Passwörter knacken
mit
John the Ripper

Allgemein

Bereits geknacktes Passwort für eine Datei anzeigen:
$ john --show holiday_rockyou.hash

Passwort-Cache bereits geknackter Passwörter löschen:
$ rm ~/.john/john.pot

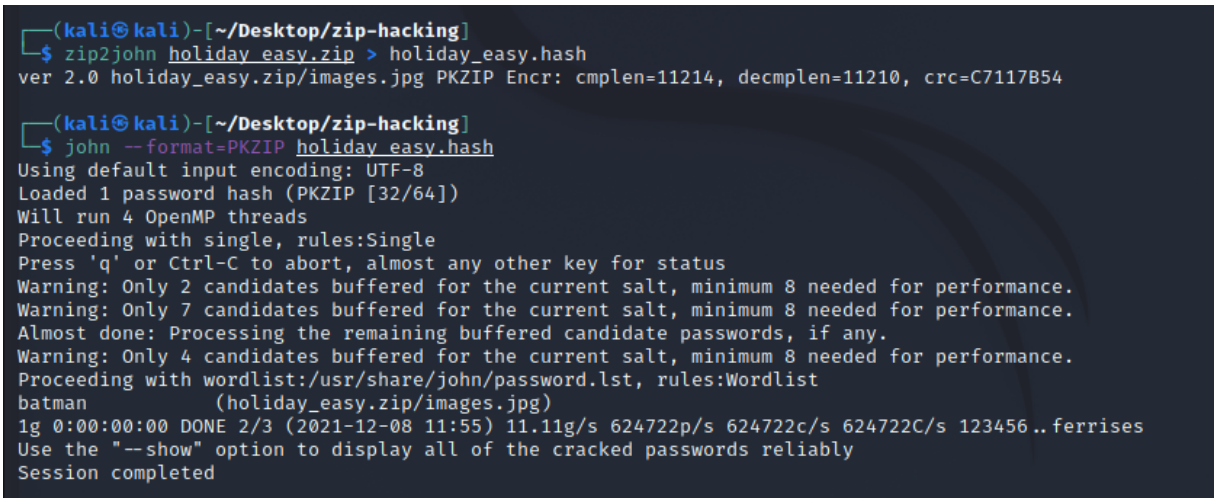
[holiday_easy] (schwaches Passwort, steht in JTR-Standardliste)

Passwort-Hash aus Zip lesen

$ zip2john holiday_easy.zip > holiday_easy.hash

Passwort knacken – Treffer in interner Passwortliste

$ john --format=PKZIP holiday_easy.hash



[holiday_rockyou] (schwaches Passwort, steht in Passwortlisten)

Passwort-Hash aus Zip lesen

$ zip2john holiday_rockyou.zip > holiday_rockyou.hash

Passwort knacken - Interne Wordlist ohne Treffer

$ john --format=PKZIP holiday_rockyou.hash

```
┌──(kali㉿kali)-[~/Desktop/zip-hacking]
└─$ john --format=PKZIP holiday_rockyou.hash
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 4 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 5 candidates buffered for the current salt, minimum 8 needed for performance.
Warning: Only 4 candidates buffered for the current salt, minimum 8 needed for performance.
Warning: Only 7 candidates buffered for the current salt, minimum 8 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Warning: Only 3 candidates buffered for the current salt, minimum 8 needed for performance.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
Proceeding with incremental:ASCII
digimon           (holiday_rockyou.zip/holiday.jpeg)
1g 0:00:00:05 DONE 3/3 (2021-12-08 12:03) 0.1760g/s 3683Kp/s 3683Kc/s 3683KC/s dinth27..diguad2
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

Passwort knacken – Verwendung Wordlist rockyou.txt

$ john --format=PKZIP --wordlist=rockyou.txt holiday_rockyou.hash

```
┌──(kali㉿kali)-[~/Desktop/zip-hacking]
└─$ john --format=PKZIP --wordlist=rockyou.txt holiday_rockyou.hash
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
digimon           (holiday_rockyou.zip/holiday.jpeg)
1g 0:00:00:00 DONE (2021-12-08 13:17) 50.00g/s 409600p/s 409600c/s 409600C/s 123456..total90
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

gish_klausur zip (8-stellige PIN)

Passwort-Hash aus Zip lesen

$ zip2john gish-klausur.zip > gish-klausur.hash

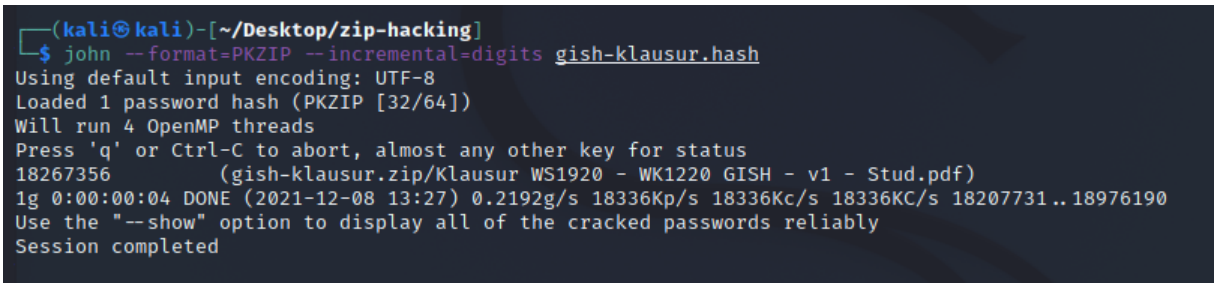
ASCII brute force

$ john --format=PKZIP gish-klausur.hash

```
┌──(kali㉿kali)-[~/Desktop/zip-hacking]
└─$ john --format=PKZIP gish-klausur.hash
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 4 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 7 candidates buffered for the current salt, minimum 8 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Warning: Only 3 candidates buffered for the current salt, minimum 8 needed for performance.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
Proceeding with incremental:ASCII
18267356          (gish-klausur.zip/Klausur WS1920 - WK1220 GISH - v1 - Stud.pdf)
1g 0:00:00:44 DONE 3/3 (2021-12-08 13:22) 0.02271g/s 12003Kp/s 12003Kc/s 12003KC/s 18264943..18723201
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

Passwort knacken - Informierter Incremental Mode – Nur Ziffern raten

$ john --format=PKZIP --incremental=digits gish-klausur.hash



pw-gen alphanum lower case + upper case - 8 Stellen.zip

Passwort-Hash aus Zip lesen

$ zip2john "pw-gen alphanum LC + UC 8 Stellen.zip" > "pw-gen alphanum LC + UC 8 Stellen.hash"

Passwort knacken - JTR Incremental Mode

$ john --format=PKZIP "pw-gen alphanum LC + UC 8 Stellen.hash"

pw-gen secure - alle Zeichen - 16 Stellen.zip

Passwort-Hash aus Zip lesen

$ zip2john "pw-gen secure - alle Zeichen - 16 Stellen.zip" > "pw-gen secure - alle Zeichen - 16 Stellen.hash"

Passwort knacken - JTR Incremental Mode

$ john --format=PKZIP "pw-gen secure - alle Zeichen - 16 Stellen.hash"