NetSec Labreport 1

Kolja Hopfmann
Jonas Sander
Universität Hamburg, Projekt: Netzsicherheit

April 6, 2018

---

1 Abeiten mit der Linux-Kommandozeile(bash)

1.1 Befehle man und help

Mit den Befehlen man(Manual) und help(–help flag) lassen sich nützliche Informationen über ein Programm über die Kommandozeile einblenden lassen. "man" öffnet hierbei ein Textfeld und gibt eine detaillierte Dokumentation zu dem Programm aus. "–help" gibt eine kurze Beschreibung und mögliche flags für das Programm aus.

1.2 Script

Script ist ein Unix-Programm welches die momentane Shell-Session in einer Datei abspeichert bzw. aufzeichnet. Mit "Script Dateiname.txt" startet die Aufzeichnung und alle eingetippten Befehle landen in Dateiname.txt. Wird keine Datei angegeben wird eine default-Datei verwendet. Dieses tool kann dabei helfen mögliche Lösungen für Aufgaben zu präsentieren.

2 Benutzerkonten und Verwaltung

Es wurde ein neuer user mit dem Namen "labmate" mit dem Befehl "adduser labmate" angelegt.

Um herauszufinden zu welcher Gruppe labmate gehört wurde "groups labmate" benutzt.
Eine neue Gruppe "labortests" wurde mit "addgrp labortests" angelegt.
Der User labmate wurde mit "sudo usermod -aG labmate labortests" der Gruppe labortests hinzugefügt.
Mit dem Befehl "sudo usermod -aG labmate sudo" gaben wir labmate Sudo-Berechtigung.

3 Datei- und Rechteverwaltung

Der Benutzer wurde von user zu labmate gewechselt.
Das Verzeichnis /home/labreports wurde angelegt.
Im Verzeichnis labreports wurde mit "touch bericht1.txt" eine neue Datei angelegt. Anschließend wurde diese über vim mit dem Text "dies ist ein Test" befüllt.
Mit dem Befehl "chmod g+rw bericht1.txt" wurden die Rechte auf der Datei so gesetzt, dass für Eigentümer und Gruppenmitglieder Lese- und Schreibrechte vergeben wurden. Die Gruppe der Datei bericht1.txt ist labortests.
Mit "wget http://www.uni-hamburg.de/index.html" wurde der Inhalt der Seite in das Verzeichnis labreports gespeichert.
Die Zugreiffberechtigung wurde mit "chmod 0660 labreports" so geändert, dass Dateieigentümer und Gruppe Lese- und Schreibzugriff haben.
Ein neues Verzeichnis test wurde unter /opt angelegt. Die Gruppe von test wurde auf user gesetzt, der Owner ist labmate. Die Rechte von test wurden mit "chmod 0770 test" auf Lese- Schreib- und Executezugriff (rwx) für Owner und Gruppenmitglieder gesetzt.In der Zahl mit der die Rechte gesetzt werden steht die 2. Stelle für die rechte des Owners, die 3. Stelle für die Rechte der Gruppenmitglieder und die 4. Stelle für die Rechte aller anderen. Die Flags r, w und x werden durch jeweils ein Bit dargestellt, wobei $r = 100_2 = 4_{10}$, $w = 010_2 = 2_{10}$ und $x = 001_2 = 1_{10}$ gilt.
Mit "cp index.html test" wurde die Datei index.html von labreports nach test kopiert.
Mit "groupadd specialrights" wurde eine neue Gruppe angelegt. Dieser Gruppe wurden user und labmate hinzugefügt, die Gruppe von index.html wurde auf specialrights geändert und der Owner auf labmate gesetzt. Dies wäre im Nachhinein auch einfacher gegangen, indem die Gruppe von indes.html

auf user gesetzt wird. Die Rechte von index.html wurden mit "chmod 0640 index.html" so gesetzt, dass der Owner (labmate) die Lese- und Schreibrecht hat und die Gruppenmitglieder (hier user) Leseberechtigung haben.
Mit exit wurde der user labmate ausgeloggt und anschließend der user user angemeldet.
Mit dem Befehl "cat index.html" lies sich die Datei erfolgreich auslesen.
Die Datei wurde mit "vim index.html" erfolgreich geöffnet. Ein Abspeichern war nicht möglich, da die Datei read-only war.
Unter dem Benutzer user wurde die Datei index.html kopiert. Ein Bearbeiten und Abspeichern der Datei war nun möglich, da user der Owner der Kopie war und somit rw Berechtigung hatte.
Mit "rm index.html" wurde als user erfolgreich die Datei gelöscht, von der labmate der Owner war. Dies war möglich, da für rm die Schreibberechtigung auf dem übergeordnetem Verzeichnis nötig ist, nicht die Berechtigung auf der Datei selber.

4 Administration und Akualisierung

4.1 apt update und apt upgrade

Mit den Parametern "update" und "upgrade" von "apt" (aptitude) lassen sich Pakete auf den neuesten Stand aktualisieren. Update verzeichnet alle neuen Versionen von Installierten Paketen. Upgrade benutzt dann die von Update aktualisierten Versionen und downloaded/installiert diese.

4.2 apt install

Mit "apt install PAKETNAME" installiert man ein gewünschtes Paket.
Es wurde mit "apt install cowsay" das Paket: cowsay installiert.
Mit dem Befehl "cowsay WORT" war es nun möglich eine ASCII-Kuh zu generieren, welche das Wort, welches als Parameter angegeben wurde "ausspricht".

5 Prozesse und Prozessverwaltung

5.1 top und ps

Top ist das equivalent zum Taskmanager von Windows. Mit top lassen sich alle momentan laufenden Prozesse ausgeben.
Ps gibt mit "ps PROZESSID" eine detaillierte Auskunft über einen bestimmten Prozess. Ps gibt im Gegensatz von top nur einen snapshot aus, wobei top seine Ausgabe in regelmäßigen Zeitabständen akualisiert.

5.2

Mit "su - labmate" wurde in einem neuen Terminal zum Benutzer labmate gewechselt.
Nach dem Ausführen von "cat /dev/urandom" erscheint ein Strom von zufälligen characters auf der Konsole.
Über top konnte man nun beobachten wie ein bestimmter Prozess vom User labmate nun eine hohe Auslastung hatte.
Mit dem Befehl kill war es als User "user" nicht möglich den laufenden Prozess von labmate zu beenden.
Die Ausführung von kill als root funktionierte.
Mit "sudo reboot" wird das System neugestartet. "Sudo shutdown" fährt das System herunter.
Es wurde eine Datei "zeitstempel.txt" mit "touch zeitstempel.txt" im /home-/labmate/ Verzeichnis erstellt.
Mit "crontab -e" wurde die Datei zum Bearbeiten der Cronjobs geöffnet.
Die Zeile "*/5 * * * * date > > /home/labmate/zeitstempel.txt" erzeugt einen neuen Cronjob der alle 5 Minuten das aktuelle Datum mit Zeit in die zeitstempel.txt schreibt.

6 VMware-Tools

Die VM wurde hochgefahrenDer Benutzer "user" wurde angemeldet.
Die Installations-CD wurde über die Aktion "Install VMware-Tools" gemountet.
Die gepackte Datei wurde mit "tar -C /dir tarfile" in das gewünschte Verzeichnis entpackt.

Mit "perl vmware-install.pl" wurde das Installationsskript gestartet. Es wurden alle vorgeschlagenen Einstellungen übernommen.
Es erschien keine Fehlermeldung.

7 Bedienung von VMware