Blatt 2 - Kennwortsicherheit

Kolja Hopfmann, Jonas Sander

00/00/0000

---

1 1. - Sicherheit lokaler Rechner

1.1 1.1

1.2 1.2

1.3 1.3

2 2. - Sichere Speicherung von Kennwörtern

2.1 2.1

1. Zuerst wurde in das Verzeichnis von rcracki navigiert.

```
cd webadmin/Rainbowtables/rcracki_mt_0.7.0_Linux:x86_64
```

Hier wurde dann rcracki auf der Datei mit den Passwörtern ausgeführt.

```
./cracki -l [password txt] [path to rainbow table]
```

Hierbei wurden Passwort Nummer 4: ulardi und Passwort Nummer 5: avanti gefunden. 2. Die Restlichen Passwörter konnten mit der Verwendeten Rainbowtable nicht geknackt werden. Dies ist darauf zurück zu führen, dass die Passwörter nicht als Wörter in der Tabelle enthalten sind. Ein erneuter Versuch mit einer anderen Rainbowtable könnte weitere Passwörter knacken,

jedoch ist dies keineswegs sicher.
Für das Abspeichern der MD5-Hashes aller alphanumerischen Passwörtern der Länge 1-7 wäre ein Speicher von $\sum_1^7(62^i \cdot 32byte) = 1,1 \cdot 10^{14}Byte = 110TB$ nötig. Dies ist um den Faktor 10^4 größer als die verwendete Rainbowtable und deutlich zu groß zur Speicherung.

2.2 2.2

Unsere Lösung war auf dem Alphabet bestehend aus 0-9 und a-z iterativ alle möglichen Strings durch zu probieren. Hierfür haben wird eine Java Klasse geschrieben, die in einer Schleife von 0 bis $36^7 - 1$ iteriert. In Jeder Iteration wird ein String zusammengesetzt, dieser mit dem Salt gehasht und das Ergebnis des Hashes mit dem in der Passwort-Datei gefundenem Hash verglichen. Hierbei werden erst alle 1-Stelligen, dann alle 2-Stelligen Passwörter durchlaufen etc. Hiermit wurde das Passwort s1v3s gefunden.

2.3 2.3

3 3. - Forensische Wiederherstellung von Kennwörtern

4 4. - Unsicherer Umgang mit passwörtern in Java