TECH STARTER

1.2.6. Sicherheitsgrundlagen in Linux

Übungsaufgabe I

Aufgabe 1: Benutzerverwaltung

1. **Neuen Benutzer erstellen:**
   - Erstelle einen neuen Benutzer „testuser“ mit dem Befehl `useradd`.

     sudo useradd -m -s /bin/bash testuser

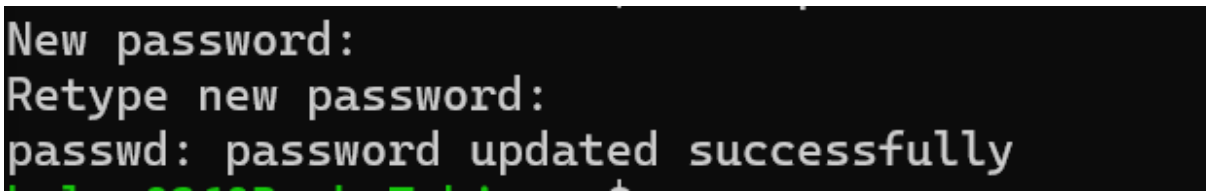
   - Überprüfe die Informationen zu diesem Benutzer in der Datei `/etc/passwd`.

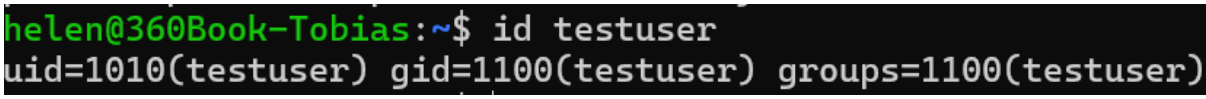
     cat /etc/passwd | grep testuser

2. **Befehlshilfe**:
   - `sudo useradd testuser`
   - `cat /etc/passwd | grep testuser`
3. **Passwort für den Benutzer setzen:**
   - Setze ein Passwort für „testuser“.

     sudo passwd testuser

4. **Befehlshilfe:**
   - `sudo passwd testuser`
5. **Benutzerinformationen abrufen:**
   - Zeige die Benutzer-ID (UID), Gruppen-ID (GID) und alle Gruppenmitgliedschaften von „testuser“ an.

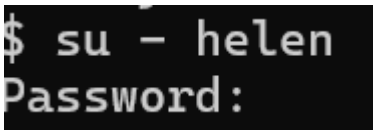
   Befehlshilfe:

   - `id testuser`

Aufgabe 2: Superuser-Account und sudo-Befehl

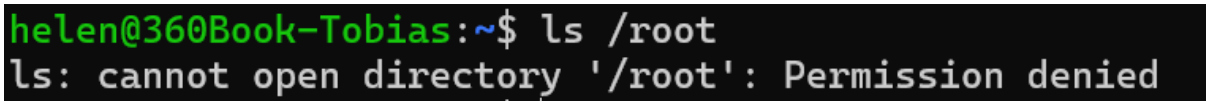
1. **Wechsel zum Superuser:**
   - Wechsle zum Superuser `root` mit dem Befehl `su`, und kehre dann zum regulären Benutzer zurück.

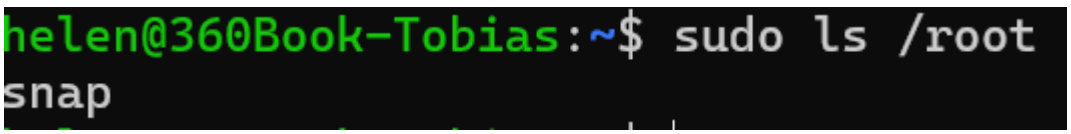
     su - (dann muss das root-Passwort eingegeben werden, in der Praxis sollte aber ein normaler Benutzer dieses nicht haben, das wäre ein Sicherheitsrisiko)
     i.A. versuchen wir mit su - <username> den Benutzer zu wechseln

     Achtung!! Wir brauchen dann aber das Passwort von unserem User!

2. **Befehlshilfe**:
   - `su -`
   - `exit`
3. **Verwendung von sudo:**
   - Versuche, den Befehl `sudo ls /root` mit einem normalen Benutzer auszuführen, und gib dein Passwort ein, wenn du dazu aufgefordert wirst.

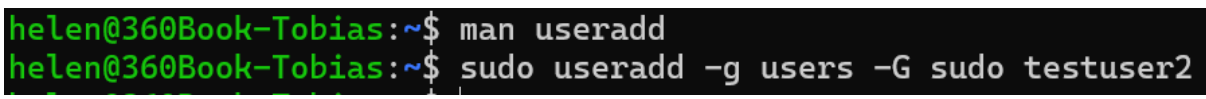
     

4. **Befehlshilfe:**
   - `sudo ls /root`

Aufgabe 3: Gruppenzuordnung

1. **Primäre und sekundäre Gruppen:**
   - Erstelle einen Benutzer „testuser2“ und ordne ihm eine primäre Gruppe „users“ zu. Füge ihn auch der Gruppe „sudo“ als sekundäre Gruppe hinzu.

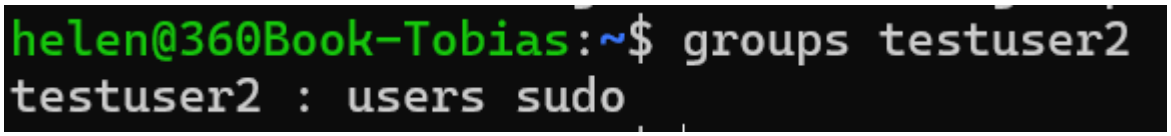
     

     Ich habe erstmal die Manpage aufgerufen und dann nach /group gesucht, um zu erfahren, wie ich die primäre Gruppe (mit -g) und die sekundären Gruppen (-G) bei einem User mit erstellen kann.

Dann habe ich den Befehl sudo useradd mit diesen Parametern durchgeführt.

- -g users: Hier setze ich die primäre Gruppe auf die Gruppe users
- -G sudo: Hier füge ich den neu erstellten Benutzer zur sudo-Gruppe hinzu

2. **Befehlshilfe**:
   - `sudo useradd -g users -G sudo testuser2`
   - `id testuser2`
3. **Gruppenmitgliedschaften anzeigen:**
   - Überprüfe, zu welchen Gruppen der Benutzer „testuser2“ gehört.



4. **Befehlshilfe:**
   - `groups testuser2`

Aufgabe 4: System- und Servicekonten

1. **Systemkonten identifizieren:**
   - Zeige die Informationen für Systemkonten mit UID unter 100 an, indem du die Datei `/etc/passwd` durchsucht.

2. **Befehlshilfe**:
   - `cat /etc/passwd | awk -F':' '{ if ($3 < 100) print $1, $3}'`
3. **Servicekonten erstellen:**

- Erstelle einen neuen Benutzer „serviceuser“ mit einer UID über 1000, ohne ein Home-Verzeichnis und ohne Login-Shell (z.B. `/sbin/nologin`).

```
helen@360Book-Tobias:~$ man useradd
helen@360Book-Tobias:~$ sudo useradd -M -s /sbin/nologin serviceus
er
helen@360Book-Tobias:~$ cat /etc/passwd | grep serviceuser
serviceuser:x:1012:1012::/home/serviceuser:/sbin/nologin
helen@360Book-Tobias:~$ sudo ls /home
andre  helen  new  testuser  tre  wasser
```

Ich öffne die Manpage, um herauszufinden, wie ich einen Account ohne Home-Verzeichnis anlegen kann → -M
Darüber hinaus möchte ich mit -s eine ungültige Login-Shell hinterlegen. Diese hat den Namen /sbin/nologin

Wenn wir den user dann erstellt haben, sehen wir dass er eine UID über 1000 hat. Das ist normal bei Serviceaccounts. Systemaccounts haben dahingegen eine UID von < 100, also 2-stellig, aber haben auch kein Home-Verzeichnis und keine gültige Login-Shell.

4. **Befehlshilfe:**
   - `sudo useradd -M -s /sbin/nologin serviceuser`
   - `cat /etc/passwd | grep serviceuser`

Aufgabe 5: Home-Verzeichnisse und Login-Shells

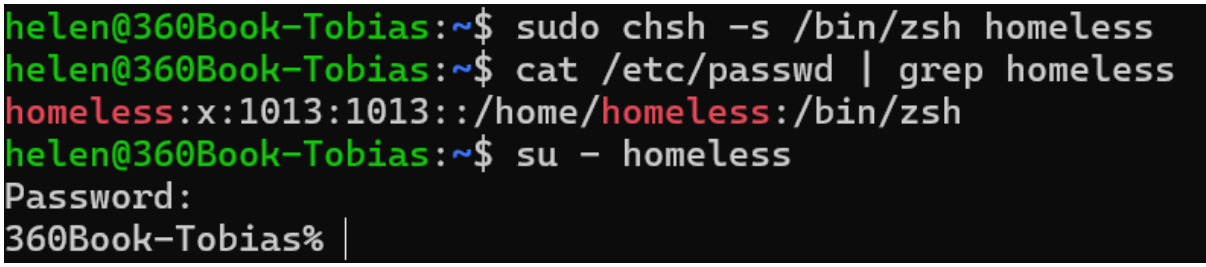
1. **Home-Verzeichnis anlegen:**
   - Erstelle einen Benutzer „homeless“ ohne automatisches Home-Verzeichnis. Füge dann manuell ein Home-Verzeichnis für diesen Benutzer hinzu.

```
helen@360Book-Tobias:~$ sudo useradd -M homeless
helen@360Book-Tobias:~$ cat /etc/passwd | grep homeless
homeless:x:1013:1013::/home/homeless:/bin/sh
helen@360Book-Tobias:~$ sudo ls /home
andre  helen  new  testuser  tre  wasser
helen@360Book-Tobias:~$ sudo mkdir /home/homeless
helen@360Book-Tobias:~$ sudo chown homeless:homeless /home/homeles
s
helen@360Book-Tobias:~$ sudo passwd homeless
New password:
Retype new password:
passwd: password updated successfully
helen@360Book-Tobias:~$ su - homeless
```

Ich habe den user mit useradd -M angelegt, also ohne Home-Verzeichnis.

Nachträglich habe ich in /home ein /homeless-Unterverzeichnis angelegt (brauchen sudo-Rechte). Hiervon mussten wir aber noch den Besitz auf unseren homeless-User ändern. Ansonsten hat dieser keine Schreibrechte auf sein Home-Verzeichnis. Wir können das testen, indem wir uns mit dem homeless user mit su - homeless anmelden (Achtung: Wir brauchen vorher ein Passwort, das wir mit sudo passwd homeless setzen). Dann sehen wir ein Home-Verzeichnis.

2. **Befehlshilfe:**
   - `sudo useradd -M homeless`
   - `sudo mkdir /home/homeless`
   - `sudo chown homeless:homeless /home/homeless`
   - `ls -ld /home/homeless`
3. **Login-Shell ändern:**
   - Ändere die Login-Shell von „homeless“ auf Bash.



4. **Befehlshilfe:**
   - `sudo chsh -s /bin/bash homeless`

Aufgabe 6: Benutzerinformationen und Logins

1. **Anmeldungen überprüfen:**
   - Verwende den Befehl `who`, um die derzeit angemeldeten Benutzer anzuzeigen.
2. **Befehlshilfe:**
   - `who`
3. **Letzte Anmeldungen anzeigen:**
   - Verwende den Befehl `last`, um die letzten Benutzeranmeldungen auf dem System anzuzeigen.
4. **Befehlshilfe:**
   - `last`