

Wörterbuchangriff auf ein Passwort-Leak

Nicht aufgepasst

Die Firma Wolkendienste GmbH hat nicht aufgepasst und eine Datei mit gehashten Passwörtern verloren - hier ist sie

pws.zip

John

John ist ein Programm, mit dem man einen Wörterbuchangriff (oder auch einen Brute-force Angriff) auf eine solche Passwortliste ausführen kann. Bei Kali-Linux ist John bereits dabei.

Die einfachste Weise, john zu verwenden, wenn die gehashten Passworte in der Datei passworte gespeichert sind, ist:

```
john passworte
```

Dabei verwendet john ein mit dem Programm ausgeliefertes Wörterbuch, um Passwörter zu hashen und mit den gespeicherten Passwörtern zu vergleichen.



(A1)

- Entpacke die Datei mit den geleakten Kennwörtern und öffne sie mit einem Texteditor - welche Struktur hat sie?
- Führe einfachen john Befehl von oben mit der entpackten Datei aus.
- Analysiere die Ausgaben des Programms beim Programmstart. Wieviele Hashes wurden geladen und welche Informationen über diese hat john bereits vor dem Beginn des Angriffs ermittelt (Du kannst Informationen zu CUDA Support und Warnungen ignorieren)?
- Nachdem john einige (sehr einfach Passworte) ermittelt hat, probiert es weitere Passworte aus. Breche den Vorgang mit STRG-C ab, führe den john Befehl anschließend erneut aus. Analysiere wieder, wieviele Hashes geladen wurden, achte darauf wieviele Hashes john als „remaining“ betrachtet - was fällt auf?



John führt Buch über die bereits ermittelten Kennworte - geknackte Hashes werden nicht erneut geladen, das Programm merkt sich auch, wie weit es beim probierten gekommen ist. Mit dem Befehl `john -show passworte` kann man sich bereits gefundene Kennworte anzeigen

lassen.



Um john in seinen Ausgangszustand zu versetzen, kann man die Dateien im Verzeichnis ~/ .john löschen.

From:

<https://wiki.qg-moessingen.de/> - QG Wiki

Permanent link:

<https://wiki.qg-moessingen.de/faecher:informatik:oberstufe:netzwerke:pthack:john:start?rev=1652893249>

Last update: **18.05.2022 19:00**

