Blatt Nr. 2 (Ausgabe: 14. April 2016, Abgabe: 04. Mai 2016)

Kennwortsicherheit

Übungsaufgabe 1. Sicherheit lokaler Rechner

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

Überblick über die VM.

- *Blatt2-Admin-PC.vmwarevm* wurde aus */home/vmware* nach */home/ss16g07/vmware* kopiert
- wurde über *File -> Open...* importiert (die virtuelle Festplatte wurde eingelesen)
- VM wurde gestartet; beim Boot wurde danach gefragt, ob die VM kopiert oder verschoben wurde; nach Aufgabe wurde "kopiert" ausgewählt

Booten von der CD

- *grml*-iso wurde aus */home/vmware* nach */home/ss16g07/vmware* kopiert
- Neues Image wurde in den VM-Einstellungen in das CD-Laufwerk eingelegt
- Ebenfalls unter den VM-Einstellungen wurde das CD-Laufwerk verbunden
- Während des Bootens der VM wurde das BIOS aufgerufen, um sicherzustellen, dass von der CD gebootet wird

Einlesen und durchsuchen der Root-Partition

- durch drücken von *d* und *Enter* wurde das deutscha tastaturlayout ausgewählt
- mit *mount -r /dev/sda1* wurde die FEstplatte gemountet
- unter */etc/fstab* wurde herausgefunden, dass das Verzeichnis nun unter */mnt/sda1* zugreifbar ist
- die Dateien *passwd* und *shadow* wurden mit *cat $Dateiname* geöfnnet:
  - *passwd* enthält Einträge der folgenden Form: [1]
    - *$Nutzername*:x[1]:*$Nutzer ID*:*$Gruppen ID*:*$Nutzer ID Info*:*$home Verzeichnis*:*$Shell*
  - *shadow* enthält Einträge der folgenden Form: [2]
    - *$Nutzername*:*$verschlüsseltes Password*:*$Tag der letzen Passwortänderung*[2]:*$minimaler Zeitabstand zwischen Passwortänderungen*:*$maximaler Zeitabstand zwischen Passwortänderungen*:*$Warnungszeitrau für auslaufende Passwörter*:*$Zeit nach der ein Password ausläuft nach Inaktivität des Accounts*:*$Zeit die seit der Inaktivität des Accounts vergangen ist*:
- es gibt die Benutzer *webadmin* und *georg*
- durch Eingabe von *cat group|grep $Benutzername* wurden die Gruppen der Nutzer herausgefunden:
  - georg
    - admin
    - georg
  - webadmin
    - adm
    - dialout

[1] Das x indiziert, dass ein verschlüsseltes Passwort für diesen Nutzer existiert
[2] in Tagen seit dem 1. Jan 1970

- cdrom
- plugdev
- lpadmin
- webadmin
- sambashare

Aufgabe 1.2 Auslesen von Kennwörter

- salting: Hinzufügen einer zufälligen Zeichenkette ("salt")
- hashing: Umrechnung der Daten in Hash-Werte[1]

Installieren und Verwendung von *john*

- John wurde installiert mit *apt-get install john*, es konnte jedoch nicht authentifiziert werden
- Einfaches Ausführen von *john* zeigt die Hilfe-Seite
- Eingabe des Befehls *john –incremental –users=webadmin /mnt/sda1/etc/shadow*, um das Passwort von *webadmin* im *incremental*-Mode zu ermitteln
- Nach 5 Minuten wurde eine manuelle Terminierung durchgeführt

Wörterbuchangriff

- es wurde in das home Verzeichnis navigiert damit wieder Schreibzugriff besteht
- mit *wget http:download.openwall.net/pub/wordlists/all.gz* wurde ein Wörterbuch runtergeladen
- durch *gunzip all.gz* wurde das Wörterbuch entpackt
- und mit *john –wordlist=all –users=webadmin /mnt/sda1/etc/shadow* der Angriff gestartet
- nach 21.01 sec war das Passwort herausgefunden: mockingbird

Aufgabe 1.3 Setzen von neuen Kennwörtern

- Das Passwort von georg ist nicht ohne weiteres ermittelbar, weil es wahrscheinlich nicht im Wörterbuch steht
- zum unmounten von sda1 wurde *umount /dev/sda1* eingegeben
- zum erneuten mounten wurde *mount -w /dev/sda1* eingegeben
- zum Ändern des root Verzeichnsises mit shell Wechsel wurde *chroot /mnt/sda1/ /bin/sh* eigegeben
- nun wurde das Passwort von georg auf *1* gesetzt: *passwd georg 1*
- es wurde das sytem durch *exit* gefolgt von *shutdown -r now* neu gestartet und sich als georg eingeloggt

[1] Werte fester Länge, typischerweise hexadezimal codiert [3]

Übungsaufgabe 2. Sichere Speicherung von Kennwörtern

Aufgabe 2.1 Angriffe mit Hashdatenbanken und Rainbow-Tables

- es wurde in das home Verzeichnis von webadmin navigiert durch *cd /home/webadmin/*
- Wechseln in das Unterverzeichnis *Rainbowtables/rcracki*
- Ausführung von *rcracki* mit *./rcracki <table-path> -l <password-file>*
- es konnten nicht alle Passwörter ermittelt werden.Vermutlich weil nicht alle Passwörter in der benutzten RainbowTable codiert waren
- eigene Programme sind immer gut, weil man weiß, was sie können, dementprecehnd dauert es aber auch lange, viel Umfang einzbauen
- diese Speicherung würde (da jedes Passwort einen Hash der Länge 128 Bit[4] generiert) $\Sigma_{i=1}^{7} 128^i$ Bit $\approxeq$ 71 Terabyte verbrauchen, während eine der gegebenen Rainbowtables nur ca. 40 MB groß ist

Aufgabe 2.2 Eigener Passwort-Cracker

Aufgabe 2.3 Eigene Kennwort-Speicherfunktion in Java

Übungsaufgabe 3. Forensische Wiederherstellung von Kennwörtern

Übungsaufgabe 4. Unsicherer Umgang mit Passwörtern in Java

Literatur

[1] http://www.cyberciti.biz/faq/understanding-etcpasswd-file-format/

[2] http://www.cyberciti.biz/faq/understanding-etcshadow-file/

[3] http://zeitstempel.hauke-laging.de/hashinfo.php

[4] http://de.wikipedia.org/wiki/Message-Digest_Algorithm_5