Benutzer- und Rechte-Verwaltung Teil 2

Linux-Kurs der Unix-AG

Zinching Dang

30./31. Mai 2012

UNIX AG
TU Kaiserslautern

RH Regionales Hochschul-
Rechenzentrum Kaiserslautern RK

Benutzer- und Gruppen-Datenbank

- Benutzer- bzw. Gruppen-Informationen sind in einzelnen Dateien gespeichert:
  - Benutzer: `/etc/passwd`
  - Benutzer-Passwörter: `/etc/shadow`
  - Gruppenzugehörigkeiten: `/etc/group`
  - Gruppen-Passwörter: `/etc/gshadow`
- Benutzer- und Gruppen-Datenbank für jeden Benutzer lesbar
- Passwort-Datenbank nicht für jeden Benutzer lesbar

Benutzer- und Gruppen-Datenbank

Grundsätzlicher Aufbau

- mehrere Spalten, jeweils durch ein „:“ getrennt
- in `/etc/passwd` bzw. `/etc/group` steht ein `x` in der zweiten Spalte (Passwortspalte)
  - Verweis auf `/etc/shadow` bzw. `/etc/gshadow`
- bei modernen Linux-Distributionen: Passwörter in `/etc/shadow` und `/etc/gshadow` sind in verschlüsselter Form (üblicherweise MD5, SHA-256 oder SHA-512 Hash mit salt)

Benutzerdatenbank

Zugriffsrechte:

- `-rw-r--r-- 1 root root 1879 /etc/passwd`

Spaltenbedeutung:

- Benutzername
- Passwort („`x`“)
- UID (Benutzerkennung)
- GID (primäre Gruppenkennung)
- GECOS (Kommentarfeld)
- `home`-Verzeichnis
- Shell

Beispiel 1: Benutzerdatenbank

- Auszug aus `/etc/passwd`:
  - `root:x:0:0:root:/root:/bin/bash`
  - `daemon:x:1:1:daemon:/usr/sbin:/bin/sh`
  - `www-data:x:33:33:www-data:/var/www:/bin/sh`
  - `haldaemon:x:108:116:Hardware abstraction layer,,,:/var/run/hald:/bin/false`
  - `linuxkurs:x:1000:1000::/home/linuxkurs:/bin/bash`

Passwortdatenbank

Zugriffsrechte:

- `-rw-r----- 1 root shadow 5164 /etc/shadow`

Spaltenbedeutung:

- Benutzername
- Passwort (hashed)
- letzte Passwort-Änderung
- Mindest- und Höchst-Alter des Passwortes
- Warnung und Frist vor Passwort-Ablauf, Konto-Sperre

Benutzerdatenbank (3)

Anmerkungen:

- Wert für letzte Passwort-Änderung und Konto-Sperre steht für die Anzahl der Tage seit dem 01.01.1970
- „*“ oder „!“ bei Passwort verbietet Passwort-basierten Login
- kein Zeichen im Passwortfeld bedeutet, dass ein Login ohne Passwort möglich ist

Beispiel 2: Passwortdatenbank

- Auszug aus `/etc/shadow`:
  - `root:$6$Vj8LKr7f$ljGFRjhnZr568HFefGiJg6i4 9nvcYaWQ25tzui85gdnGFRHu9hgfRhjIrzonjkQmLgrBpo 0642XY.uhtFCr3H.:15032:0:99999:7:::`
  - `daemon:*:15032:0:99999:7:::`
  - `www-data:*:15032:0:99999:7:::`
  - `haldaemon:*:15037:0:99999:7:::`

Gruppendatenbank

Zugriffsrechte:

- `-rw-r--r-- 1 root root 972 /etc/group`

Spaltenbedeutung:

- Gruppenname
- Passwort (wie in `/etc/passwd` ein `x`)
- Gruppenkennung (GID)
- Mitglieder (Login-Namen der Benutzer)

Beispiel 3: Gruppendatenbank

- Auszug aus `/etc/group`:
  - `root:x:0:`
  - `admin:x:1002:admin,linuxkurs`
  - `linuxkurs:x:1234:linuxkurs,sam,kim`
  - `audio:x:29:sam,kim`

Übersicht

- Befehle für die Benutzerverwaltung
  - `passwd`
  - `chfn`
  - `useradd`
  - `userdel`
  - `usermod`
  - `groupadd`
  - `groupdel`
  - `groupmod`
- Befehle für die Rechteverwaltung
  - `chmod`
  - `chown`
  - `chgrp`

passwd

- ändert das aktuelle Passwort eines Benutzers
- wichtige Optionen:
  - `-S`: zeigt Status-Informationen an:
    - Benutzernamen
    - Account-Status (**L**ocked, **N**o **P**assword, **P**assword)
    - letzte Passwortänderung als Datum
    - Mindest- und Höchst-Alter des Passwortes
    - Warnung und Frist vor Passwort-Ablauf
  - `-d`: löscht das Passwort eines Benutzers (lokaler Login ohne Passwort danach möglich)
  - `-l`: sperrt den Account eines Benutzers
  - `-u`: entsperrt den Account eines Benutzers
- Argument:
  - optional: Benutzername (nur `root` kann Passwörter anderer Benutzer ändern)
  - ohne Argument: wie Aufruf mit eigenem Benutzernamen

chfn

- ändert den GECOS-Eintrag (Kommentarfeld) eines Benutzers
- wichtige Optionen:
  - `-f NEUER_NAME`: ändert den anzeigten Namen des Benutzers
- Argument:
  - optional: Benutzername (nur `root` kann Daten anderer Benutzer ändern)
  - ohne Argument: wie Aufruf mit eigenem Benutzernamen

useradd

- erstellt einen neuen Benutzer für das System
- wichtige Optionen:
  - `-c KOMMENTAR`: Eintrag für das Kommentarfeld (GECOS)
  - `-d HOME`: Verzeichnis für das `home`-Verzeichnis
  - `-m`: erstellt das `home`-Verzeichnis für den Benutzer (bei Standard-Einstellung wird kein `home`-Verzeichnis erstellt)
  - `-g GID`: primäre Gruppe als GID oder Name
  - `-G GRUPPE1,GRUPPE2`: sekundäre Gruppe(n) als GID oder Name, jeweils mit einem Komma getrennt
  - `-u UID`: UID des neuen Benutzers, in Kombination mit `-o` können bereits vergebene UIDs benutzt werden
- Argument:
  - Benutzername (Login-Name) des Benutzers

userdel

- löscht einen Benutzer-Account
- wichtige Optionen:
  - `-r`: löscht zusätzlich das (`home`)-Verzeichnis und Mail-Spool des Benutzers
- Argument:
  - Benutzernamen (Login-Name) des Benutzers

usermod

- ändert einen Benutzer-Account ab
- wichtige Optionen:
  - `-d NEUES_HOME`: gibt das neue (`home`)-Verzeichnis des Benutzers an, in Kombination mit `-m` wird das aktuelle `home`-Verzeichnis in das neue verschoben
  - `-G GRUPPE1,GRUPPE2...`: legt die sekundären Gruppen fest, in Kombination mit `-a` werden neue Gruppen hinzugefügt
  - `-u NEUE_UID`: ändert die aktuelle UID des Benutzer, in Kombination mit `-o` können bereits vergebene UID benutzt werden
  - `-g GRUPPE`: ändert die aktuelle GID des Benutzers, die neue Gruppe muss bereits existieren
- Argument:
  - Benutzernamen (Login-Name) des Benutzers

groupadd

- erstellt eine neue Gruppe
- wichtige Optionen:
  - `-g GID`: gibt die GID der neuen Gruppe an, in Kombination mit `-o` können bereits vergebene GIDs benutzt werden
- Argument:
  - Gruppen-Name der neuen Gruppe

groupdel

- löscht eine Gruppe
- hat keine Optionen
- Argument:
  - Gruppen-Name
- Anmerkung:
  - Es können nur leere Gruppen gelöscht werden

groupmod

- ändert Eigenschaften einer Gruppe
- wichtige Optionen:
  - `-g NEUE_GID`: ändert die aktuelle GID, in Kombination mit `-o` können bereits vergebene GIDs benutzt werden
  - `-n NEUER_GRUPPEN-NAME`: ändert den aktuellen Gruppen-Namen
- Argument:
  - Gruppen-Name

Debian-spezifisch: adduser, deluser, addgroup, delgroup

- nur bei Debian-basierte Systemen (Debian, (X,K,L)Ubuntu)

Vorteile:

- interaktiv, benutzerfreundlicher
- Standard-Einstellungen lassen sich konfigurieren

Argument:

- analog zu `useradd`, `userdel`, `groupadd`, `groupdel`

chmod

- ändert die Zugriffsrechte von Dateien und Verzeichnissen
- symbolische und numerische (oktale) Notation möglich
  - symbolisch: [ugoa]*[+-=][rwxXst]*
  - oktal: [0-7][0-7][0-7][0-7]
- wichtige Optionen
  - `-c`: bei Modifikation anzeigen, was durchgeführt wurde
  - `-R`: rekursiv Dateien und Verzeichnisse ändern
- Argumente:
  - neue Zugriffsrechte (oktale oder symbolische Darstellung) und Datei/Verzeichnis

Beispiel 4: chmod (1)

```
chmod 0750 DATEI
chmod 750 DATEI
chmod u=rwx,g=rx,o-rwx DATEI
```

selbe Datei-Modifikation:

- Lese-, Schreib- und Ausführungs-Rechte für den Besitzer
- Lese- und Ausführungsrechte für Gruppenmitglieder
- keine Rechte für alle anderen

Beispiel 4: chmod (2)

```
chmod 0750 DATEI
chmod 750 DATEI
chmod u=rwx,g=rx,o-rwx DATEI
```

oktale Notation

- erste Ziffer für besondere Zugriffsrechte (SUID, SGID, Sticky Bit), kann bei Nichtverwendung weggelassen werden
- Setzen der Zugriffsrechte bei einer Ziffer für alle anderen, bei zwei Ziffern für Gruppenmitglieder und alle anderen und bei drei für Besitzer, Gruppenmitglieder und alle anderen

Beispiel 4: chmod (3)

```
chmod 0750 DATEI
chmod 750 DATEI
chmod u=rwx,g=rx,o-rwx DATEI
```

oktale Notation

- `0` für keine Zugriffsrechte, `1` für Ausführ-, `2` für Schreib-, `4` für Lese-Rechte
- Kombination von Rechten ergeben Summe der Ziffern
- für besondere Rechte: `1` für Sticky Bit, `2` für SGID, `4` für SUID

Beispiel 4: chmod (4)

```
chmod 0750 DATEI
chmod 750 DATEI
chmod u=rwx,g=rx,o-rwx DATEI
```

symbolische Notation

- u für Besitzer, g für Gruppenmitglieder und o für alle anderen
- = setzt die Zugriffsrechte, + fügt diese hinzu und - entfernt diese
- **r**ead, **w**rite, e**x**ecute, **s**et UID/GID
- **t** für Sticky Bit, **X** ausführbare Dateien werden für jeden ausführbar und Verzeichnisse werden alle ausführbar

chown

- ändert den Besitzer und Gruppe von Dateien und Verzeichnissen
- wichtige Optionen:
  - `-c`: bei Modifikation anzeigen, was durchgeführt wurde
  - `-R`: rekursiv Dateien und Verzeichnisse ändern
- Argumente:
  - neuer Benutzer und Datei/Verzeichnis
  - optional: neue Gruppe, durch „:“ vom Benutzer getrennt

chgrp

- ändert die Gruppe von Dateien und Verzeichnissen
- wichtige Optionen:
  - `-c`: bei Modifikation anzeigen, was durchgeführt wurde
  - `-R`: rekursiv Dateien und Verzeichnisse ändern
- Argumente:
  - neue Gruppe und Datei/Verzeichnis

Spickzettel

Alle Befehle

Befehl	Optionen	Argument
`passwd`	`-S, -d, -l, -u`	[Benutzername]
`chfn`	`-f NEUER_NAME`	[Benutzername]
`useradd`	`-c, -d, -m, -g, -G, -u`	Benutzername
`userdel`	`-r`	Benutzername
`usermod`	`-d, -G, -u , -g`	Benutzername
`groupadd`	`-g`	Gruppen-Name
`groupdel`		Gruppen-Name
`groupmod`	`-g, -n`	Gruppen-Name
`chmod`	`-c, -R`	Zugriffsrechte, Datei
`chown`	`-c, -R`	Besitzer:Gruppe, Datei
`chgrp`	`-c, -R`	Gruppe, Datei