5.2 Lektion 1

Zertifikat:	Linux Essentials
Version:	1.6
Thema:	5 Sicherheit und Dateiberechtigungen
Lernziel:	5.2 Benutzer und Gruppen anlegen
Lektion:	1 von 1

Einführung

Die Verwaltung von Benutzern und Gruppen auf einer Linux-Maschine ist eine der wichtigsten Aufgaben der Systemadministration, denn Linux ist ein Mehrbenutzerbetriebssystem, bei dem mehrere Benutzer gleichzeitig dieselbe Maschine benutzen können.

Informationen über Benutzer und Gruppen werden in vier Dateien innerhalb des `/etc/`-Verzeichnisbaums gespeichert:

`/etc/passwd`
: Datei mit sieben durch Doppelpunkte getrennten Feldern, die grundlegende Informationen über die Benutzer enthalten.

`/etc/group`
: Datei mit vier durch Doppelpunkte getrennten Feldern, die grundlegende Informationen über Gruppen enthalten.

`/etc/shadow`
: Datei mit neun durch Doppelpunkte getrennten Feldern, die verschlüsselte Benutzerpasswörter enthalten.

`/etc/gshadow`
: Datei mit vier durch Doppelpunkte getrennten Feldern, die verschlüsselte Gruppenpasswörter enthalten.

All diese Dateien werden durch eine Reihe von Befehlszeilen-Tools zur Benutzer- und Gruppenverwaltung aktualisiert, die wir später in dieser Lektion kennenlernen werden. Sie können auch durch grafische Anwendungen, die für jede Linux-Distribution spezifisch sind, verwaltet werden, die einfacher und intuitiver zu bedienen sind.

Warning Auch wenn die Dateien im reinen Textformat vorliegen, sollten Sie sie nicht direkt bearbeiten. Benutzen Sie immer die mit Ihrer Distribution mitgelieferten Werkzeuge für diesen Zweck.

Die Datei `/etc/passwd`

`/etc/passwd` ist eine von allen lesbare Datei mit einer Liste von Benutzern — jeder in einer eigenen Zeile:

```
frank:x:1001:1001::/home/frank:/bin/bash
```

Jede Zeile besteht aus sieben durch Doppelpunkte getrennten Feldern:

Benutzername

Der Name, mit dem sich der Benutzer am System anmeldet.

Passwort
: Das verschlüsselte Passwort (oder ein `x`, wenn Shadow-Passwörter verwendet werden).

Benutzer-ID (UID)
: Die dem Benutzer im System zugewiesene ID-Nummer.

Gruppen-ID (GID)
: Die primäre Gruppennummer des Benutzers im System.

GECOS
: Ein optionales Kommentarfeld für zusätzliche Informationen über den Benutzer, z.B. den vollständigen Namen. Das Feld kann mehrere durch Komma getrennte Einträge enthalten.

Home-Verzeichnis
: Der absolute Pfad des Home-Verzeichnisses des Benutzers.

Shell
: Der absolute Pfad des Programms, das automatisch gestartet wird, wenn sich der Benutzer am System anmeldet (normalerweise eine interaktive Shell wie `/bin/bash`).

Die Datei `/etc/group`

`/etc/group` ist eine von allen lesbare Datei mit einer Liste von Gruppen — jede in einer eigenen Zeile:

```
developer:x:1002:
```

Jede Zeile besteht aus vier durch Doppelpunkte getrennten Feldern:

Gruppenname
: Der Name der Gruppe.

Gruppenpasswort
: Das verschlüsselte Passwort der Gruppe (oder ein `x`, wenn Shadow-Passwörter verwendet werden).

Gruppen-ID (GID)
: Die ID, die der Gruppe im System zugeordnet ist.

Mitgliederliste
: Eine kommaseparierte Liste der Benutzer, die der Gruppe angehören, mit Ausnahme derer, für die dies die Hauptgruppe ist.

Die Datei `/etc/shadow`

`/etc/shadow` kann nur von root und Benutzern mit root-Rechten gelesen werden. Sie enthält die verschlüsselten Passwörter der Benutzer — jedes in einer eigenen Zeile:

```
frank:$6$i9gjM4Md4MuelZCd$7jJa8Cd2bbADFH4dwtfvTvJLOYCCCBf/.jYbK1IMYx7Wh4fEr
Xcc2xQVU2N1gb97yIYaiqH.jjJammzof2Jfr/:18029:0:99999:7:::
```

Jede Zeile besteht aus neun durch Doppelpunkte getrennten Feldern:

Benutzername
: Der Name, mit dem sich der Benutzer am System anmeldet.

Verschlüsseltes Passwort
: Das verschlüsselte Passwort des Benutzers (wenn der Wert `!` ist, ist das Konto gesperrt).

Datum der letzten Passwortänderung
: Als Anzahl der Tage seit dem 01.01.1970. Ein Wert von `0` bedeutet, dass der Benutzer das Passwort beim nächsten Zugriff ändern muss.

Mindestalter des Passworts
: Die Mindestanzahl von Tagen, die nach einer Passwortänderung vergehen muss, bevor der Benutzer das Passwort erneut ändern darf.

Maximales Passwortalter
: Die maximale Anzahl von Tagen, die vergehen muss, bevor eine Kennwortänderung erforderlich ist.

Passwort-Warnzeitraum
: Die Anzahl der Tage, bevor das Passwort abläuft — in dieser Zeit wird der Benutzer aufgefordert, das Passwort zu ändern.

Passwort-Inaktivität
: Die Anzahl der Tage nach Ablauf eines Passworts, während derer der Benutzer das Passwort aktualisieren sollte. Das Konto wird deaktiviert, wenn der Benutzer das Passwort nicht innerhalb dieser Frist ändert.

Ablaufdatum des Benutzerkontos
: Das Datum, als Anzahl der Tage seit dem 01.01.1970, zu dem das Benutzerkonto deaktiviert wird. Ein leeres Feld bedeutet, dass das Benutzerkonto nie abläuft.

Reserviertes Feld
: Ein Feld, das für eine zukünftige Verwendung reserviert ist.

Die Datei `/etc/gshadow`

`/etc/gshadow` kann nur von root und von Benutzern mit root-Rechten gelesen werden. Sie enthält verschlüsselte Passwörter für Gruppen — jedes in einer eigenen Zeile:

```
developer:$6$7QUIhUX1WdO6$H7kOYgsboLkDseFHpk04lwAtweSUQHipoxIgo83QNDxYtYwgmZTCU0qSCuCkErmyR263rvHiLctZVDR7Ya9Ai1::
```

Jede Zeile besteht aus vier durch Doppelpunkte getrennten Feldern:

Gruppenname
: Der Name der Gruppe.

Verschlüsseltes Passwort
: Das verschlüsselte Passwort für die Gruppe. Es wird verwendet, wenn ein Benutzer, der nicht Mitglied der Gruppe ist, der Gruppe mit dem

Befehl `newgrp` beitreten will. Wenn das Passwort mit `!` beginnt, darf niemand auf die Gruppe mit `newgrp` zugreifen.

Gruppenadministratoren
: Eine kommaseparierte Liste der Administratoren der Gruppe. Sie können das Passwort der Gruppe ändern und Gruppenmitglieder mit dem Befehl `gpasswd` hinzufügen oder entfernen.

Gruppenmitglieder
: Eine kommaseparierte Liste der Mitglieder der Gruppe.

Nachdem wir gesehen haben, wo Benutzer- und Gruppeninformationen gespeichert sind, schauen wir uns die wichtigsten Kommandozeilen-Tools zum Aktualisieren dieser Dateien an.

Hinzufügen und Löschen von Benutzerkonten

Unter Linux fügt man mit dem Befehl `useradd` ein neues Benutzerkonto hinzu und löscht ein Benutzerkonto mit dem Befehl `userdel`.

Wenn Sie ein neues Benutzerkonto namens `frank` mit Standardeinstellungen anlegen möchten, führen Sie Folgendes aus:

```
# useradd frank
```

Nachdem Sie den neuen Benutzer angelegt haben, können Sie mit `passwd` ein Passwort festlegen:

```
# passwd frank
Changing password for user frank.
New UNIX password:
Retype new UNIX password:
passwd: all authentication tokens updated successfully.
```

Diese beiden Befehle erfordern root-Rechte. Wenn Sie den Befehl `useradd` ausführen, werden die in den Passwort- und Gruppendatenbanken gespeicherten Benutzer- und Gruppeninformationen für den neu erstellten Benutzer-Account aktualisiert und, falls angegeben, das Home-Verzeichnis des neuen Benutzers sowie eine Gruppe mit dem gleichen Namen wie der Benutzer-Account erstellt.

Tip

Denken Sie daran, dass Sie immer das Programm `grep` verwenden können, um die Passwort- und Gruppendatenbanken zu filtern, wobei nur der Eintrag angezeigt wird, der sich auf einen bestimmten Benutzer oder eine bestimmte Gruppe bezieht. Für das obige Beispiel können Sie

```
cat /etc/passwd | grep frank
```

oder

```
grep frank /etc/passwd
```

aufrufen, um grundlegende Informationen über das neu eingerichtete Konto `frank` zu sehen.

Die wichtigsten Optionen für den Befehl `useradd` sind:

`-c`
: Erstellt ein neues Benutzerkonto mit Kommentaren (z.B. dem vollen Namen).

`-d`
: Erstellt ein neues Benutzerkonto mit dem angegebenen Home-Verzeichnis.

`-e`
: Erstellt ein neues Benutzerkonto, das zu dem angegebenen Datum deaktiviert wird.

`-f`
: Erstellt ein neues Benutzerkonto; innerhalb der angegebenen Anzahl von Tagen muss der Benutzer nach Ablauf des Passworts das Passwort aktualisieren.

`-g`
: Erstellt ein neues Benutzerkonto mit der angegebenen GID.

`-G`
: Erstellt ein neues Benutzerkonto, das den angegebenen sekundären Gruppen hinzufügt wird.

`-m`
: Erstellt ein neues Benutzerkonto mit dem angegebenen Home-Verzeichnis.

`-M`
: Erstellt ein neues Benutzerkonto ohne Home-Verzeichnis.

`-s`
: Erstellt ein neues Benutzerkonto mit der angegebenen Login-Shell.

`-u`
: Erstellt ein neues Benutzerkonto mit der angegebenen UID.

Sobald das neue Benutzerkonto erstellt ist, können Sie die Befehle `id` und `groups` verwenden, um seine UID, GID und die Gruppen, zu denen es gehört, zu ermitteln.

```
# id frank
uid=1000(frank) gid=1000(frank) groups=1000(frank)
# groups frank
frank : frank
```

Tip Denken Sie daran, die Datei `/etc/login.defs` zu überprüfen und eventuell zu editieren; sie definiert die Konfigurationsparameter, die die Erstellung von Benutzern und Gruppen steuern. Zum Beispiel können Sie den Bereich der UIDs und GIDs festlegen, die neuen Benutzer- und Gruppen-Accounts zugewiesen werden können, oder festlegen, dass Sie die Option `-m` nicht benutzen müssen, um das Home-Verzeichnis des neuen Benutzers zu erstellen, und ob das System automatisch eine neue Gruppe für jeden neuen Benutzer erstellen soll.

Um einen Benutzer-Account zu löschen, können Sie den Befehl `userdel` verwenden. Der Befehl aktualisiert die Informationen in den Account-Datenbanken und löscht alle Einträge, die sich auf den angegebenen Benutzer beziehen. Die Option `-r` entfernt auch das Home-Verzeichnis des Benutzers und seinen gesamten Inhalt sowie den Mail-Spool des Benutzers. Weitere Dateien, die sich anderswo befinden, müssen manuell gesucht und gelöscht werden.

```
# userdel -r frank
```

Auch um Benutzer-Accounts zu löschen, benötigen Sie root-Rechte.

Das Skeleton-Verzeichnis

Wenn Sie einen neuen Benutzer-Account hinzufügen und auch wenn Sie sein Home-Verzeichnis erstellen, wird das neu erstellte Home-Verzeichnis mit Dateien und Ordnern gefüllt, die aus dem Skeleton-, also Skelett-Verzeichnis (standardmäßig `/etc/skel`) kopiert werden. Die Idee dahinter ist einfach: Ein Systemadministrator möchte neue Benutzer hinzufügen, die alle dieselben Dateien und Verzeichnisse in ihrem Home-Verzeichnis haben. Wenn Sie also die Dateien und Ordner, die automatisch im Home-Verzeichnis der neuen Benutzer-Accounts erstellt werden, anpassen möchten, müssen Sie diese neuen Dateien und Ordner zum Skeleton-Verzeichnis hinzufügen.

Tip Beachten Sie, dass die Profildateien, die sich normalerweise im Skeleton-Verzeichnis befinden, versteckte Dateien sind. Wenn Sie also alle Dateien und Verzeichnisse im Skelett-Verzeichnis auflisten wollen, die in das Home-Verzeichnis der neu angelegten Benutzer kopiert werden, müssen Sie den Befehl `ls -Al` verwenden.

Hinzufügen und Löschen von Gruppen

Was die Gruppenverwaltung betrifft, können Sie mit den Befehlen `groupadd` und `groupdel` Gruppen hinzufügen oder löschen.

Um eine neue Gruppe namens `developer` zu erstellen, führen Sie den folgenden Befehl als root aus:

```
# groupadd -g 1090 developer
```

Die Option `-g` erzeugt eine Gruppe mit einer bestimmten GID.

Um die Gruppe `developer` zu löschen, führen Sie folgenden Befehl aus:

```
# groupdel developer
```

Warning Denken Sie daran, dass beim Hinzufügen eines neuen Benutzerkontos die primäre Gruppe und die sekundären Gruppen, zu denen es gehört, existieren müssen, bevor Sie den Befehl `useradd` starten. Außerdem können Sie eine Gruppe nicht löschen, wenn sie die primäre Gruppe eines Benutzerkontos ist.

Der Befehl `passwd`

Dieser Befehl wird in erster Linie verwendet, um das Passwort eines Benutzers zu ändern. Jeder Benutzer kann sein Passwort ändern, aber nur root kann das Passwort eines beliebigen Benutzers ändern.

Abhängig von der verwendeten `passwd`-Option können Sie Aspekte der Passwortgültigkeit kontrollieren:

`-d`
: Löscht das Passwort eines Benutzerkontos (und deaktiviert damit den Benutzer).

`-e`
: Zwingt den Benutzer, das Passwort zu ändern.

`-l`
: Sperrt das Benutzerkonto (dem verschlüsselten Passwort wird ein Ausrufezeichen vorangestellt).

`-u`
: Entsperrt das Benutzerkonto (entfernt das Ausrufezeichen).

`-S`
: Gibt Informationen über den Passwortstatus für ein bestimmtes Konto aus.

Diese Optionen stehen nur root zur Verfügung. Die vollständige Liste der Optionen finden Sie in den Man Pages.

Geführte Übungen

1. Geben Sie für jeden der folgenden Einträge die Datei an, auf die er sich bezieht:
   - `developer:x:1010:frank,grace,dave`
   - `root:x:0:0:root:/root:/bin/bash`
   - `henry:$1$.AbCdEfGh123456789A1b2C3d4.:18015:20:90:5:30::`
   - `henry:x:1000:1000:User Henry:/home/henry:/bin/bash`
   - `staff:!:dave:carol,emma`
2. Betrachten Sie die folgende Ausgabe, um die nächsten sieben Fragen zu beantworten:

```
# cat /etc/passwd | tail -3
dave:x:1050:1050:User Dave:/home/dave:/bin/bash
carol:x:1051:1015:User Carol:/home/carol:/bin/sh
henry:x:1052:1005:User Henry:/home/henry:/bin/tcsh
# cat /etc/group | tail -3
web_admin:x:1005:frank,emma
web_developer:x:1010:grace,kevin,christian
dave:x:1050:
# cat /etc/shadow | tail -3
dave:$6$AbCdEfGh123456789A1b2C3D4e5F6G7h8i9:0:20:90:7:30::
carol:$6$q1w2e3r4t5y6u7i8AbcDeFgHiLmNoPqRsTu:18015:0:60:7:::
henry:!$6$123456789aBcDeFgHa1B2c3d4E5f6g7H8I9:18015:0:20:5:::
# cat /etc/gshadow | tail -3
web_admin:!:frank:frank,emma
web_developer:!:kevin:grace,kevin,christian
dave:!::
```

   - Was ist die Benutzer-ID (UID) und Gruppen-ID (GID) von `carol`?
   - Welche Shell ist für `dave` und `henry` eingestellt?
   - Wie ist der Name der Hauptgruppe von `henry`?
   - Welche sind die Mitglieder der Gruppe `web_developer`? Welche von ihnen sind Gruppenadministratoren?
   - Welcher Benutzer kann sich nicht in das System einloggen?
   - Welcher Benutzer sollte das Passwort bei der nächsten Anmeldung am System ändern?
   - Wie viele Tage müssen vergehen, bis eine Passwortänderung für `carol` erforderlich ist?

Offene Übungen

1. Wenn Sie als root arbeiten, führen Sie den Befehl `useradd -m dave` aus, um einen neuen Benutzer-Account hinzuzufügen. Welche Operationen führt dieser Befehl aus? Nehmen Sie an, dass `CREATE_HOME` und `USERGROUPS_ENAB` in `/etc/login.defs` auf `yes` gesetzt sind.
2. Nun, da Sie das `dave`-Konto erstellt haben, kann sich dieser Benutzer am System anmelden?
3. Ermitteln Sie die Benutzer-ID (UID) und Gruppen-ID (GID) von `dave` und allen Mitgliedern der Gruppe `dave`.
4. Erstellen Sie die Gruppen `sys_admin`, `web_admin` und `db_admin` und ermitteln Sie deren Gruppen-IDs (GIDs).
5. Fügen Sie ein neues Benutzerkonto namens `carol` mit der UID 1035 hinzu und setzen Sie `sys_admin` als primäre Gruppe und `web_admin` und `db_admin` als sekundäre Gruppen.
6. Löschen Sie die Benutzerkonten `dave` und `carol` sowie die Gruppen `sys_admin`, `web_admin` und `db_admin`, die Sie zuvor erstellt haben.
7. Führen Sie den Befehl `ls -l /etc/passwd /etc/group /etc/shadow /etc/gshadow` aus und beschreiben Sie die Ausgabe, die er Ihnen in Bezug auf die Dateirechte gibt. Welche dieser vier Dateien werden aus Sicherheitsgründen shadowed, vorausgesetzt Ihr System verwendet Shadow-Passwörter.
8. Führen Sie den Befehl `ls -l /usr/bin/passwd` aus. Welches spezielle Bit ist gesetzt und was ist seine Bedeutung?

Zusammenfassung

In dieser Lektion haben Sie gelernt:

- Die Grundlagen der Benutzer- und Gruppenverwaltung unter Linux
- Verwalten von Benutzer- und Gruppeninformationen, die in Kennwort- und Gruppendatenbanken gespeichert sind
- Pflegen des Skeleton-Verzeichnisses
- Hinzufügen und Entfernen von Benutzerkonten
- Hinzufügen und Entfernen von Gruppenkonten
- Ändern des Kennworts von Benutzerkonten

Die folgenden Befehle wurden in dieser Lektion behandelt:

`useradd`
: Erstellt ein neues Benutzerkonto.

`groupadd`
: Erstellt ein neues Gruppenkonto.

`userdel`
: Löscht ein Benutzerkonto.

`groupdel`

Löscht ein Gruppenkonto.

`passwd`
: Ändert das Passwort von Benutzerkonten und kontrolliert alle Aspekte der Passwortgültigkeit.