ingenieur
wissenschaften
htw saar

Hochschule für Technik und
Wirtschaft des Saarlandes

PIBWI54

IT Forensik

Marian Müller
Mike Franz
Michael Sebastian Koch
Urs Oberdorf

2. Februar 2015

Inhaltsverzeichnis

grober Ablauf: *Aufgabenstellung *Planung *Durchfuehrung -tests *Ergebnisse *Timeline

1 Aufgabenstellung

Der Betreiber eines Webservers hat am 29.01.2010 festgestellte, dass mit dem Server etwas nicht stimmt. Am Vortag hat der Betreiber zuletzt gegen 22:15 Arbeiten am Webserver durchgeführt.
Ein Image des Servers (ca. 3Gb) wurde erstellt.
Das Image wurde mit bzip2 komprimiert (ca. 500 MB).
MD5-Hashwert des Images:

4afc088a94dd6c36e750b7462e737162 img.dd

Rekonstruieren Sie den Vorfall und erstellen Sie einen gerichtsverwertbaren Bericht.

2 Planung

Um den Vorfall zu bearbeiten und die gestellte Aufgabe zu lösen sammelten wir in einem Brainstorming Ideen was alles überprüft werden sollte. Um den Projektablauf besser zu strukturieren kategorisierten wir diese anschließend und formulierten sie als Tests welche durchgefuehrt werden sollten. Wir gestalteten die Tests als Einstiegspunkte in unsere Untersuchung da wir erwarteten je nach Ergebniss unsere Aktionen sehr dynamisch fortführen zu müssen.

- Logins
  Die Datei `/var/log/auth.log` soll auf Auffaelligkeiten überprüft werden. Sie enthält alle login und logout Ergeignisse von normalen Benutzern sowie System Prozessen. Wir erhoffen uns aus diesen Ereignissen weiterführende Hinweise auf nicht authorisierte Zugriffe auf das System.

- Benutzer
  In der Datei `/etc/shadow` sind alle Benutzer des Systems hinterlegt. Sollten Benutzer hier hinterlegt sein welche Auffaelligkeiten aufweisen wie Name oder Erstellungsdatum können wir verfolgen was der Benutzer am System verändert hat.

- Module
  Der befehl `lsmod` listet alle geladenen Module des Systems. Sollten auffaellige Module geladen sein kann mittels Reverse Engineering deren Zweck ermittelt werden.

3 Vorbereitung

Nach dem entpacken des Images stellten wir die in der Vorlesung erwähnte Abweichung der MD5 Summe fest.

Die erwartete Summe war

4afc088a94dd6c36e750b7462e737162 img.dd

Unser Ergebniss mit `md5sum` betrug

06d111e7ad654c1b7d47676fb6661540 image.dd

Mit `fdisk -l image.dd` entnahmen wir folgende Partitionsinformationen:

```
 Disk image.dd: 3221 MB, 3221225472 bytes
255 heads, 63 sectors/track, 391 cylinders, total 6291456 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x0009d1b1

Device Boot Start End Blocks Id System
image.dd1 * 0 3518171 1759086 83 Linux
image.dd2 3518235 4305419 393592+ 82 Linux swap / Solaris
image.dd3 4305420 6281414 987997+ 5 Extended
image.dd5 4305483 6281414 987966 83 Linux
```

```
Disk image.dd: 3221 MB, 3221225472 bytes
255 heads, 63 sectors/track, 391 cylinders, total 6291456 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x0009d1b1

   Device Boot      Start         End      Blocks   Id  System
image.dd1   *           0     3518171     1759086   83  Linux
image.dd2         3518235     4305419      393592+  82  Linux swap / Solaris
image.dd3         4305420     6281414      987997+   5  Extended
image.dd5         4305483     6281414      987966   83  Linux
```

Um die einzelnen Partitionen als Loopback Device mounten zu können muss ein Offset dem `losetup` Program übergeben werden. Dieser berechnet sich aus dem Startsektor sowie der Größe eines Sektors.

$$startsector * sectorsize = offset$$

Aus dieser Berechnung ergeben sich folgende `losetup`-Befehle:

```
  losetup -v -r -o 32256 /dev/loop0 image.dd[1]
losetup -v -r -o 1801336320 /dev/loop1 image.dd
losetup -v -r -o 2204407296 /dev/loop2 image.dd
```

Um die Loopback Devices nun einzubinden musste mit `fsstat` das Dateisystem ermittelt werden.

[1]Da sich auf der ersten Partition der MBR befindet muss als Startsektor 63 gewaehlt werden.