Blatt 2 - Kennwortsicherheit

Kolja Hopfmann, Jonas Sander

26. April 2018

---

1 Sicherheit lokaler Rechner

1.1

1.1.1

Die VM wurde mit der grml-CD gebootet und der Festplatteninhalt der eigentlichen VM wurde gemountet.

```
lsblk
mount -r /dev/sda1
```

Der Aufbau von */etc/passwd/* ist:
Name:Passwort:UserID:GroupID:Kommentar:Verzeichnis:Shell , wobei hier das Passwort in der */etc/shadow/* Datei als Hash ausgelagert ist.
Es existieren die User *Georg* und *webadmin*. Der User *Georg* hat Sudo-Berechtigung

1.2

1.2.1

Eine kryptographische Hashfunktion ist eine Funktion welche einen beliebigen Eingabeparameter so verändert, dass es praktisch unmöglich ist, mittels Berechnung auf den ursprünglichen Eingabewert zu schließen. Ein Salt ist ein

randomisierter Eingabewert, welcher mit dem Passwort konkateniert wird und gemeinsam gehasht wird. Dadurch ist der Hash eines bestimmten Klartextes mit Salt nicht immer der selbe. Die bedeutet das man das Ursprüngliche Passwort nur durch mehrfaches Ausprobieren herausfinden kann.

1.2.2

John wurde installiert und die Manual wurde gelesen:

```
sudo apt install john
man john
```

John wurde im Incremental-Mode gestartet:

```
john -incremental /etc/shadow
```

Der Versuch war nicht erfolgreich. Grund: Incremental Mode iteriert von Anfang über alle möglichen Passwort-Strings, für einen Zeitraum von 15 Minuten war das Passwort zu lang um es über Incremental zu ermitteln.

1.2.3

Es wurde eine Wordlist runtergeladen,entpackt und anschließend für einen weiteren Versuch mit John The Ripper benutzt.

```
wget http://download.openwall.net/pub/wordlists/all.gz
gunzip all.gz
john --wordlist=all /etc/shadow
```

Das Passwort für den User *webadmin* wurde nach kurzer Zeit gefunden: *mockingbird*. Eine Nachricht auf seinem Blog wurde hinterlassen.

1.3

Das Passwort für den User *georg* war nicht in der Wordlist enthalten.

Das VM-Image wurde erneut gemountet, diesmal mit Schreibzugriff. Daraufhin wurde mit *chroot* eine neue Bash-Session gestartet mit dem VM-Image

root als root. Somit konnte man mit Rootrechten das Passwort von *georg* ändern.

```
mount /dev/sda1
chroot /media/sda1 /bin/bash
passwd georg
exit
```

2 Sichere Speicherung von Kennwörtern

2.1

2.2

2.3

3 Forensische Wiederherstellung von Kennwörtern

3.1

Aus den empfohlenen Quellen zu Blatt 2 unter "Zum sicheren Umgang mit Passwörtern im Speicher" geht hervor, dass viele Anwendungen Passwörter als Klartext im Arbeitsspeicher ablegen. Dadurch ist es Möglich das Passwort (für kurze Zeit) selbst nach ausschalten des Systems aus dem Speicher zu extrahieren. Desweiteren Dient eine Swap-Partition als zusätzlicher Arbeitsspeicher. So ist es Möglich aus der Swap-Partition Passwörter zu extrahieren.

3.2

Unter grml wurde der Inhalt der VM gemountet:

```
mount /dev/sda1
```

Unter */home/user/.bash_history* befinden sich die letzten commands welcher der user in der letzten bash-session in die shell eingetippt hat.

3.3

Da der Admin zunächst mit Jedit die Server-File editiert hatte haben wir zunächst in den Jedit config-Files gesucht, unter *home/.jedit*. Da war zu erkennen dass das alte Passwort "Flugentenfederkiel/991199" war, mit dem User "bloguser".

Daraufhin wurde versucht mit dem Programm photorec, Teile der Swap-Parition wiederherzustellen:

```
lsblk
photorec /dev/sda5
```

Die wiederhergestellten Dateien wurden aufgrund Platzmangel der grml-CD unter */dev/sda*1 abgelegt. Nun wurde versucht die Dateien nach dem String "PASSWORD" zu untersuchen da dies in der Server-Datei vor dem tatsächlichen Passwort stand.

```
find . -name "*.elf" | xargs grep -E 'PASSWORD'
find . -name "*.txt" | xargs grep -E 'PASSWORD'
find . -name "*.java" | xargs grep -E 'PASSWORD'
grep -a 'PASSWORD' f0402684.elf
grep -a 'PASSWORD' f0853144.elf
grep -a 'PASSWORD' f0932456.elf
grep -a 'PASSWORD' f0052256.elf
```

In der Datei *f*0853144.*elf* befand sich das Passwort als Klartext: "Kindergeburtstag/119911"

4 Unsicherer Umgang mit Passwörtern in Java