TECH STARTER

1.2.6. Sicherheitsgrundlagen in Linux

Übungsaufgabe II

Aufgabe 1: Dateiberechtigungen abfragen und ändern

1. **Dateiberechtigungen anzeigen**:
   - Erstelle eine neue Datei „logfile.txt“ in deinem Home-Verzeichnis.
   - Zeige die detaillierten Dateiberechtigungen an.
2. **Befehlshilfe**:
   - `touch logfile.txt`
   - `ls -l logfile.txt`
3. **Dateiberechtigungen ändern**:
   - Ändere die Berechtigungen von „logfile.txt“, sodass der Besitzer lesen und schreiben, die Gruppe nur lesen und andere keine Berechtigungen haben.
4. **Befehlshilfe**:
   - `chmod 640 logfile.txt`
   - `ls -l logfile.txt`

Aufgabe 2: Verzeichnisse und spezielle Berechtigungen

1. **Verzeichnis erstellen und Berechtigungen setzen**:
   - Erstelle im `/tmp`-Verzeichnis einen Ordner „backup“.
   - Setze die Berechtigungen so, dass der Besitzer alles (lesen, schreiben, ausführen) darf, die Gruppe nur lesen und ausführen, und andere keine Rechte haben.
2. **Befehlshilfe**:
   - `mkdir /tmp/backup`
   - `chmod 750 /tmp/backup`
   - `ls -ld /tmp/backup`
3. **Sticky Bit setzen**:
   - Setze das Sticky Bit auf das Verzeichnis „backup“, damit nur der Besitzer Dateien darin löschen kann.
4. **Befehlshilfe**:
   - `chmod +t /tmp/backup`
   - `ls -ld /tmp/backup`

Aufgabe 3: Symbolische und Hard Links

1. **Symbolischen Link erstellen**:
   - Erstelle einen symbolischen Link „log_link.txt“ im `/tmp`-Verzeichnis, der auf die Datei „logfile.txt“ in deinem Home-Verzeichnis verweist.
2. **Befehlshilfe**:

   - `ln -s ~/logfile.txt /tmp/log_link.txt`
   - `ls -l /tmp/log_link.txt`
3. **Hard Link erstellen**:
   - Erstelle einen Hard Link „log_hardlink.txt“ im `/tmp`-Verzeichnis, der ebenfalls auf „logfile.txt“ verweist.
4. **Befehlshilfe**:
   - `ln ~/logfile.txt /tmp/log_hardlink.txt`
   - `ls -l /tmp/log_hardlink.txt`

Aufgabe 4: Erweiterte Berechtigungen mit SUID und SGID

1. **SUID-Bit setzen**:
   - Erstelle ein Skript „run_me.sh“ in deinem Home-Verzeichnis und setze das SUID-Bit, damit es immer mit den Rechten des Dateibesitzers ausgeführt wird.
2. **Befehlshilfe**:
   - `touch ~/run_me.sh`
   - `chmod u+s ~/run_me.sh`
   - `ls -l ~/run_me.sh`
3. **SGID-Bit auf einem Verzeichnis setzen**:
   - Erstelle ein Verzeichnis „shared_dir“ in deinem Home-Verzeichnis. Setze das SGID-Bit, sodass alle darin erstellten Dateien die Gruppenzugehörigkeit des Verzeichnisses erben.
4. **Befehlshilfe**:
   - `mkdir ~/shared_dir`
   - `chmod g+s ~/shared_dir`
   - `ls -ld ~/shared_dir`

Aufgabe 5: Dateibesitz ändern

1. **Besitzer einer Datei ändern**:
   - Ändere den Besitzer der Datei „logfile.txt“ auf den Benutzer „nobody“ und die Gruppe auf „nogroup“.
2. **Befehlshilfe**:
   - `sudo chown nobody:nogroup ~/logfile.txt`
   - `ls -l ~/logfile.txt`
3. **Besitzer eines Verzeichnisses und seiner Inhalte ändern**:
   - Ändere den Besitzer des Verzeichnisses „shared_dir“ und aller darin befindlichen Dateien rekursiv auf den Benutzer „nobody“.
4. **Befehlshilfe**:
   - `sudo chown -R nobody ~/shared_dir`
   - `ls -ld ~/shared_dir`

Aufgabe 6: Temporäre Dateien und Berechtigungen

1. **Temporäre Dateien erstellen und Berechtigungen überprüfen**:
    - Erstelle eine temporäre Datei „tempfile.txt“ im `/tmp`-Verzeichnis und überprüfe die standardmäßigen Dateiberechtigungen.
2. **Befehlshilfe**:
    - `touch /tmp/tempfile.txt`
    - `ls -l /tmp/tempfile.txt`
3. **Berechtigungen von temporären Dateien ändern**:
    - Ändere die Berechtigungen der temporären Datei „tempfile.txt“, sodass nur der Besitzer alle Rechte hat und Gruppe sowie andere keine Rechte haben.
4. **Befehlshilfe**:
    - `chmod 700 /tmp/tempfile.txt`
    - `ls -l /tmp/tempfile.txt`