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

Einstieg in "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.
- Erstelle ein kurzes Ablaufdiagramm: Wie geht das `john` schrittweise vor, um zu ermitteln, welches Passwort ein Benutzer in der Passwortdatei hat?
- 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 darum 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.

Wörterbücher und Kombinationen

Die sehr einfachen Kennworte hat `john` fast unmittelbar nach dem Start bereits ausgegeben - diese standen in seinem Standardwörterbuch weit oben. Ob ein Angriff zum Erfolg führt hängt sehr davon ab, ob man ein Wörterbuch verwendet, das zur Zielgruppe passt. Wenn man beispielsweise ein eigenes Kennwort vergessen hat, sich aber noch an Bestandteile erinnert, kann man sich ein "maßgeschneidertes" Wörterbuch für dieses Zweck schreiben.

Weiß man wenig über die verwendeten Kennworte, kann man auf umfangreichere Wortlisten wie von Probable Wordlists oder welche von dort zurückgreifen. Achtung, solche Listen sind schnell sehr groß. Recht populär bei überschaubarer Größe ist z.B. `rockyou.txt`.

(A2)

- Lade die Datei `rockyou.txt.bz2` herunter und entpacke sie
- Schau dir ihren Inhalt an
- Führe den Befehl `john –wordlist="rockyou.txt" passworte` aus und begutache das Ergebnis - wie erklärst du dir das?

(A3) Eigene Kennworte testen

Mit dem Befehl

```
openssl passwd -5 -salt Salt Passwort
```

kannst du zum Passwort "Passwort" den mit "Salt" gesalzenen Hash erzeugen.

Passe *Salt* und *Passwort* entsprechend an und probiere den Befehl aus. Nun kannst du weitere Zeilen in die passworte-Datei einfügen, um eigene Kennwörter zu testen.