Studienprogramm Sachbearbeiter:in Digitale Forensik
Praktikum Betriebssysteme
Dozent: Tim Wetterau
Kontakt: wetterau@hs-mittweida.de
Stand: 08.07.2024

HOCHSCHULE MITTWEIDA
University of Applied Sciences

Betriebssysteme

Praktikum 1 - Grundlagen Linux

Dieses Praktikum stellt eine Wiederholung der Praktikumsinhalte aus dem Modul Grundlagen Digitale Forensik dar. Sie sollen sich erneut mit einigen dort kennengelernte Befehlen auseinandersetzen und sich die Anwendung einiger weiterer Befehle selbst aneignen. Weiterhin schauen wir uns die Verwendung von apt an.

Die folgenden Inhalte werden in diesem beleuchtet:

- Wiederholung Inhalte Praktikum Linux Digitale Forensik
- weitere Hinweise zur Handhabung der Bash
- Selbststudium Befehle
- Paketmanager apt

Vorbereitung

Für dieses Praktikum benötigen Sie eine lauffähige Installation der Linux-Mint-BKA VM, welche wir bereits im Praktikum Grundlagen Digitale Forensik verwendet haben. Sollte Sie diese bereits installiert haben, testen Sie diese. Sollte diese funktionieren, besteht an der Stelle für Sie kein Handlungsbedarf.

Außerdem ist es sinnig Ihre Ausarbeitungen von Grundlagen Digitale Forensik zu Hilfe zu nehmen, da wir hier auf diesen Inhalten aufbauen.

Wiederholung Inhalte Praktikum Linux

Zur Wiederholung bitte ich Sie die folgenden Befehle sich erneut zu verdeutlichen:

- **`whoami`**
- **`who`**
- **`groups`**
- **`cat`**
- **`id`**
- **`env`**
- **`hostname`**

Zudem sollte Ihnen die Bedeutung der Dateien **`/etc/passwd`** und **`/etc/group`** klar sein und wie diese aufgebaut sind. Sie seien dazu hingewiesen, dass vorausgesetzt wird, dass Sie bei Bedarf die Manpages der entsprechenden Befehle konsultieren. *Machen Sie sich auch wieder bewusst, wie Variablen in der Bash behandelt, also belegt und wieder abgerufen werden.*

```
$ var=wert        # Belegung
$ [echo] $wert    # Abrufen des Variablenwertes (echo nur zum Anzeigen auf Terminal)
```

Weitere Hinweise zur Handhabung der Bash

Zum Absolvieren der Praktikumsaufgaben sollen Sie außerdem einige weitere Hinweise zum Umgang mit der Bash bekommen. Wie bereits gezeigt können Sie mit den Pfeiltasten oben/unten durch die zuletzt verwendeten Befehle

navigieren. Das ist besonders dann nützlich, wenn man Befehle öfter verwendet oder man lange Befehle baut, die ggf. Fehler werfen. So kann man sich den eingegebenen Befehl schnell erneut anschauen und diesen anpassen.

Das wird möglich durch den Verlauf der eingegebenen Befehle. Dieser ist in Ihrem Home-Verzeichnis abgespeichert unter „**`.bash_history`**“. *Rufen Sie diese Datei auf und schauen Sie sich Ihre zuletzt eingegebenen Befehle an.*

Zur Übung der bereits gelernten Befehle geben Sie den Befehl zur Lösung folgender Aufgabe an:

- *Geben Sie alle Befehle sortiert nach dem Alphabet aus*
- *Löschen Sie aus der Ausgabe alle doppelt auftretenden Befehle*
- *Schreiben Sie das Ergebnis des Befehls in eine neue Datei sorted_history*

```
$ cat .bash_history
$ cat .bash_history | sort | uniq > sorted_history
```

Ein weiteres Feature ist die „Autovervollständigung“ durch die Bash. Diese kann genutzt werden durch das Drücken der Tabulator-Taste. Durch das Einmalige Drücken der Taste wird bei bereits vorhandener Eindeutigkeit mit dem vollständigen Namen ergänzt. Ist der Name nicht eindeutig, kann die Bash zmd. eine Liste von möglichen Dateinamen ausgaben, die auf das bereits eingegebene Stück Text passen.

Testen Sie dieses Feature selbstständig einmal und machen Sie sich damit kurz ein wenig vertraut. Das erleichtert ihre Arbeit ein wenig.

Selbststudium Befehle

Weiterhin schauen Sie sich folgende Befehle an und machen Sie sich mit deren Handhabung vertraut:

- **`ps`**
- **`top`**
- **`kill`**
- **`systemctl`**
- **`passwd`**
- **`shutdown, poweroff, reboot`**
- **`grep`**

Welchen Zweck erfüllen die einzelnen Befehle? Welche Optionen werden unterstützt und wie können diese genutzt werden? Testen Sie die Befehle selbstständig und machen Sie sich deren Wirkung deutlich. Probieren Sie selbstgewählte Beispiele.

```
$ ps – process snapshot     -       Anzeige von Prozessen
$ top – Laufende Prozesse in Echtzeit anzeigen
$ kill – Prozess mit einer PID beenden
$ systemctl – Verwaltung für den systemdeamon und Servicemanager
$ passwd – password – Ändern von Passwörtern → nur Root kann Passwort eines anderen Nutzers ändern
$ shutdown – Befehl zum Stoppen, neustarten, herunterfahren des PCs
        ○   verschiedene Optionen zur Bestimmung des Zeitpunktes und ggf. Message
$ poweroff, reboot – System herunterfahren oder neustarten
```

Paketmanager apt

Apt ist ein Paketmanager unter Linux, welcher verwendet wird, um Pakete (Anwendungen) zu installieren und zu deinstallieren. Dieser kann außerdem verwendet werden, um die Hauptversion des BS zu aktualisieren. Am Ende des Praktikums wollen wir uns anschauen, ob wir alle Tools für das nächste Praktikum haben und diese ggf. nachinstallieren.

Um Updates auf einem System zu installieren, brauchen Sie generell Superuser-Berechtigungen. Die Konfigurationsdatei für zusätzliche Repositories in apt liegt unter dem Verzeichnis **`/etc/apt/sources.list`**. Die offiziellen Paketquellen finden Sie hingegen unter **`/etc/apt/sources.list.d/official-package-repositories.list`**. Diese Datei sollte von Ihnen nicht verändert werden. Sie können sich die bereits installierten Pakete mit dem folgenden Befehl anzeigen lassen.

```
$ sudo apt list --installed
```

Aktualisieren Sie die bestehenden Pakete mit dem folgenden Befehl:

```
$ sudo apt update
```

Hierdurch werden die Paketlisten der Repositories gelesen und Sie erhalten Sie eine Übersicht, wie viele Pakete aktualisiert werden können. Bedenken Sie: update aktualisiert nicht das System, sondern nur die Paketlisten. Das eigentliche Update der Pakete erfolgt durch den Befehl:

```
$ sudo apt dist-upgrade
```

Durch den Befehl „**`add-apt-repository <Repository>`**“ kann eine neue Paketquelle hinzugefügt werden. Dies wird teilweise bei der Installation von PHP für Webserver verwendet. Dabei kann die Quelle **`ppa:ondrej/php`** als neues Repo hinzugefügt werden und folglich darüber PHP installiert werden. *Versuchen Sie diese mit dem erworbenen Wissen hinzuzufügen. Updaten Sie nach dem Hinzufügen erneut die Paketlisten und führen ebenso ein neues upgrade durch. Schauen Sie sich die neu hinzugefügten Repositories in den Konfigurationsdateien an.*

```
$   sudo add-apt-repository ppa:ondrej/php
$   sudo apt update
$   sudo apt upgrade
$   cat /etc/apt/sources.list
```

Für das nächste Praktikum brauchen wir zwei Programme, deren Installation Sie an der Stelle überprüfen sollen. Diese Programme sind **`openssh-client`**, **`nmap und john`**. *Prüfen Sie ob die genannten Pakete installiert sind. Machen Sie sich den Befehl grep zunutze. Sollten Sie feststellen, dass die Programme nicht installiert sind, dann installieren Sie bitte die Pakete mit den oben bereits aufgeführten Paketnamen und prüfen den Erfolg der Installation.*

```
$ sudo apt list --installed | grep ssh
$ sudo apt list --installed | grep nmap
$ sudo apt install openssh-client nmap
```