



# Praktikum 3

## Dateirechte

Zu bearbeiten bis zum 09. Mai 2023

Cybersecurity im Sommersemester 2023

Jan Wichelmann, Anja Köhl

### Einführung

Ziel dieses Praktikums ist ein tieferes Verständnis der Funktionsweise von Linux-Dateirechten. Im Rahmen der Praktikumszeit soll ein Home-Verzeichnis abgesichert werden, wobei jedoch einige spezielle Zugänge für bestimmte Benutzer gewährleistet werden müssen.

### Aufgabe 1 Vorbereitung

Informieren Sie sich über Linux-Dateirechte und die Verwendung der Befehle `chmod`, `chown` und `chgrp`.

Bearbeiten Sie anschließend die Verständnisfragen auf dem Praktikumsserver.



### Aufgabe 2 Home-Verzeichnis absichern

Loggen Sie sich auf dem zum Praktikum gehörenden Linuxsystem per SSH ein:

```
ssh -p 10001 <user>@teaching.its.uni-luebeck.de
```

Die entsprechenden Zugangsdaten können auf dem Praktikumsserver eingesehen werden.

Sie finden in Ihrem Home-Verzeichnis einige Dateien vor (die Sie nicht löschen dürfen), zusätzlich sollen weitere Dateien angelegt werden. Ziel ist es, das Home-Verzeichnis vollständig abzusichern, sodass die vorhandenen und neu erstellten Dateien nur ganz bestimmten Nutzern und Gruppen zugänglich sind.





Das System hat neben den Gruppenaccounts vier zusätzliche Nutzer:

- Ihre gute Freundin `alice`, die sich gleichzeitig mit Ihnen in der Gruppe `friends` befindet.
- Den zurückhaltenden `bob`, den Sie kaum kennen.
- Ihr Kumpel `carl`, der ebenfalls in `friends` ist.
- Ihr Gegenspieler, der böse Nachwuchshacker `fridolin`, der bei Eve ein Praktikum zum Ausspähen fremder Daten macht.

Im Folgenden werden Sie einige Dateien anlegen und Zugriffsrechte so setzen, dass auch andere Nutzer diese lesen können. Hierzu finden Sie auf dem Praktikumsserver einige automatisch bewertbare Aufgaben (mit Präfix „(positiv)“), die nur die erlaubten Zugriffe testen (es findet also noch kein Angriff statt). So können Sie leicht erkennen, ob Dateien falsch benannt sind oder Sie die Rechte zu stark eingeschränkt haben. Im Anschluss gibt es noch zwei Aufgaben (mit Präfix „(positiv + negativ)“), die alle Eigenschaften nochmals zusammen testen und zusätzlich einen Angriff simulieren.

Vor der Bewertung jeder Aufgabe sollten Sie das Skript `check_status_repeat.sh` starten. Dieses fragt in regelmäßigen Abständen den Status des Bewertungsskripts ab, und zeigt Ihnen gegebenenfalls entsprechende Fehlermeldungen


an. Diese sollen Ihnen beim Identifizieren von fehlerhaften Berechtigungen helfen. Sie können das Skript nach Beenden des Bewertungsvorgangs mit `Strg+C` beenden.

1. Sorgen Sie dafür, dass nur Sie Schreibzugriff auf Ihr Homeverzeichnis haben.
2. Erstellen Sie eine Datei `public.txt` mit einer Information, die alle Benutzer des Systems erfahren dürfen. Sorgen Sie dafür, dass jeder diese Datei lesen kann.  15 / 3
3. Erstellen Sie eine Datei `message-to-alice.txt` mit einer Nachricht für Alice. Sorgen Sie dafür, dass Sie und Alice diese lesen können, Fridolin jedoch nicht.  25 / 5
4. Sorgen Sie dafür, dass Sie und Alice die Datei `share/house.png` lesen können. Alice sollte jedoch keine Möglichkeit haben, das Verzeichnis `share/` aufzulisten.  35 / 7
5. Erstellen Sie eine Datei `secret.txt` mit einer Information, die nur Sie und Alice lesen dürfen (also eine nicht leere Datei). Alice sollte darauf jedoch nicht direkt zugreifen können, sondern nur über das (vorkompilierte) Programm `show-secret` und unter Eingabe des Passworts aus `password.txt`. Alice soll auch `password.txt` nicht selbst lesen dürfen, da Sie ihr das Passwort bereits persönlich übergeben haben.  45 / 9

Sie haben nun alle nötigen Dateien angelegt und Zugriffsrechte so verteilt, dass alle autorisierten Nutzer diese einsehen können. Aber ist das auch die minimale Lösung? Alice hat Ihnen angeboten, die sie betreffenden Einschränkungen zu testen, damit auch im Falle einer Kompromittierung ihres Accounts nicht mehr Daten preisgegeben werden als unbedingt nötig. Genauer gesagt sollte sie folgende Dinge *nicht* tun können:

- Den Inhalt von `share/` auflisten.
- Andere Dateien als `house.png` in `share/` lesen.
- Die Datei `password.txt` lesen.
- Die Datei `secret.txt` lesen, ohne das Passwort zu kennen.


Sind Sie sicher, dass Sie alles berücksichtigt haben? Wenn ja:

6. Starten Sie das Skript `check_status_repeat.sh`, und klicken Sie anschließend auf „Bewerten“. Bei erfolgreichen Angriffen wird eine Statusmeldung generiert, die Ihnen von `check_status_repeat.sh` angezeigt wird.  70 / 10

Wenn Sie hier ankommen, ist Ihr Verzeichnis gegen eine von bösen Mächten besessene Alice geschützt. Super! Aber reicht das, um sich auch gegen den fiesen Hackerlehrling Fridolin zu wehren? Ihm sollte folgendes *nicht* gelingen:

- Die Datei `message-to-alice.txt` lesen.
- Den Inhalt von `share/` auflisten.
- Eine beliebige Datei aus `share/` lesen.
- Die Datei `password.txt` lesen.
- Den Inhalt von `secret.txt` erfahren, auch wenn er Alice das Passwort gestohlen haben sollte.
- 2 KB Daten in Ihrem Homeverzeichnis ablegen.

Ein letzter Blick? Bereit alles zu riskieren und den schlafenden Drachen zu wecken? Na dann:

7. Starten Sie wieder das Skript `check_status_repeat.sh` und klicken Sie auf „Bewerten“. Das Skript benachrichtigt Sie, wenn Fridolin erfolgreich ist. Viel Glück!  120 / 15

### Aufgabe 3 Access Control Lists (freiwillig)

Sie wollen Fridolin ein für allemal zeigen, dass Sie keine Angst vor ihm haben, und Ihre überlegenen Hacker-Skills demonstrieren, indem Sie eine Datei mit möglichst komplizierten Zugriffsrechten versehen.

Informieren Sie sich hierzu zuerst über die Funktionsweise von ACLs unter Linux<sup>1</sup>, und dann mittels `man <befehl>` über die Benutzung der Befehle `getfacl` und `setfacl`.

Erstellen Sie anschließend in Ihrem Homeverzeichnis eine Datei `acl.txt` mit den folgenden Zugriffsrechten:

1. Sie selbst dürfen lesen und schreiben.
2. Mitglieder der Gruppe `friends` dürfen lesen.
3. Alice darf zusätzlich auch schreiben.
4. Bob darf lesen.
5. Fridolin darf (natürlich) gar nichts.

Testen Sie Ihre Konfiguration anschließend mit einem Klick auf den „Bewerten“-Button.

◀ 80 / 16

---

<sup>1</sup>Ein guter Startpunkt ist hier das ubuntuusers-Wiki: <https://wiki.ubuntuusers.de/ACL/>