Labreport 02

Tronje Krabbe, Julian Deinert

28. April 2016

Inhaltsverzeichnis

Aufgabe 1

1.1 Zugriff auf /etc/passwd und /etc/shadow des Webservers

- Wir haben den Ordner mit dem **File Browser** in unseren vmware-Ordner kopiert.
- Wir änderen die Einstellungen unserer VM so, dass das grml-Abbild im virtuellen CD/DVD-Laufwerk liegt und setzen den Haken bei *connect on power on*. Letzteres sorgt dafür, dass das image geladen wird, bevor Ubuntu gestartet wird.
- Nach dem Starten von *grml* mounten wir die *Root-Partition* nach `/mnt`. Mit `lsblk` ergibt sich aus dem output

```
NAME   MAJ:MIN RM   SIZE RO TYPE MOUNTPOINT
fd0      2:0    1     4K  0 disk
sda      8:0    0    20G  0 disk
|-sda1   8:1    0  19.1G  0 part
|-sda2   8:2    0     1K  0 part
|-sda5   8:3    0   895M  0 part
```

  dass die *Root-Partition* auf `sda1` liegt. Wir mounten diese also mit `sudo mount /dev/sda1 /mnt` in den Ordner `/mnt`.
- Die Datei *passwd* enthält für jeden User eine Zeile, die aus folgenden Feldern besteht:
  - Dem Login-Namen
  - Dem verschlüsseltem Password des Users (optional)
  - Der User-ID
  - Der Gruppen-ID
  - Dem User-Namen oder einem Kommentar
  - Dem *home directory* des Users
  - Der *shell* des Users (optional)
- Die Datei *shadow* speichert die gehashten Passwörter der User im folgenden Format:
  <login name>:<encrypted password>:<date of last password change>:

<minimum password age>:<maximum password age>:<password warning period>:<password inactivity period>:<account expiration date>:<reserved field>

In beiden Datien gibt es neben diversen Usern für Services und Programme die User `root`, `georg` und `webadmin`.

- Der User `georg` gehört der Gruppe `admin` an. `webadmin` gehört den Gruppen `adm, dialout, cdrom, plugdev, lpadmin`
sowie `sambashare` an.

1.2 Auslesen von Kennwörtern

- Ein gesaltetes, gehashtes Passwort ist ein Passwort, das erst mit einem sogenannten Salt kombiniert und danach mit einer Hash-Funktion gehasht wurde. Eine Hash-Funktion verändert ihren Input deterministisch so, dass das Ergebnis nicht (ohne Weiteres) zurück zum Input transformiert werden kann. Der Salt kann eine beliebige Zeichenkombination sein, dessen Nutzung die Anwendung von Rainbow-Tables verhindern soll. Insbesondere erschwert der Hash das Reversieren des gehashten Wertes zum Original.

- Die `--incremental` Option führt einen Brute-Force-Angriff auf das Passwort auf, was sehr, sehr langsam ist aufgrund der vielen möglichen Kombinationen von Zeichen.

- Der Wörterbuch-Angriff funktioniert sehr viel schneller, und das Passwort lautet *mockingbird*.

1.3 Setzen von neuen Kennwörtern

Das Passwort von *georg* konnte nicht mit `john` ermittelt werden, da es nicht in unserem (und daher wahrscheinlich auch in keinem anderen) Wörterbuch vorkommt.

Aufgabe 2

2.1 Angriffe mit Hashdatenbanken und Rainbow-Tables

Die ermittelten Kennwörter sind:

- ente

- ball
- borkeni
- ulardi
- avanti

Zur Idee von Black Hat: es gibt 62 alphanumerische Zeichen (26 Klein- und 26 Großbuchstaben, sowie 10 Ziffern). Das ergibt

$$\sum_{1}^{n=7} 62^i = 3.579.345.993.194$$

mögliche Hashes, jeder mit einer Größe von 32 Byte, bzw. 33 Byte inklusive des Separators, was insgesamt 118,1 TB belegt. Wer hier pedantisch sein möchte, könnte bemerken, dass wir ein Byte zu viel eingerechnet haben, da nach dem letzten Eintrag kein Separator benötigt wird. Trotzdem ist dies ein exorbitanter Speicherplatzbedarf, der uns auch nur weiterhilft, wenn das Passwort tatsächlich nur aus alphanumerischen Zeichen besteht. Die Rainbow-Tables dagegen belegen lediglich 12,2 GB.

2.2 Eigener Passwort-Cracker

Wir haben unseren Passwort-Cracker in Python geschrieben; er sieht so aus:

```
#!/usr/bin/env python

import sys
import string
import hashlib
from itertools import permutations

target = b'2b2935865b8a6749b0fd31697b467bd7'
salt = b'8kofferradio'

symbols = string.ascii_lowercase + '0123456789'

for i in range(1,7):
    print(i)
    sys.stdout.flush()
    for elem in permutations(symbols, i):
        elem_bytes = b''
```

```
            for c in elem:
                elem_bytes += bytes(c, 'utf8')
            m = hashlib.md5()
            m.update(salt + elem_bytes)
            if m.hexdigest() == target.decode():
                print("success; found match!")
                print(elem_bytes)
                sys.stdout.flush()
                sys.exit(0)

print("failed; couldn't find a match!")
sys.exit(1)
```

Das Ergebnis ist: penispenis123. QED bitch!