

A Übungsziel

In dieser Übung wollen wir die Zugriffssteuerung auf Dateien und Ordner unter Linux kennen und anwenden lernen. Dazu werden wir beispielhaft eine Berechtigungsstruktur einer kleinen Firma anlegen.

B Plattform und Durchführung

Sie benötigen für diese Übung wieder ein Kali-Linux-System, auf dem Sie als Benutzer das Recht haben, Superuser-(root)-Privilegien (etwa mittels **sudo**) zu erhalten. Am besten verwenden Sie eine der vorbereiteten virtuellen Maschinen – dort ist es der User **junioradmin**, also mit **junioradmin** anmelden!

Dokumentieren Sie in Ihrem Protokoll *jede* der verwendeten Befehlszeilen!

C Wiederholung Benutzererstellung (siehe letzte Übung)

Legen Sie mittels Skript die folgenden Gruppen und Benutzer (und Verzeichnisse) an: Verwenden Sie in dieser Übung statt **IhrLogin** Ihren Schul-Loginnamen mit Ihrer 4-stelligen Nummer und vorangestelltem “s” (z.B. s9999)!

Benutzername	Name	Hauptgruppe	Benutzerverzeichnis	Passwort
abuchmacher	Alf Buchmacher	buchhaltung	/home/bh/abuchmacher	pferde2525
bfernerreiser	Bert Fernreiser	buchhaltung	/home/bh/bfernerreiser	karibiktraum25
hscheffe	Herbert Scheffe	mgmt	/home/mgmt/hscheffe	king
IhrLogin	IhrName	mgmt	/home/mgmt/IhrLogin	ganzgeheim2525
utipp	Ulla Tipp	verwaltung	/home/verwaltung/utipp	blumenkind
hhuber	Hans Huber	personal	/home/personal/hhuber	IchWerdeChef
ggruber	Gabi Gruber	personal	/home/personal/ggruber	gabi73

Jeder User soll im Skript mit einer einzigen Befehlszeile und obigen Daten angelegt werden.

Tipp 1: Legen Sie zuerst die Unterverzeichnisse **bh**, **mgmt**, **verwaltung** und **personal** an!

Tipp 2: Wieder wollen Sie in der Regel die Passwortvergabe nicht von Hand mit dem Befehl **passwd** vornehmen, sondern auch über unser Skript automatisieren (*was ist aber am Skripten der Passwortheingabe eventuell problematisch - was muss man auf jeden Fall beachten?*) – Sie können Sie dazu den Befehl **chpasswd** verwenden (mittels der Befehlszeile: **echo user:password | chpasswd**)!

D Dateiberechtigungen – Befehle

Schauen Sie sich die *Manual-Pages* (oder Web-Recherche, z.B. Suche nach **man chown** führt meist zum Ziel) zu folgenden Befehlen an: **chmod**, **chown**, **chgrp** und beantworten Sie damit die folgende Fragen:

- (1) Wie können Sie sich die Berechtigungen einer Datei oder eines Verzeichnisses anzeigen lassen?
- (2) Wie können Sie Besitzer und Gruppe einer Datei bzw. eines Verzeichnisses mit *einem* Befehl ändern bzw. zuweisen?
- (3) Wie können Sie den Besitzer von einem Verzeichnis sowie von allen Unterverzeichnissen und Dateien darunter auf einmal verändern?
- (4) Was macht der Parameter **-c** im Befehl **chown** bzw. im Befehl **chgrp**?

- (5) Was macht **chmod** mit symbolischen Links (*wirkt es auf den Link oder die Zielfeile - bitte ausprobieren mit `ln -s`!*)?
- (6) Was bedeutet das *Sticky-Bit* auf Verzeichnissen (*Tipp: Handout S.3*)?
- Sie können und sollten Ihre Antworten auch durch Ausprobieren (Testen) in Ihrer Linux-VM verifizieren!

D Dateiberechtigungen – Praxis I

- (7) Dokumentieren Sie und beschreiben Sie die Bedeutung der Berechtigungen der Dateien **/etc/passwd**, **/etc/shadow**, **/usr/bin/passwd**, **/var/log/dmesg** und des Ordners **/home**! Wie würde die oktale Schreibweise dieser Berechtigungen ausschauen?
- (8) Betrachten Sie die Berechtigungen der oben erzeugten Benutzerverzeichnisse
- Wer ist Besitzer? Welche ist die zugehörige Gruppe? (z. B. **/home/bh/abuchmacher**)
 - Welche Berechtigungen existieren - „wer kann was“ in diesen Verzeichnissen machen?
- Achtung: bitte Namen angeben, z.B. „Hans darf ...“ und nicht „der Besitzer darf ...“

Verändern Sie die zugehörige Gruppe der den Benutzer-(Heimat-)Verzeichnissen übergeordneten Ordner wie folgt (*geben Sie die verwendeten Befehle an*):

- **/home/bh** zugehörige Gruppe: **buchhaltung**
- **/home/personal** zugehörige Gruppe: **personal**
- **/home/verwaltung** zugehörige Gruppe: **verwaltung**
- **/home/mgmt** zugehörige Gruppe: **mgmt**

F Dateiberechtigungen – Praxis II

Achtung:

- *Geben Sie stets die **verwendeten Befehle** an!*
 - *Geben Sie nach Fertigstellung und Test der Ordnerberechtigungen die **Ausgabe eines Listings `ls -ld`** eines jeden erzeugten Ordners in Ihr Protokoll, damit die letztendlich gesetzten Berechtigungen dokumentiert und nachvollziehbar sind (Beispiel: Ausgabe von `ls -ld /data_xxxx/buchhaltung`)!*
- (9) Wir wollen gemeinsam genutzte Ordner für die Arbeitsdokumente der einzelnen Abteilungen anlegen:
- a. Erzeugen Sie ein Verzeichnis **/data_xxxx/buchhaltung** (mit `xxxx`=Ihrer vierstelligen Eduvidual-Nummer; der Besitzer des Verzeichnisses soll **root** sein), in dem alle Mitglieder der Gruppe **buchhaltung** schreiben können und alle anderen keinerlei Berechtigungen haben (natürlich sollen die berechtigten Benutzer auch das Verzeichnis lesen bzw. in das Verzeichnis wechseln dürfen).
 - b. Erzeugen Sie weiters die Verzeichnisse **/data_xxxx/personal** sowie **/data_xxxx/verwaltung**, in denen analog zuvor wieder nur die entsprechenden Gruppen schreiben dürfen.
 - c. *IhrLogin* soll allerdings überall schreiben dürfen!
- (10) **WICHTIG:** *Testen der Sicherheitsstruktur.* Überlegen Sie sich für jede der folgenden Aktionen, ob sie theoretisch möglich ist oder nicht. Dann führen Sie die Aktion aus und dokumentieren Sie! Schreiben Sie also in dieses *Testprotokoll*, ob es gehen sollte oder nicht und das tatsächliche Ergebnis Ihres Tests

(Empfehlung: **Tabelle** – welcher Befehl, welcher Benutzer, erwartetes Ergebnis, wirkliches Ergebnis, in Ordnung?):

- a. Erzeugen Sie eine Datei im Verzeichnis **/data_xxxx/buchhaltung** als Benutzer **abuchmacher**.
- b. Erzeugen Sie eine Datei im Verzeichnis **/data_xxxx/verwaltung** als Benutzerin **utipp**.
- c. Erzeugen Sie einen neuen Ordner im Verzeichnis **/data_xxxx/personal** als Benutzer **hhuber**.
- d. Lassen Sie sich alle Dateien des Ordners **/data_xxxx/buchhaltung** als Benutzerin **utipp** anzeigen.
- e. Lassen Sie sich alle Dateien der Verzeichnisse **data_xxxx/buchhaltung**, **/data_xxxx/personal** und **/data_xxxx/verwaltung** als Benutzer *IhrLogin* anzeigen.
- f. **ggruber** soll eine Datei im Verzeichnis **/data_xxxx/buchhaltung** erzeugen.
- g. Erzeugen Sie eine Datei im Verzeichnis **/data_xxxx/personal** als Benutzer/in *IhrLogin*.
- h. Wie fügen Sie als Benutzer/in *IhrLogin* an das Ende einer Datei im Verzeichnis **/data_xxxx/buchhaltung** den Text “Der Chef war da!” hinzu? Funktioniert das? Warum?
- i. Löschen Sie als Benutzer/in *IhrLogin* eine Datei im Verzeichnis **/data_xxxx/buchhaltung**! Funktioniert das? Warum?
- j. Erzeugen Sie ein Verzeichnis **/data_xxxx/fueralle**, das der Gruppe **mgmt** und dem/der Benutzer/in *IhrLogin* gehört, der in diesem Verzeichnis Dateien anlegen, löschen und umbenennen darf. Alle anderen Mitarbeiter des Konzerns dürfen darin nur lesen (also Inhalt auflisten und in das Verzeichnis wechseln).

Viel Spaß!