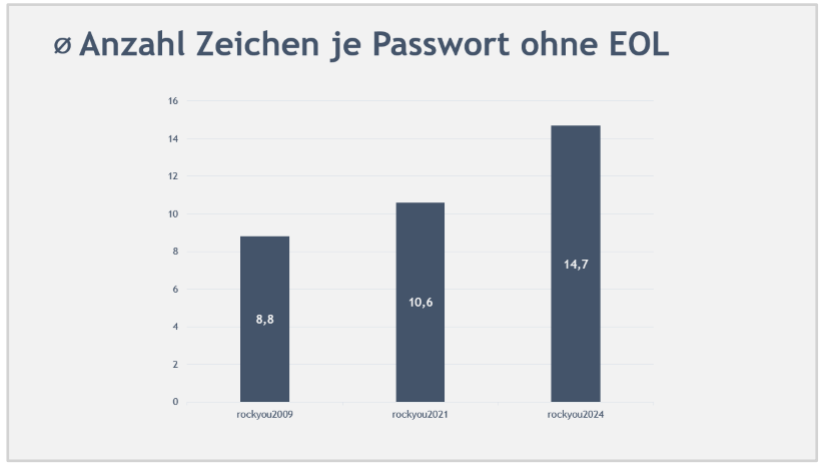
Die rockyou Dictonairies

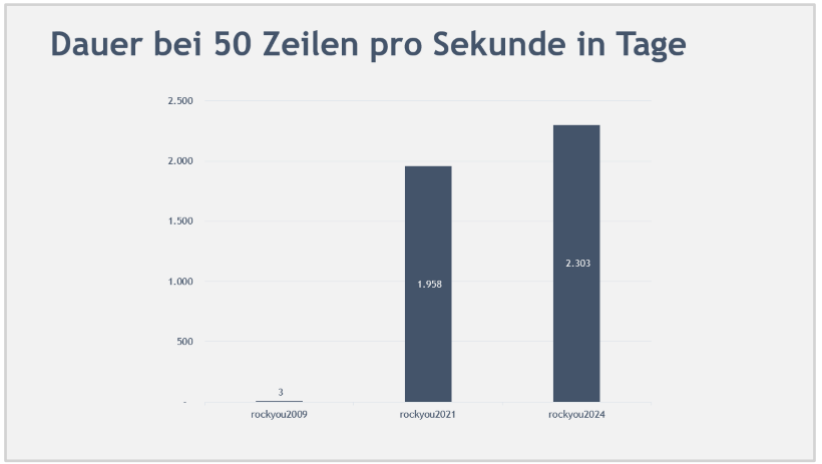
	rockyou2009	rockyou2021	rockyou2024
Passwords:	14 Millionen	8,5 Milliarden (x 600)	9,9 Milliarden (x 700)
Size:	133 MB 8,8 Zeichen/Passwort	92 GB (x 700) 10,6 Zeichen/Passwort	146 GB (x 1.100) 14,7 Zeichen/Passwort
Filetype:	UTF-8 text	ASCII text	Data
Line Ending:	LF (UNIX)	CRLF (DOS) / LF (UNIX)	

Die rockyou Dictonairies









Die Passwörter

Ein Blick ins Innere

Rockyou2009 - Auszug

head -5	+999.995	-9.995	tail -5
123456	bunnyta	#1badgurl	xCvBnM,
12345	bunnys4	#1badestgal	ie168
123456789	bunnyrock	#1badestchick	abygurl69
password	bunnyr	#1badest	a6_123
iloveyou	bunnypower	#1baddestbitch	*7¡Vamos!

Rockyou2021 - Auszug

head -5	+999.995	-9.995	tail -5
????l}2	!1nckert	~|cff3399ffcru~	~~~~~~~~~~~~~~~~~!
???c?	!1nckes	~|cffffCru~1995	~~~~~~~~~~~~~~~~~~
?\??c?	!1nckon	~|cffffCru~972	~~~~~~~~~~~~~~~~~!
_l?	!1ncks	~|cffffcru~1995	~~~~~~~~~~~~~~~~~~~
_q?6?	!1nckx	~|cffffcru~972	~~~~~~~~~~~~~~~~~~~~

Rockyou2024 - Auszug

head -5	+999.995	-9.995	tail -5
	!0ve!ygreen	□□□□□□□□1997756	□
	!0ve!ygummy	□□□□□□□□199796	□eliya@front.ru
5c163fa760d6fffd8ebf4	!0ve!ygur!	□□□□□□□□1997□□□	□udmila7800@rambler.ru
>#%m[V}"B	!0ve!ygur!s	□□□□□□□□1997□□□□	□a61na@gmail.com
@r	!0ve!yguy	□□□□□□□□1997□□□□mama	□d\x9E\xE5\xE7

Die Vorbereitung

Aufräumen der Wörterbücher

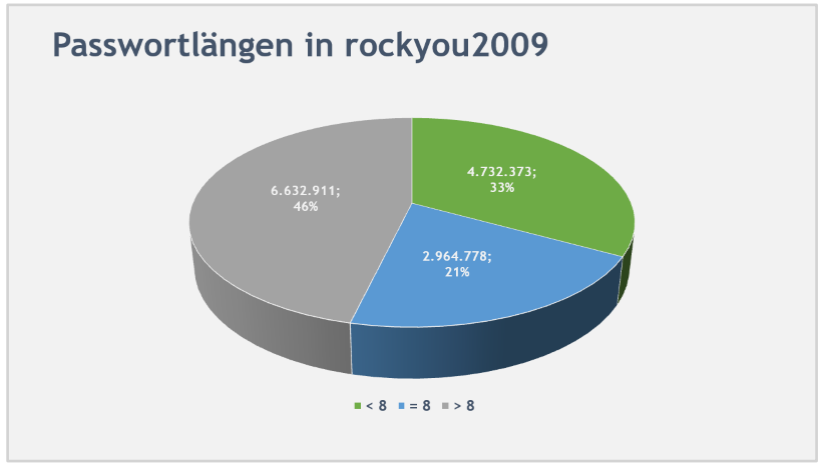
Aufräumen und vorbereiten

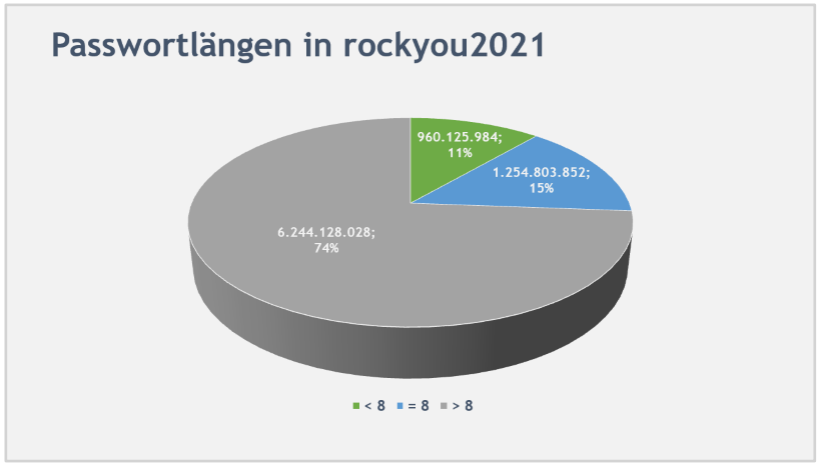
1. Alle Zeilen, die Nicht-ASCII Zeichen enthalten werden komplett entfernt (= asc).
2. Aufteilung in 3 Teile: <8 Stellen, =8 Stellen, >8 Stellen.
3. Für DES: Alles, was 9 oder mehr Stellen hat auf genau 8 Stellen kürzen, mit den originalen 8 Stellen zusammenfassen, sortieren und Doubletten entfernen (= combined8chars).
4. Die großen Wörterbücher rockyou2021 und rockyou2024 in kleinere Teile zerlegen (z. B. mit `split`), um die Schnittmengenbestimmung durchführen zu können (92 GB und 146 GB sind für die meisten Home Rechner zu groß).

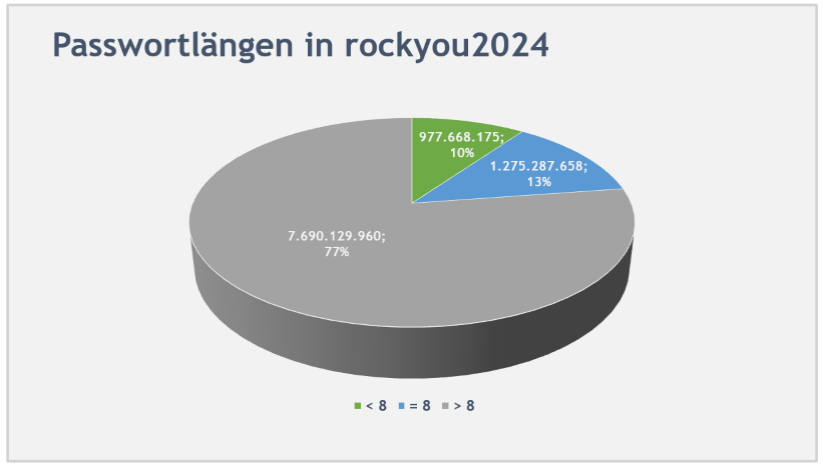
Ergebnis nach dem Aufräumen

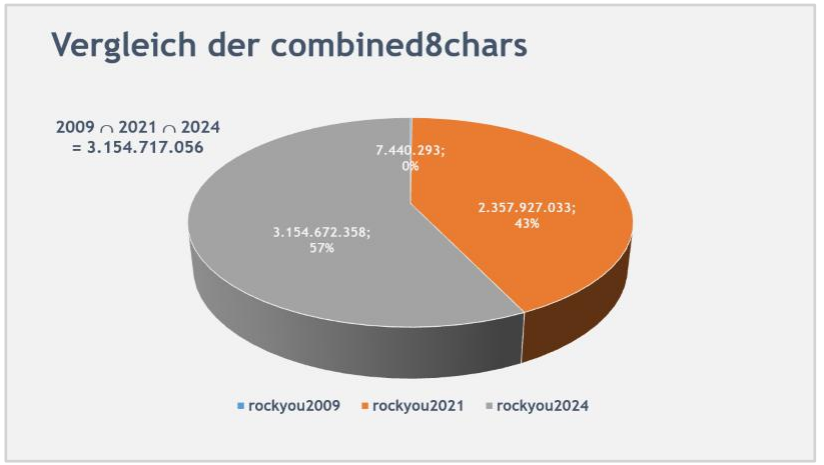
	rockyou2009	rockyou2021	rockyou2024
	14.344.391 Passwörter 133 MB	8.459.060.239 Passwörter 92 GB	9.948.575.739 Passwörter 146 GB
Time:	0:00:36 (asc) 0:00:12 (combined8chars) **0:00:48 Gesamt**	2:40:24 (asc) 2:29:33 (combined8chars) **5:09:57 Gesamt**	4:55:51 (asc) 3:16:30 (combined8chars) **8:12:21 Gesamt**
Records:	14.330.062 (asc) 7.440.293 (combined8chars)	8.459.057.864 2.357.927.033	9.943.085.793 3.154.672.358
Size:	139.682.934 (asc) 66.962.637 (combined8chars)	97.552.035.939 21.221.343.297	155.017.236.503 28.392.051.222
Filetype:	ASCII text	ASCII text	ASCII text
Line Ending:	LF (UNIX)	LF (UNIX)	LF (UNIX)

Passwortlängen im Vergleich





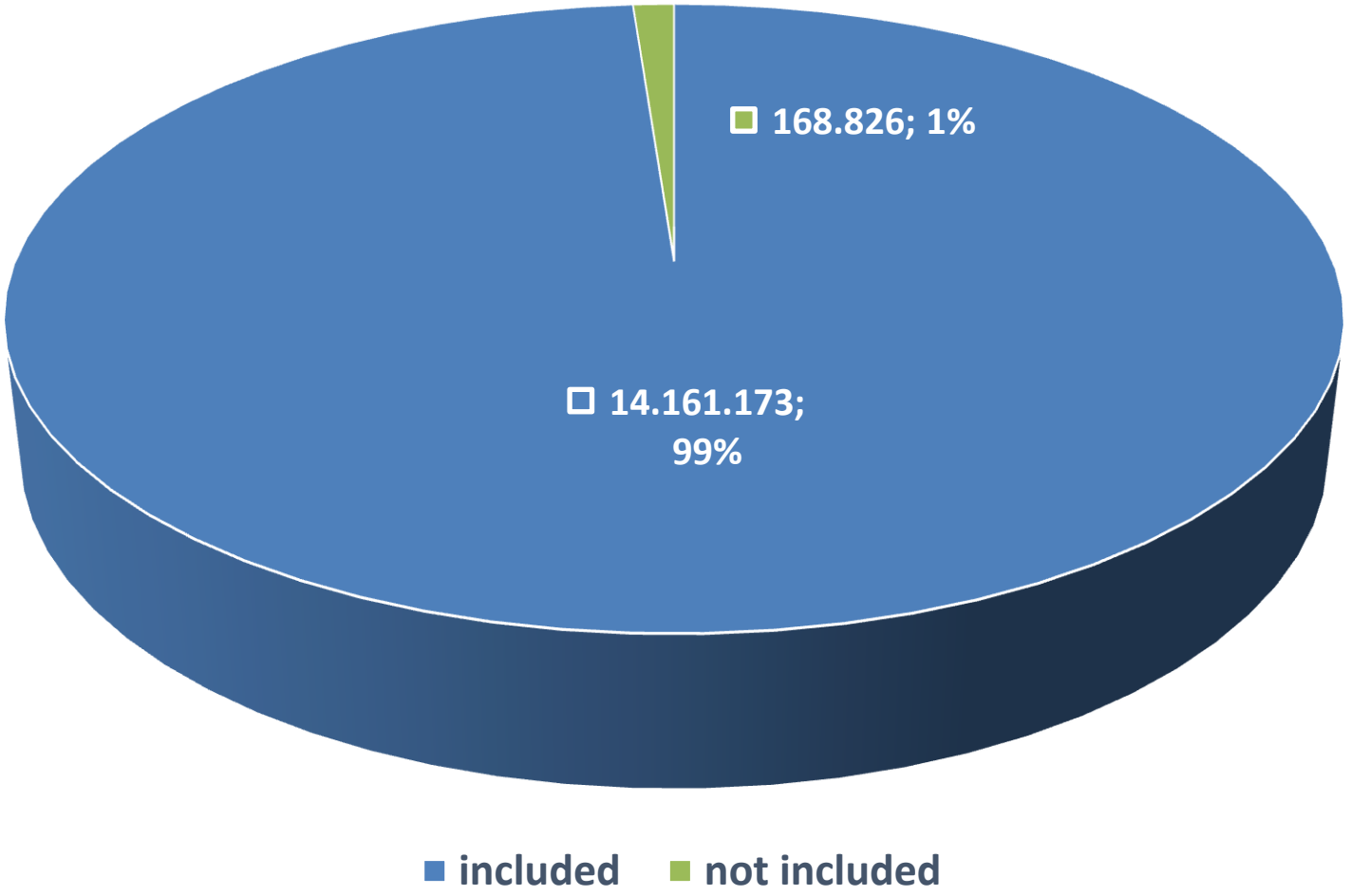




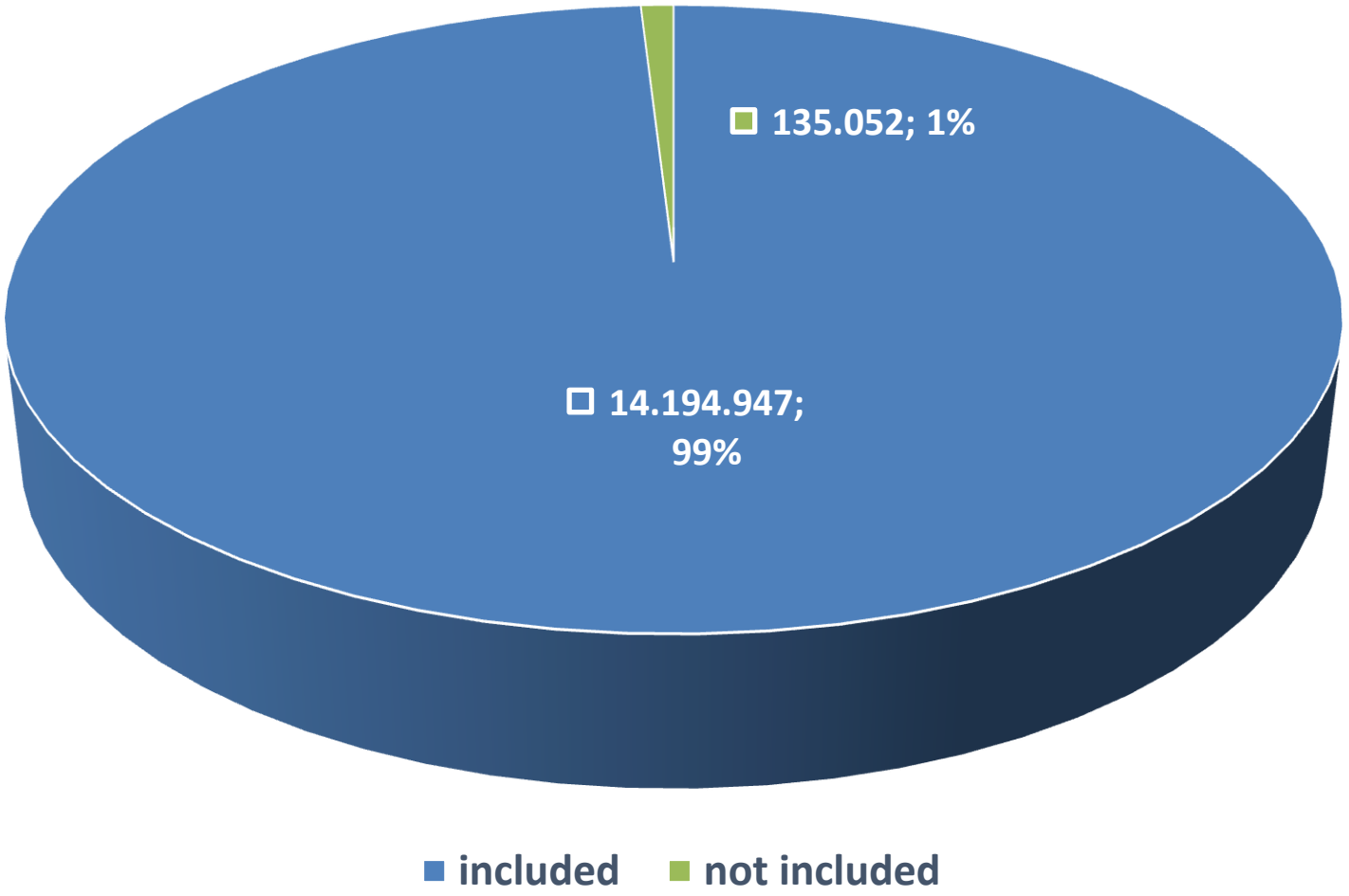
Schnittmengen

Anzahl der rockyou2009 Passwörter in den anderen beiden Wörterbüchern

Passwörter aus rockyou2009 in rockyou2021



Passwörter aus rockyou2009 in rockyou2024



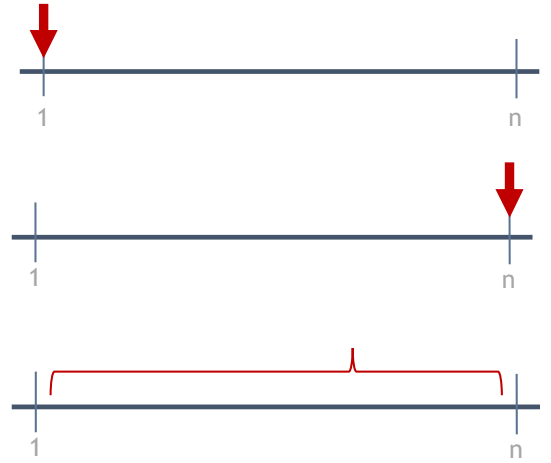
Let's crack

5.000 DES Hashe mit john und hashcat

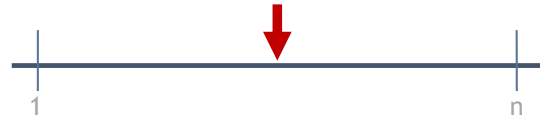
Wie lange dauert das cracken?

Passwortcracken ist endlich. Daher gibt es nur drei wesentliche Möglichkeiten, die man betrachten sollte beziehungsweise unterscheiden kann:

- Man findet das Passwort im ersten Versuch
- Man findet das Passwort im letzten Versuch
- Es liegt irgendwo dazwischen



Wenn man von einer Gleichverteilung ausgeht (nicht mit der Normalverteilung verwechseln), liegt die Wahrscheinlichkeit ein Passworthash zu cracken bei der halben Gesamtdauer (Gesamtcrackzeit ÷ 2).

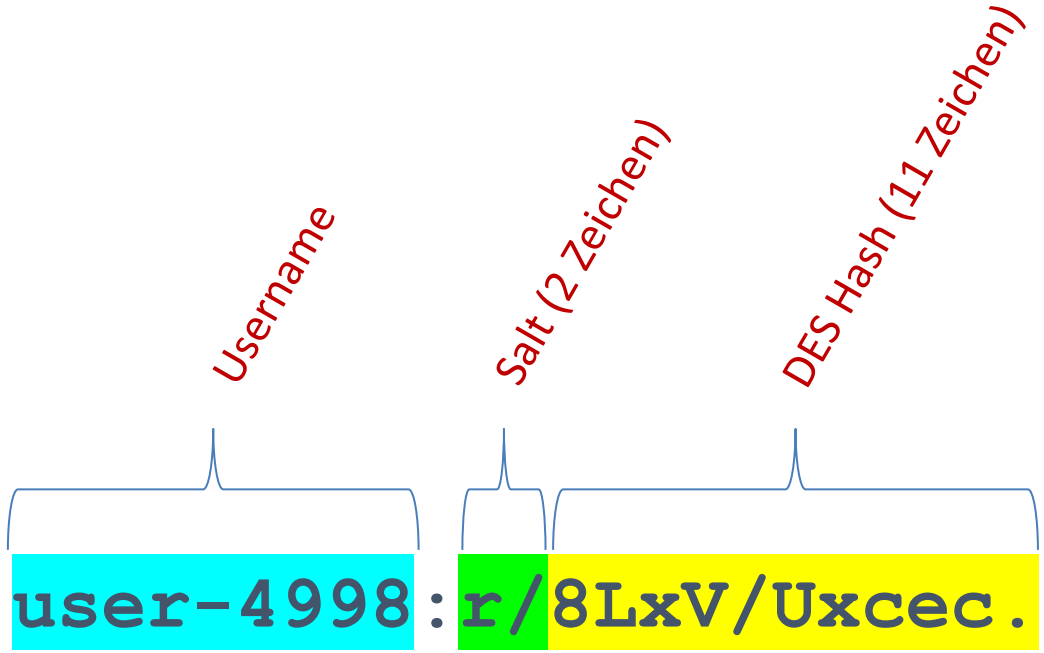


5.000 DES Passworthashe cracken

```
user-0001:p5pW88uib3DbA
user-0002:pcPHFxgkuhoMQ
user-0003:pzEgwiFCNiMtw
user-0004:q.0GnJiGgGQlA
user-0005:q/B4MmqJRVKMQ
user-0006:q1Oek8e12bt62
  .    .    .    .    .
  .    .    .    .    .
  .   (+ 4.990)    .
  .    .    .    .    .
user-4997:t/KGjE/vdEu/w
user-4998:r/8LxV/Uxcec.
user-4999:sQcsckBbkRc8Y
user-5000:t74t2w2PKj09g
```

Das verwendete Hashverfahren:

DES, Crypt, DES-Crypt, Standard DES



Ein paar Infos zu DES (descrypt, traditional)

⇒ DES war schon bei der Entwicklung Anfang der 1970er gegen differenzielle Kryptoanalyse resistent, obwohl diese Methode erst 1991 veröffentlicht wurde. Die DES-Entwickler beziehungsweise die NSA kannten die differentielle Kryptoanalyse schon über 15 Jahre vor der offiziellen Veröffentlichung.

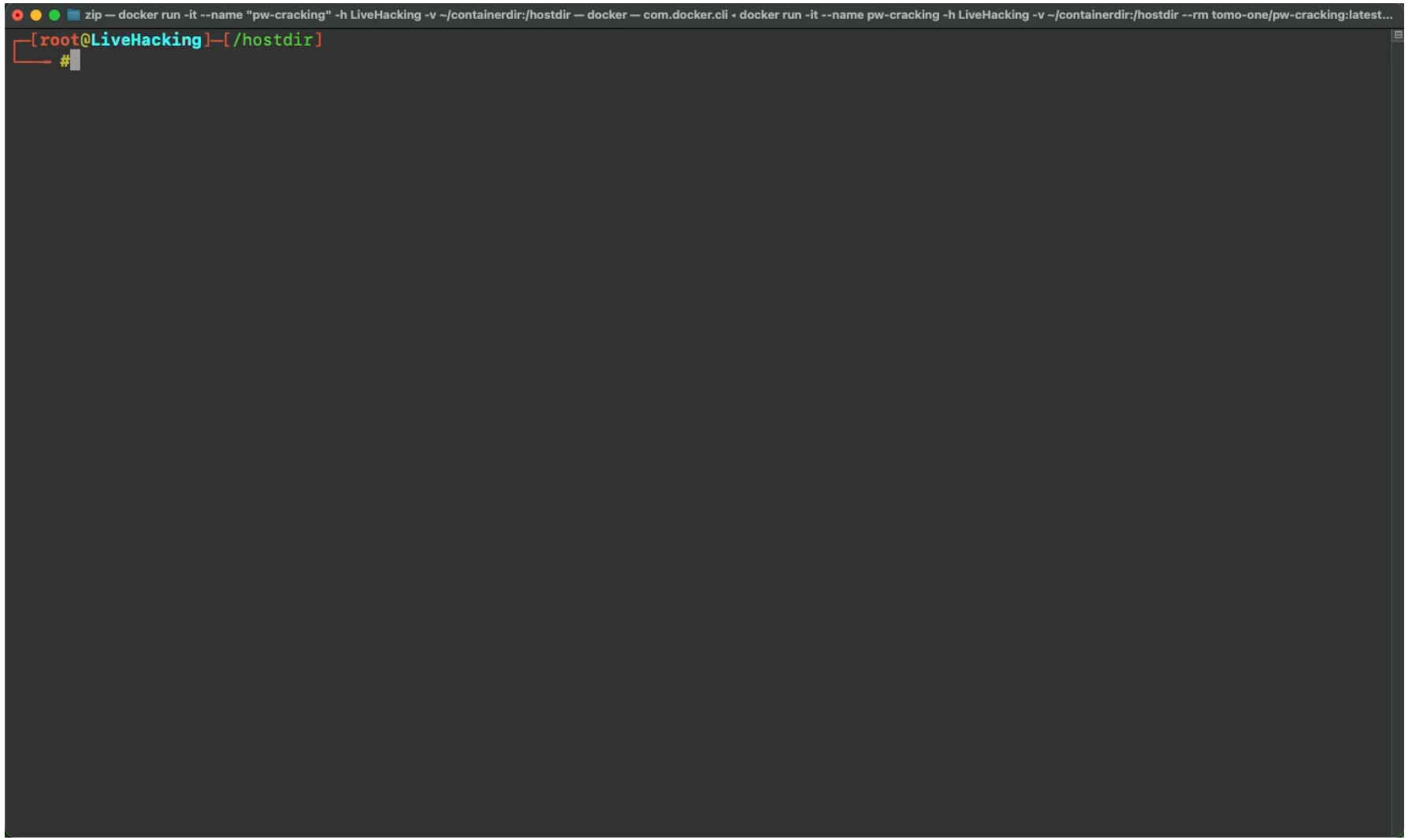
⇒ Der gesamte String besteht aus 13 Zeichen. Die ersten beiden Zeichen sind das Salt. Die verbleibenden 11 der eigentliche Hash. DES Hash ist theoretisch kollisionsresistent: 95^8 = 6.634.204.312.890.625 ≈ 6,6 x 10^15 vs. 64^11 = 73.786.976.294.838.206.464 ≈ 73.787 x 10^15 ≈ Faktor 11.000

⇒ DES kann nur einen Hash über maximal 8 Zeichen erzeugen und hat eine Schlüssellänge von 56 Bit (Kompromiss von NSA und IBM: 48/64 Bit).

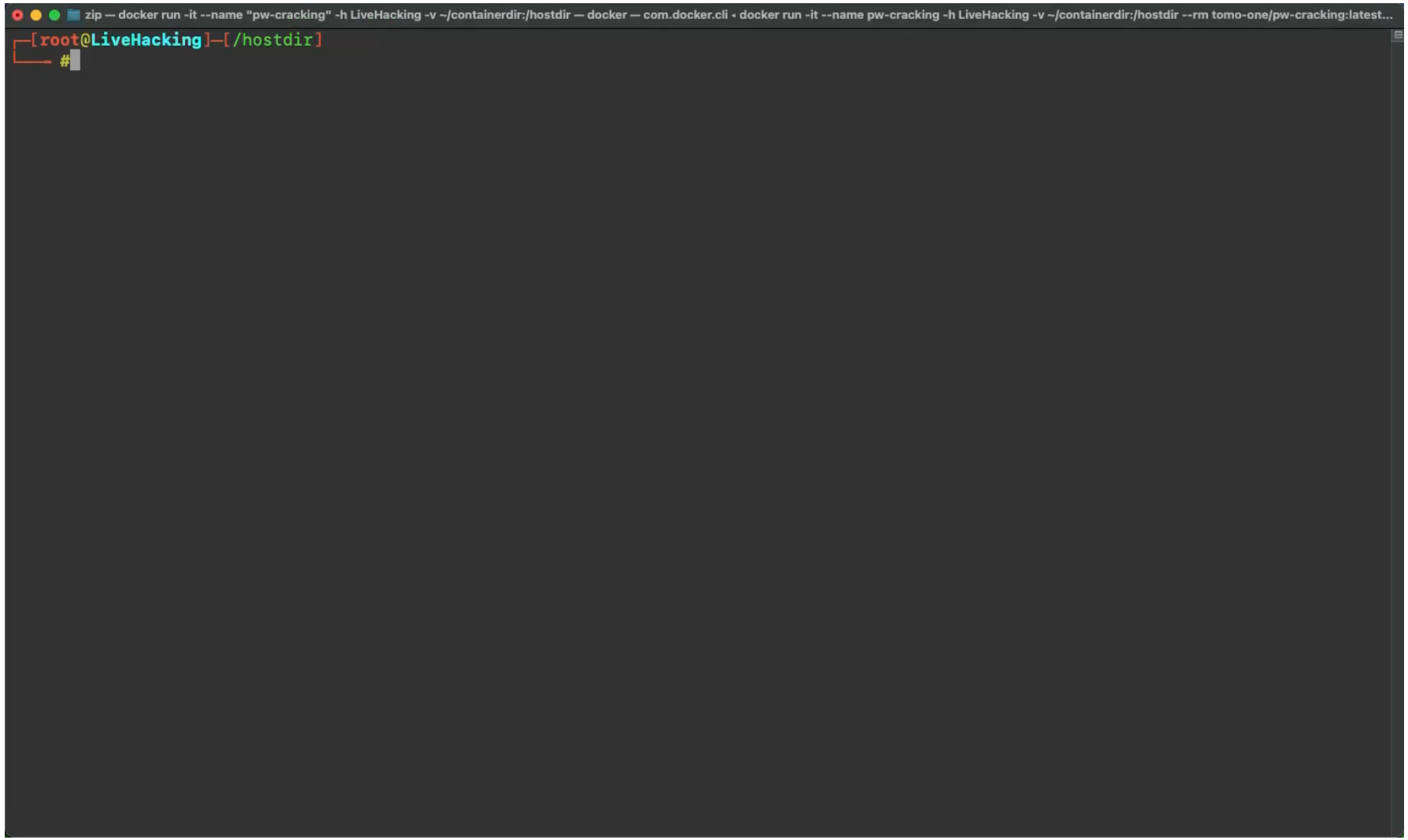
```
>>> des_crypt.hash("12345678", salt="x.")
'x.KxRJcXiV/jk'
```

```
>>> des_crypt.hash("123456789", salt="x.")
'x.KxRJcXiV/jk'
```

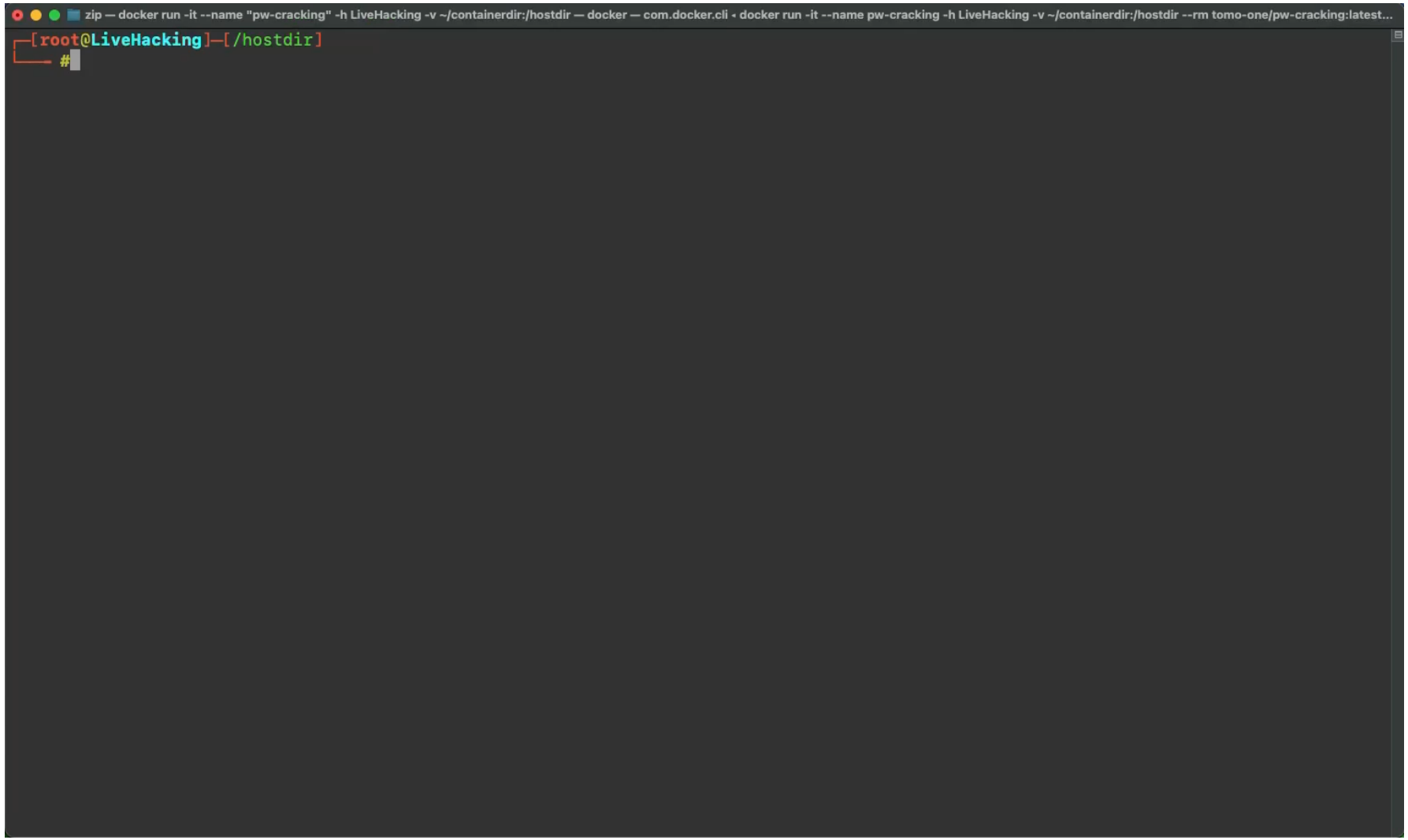
Cracken mit john



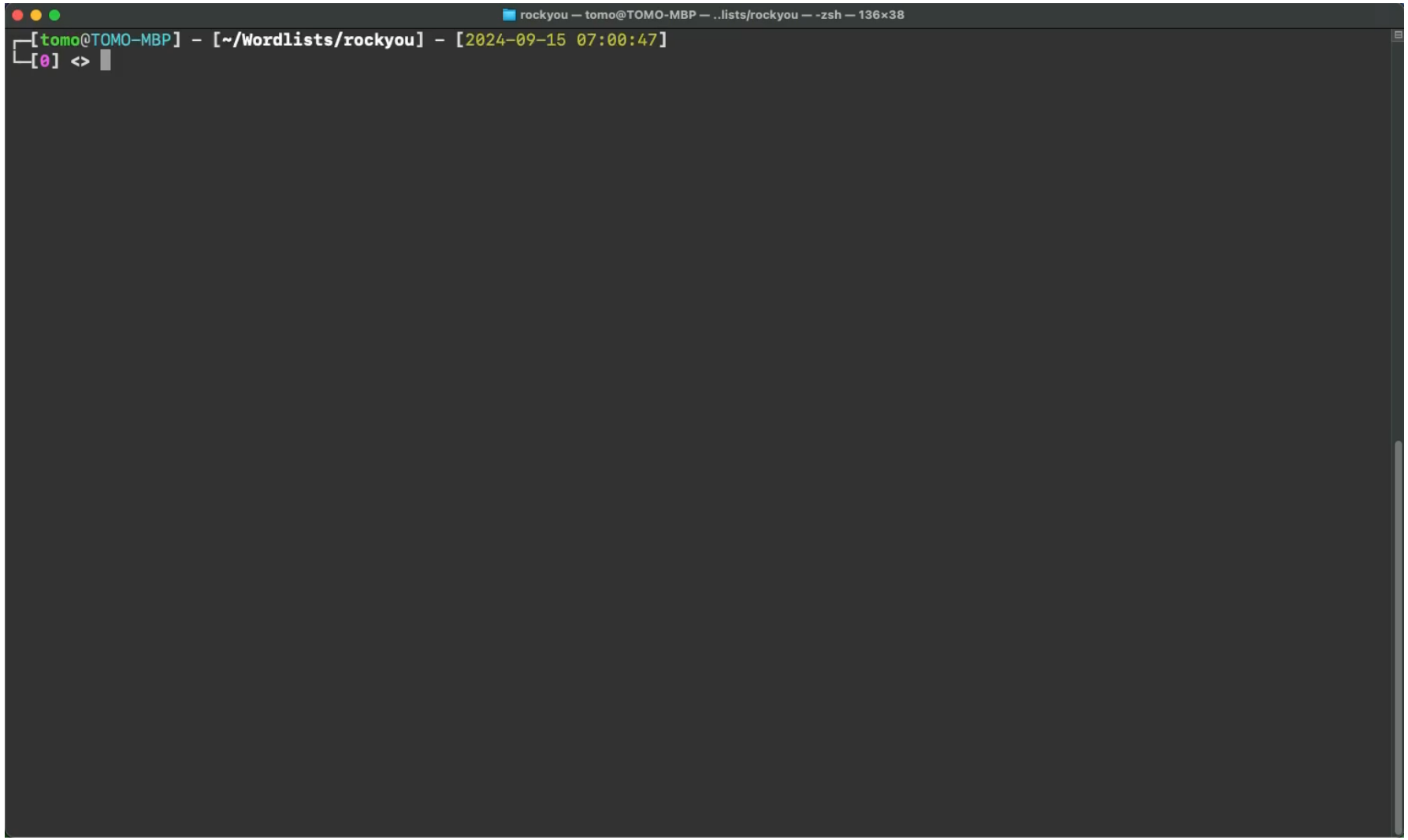
Cracken mit john



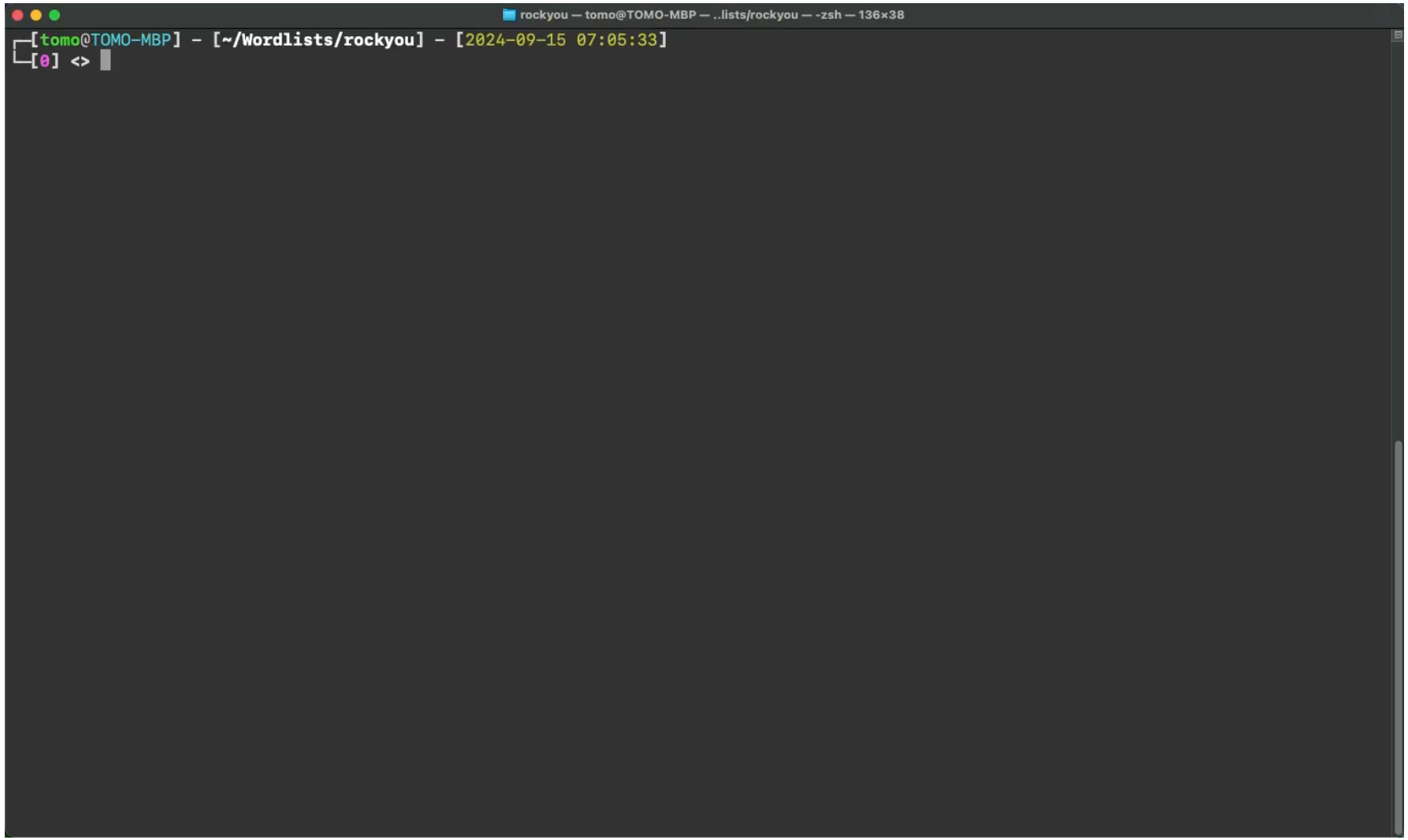
Cracken mit john



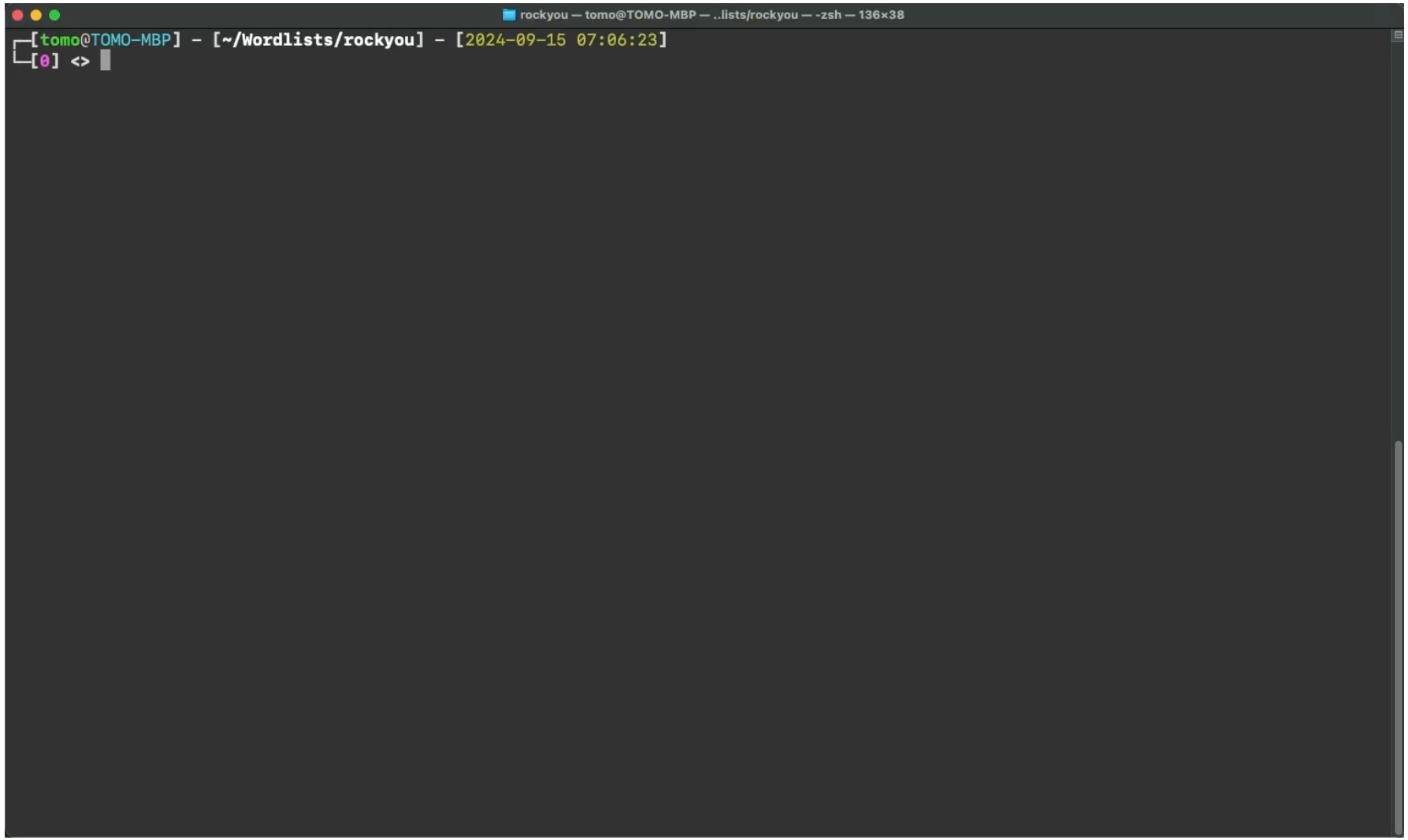
Cracken mit hashcat



Cracken mit hashcat



Cracken mit hashcat



Und so ist es ausgegangen ...

	rockyou2009	rockyou2021	rockyou2024
John mit original:	2.059 in 0:00:54	3.924 in 3:24:07	3.929 in 4:26:46
John mit ASCII reduced:	2.059 in 0:00:57	3.924 in 3:28:49	3.929 in 4:25:02
John combined:	2.059 in 0:00:35	3.924 in 2:34:07	3.929 in 3:17:51
Hashcat mit original:	1.905 in 0:00:24	3.840 in 1:39:05	3.842 in 1:41:44
Hashcat mit ASCII reduced:	1.905 in 0:00:24	3.840 in 1:38:40	3.842 in 1:42:49
Hashcat combined:	2.059 in 0:00:22	3.924 in 1:39:37	3.929 in 1:56:21

Die Bearbeitungszeiten in der Vorbereitung

ASCII	Passwords	Filesize	Filter Time
rockyou2009	14.344.391	139.921.497	00:00:36
rockyou2021	8.459.060.239	98.378.212.907	02:40:24
rockyou2024	9.948.575.739	155.978.020.956	04:55:51

Combined 8 Chars	Passwords	Filesize	Combine Time
rockyou2009	14.344.391	139.921.497	00:00:12
rockyou2021	8.459.060.239	98.378.212.907	02:29:33
rockyou2024	9.948.575.739	155.978.020.956	03:16:30

Lohnen sich rockyou2021 und rockyou2024?

- Mit 3.924 fast doppelt so viele aufgedeckte Passwörter, aber mit ca. 3:30 Std. Mehraufwand bei rockyou2021 und ca. 4:30 Stunden bei rockyou2024. Es lohnt sich, wenn man es häufiger braucht.

- Wenn man diese Zeit (in diesem Beispiel mit DES) für Brute Force nutzt, kommt man auf 3.860 (mit john) gecrackte Passwörter.

Ein Rant über Passwortsicherheit

Ein Rant über Passwortsicherheit

Passwortcheck.ch

Password to be verified:

MVemjSunP

☑ **Show password**

The entered password will be verified locally and never transmitted to the server.

The password is **weak** because the estimated search time is less than one year.

Chosen dictionaries

☑ **German** ☐ **French** ☐ **Italian**

☐ **Rhaeto-Romanic** ☑ **English**

Substrings	Length	Type	Size	Number of attempts	Entropy	Computation time
Sun (sun)	3	Word (English)	97'531	97'531	17 Bit	
MVemjP	6	Other characters	52	1.977e+10	34 Bit	
Time and effort estimation				1.928e+15	51 Bit	5 hours

Ein Rant über Passwortsicherheit

Passwortcheck.ch

Password to be verified:

MVemjSunP

☑ **Show password**

The entered password will be verified locally and never transmitted to the server.

The password is **weak** because the estimated search time is less than one year.

Chosen dictionaries

☐ **German** ☐ **French** ☐ **Italian**

☐ **Rhaeto-Romanic** ☐ **English**

Substrings	Length	Type	Size	Number of attempts	Entropy	Computation time
MVemjSunP	9	Other characters	52	2.780e+15	51 Bit	
Time and effort estimation				2.780e+15	51 Bit	**8 hours**

Ein Rant über Passwortsicherheit

Passwortcheck.ch

Das zu prüfende Password lautet:

MVemjSu9P

☑ **Passwort anzeigen**

Das eingegebene Passwort wird lokal überprüft und nie an den Server übermittelt.

Das Passwort ist **Schwach**, weil die geschätzte Zeit für die Suche unter einem Jahr ist.

Ausgewählte Wörterbücher

☑ **Deutsch**	☐ **Französisch**	☐ **Italienisch**
☐ **Rätoromanisch**	☑ **Englisch**	

Teilwörter	Länge	Typ	Raumgrösse	Anzahl Versuche	Entropie	Rechenzeit
MVemjSu9P	9	Übrige Zeichen	62	1.354e+16	54 Bit	
Aufwandschätzung				1.354e+16	54 Bit	2 Tage

Ein Rant über Passwortsicherheit

PC 112

Passwort Check – Ihr Sicherheitstest

Uns liegt die Sicherheit beim Arbeiten mit Computern und Co am Herzen. Egal ob Updates, Virenschutz oder sichere Passwörter – gern machen wir es Eindringlingen so schwer wie möglich.

Schützen Sie sich als erstes mit einem starken Passwort. Prüfen Sie hier kostenlos und sofort, wie sicher Ihre bisherigen Passwörter sind.

Für Ihre eigene Sicherheit: Bitte geben Sie zum Prüfen keine „echten" Passwörter ein, also keine die Sie tatsächlich verwenden, sondern lediglich welche, die im Aufbau Ihrem tatsächlichen Passwort ähnlich sind.

MVemjSunP erneut testen

Ihr Passwort ist unsicher

Um Ihr Passwort zu klassifizieren benutzen wir ein Punktesystem.
Ein schwaches Passwort erreicht maximal 60 Punkte.
Ein halbwegs sicheres Passwort erreicht zwischen 65 und 75 Punkte.
Ein sicheres Passwort erreicht mindestens 80 Punkte.

Um die Punkte und damit die Stärke Ihres Passwortes zu ermitteln haben wir zunächst 100 Punkten als Startwert festgesetzt und ziehen für folgende Bewertungskriterien davon jeweils 'Strafpunkte' ab.

Kriterium	Spezifikation	Abzug	Passwort
Passwortlänge sollte min. 10 Zeichen lang sein	pro fehlendem Zeichen	5	-5
Keine klein geschriebenen Buchstaben	a bis z	20	0
Keine groß geschriebenen Buchstaben (ab 2. Buchstaben)	A bis Z	20	0
Keine Ziffern	0 bis 9	20	-20
Fehlende Sonderzeichen	,.-:;_=()*+|"$@#£§%&\/{}[]¹^!?'`´–	20	-20
Umlaute, Leertaste, nicht druckbare Zeichen enthalten	öäüÖÄÜçÿéèéÉÈàÀ	20	0
gleiche Zeichen mehrfach hintereinander	ab dem 3. Zeichen	20	0
Buchstaben- (abc..)oder Ziffernfolgen (123..)	ab dem 3. Zeichen	20	0
Zeichenfolge auf Tastatur vorhanden	ab dem 3. Zeichen	20	0
Wörterbuchprüfung	deutsch und englisch	20	0
Gesamtpunktzahl			55

Ein Rant über Passwortsicherheit

PC 112

Passwort Check – Ihr Sicherheitstest

Uns liegt die Sicherheit beim Arbeiten mit Computern und Co am Herzen. Egal ob Updates, Virenschutz oder sichere Passwörter – gern machen wir es Eindringlingen so schwer wie möglich.

Schützen Sie sich als erstes mit einem starken Passwort. Prüfen Sie hier kostenlos und sofort, wie sicher Ihre bisherigen Passwörter sind.

Für Ihre eigene Sicherheit: Bitte geben Sie zum Prüfen keine „echten" Passwörter ein, also keine die Sie tatsächlich verwenden, sondern lediglich welche, die im Aufbau Ihrem tatsächlichen Passwort ähnlich sind.

MVemjSu9P erneut testen

Ihr Passwort ist halbwegs sicher

Um Ihr Passwort zu klassifizieren benutzen wir ein Punktesystem.
Ein schwaches Passwort erreicht maximal 60 Punkte.
Ein halbwegs sicheres Passwort erreicht zwischen 65 und 75 Punkte.
Ein sicheres Passwort erreicht mindestens 80 Punkte.

Um die Punkte und damit die Stärke Ihres Passwortes zu ermitteln haben wir zunächst 100 Punkten als Startwert festgesetzt und ziehen für folgende Bewertungskriterien davon jeweils 'Strafpunkte' ab.

Kriterium	Spezifikation	Abzug	Passwort
Passwortlänge sollte min. 10 Zeichen lang sein	pro fehlendem Zeichen	5	-5
Keine klein geschriebenen Buchstaben	a bis z	20	0
Keine groß geschriebenen Buchstaben (ab 2. Buchstaben)	A bis Z	20	0
Keine Ziffern	0 bis 9	20	0
Fehlende Sonderzeichen	,.-;_=()*+|'§@#£§%&\/{}[]¹²³?'`–	20	-20
Umlaute, Leertaste, nicht druckbare Zeichen enthalten	öäüÖÄÜçÿéèÉÈàÀ	20	0
gleiche Zeichen mehrfach hintereinander	ab dem 3. Zeichen	20	0
Buchstaben- (abc..)oder Ziffernfolgen (123..)	ab dem 3. Zeichen	20	0
Zeichenfolge auf Tastatur vorhanden	ab dem 3. Zeichen	20	0
Wörterbuchprüfung	deutsch und englisch	20	0
Gesamtpunktzahl			75

Das war …

We will rockyou2009, rockyou2021, rockyou2024

Tom Gries (TOMO) | September 2024

@tomo@chaos.social

2024-09-18