Übung 4: Dateirechte

1) Accessing Another User's Home Directory

Der Superuser (`root`) setzt folgendes Kommando ab. Zur Erinnerung - er darf auf jedes Objekt des Filesystems zugreifen.

```
# ls -la /home/anyuser

(1) drwxrwx--x 2 anyuser users 8192  2025-03-14 18:33 .
(2) drwx--x--x 9 anyuser users 16384 2025-03-11 08:00 ..
(3) -rw-r--r-- 1 anyuser users 2942  2025-03-16 13:45 afile
(4) drwx------ 2 anyuser users 4096  2025-03-14 18:33 dir
(5) -rw-r--r-- 1 anyuser users 4039  2025-09-22 08:18 .profile
```

Beantworten Sie folgende Fragen und begründen Sie Ihre Anwort:

1. Einem Eindringling ist es gelungen, den Account eines Standardbenutzers (nicht den des Superusers) zu knacken. Dieser Account ist NICHT Mitglied der Gruppe `users` und es handelt sich nicht um den Account `anyuser`. Welche Ausgabe produziert das Kommando `ls /home`, wenn es von diesem Eindringling abgesetzt wird?

Lösung:

Das Kommando `ls /home` produziert "*permission denied*", da hier die Rechte für `others` am Verzeichnis `/home` gelten. Der Eindringling gehört zur Gruppe `others` und `others` hat keine Leserechte (r-Recht) am Verzeichnis `/home`. (siehe Zeile 2 im Beispiel)

2. Der Eindringling weiß, daß es einen Benutzer `anyuser` gibt. Was passiert, wenn der Eindringling folgende Kommandos eingibt?

   ```
   cd /home/anyuser
   ls
   ```

Lösung:

Das Kommando `cd /home/anyuser` funktioniert, da das x-Recht das `cd`-Kommando für die Gruppe `others` erlaubt. (siehe Zeile 1 und 2 im Beispiel).
Das Kommando `ls` aber liefert für die Gruppe `others` ein "*permission denied*", da hier das r-Recht für die Gruppe `others` am Verzeichnis `/home/anyuser` notwendig wäre, aber fehlt. (siehe Zeile 1 im Beispiel)

3. Der Eindringling versucht die Datei `.profile` des Benutzers `anyuser` mit einem Editor zu öffnen. Zum Beispiel mit dem Kommando `nano .profile`. Was passiert?

Lösung:

Bei diesem Kommando gelten die Rechte für die Datei `.profile`. Der Eindringling kann zwar den Dateinamen nicht sehen, weil er kein `ls` absetzen kann. Wenn er aber weiß, dass diese Datei existiert, kann er die Datei lesend mit dem Editor öffnen. Änderungen kann er aber nicht speichern, da ihm das Schreibrecht auf `.profile` fehlt. (siehe Zeile 5 im Beispiel)

4. Ein anderer Benutzer mit dem Account `good_guy`, der Mitglied der Gruppe `users` ist, gibt folgende Kommandos ein. Beschreiben Sie die Wirkung jedes einzelnen Kommandos und begründen Sie die Antworten.

```
cd /home/anyuser
ls
rm afile
```

Lösung:

- Kommando `cd /home/anyuser`: Funktioniert, da die Gruppe `users` auf `/home` und `/home/anyuser` das x-Recht hat. (Zeile 1 und Zeile 2)
- Kommando `ls`: Funktioniert, da die Gruppe `users` auf `/home/anyuser` das r-Recht hat. (Zeile 1)
- Kommando `rm afile`: Funktioniert auch, da hierfür nur das Schreibrecht am Verzeichnis `/home/anyuser` notwendig ist. (Zeile 1). Die Berechtigung auf dem File `afile` spielen für das Löschen eines Files keine Rolle (Zeile 3).

5. Nun probiert der Benutzer `good_guy` folgendes Kommando `cd dir`. Was passiert?

Lösung:

Liefert "*permission denied*", da keinerlei Rechte für die Gruppe `users` auf dem Verzeichnis `dir` existieren (Zeile 4)

2) Controlling Default Permissions

Ein Anwender gibt folgendes Kommando ein:

```
umask 027
```

Dann führt er folgende Kommandos aus:

```
touch a
mkdir d
```

1. Welche Berechtigungsbits wurden für die Datei `a` und das Verzeichnis `d` gesetzt?

Lösung:

```
-rw-r----- 1 root root 0    Jun 24 14:11 a
drwxr-x--- 2 root root 4096 Jun 24 14:11 d
```

Berechnung: Verzeichnis: 777 – 027 = 750 (rwxr-x---) File: 666 – 026 = 640 (rw-r-----)

2. Welche `umask` wäre notwendig um folgende Berechtigungsbits zu erhalten?

```
-rw------- 1 root root 0    Jun 24 14:11 a
drwx------ 2 root root 4096 Jun 24 14:11 d
```

Lösung:

```
umask 077
```

Berechnung:
Verzeichnis: 777 - ? =700 (=> ?=077)
File: 666 -? = 600 (=> ?=066)
Allerdings wird IMMER nur eine `umask` verwendet, man nimmt die für das Verzeichnis gültige `umask`, daher `umask 077`.

3) Protecting Files From Yourself!

In Ihrem Home-Verzeichnis befindet sich die finale Version Ihrer Bachelorarbeit, gespeichert in der Datei `thesis_final.doc`. Weder der Name dieser Datei noch ihr Inhalt darf verändert werden (auch nicht durch Sie selbst), da Sie sie bereits abgegeben haben. Dazu gehört auch, daß Sie sie vor ungewollten Dateimanipulationen (z.b. durch die Kommandos `mv` oder `cp` , die von Ihnen selbst abgesetzt wurden) schützen müssen. Wie gehen Sie vor?

Lösung:

1. Neues Unterverzeichnis anlegen (z.B. `thesis`) und Dokument `thesis_final.doc` dorthin kopieren.
2. Auf `thesis_final.doc` folgende Rechte setzen: (`user` sind Sie selbst, `group` und `others` spielen keine Rolle)

```
-r-------- ... thesis_final.doc
cd ..
```

3. Nun auf das Verzeichnis `thesis` das r- und x- Recht für `user`, aber keine Rechte für `group` und `others` setzen. (`user` sind Sie selbst, `group` und `others` spielen keine Rolle)

```
dr-x------ ... thesis
```

4) Sharing Files (Carefully)

Sie waren auf Urlaub und haben viele digitale Fotos gemacht, die Sie den Studienkollegen Ihres Jahrgangs nicht vorenthalten wollen, allen anderen Benutzern des Systems wollen Sie jedoch keine Einsicht in Ihre Urlaubserinnerungen geben. Sie beschließen, die Fotos in ein Verzeichnis `xfotos`, das sich unter Ihrem Homeverzeichnis befindet, zu kopieren.

- Setzen Sie die Rechte so, daß Sie selbst alle Fotos ansehen und bearbeiten können, Ihre Studienkollegen allerdings keine Rechte haben, die Fotos zu bearbeiten, umzubenennen oder gar zu löschen.
- Können Sie dieses Vorhaben alleine realisieren oder brauchen Sie für die Umsetzung die Unterstützung des Superusers?

Lösung:

Sie brauchen eine Gruppe für Ihre KollegInnen (z.B. eine Gruppe `collegues`). Falls Sie superuser Rechte haben (z.B. `sudo`) können Sie diese Gruppe selbst anlegen und alle betroffenen Kollegen in die Gruppe eintragen, sonst brauchen Sie den Superuser zum Anlegen und Einfügen der KollegInnen in diese Gruppe.

Dann legen Sie das Verzeichnis `xfotos` in Ihrem Homeverzeichnis an und kopieren alle Fotos in dieses Verzeichnis `xfotos`. Die Rechte sind folgender maßen zu setzen (angenommen Ihr Benutzername wäre `mustermann`):

```
drwxr-x--- 2 mustermann collegues 4096 Jun 24 14:11 xfotos

cd xfotos
ls -l

-rw-r----- 2 mustermann collegues 1276 Jun 24 14:11 pic01.jpg
-rw-r----- 2 mustermann collegues 3417 Jun 24 14:11 pic02.jpg
-rw-r----- 2 mustermann collegues 1232 Jun 24 14:11 pic03.jpg
...
-rw-r----- 2 mustermann collegues 1211 Jun 24 14:11 pic99.jpg
```