1 b. Zusatzaufgaben zu Linux-Benutzern, sudo, Besitzrechten und Sonderrechten.

1. Der Benutzer `hund` soll Superuser-/Root-Rechte erhalten. Was ist zu tun?

Antwort anzeigen

Der Benutzer muss zur Gruppe der Administratoren (sudo-Gruppe) hinzugefügt werden:

```
sudo usermod -aG sudo hund
```

Danach muss sich der Benutzer neu anmelden, damit die Gruppenrechte aktiv werden.

---

2. Der Benutzer `hund` kann mit `sudo <befehl>` arbeiten und muss dabei sein Passwort eingeben. Gibt es eine Möglichkeit, ohne Passwortabfrage zu arbeiten?

Antwort anzeigen

Ja, dies ist über die Konfigurationsdatei `/etc/sudoers` möglich.

Ein entsprechender Eintrag lautet:

```
hund ALL=(ALL:ALL) NOPASSWD: ALL
```

Die Datei sollte aus Sicherheitsgründen nicht direkt bearbeitet werden, sondern mit:

```
sudo visudo
```

---

3. Der `tagesplan` soll in den Besitz des Benutzers `hund` übergehen und in seinen Heimatordner verschoben werden. Was ist zu tun?

Antwort anzeigen

Zuerst wird der Besitzer der Datei geändert:

```
sudo chown hund:hund tagesplan
```

Danach wird die Datei in das Heimatverzeichnis verschoben:

```
mv tagesplan /home/hund/
```

Je nach Speicherort der Datei muss der Pfad angepasst werden.

---

4. Beim Anlegen von Benutzern sind manchmal schon Dateien oder Ordner vorhanden, zum Beispiel unter `ubuntu` die Datei `examples.desktop`. Woher kommen diese?

Antwort anzeigen

Diese Dateien stammen aus dem Vorlagenverzeichnis für neue Benutzer:

`/etc/skel`

Beim Anlegen eines neuen Benutzers wird dieses Verzeichnis in das Home-Verzeichnis kopiert.

---

5. Was ist der Nutzen solcher bereits vorhandenen Dateien und Ordner im Home-Verzeichnis?

Antwort anzeigen

Diese Dateien stellen eine Grundausstattung für neue Benutzer bereit.

Dazu gehören beispielsweise:

- Beispiel-Dateien
- voreingestellte Konfigurationen
- vorbereitete Ordnerstrukturen

Dadurch kann der Benutzer sofort mit einer sinnvollen Umgebung arbeiten.

---

6. Welche Aufgabe hat das Set-UID-Recht (SUID-Bit)?

Antwort anzeigen

Ein Programm wird mit den Rechten des Dateibesitzers ausgeführt und nicht mit den Rechten des Benutzers, der es startet.

Dadurch können Programme kurzfristig mit erweiterten Rechten ausgeführt werden.

---

7. Welche Aufgabe hat das Set-GID-Recht (SGID-Bit)?

Antwort anzeigen

Bei Dateien wird ein Programm mit den Rechten der Gruppe ausgeführt.

Bei Verzeichnissen sorgt das SGID-Bit dafür, dass neu angelegte Dateien und Ordner automatisch die Gruppe des Verzeichnisses übernehmen.

---

8. Welche Aufgabe hat das Sticky-Bit?

Antwort anzeigen

In einem Verzeichnis mit gesetztem Sticky-Bit dürfen Dateien nur vom jeweiligen Eigentümer, vom Verzeichnisbesitzer oder von root gelöscht oder umbenannt werden.

Ein typisches Beispiel ist das Verzeichnis:

`/tmp`

---

9. Wie werden diese Sonderrechte gesetzt und dargestellt?

Antwort anzeigen

Die Sonderrechte werden mit dem Befehl `chmod` gesetzt:

SUID setzen:
`chmod u+s datei`

SGID setzen:
`chmod g+s datei`

Sticky-Bit setzen:
`chmod +t verzeichnis`

Die Darstellung erfolgt mit `ls -l`:

- SUID: `s` oder `S` im Benutzer-Bereich
- SGID: `s` oder `S` im Gruppen-Bereich
- Sticky-Bit: `t` oder `T` im Other-Bereich

Kleinbuchstaben bedeuten, dass zusätzlich das Ausführungsrecht gesetzt ist.
Großbuchstaben bedeuten, dass das Ausführungsrecht fehlt.

---

10. Welchen Vorteil hat das Sticky-Bit gegenüber dem normalen Schreibrecht auf einen Ordner?

Antwort anzeigen

Ohne Sticky-Bit kann jeder Benutzer mit Schreibrechten in einem Verzeichnis auch Dateien anderer Benutzer löschen.

Mit gesetztem Sticky-Bit wird dies verhindert, sodass Benutzer nur ihre eigenen Dateien löschen können.

Dadurch wird die Sicherheit in gemeinsam genutzten Verzeichnissen erhöht.

Revision #5
Created 14 April 2026 23:40:16 by Admin
Updated 19 May 2026 07:12:35 by Admin