Blatt 2 - Kennwortsicherheit

Kolja Hopfmann, Jonas Sander

00/00/0000

---

1 Sicherheit lokaler Rechner

1.1

1.2

1.3

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 f0402684.elf
grep -a f0853144.elf
grep -a f0932456.elf
grep -a f0052256.elf
```

In der Datei f0853144.elf befand sich das Passwort als Klartext: Kindergeburtstag/119911

4 Unsicherer Umgang mit Passwörtern in Java