Projekt Network Security

Modul: InfB-Proj

Veranstaltung: 64-185

Donnerstag, 12.00 - 18.00

F-027

Utz Pöhlmann
4poehlma@informatik.uni-hamburg.de
6663579

Louis Kobras
4kobras@informatik.uni-hamburg.de
6658699

13. April 2016

Zettel Nr. 1 (Ausgabe: 07. April 2016, Abgabe: 14. April 2016)

Übungsaufgabe 1.1: Hilfe zu Befehlen

Beim Aufruf von "`man ls`" im Terminal wird eine Liste von Optionen und Parametern angegeben, die mit dem Befehl "`ls`" verwendet werden können. `ls` zeigt alle Dateien und Verzeichnisse, die direkte Kinder des aktuellen Arbeitsverzeichnisses sind. Die `Manual page` muss durch drücken der q-Taste verlassen werden.

Wird statt "`man ls`" "`ls help`" eingegeben, so wird der komplette Hilfetext ins Terminal gedruckt und anschließend direkt der Prompt wieder angegeben.

Der Befehl "`script`" startet eine Wrapper-Shell (Default: Bourne Shell, wenn der `SHELL` Parameter nicht gesetzt ist) und zeichnet alle I/O-Streams in der beim Aufruf angegebenen Datei auf. Die Wrapper-Shell kann mit `Ctrl+D` (oder exit) beendet werden. Die Formatierung ist für den neuen Nutzer bzw. auf den ersten Blick ein wenig ungewohnt, dafür enthält die Datei alle relevanten Informationen. Dies ist bei "`man script`" unter BUGS vermerkt, und zwar dass "`script`" alles in den log file schreibt, inklusive line feeds und Backspaces. "This is not what the naive user expects."[1] Der Befehl kann in soweit helfen, als dass der komplette Shell-Dialog aufgezeichnet wird.

Übungsaufgabe 1.2: Benutzerkonten und -Verwaltung

Es wurde ein neuer Benutzer angelegt mit "`sudo adduser <username>`" [1], wobei für `<username>` in diesem Fall `labmate` eingesetzt wird. Nach Eingabe von sudo ist die Authentifizierung mit dem eigenen Passwort erforderlich. Ist dies geschehen, so wird man aufgefordert, zunächst das Passwort und dann weitere persönliche Daten für `labmate` einzugeben (Passwort `laborratte`). Es wurden die Default-Werte angenommen (welche in diesem Fall leer waren).

Die Benutzergruppen von `labmate` werden mit "`groups labmate`" angezeigt. Output:

`labmate : labmate`[2]

Die neue Gruppe `labortests` wird erstellt mit dem Befehl "`sudo addgroup labortests`" [1].

`labmate` wird der Gruppe `labortests` mit dem Befehl "`sudo adduser labmate labortests`"[1] zugewiesen. Alternativ kann dazu der Befehl "`sudo usermod -aG labortests labmate`" verwendet werden[1]. `usermod` ist ein Befehl zur Benutzerverwaltung und -manipulation, welcher sicherstellt, dass Manipulation der Nutzerdaten keine laufenden Prozesse beeinflusst[7].

Um `labmate` zu erlauben, `sudo` zu benutzen, muss er der entsprechenden Gruppe namens `admin` (seit Ubuntu-Version 12.04 `sudo`) hinzugefügt werden: "`sudo adduser labmate admin`" [2].

Übungsaufgabe 1.3: Datei- und Rechteverwaltung

Das Wechseln des Benutzers erfolgt mit "`su <username>`" [3]. Dabei muss man das Passwort des neuen Nutzers eingeben.

Das Wechseln in das home-Verzeichnis erfolgt (unabhängig vom Nutzer) mit "`cd ~`" oder synonym mit "`cd`". Der aktuelle Pfad wird mit `pwd` angezeigt.

Das neue Verzeichnis wird mit "`mkdir <pathname>`" angelegt (hierbei ist wiederum `sudo` vonnöten).

Der Wechsel in den neuen Ordner geschieht mit dem Befehl "`cd labreports`".

Das Anlegen neuer Dateien erfolgt mit "`touch bericht1.txt`". Geöffnet wird die Datei mit "`pico bericht1.txt`". Es wurden folgende Zeichen eingegeben: *hkgfhk*. Speichern erfolgt mit `Ctrl+O`, Beenden mit `Ctrl+X`.

Das Verändern der Zugriffsrechte erfolgt mithilfe der Befehle `chgrp` [4] und `chmod` [5]. Zunächst muss mit "`chgrp labortests beispiel1.txt`" die Gruppe, der die Datei gehört, auf `labortests` gesetzt werden (sonst gehört die Datei der Gruppe, die nur den Eigentümer enthält). Danach können mit der Oktal-Variante von `chmod` [6] die Zugriffsrechte derart gesetzt werden, dass Eigentümer und Gruppe Lese- und Schreibzugriff, sonst jedoch kein Zugriff möglich ist. Dies entspricht dem Befehl "`chmod 660 beispiel1.txt`". Die Ziffer 6 steht hierbei für einen Lese- und Schreibzugriff und die Ziffer 0 steht für Keine Zugriffsrechte. Die erste

[1] Aus der manual-Seite von `script`

[2] `labmate` ist derzeit nur in der Gruppe, die genau ihn selber enthält und genauso heißt wie er

Stelle ist die Einstufung für den Eigentümer, die zweite Stelle ist die Einstufung für die Gruppe, die dritte Stelle ist die Einstufung für andere Nutzer. (*Anmerkung: Dieser spezifische Fall ist bei [6] als eines der Anwendungsbeispiele gelistet.*)

Der Befehl `wget` lädt eine angegebene Datei herunter. Verwendung: "`wget <URL>`". Die Datei wird dabei in das aktuelle Arbeitsverzeichnis heruntergeladen.

Das Setzen der Rechte erfolgt wie oben (der `chmod`-Parameter 660 ist äquivalent zum Parameter 0660). Durch den Befehl "`sudo chmod 0660 /home/labmate/labrepots`" werden die Rechte für das Verzeichnis *labreports* wie in der Aufgabe gefordert gesetzt. In der Verzeichnisliste ist folgende Zeile zu sehen: "`drw-rw--2 labmate labmate 4096 <Timestamp> labreports`". Als Ergebnis davon kann man das Verzeichnis zwar sehen, der Versuch, in es hineinzunavigieren, scheitert jedoch aufgrund mangelnder Berechtigungen. Eine Lösung wäre, die Berechtigungen auf `0770` zu setzen, was dem Eigentümer und der Gruppe erlaubt, ausführend auf ein Verzeichnis bzw. eine Datei zuzugreifen. Damit gelingt es auch wieder, auf das Verzeichnis und seine Inhalte zuzugreifen.

Der Versuch, mit `labmate` in das Verzeichnis `/root` zu wechseln, scheitert aufgrund mangelnder Berechtigungen.

Das Verzeichnis test wird erstellt mit "`sudo mkdir test`"[1], die Rechte werden gesetzt mit "`sudo chmod 0770 test`" (dies bedeutet, dass Eigentümer und Gruppe Lese-, Schreib- und Ausführungsrechte haben, andere Nutzer gar keine). Der Eigentümer des Verzeichnisses wird mit "`sudo chown labmate test`" auf `labmate` gesetzt. Als Gruppe wird `admin` gewählt, da dies derzeit die einzige Gruppe ist, die sowohl `labmate` als auch `user` enthält. Das Setzen der Gruppe erfolgt mit "`sudo chgrp admin test`".

Die eben heruntergeladene Datei wird mit dem Befehl "`cp ~/labreports/index.html test/`" in das neue Verzeichnis kopiert ("`c(o)p(y) <source> <destination>`").

Davon ausgehend, dass `labmate` als Eigentümer ist, erfolgt die Rechte-Modifikation durch "`sudo chmod 0640 /opt/test/index.html`". Damit hat der Eigentümer Lese- und Schreiberechte, die Gruppe hat nur Leserechte, andere Nutzer haben keine Zugriffsrechte. Die Gruppe wird mit "`sudo chgrp user index.html`" auf ebenjene persönliche Benutzergruppe gesetzt, die nur `user` enthält, womit auch nur `user` neben dem Eigentümer Leserechte hat.

Durch Öffnen eines neuen Terminals mit der Tastenkombination `Ctrl+Alt+T` ist wieder ein Terminal als `user` verfügbar.

Da `user` Lesezugriffsrechte hat, gelingt es, die Datei mithilfe von "`cat /opt/test/index.html`" auszulesen.

Auch der Zugriff mit einem Texteditor wie beispielsweise `vim` oder `nano` ist möglich, da jedoch die Schreibe-Berechtigung fehlt, kann sie nicht verändert werden (`nano` warnt sofort, dass man kein Schreibrecht besitzt). Editieren ist mit beiden Editoren möglich, das Speichern jedoch scheitert an den Berechtigungen.

Die Datei wurde erfolgreich mit "`cp index.html userindex.html`" kopiert (das aktuelle Arbeitsverzeichnis ist `/opt/test`, weswegen der absolute Pfad nicht angegeben werden muss).

Durch das Anlegen der neuen Datei `userindex.html` mithilfe des Terminals wurden die Werte des Wurzelverzeichnisses für die Berechtigungen übernommen (`root` hat Lese- und Schreibzugriff und die Gruppe `root` hat Lesezugriff). Weder das Lesen noch das Schreiben gelingen als `user`. Dies kann jedoch mit `sudo` übergangen werden.

Beim Versuch, die Datei mit "`rm userindex.html`" zu löschen, wird erst gefragt, ob man die schreibgeschützte Datei löschen möchte. Bejaht man, bricht der Vorgang mangels Berechtigung ab. Durch Verwendung von `sudo` kann die Durchführung des Prozesses wiederum erzwungen werden.

Übungsaufgabe 1.4: Administration und Aktualisierung

`apt-get` ist der Paket-Manager für Ubuntu und Debian-basierende Systeme (das Stück Kernel, welches für die Installation und Verwaltung von Software-Paketen verantwortlich ist). "`apt-get upgrade`" aktualisiert sämtliche derzeit installierten Pakete. Der Parameter `-y` kann übergeben werden, um die Installation zu automatisieren (den Prompt automatisch mit 'Ja' zu beantworten). "`apt-get update`" aktualisiert die systeminterne Liste von Paketquellen[2]. Auch hier kann der Parameter `-y` übergeben werden für den gleichen

[1] Da das Stammverzeichnis `root` gehört, sind hier esudo-Rechte erforderlich

[2] Eine Reihe von Servern, von denen die installierte Software heruntergeladen wurde. Die Liste umfasst die offiziellen Ubuntu-Server sowie Adressen, die vom Benutzer hinzugefügt wurden

Effekt wie bei `upgrade`. Für beide Befehle ist die Verwendung von `sudo` erforderlich.

Zum Installieren neuer Pakete mit `apt-get install` ist ebenfalls `sudo` nötig, sodass der Befehl zur Installation letztlich so aussieht: "`sudo apt-get install cowsay`". `cowsay` nimmt Text als Parameter entgegen und druckt eine ASCII-Kuh, die den Text in einer Sprechblase über sich hat. Diese hat, je nachdem, ob `cowsay` oder `cowthink` als Befehl verwendet wird, gerade oder gekrümmte Seiten. Durch Verwendung von Variablen kann auch eine Datei eingelesen werden: "`cowsay $(cat bla.txt)`". Dann wird der Inhalt der hier gewählten `bla.txt` von `cat` ausgelesen und durch das $ als Variable gelesen, welche von `cowsay` angenommen und ausgedruckt wird. Bei `cowsay` können das Abbild der Kuh sowie Formatierungsoptionen gesetzt werden.

Übungsaufgabe 1.5: Prozesse und Prozessverwaltung

Der Befehl `ps` gibt eine Momentaufnahme aller laufenden Prozesse aus. Mit "`ps -e`" werden alle Prozesse angezeigt, die derzeit laufen. Der Befehl `top` gibt ein stetig aktualisiertes Abbild der laufenden Prozesse zurück.

Bei Verwendung des Befehls "`cat /dec/urandom`" als `labmate` erscheint im `top`-Fenster ein neuer Prozess, der `labmate` zugeordnet ist. Er hat (in diesem Fall) die Prozess-ID (`PID`) 3658.

Der direkte Aufruf von `kill`, welchem eine `PID` übergeben werden muss, gibt zurück, dass die Operation nicht zulässig ist. Nur mit "`sudo kill 3658`" ist es gelungen, den Prozess von außen zu terminieren.

Der Befehl, um als `labmate` das System neuzustarten, ist "`sudo shutdown -r now`", wobei `sudo` erforderlich ist, da der `shutdown`-Befehl Administratorrechte benötigt, `-r` gibt dem System an, dass es doch bitte auch wieder hochfahren möge, und `now` gibt den Zeitpunkt des Neustartes an.

`Cronjob`s werden in der `Crontab`-Tabelle editiert. Diese wird mit dem Befehl "`crontab -e`" geöffnet[9]. Dort wird der Befehl mit den entsprechenden Intervallen eingegeben. Vollständig sieht dies so aus:

```
# m   h   dom   mon   dow   command
*/5   *   *     *     *     echo $(sudo hwclock --show) » /home/labmate/zeitstempel.txt
```

Am Ende der `Crontable` muss eine Leerzeile oder ein Kommentar stehen[9]. Hierbei steht `m` für `Minute` (wobei `*/5` für einen 5-Minuten-Rhythmus steht), `h` für `Stunde`, `dom` für `Tag des Monats`, `mon` für `Monat`, `dow` für `Wochentag` und `command` für den auszuführenden Befehl[8]. Der Befehl setzt sich zusammen aus `echo` für eine Ausgabe von Text, der Variable `$(sudo hwlock --show)` für das Anzeigen des Zeitstempels sowie `» <path>` als Angabe für `echo`, wohin die Ausgabe erfolgen soll.

Übungsaufgabe 1.6: VMWare-Tools installieren

Der Menüpunkt zum Installieren der `VMware Tools` ist bei `Workstation 11` zu finden unter `VM -> Install VMware Tools...` Dieser Menüpunkt *mounted* ein virtuelles Medium in der VM, welches die benötigten Installationsdateien bereitstellt.

Das Installationsverzeichnis wird mit dem Befehl "`tar -xzf /media/VMware\ Tools/VMwareTools-9.9.0-2304977.tar.gz -C ~`"[10] in das home-Verzeichnis des aktuellen Nutzers (hier `user`) entpackt. Die Paramter für `tar`, nämlich `xzf`, stehen für `(e)xtrahieren`, `(g)zip` für das Dateiformat `.tar.gz` und `file` für den Dateipfad zum Stammarchiv. Mit `-C` wird ein Zielverzeichnis angegeben.

Das Perl-Skript wird mit "`perl vmware-install.pl`" ausgeführt. Die Standard-Einstellungen werden übernommen, indem bei jedem Prompt Enter gedrückt wird. Wird versucht, das Skript ohne `sudo` auszuführen, gibt es eine Fehlermeldung. Anschließend wurde die VM neu gestartet, um die Installation abzuschließen.

Übungsaufgabe 1.7: VMWare bedienen

Die VM wurde gestartet, es wurde sich mit dem User `user` angemeldet.

Ein Terminal wurde gestartet und der Befehl "`top`" wurde gestartet.

Die VM wurde mit dem gelben Pause-Button pausiert. Beim Fortfahren erschienen für einen kurzen Moment eine größere Anzahl Prozesse im Top-Fenster.

Es wurde mit dem Fullscreen-Knopf die Fullscreen-Ansicht gewechselt und diese mit ebenjenem Knopf wieder verlassen. Auch hier erschienen kurz Prozesse im Top-Fenster.

Die VM wurde mit `VM -> Power -> Power Off` beendet, wonach wieder die Hauptansicht der Workstation sichtbar ist. Es wird jedoch darauf hingewiesen, die VM vorher intern herunterzufahren.

Es wurden zwei Snapshots `top`[1] und `Browser`[2] erstellt mit `VM -> Snapshot -> Take Snapshot...`. Durch Klicken von `VM -> Snapshot -> 2. top - <timestamp>` wurde der Snapshot `top` wiederhergestellt, wodurch die VM auch wieder auf den Zustand gesetzt wurde, in dem sie war, als der Snapshot erstellt worden ist.

Die GUI-Anwendung `Calculator` wurde durch `Applications -> Accessories -> Calculator` gestartet und ein weiterer Snapshot wurde erstellt.

Die Snapshots werden derart angeordnet, dass sie in der Reihenfolge der letzten Ansprache angeordnet sind.

Snapshots müssen über `VM -> Snapshot -> Snapshot Manager` einzeln gelöscht werden; hierbei wird dem Benutzer eine Baumstruktur der Snapshot-Historie angezeigt.

Literatur

[1] https://help.ubuntu.com/community/AddUsersHowto

[2] https://help.ubuntu.com/community/RootSudo

[3] http://www.namhuy.net/44/add-delete-and-switch-user-in-ubuntu-by-command-lines.html

[4] https://wiki.ubuntuusers.de/chgrp/

[5] https://wiki.ubuntuusers.de/chmod/

[6] https://wiki.ubuntuusers.de/chmod/#Oktal-Modus

[7] http://linux.die.net/man/8/usermod

[8] https://de.wikipedia.org/wiki/Cron

[9] https://wiki.ubuntusers.de/Cron/

[10] https://wiki.ubuntusers.de/tar/

[1] während `top` lief
[2] während `Firefox` lief