Prof. Dr. Holger Schmidt
Professur für IT-Sicherheit, Informatik
Fachbereich Informatik – Fachhochschule Dortmund

Aufgabe 10.1

Als grundsätzliche Möglichkeiten zur Authentisierung sind Wissen, Besitz und persönliche Eigenschaften bzw. eine Kombination dieser Faktoren möglich. Oftmals werden bei der Authentisierung aber noch weitere Aspekte einbezogen. Nennen und erläutern Sie mindestens zwei solcher Aspekte.

Aufgabe 10.2 K10

Welche potentiellen Angriffsmöglichkeiten auf einfache Passwortverfahren sind Ihnen bekannt?

Aufgabe 10.3

Ihnen ist die Passwortdatenbank von Lisa zugespielt worden (siehe Datei „shadow“ in ILIAS/sciebo).

a) Interpretieren Sie alle Einträge der Passwortdatenbank vollständig.

b) Welche Hashing-Verfahren wurden für die Passwortdatenbank verwendet?

c) Verwenden Sie John the Ripper[1] und/oder Hashcat[2], um die in der Passwortdatenbank enthaltenen Passwörter zu knacken. (Hinweis: Der Programmlauf könnte je nach verwendetem IT-System bei *lisa11* einige Zeit (möglicherweise Tage) in Anspruch nehmen!)

d) Überprüfen Sie die Ergebnisse von John the Ripper bzw. Hashcat jeweils mithilfe der Referenz-Implementierung QuickHash[3].

Hinweis: Benutzen Sie die bereits von Ihnen vorbereitete virtuelle Maschine mit *Kali Linux*. Sie haben die Möglichkeit bei Bedarf externe Wortlisten zu nutzen.

Aufgabe 10.4 K8+3+1+2+1

Analysieren Sie eine Zwei-Faktor-Authentifikation bestehend aus zwei Passwörtern. Erlaubte Zeichen für das erste Passwort sind die lateinischen Klein- und Großbuchstaben, die Ziffern von $0-9$ und die sieben Sonderzeichen !, &, ., ?, −, +, ;. Für das erste Passwort wird eine minimale Länge von sechs Zeichen, mindestens ein Klein- sowie mindestens ein Großbuchstabe, mindestens eine Ziffer sowie mindestens zwei Sonderzeichen gefordert.

Das zweite Passwort ist ein Haustiername mit vier kleinen Buchstaben, wobei Ihnen bei Beobachtung des Systems auffällt, dass die erste Stelle immer r, m, k oder l und die letzte Stelle immer i ist.

[1] http://www.openwall.com/john/, zuletzt aufgerufen am 21.04.2016
[2] https://hashcat.net/, zuletzt aufgerufen am 21.04.2016
[3] https://www.quickhash-gui.org/, zuletzt aufgerufen am 22.06.2021

a) Was ist die *Entropie des auf dem ersten Passwortmodell basierenden Faktors*? Betrachten Sie den Fall, dass das Passwort nur die Minimallänge hat und die genannten Einschränkungen folgendermaßen erfüllt: genau zwei Sonderzeichen und zwar am Anfang und Ende des Passwortes, an zweiter Stelle ein Großbuchstabe, es enthält genau eine Ziffer und an vorletzter Stelle einen Kleinbuchstaben. Gehen Sie davon aus, dass die Zeichen ansonsten vollständig zufällig ausgewählt werden.

b) Was ist die *Entropie des auf dem zweiten Passwortmodell basierenden Faktors*?

c) Was ist die *Entropie des gesamten Systems*?

d) Wie beurteilen Sie den auf dem ersten Passwortmodell basierenden Faktor hinsichtlich *naiver Brute Force-Angriffe*? Begründen Sie Ihre Antwort.

e) Wie beurteilen Sie den auf dem ersten Passwortmodell basierenden Faktor hinsichtlich *Wörterbuch-Angriffe*? Inwieweit sind die Forderungen für das Vorhandensein bestimmter Zeichen sinnvoll? Begründen Sie Ihre Antwort.

Aufgabe 10.5

Beantworten Sie nachfolgende Fragen zu Argon2:

a) Welchen Zweck haben die Eingaben des Argon2-Algorithmus?

b) Betrachten Sie folgende Situation: Sie implementieren ein Backend für eine Web-Anwendung auf einer *Amazon EC2 AWS t2.micro* Instanz und möchten dort für Passwort-basierte Authentifikation Argon2 nutzen. Welche Werte sollten die Eingaben des Argon2-Algorithmus haben? Welche zusätzlichen Information sind ggf. notwendig, um die Werte fundiert einstellen zu können?