Zur Vorbereitung der Sicherheitsschulung testen Sie „John-the-Ripper“ (JtR), ein klassisches, mächtiges Brute-Force-Attacken-Programm. Mit John-the-Ripper können Sie in der Firma auf der Schulung demonstrieren, wie einfach schwache Passwörter gehackt werden können.

* Laden Sie ihre Ergebnisse (diese Datei in PDF-Format konvertiert) in den Moodle-Kurs hoch. Die Vorgabe für den Dateinamen ist: **JTR\_IhreNamen\_IhreKlasse.PDF**,
* Wenn alle Namen ihrer Teammitglieder im Dateinamen sind, reicht ein Teamprotokoll.
* Achten Sie auf ein korrektes Layout. Auf den Screenshots sollten die Inhalte gut lesbar sein.

**1.)** Passwörter werden vom Betriebssystem nicht in Klartext, sondern in Form von so-genannten Hashwerten auf dem PC gespeichert. Was ist ein Hashwert?

Bei einem Hashwert handelt es sich um einen Wert, welcher für bestimmte Quelldaten immer gleich ist, jedoch nicht einfach wieder zurückgerechnet werden kann. Dies erlaubt die einfache und schnelle Überprüfung von Inhalten, die nicht direkt auf dem PC gespeichert werden sollen, bspw. bei Passwörtern. Hier hätte jedes Passwort einen eindeutigen Hash, jedoch ist es nicht trivial, das Quellpasswort aus dem Hash zu berechnen.

**2.)** Lesen Sie <https://www.bleib-virenfrei.de/it-sicherheit/artikel/was-ist-passwort-hashing/>.

Was ist im Zusammenhang mit Passwörtern Salt (Salz)?

Ein Salt ist ein für das System einzigartig bestimmter Wert, der auf alle gehashten Passwörter vor dem Hashvorgang angewendet wird, um die Hashes für das System einzigartig zu machen.

**3.)** Bei Passwörtern wird auch gepfeffert (Pepper). Was ist der Unterschied zwischen Passwort-Salt und Passwort-Pepper?

Password-Peppering bezeichnet die Praxis, auf jedes Passwort einen eigenen Salt-Zusatz zu verwenden. Dies macht das nutzen von Lookup-Tables jeglicher Art nutzlos.

**4.)** Eine Hashwertfunktion sollte eine Einwegfunktion sein. Was heißt das?

Eine Einwegfunktion bezeichnet eine Funktion, deren Ausgabe nicht trivial wieder in die Eingabewerte zurücküberführt werden kann. Wenn man einen Hash-Wert hat, sollte es nicht trivial möglich kein, die Quelldaten, die zu diesem Hash geführt haben, zu ermitteln.

**5.)** Leider gab es in der Geschichte der Hash-Algorithmen Kollisionen. Was ist das?

Eine Kollision bei Hash-Algorithmen bedeutet, dass mehrere verschiedene Eingangs-Daten zu den gleichen Ausgaben/Hash-Werten führten. Hat beispielsweise eine Passworthashfunktion Kollisionen, kann das System mit mehreren verschiedenen Passwörtern erfolgreich entsperrt werden.

**6.)** Was sind Rainbow-Tables?

Eine Rainbow-Table ist eine Tabelle, die Ausgaben von oft genutzten Hashfunktionen enthält. Dies ermöglicht ein einfaches reverse lookup vom Hashwert zurück zum Ausgangsdatum, was bei einem bekannten Passworthash ermöglicht, die Originaldaten in der Tabelle zu suchen. Vorausgesetzt wird eine Hashfunktion ohne Salt.

**7.)** Was ist der Unterschied zwischen Rainbow-Tables und Passwort-Dictionaries? Schauen Sie hier: <https://www.alterahealth.com/2023/09/hackers-are-taking-your-password-seriously-you-should-too/>, um sich zu informieren.

Eine Passwort-Dictionary ist eine Liste von Passwörtern und deren Hashes, was ermöglicht, ein Lookup vom Passworthash zum Originalpasswort durchzuführen.

**8.)** Was versteht der Autor Brian Montgomery unter Tuning?

Tuning beschreibt die Praxis, aus öffentlichen Daten über eine Person (z.B. Social Media) kurze Zeichenfolgen (bspw. Haustiernamen, Familienmitglieder etc.) zu erspähen um Brute-Force-Attacken effizienter durchführen zu können.

**9.)** Wie funktioniert ein Wörterbuchangriff?

Ein Wörterbuchangriff ist eine Methode Passwörter zu knacken, indem eine Liste von Wörtern, Phrasen und anderen Daten genutzt wird, um systematisch Passwörter zu generieren.

**10.)** Wie funktioniert eine Brute-Force-Attacke?

Eine Brute-Force-Attacke beschreibt einen Angriff, bei dem viele Passwörter auf kürzestem Zeitraum durchprobiert werden. (Trial-And-Error)

**11.)** Hacker versuchen die Nadel im Heuhaufen (haystack) zu finden. Surfen Sie zum Heuhaufen. <https://www.grc.com/haystack.htm> und testen Sie einige Passwörter auf Tauglichkeit. Notieren Sie, wie schnell die unten angegebenen Passwörter jeweils „Offline Fast“ gehackt werden könnten.

|  |  |
| --- | --- |
| Passwort | Dauer der Entschlüsselung (Hacking-Zeit) |
| Meier123 | Offline Fast Attack Scenario: 36.99 minutes |
| oszimt | Offline Fast Attack Scenario: 0.00321 seconds |
| 123%%%zzz | Offline Fast Attack Scenario: 4.16 days |
| 123abc\*\*\*\*0 | Offline Fast Attack Scenario: 54.46 years |
| 1+++++++++++ | Offline Fast Attack Scenario: 13.01 years |

**12.)** Welches Passwort ist das Stärkste und warum?

Laut dem Online-Tool handelt es sich bei „123abc\*\*\*\*0“ um das stärkste Passwort, da die Offline-Cracking-Zeit am höchsten Liegt. Es hat die höchste Menge an Entropie durch viele verschiedene Zeichen.

**13.)** Um wie viel schneller könnte das Passwort kevin gehackt werden im Vergleich zu kevin2? Erläutern Sie, warum.

„kevin“ kann laut dem Tool in 0.000124 Sekunden geknackt werden, „kevin2“ dahingegen in 0.0224 Sekunden. Dies ist eine Differenz von 0.022276 Sekunden, was an der erhöhten Länge und der zusätzlichen Zahl im Passwort liegt, welche beide die Entropie erhöhen.

**14.)** Einige Passwörter haben mehr so-genannte „Entropie“ als andere, was bedeutet das?

Entropie bezeichnet den Grad der Zufälligkeit in einem System. Je weniger Entropie vorhanden ist, desto wahrscheinlicher ist es, ein bestimmtes Ereignis vorherzusagen. In der Informationstheorie bezeichnet Entropie die Angabe der durchschnittlichen Zahl an Entscheidungen, die benötigt wird, um ein bestimmtes Zeichen aus einer Zeichenkette zu bestimmen.

**15.)** Welches der oben von ihnen getesteten Passwörter hat die höchste Entropie?

Da sich das Tool auf die Entropie des Passwortes bezieht, müsste das Passwort 123abc\*\*\*\*0 die höchte Entropie haben.

**16.)** Installieren und entpacken Sie John-the-Ripper (Setup-Programm ist im Moodlekurs). John-the-Ripper legt bei der Installation ein run-Verzeichnis an. Kopieren Sie die vier zu hackenden Dateien, die sich im Moodlekurs befinden, in das run-Verzeichnis von John-the-Ripper.

👍

**17.)** Im run-Verzeichnis befinden sich viele Hacker-Tools zum Hacken von passwortgeschützten Dateien. Informieren Sie sich, wie das Passwort einer ZIP-Dateie gehackt werden kann: <https://www.pcwelt.de/article/1203160/so-knacken-sie-ihr-passwort.html>. Hacken Sie die Passwörter der ZIP-Dateien. Binden Sie von ihrem Ergebnis mit den drei gehackten Passwörtern der ZIP-Dateien einen **Screenshot** hier ins Dokument ein. Testen Sie, ob ihre gehackten Passwörter die ZIP-Dateien öffnen können.



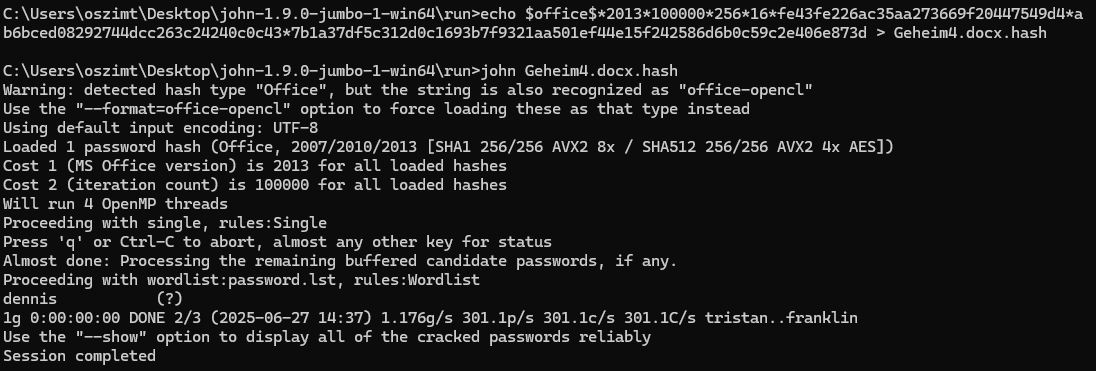
**18.)** Welche Texte konnten Sie entschlüsseln durch Öffnen der ZIP-Dateien?

Geheim1: Dieses ist eine geheime Botschaft

Geheim2: Stimmt – das Passwort war Newton

Geheim3: **Das Passwort für diese Datei war nicht in der Wörterbuchdatei und trotzdem haben Sie es herausgefunden. Wie kommt das?**

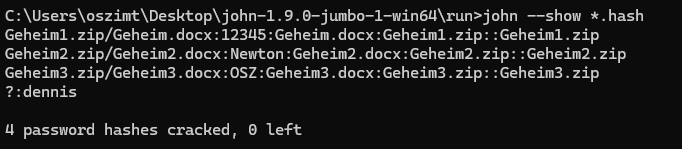
**19.)** Hacken Sie das Passwort der WORD-Datei „Geheim4.docx“. Wie das geht, steht bei PC-Welt (siehe oben). Um den Office-Hashwert vom Passwort der WORD-Datei herauszufinden, benötigen Sie die folgende Webseite. <https://hashes.com/en/decrypt/hash>. Nutzen Sie auf der Seite unter Tools „office2john“, um den Hashwert zu ermitteln. Diesen kopieren Sie in eine Textdatei (z.B. hash4.txt) und los geht’s mit einer neuen Brute-Force-Attacke. Binden Sie wieder einen **Screenshot** mit dem Ergebnis von John-the-Ripper ein. Testen Sie schließlich, ob ihr gehacktes Passwort die WORD-Datei öffnen kann.



Geheim4: Korrekt: Das Passwort war „dennis“ und stand in der Passwortdatei

**20.)** Mit welchem Kommando lassen sich mit John-the-Ripper die gehackten, gespeicherten Passwörter anzeigen? Testen Sie das Kommando.

Mit dem Befehl „john.exe –show \*.hash“ lassen sich die gefundenen Passwörter aus dem Hashdateien anzeigen.



**21.)** Beim Hacken nutzte John-the-Ripper eine Wörterbuchdatei. Wie viele Test-Passwörter enthält diese Datei insgesamt?

Die Datei password.lst beinhaltet 3546 Einträge.

**22.)** In welchem Modus wurden die Brute-Force-Attacken jeweils durchgeführt?

Der Betriebsmodus heißt „incremental:ASCII“-Mode.

**23.)** John-the-Ripper eignet sich für IT-Fachleute, um die Stärke der Passwörter der Belegschaft zu überprüfen. Anders ausgedrückt: Sie könnten testen, ob Passwörter leicht zu hacken sind oder nicht.

Nehmen wir an, Sie hätten drei Hashwerte von drei Kollegen kopiert und wollen testen, ob die zugehörigen Passwörter stark genug sind. Testen Sie, ob sie die Passwörter der Hashwerte cracken können.

Hashwert1 des Kollege Meier: $office$\*2013\*100000\*256\*16\*d7d722296ae910e1b2f944169e117927\*cbcd032bf5d29c01a493dc4e8f22a136\*fb3f3d903b685d4b8722ad0c0a22c7bc6442f87c7aed4a6b36c6707d0932faab

Haswert2 von Kollegin Strunz: $office$\*2013\*100000\*256\*16\*2b0678c28405b19ad413081be29cdfaa\*a16766f64e424cbb95489730de359555\*b853a4ddc3b4500f68e08646a060114901073fa0cc73e10fb82fa99c564937a6

Hashwert3 vom Kollegen Kunz: $office$\*2013\*100000\*256\*16\*9cad9bfd95f70fa51af3c1dd5119e9a0\*4ed717f55215ecccdcd714436ae7c655\*a6234a3ee374de11851272f5337bb9d709aed4c1b310f00cd4013723b7027295

Binden Sie wieder ein **Screenshot** mit dem Ergebnis der Brute-Force-Attacke ein, das John-the-Ripper geliefert hat.

**24.)** Falls Sie alle Passwörter hacken konnten, welche Maßnahme sollten Sie nun für die Firma veranlassen?

**25.)** Passwörter, die gehackt wurden, sollten umgehend geändert werden! Prüfen Sie, ob die Passwörter ihrer Email-Adressen schon gehackt wurden. Das ist möglich auf der Seite <https://haveibeenpwned.com/>. Sind Sie schon gehackt worden und wenn ja, wo?