htw saar

Studiengang Kommunikationsinformatik
Prof. Dr.–Ing. Damian Weber
Dipl.-Inf. Marion Bohr
Thorsten Jakobs, M.Sc.

Systemmanagement und Sicherheit

1. Übung

Vorbemerkung:

Im Labor IT-Sicherheit ISL sind die FreeBSD-Maschinen isl-c-01, ..., isl-c-13 installiert. Sie können sich entweder

- dort direkt mit Ihrem Informatik-Account einloggen, oder
- von Ihrem Laptop aus via `ssh` zu `stl-s-stud` und weiter zu einem der `isl-` Rechner:

  ```
  ssh -l username stl-s-stud.htwsaar.de
  ...
  ssh isl-c-01.htwsaar.de
  ```

  (den detaillierten Ablauf finden Sie auf der letzten Seite).

  Mögliche Editoren sind in diesem Fall `ee` (selbsterklärend, wenig Features) und `vim` (schwieriger zu erlernen, viele Features).

Lesen Sie (außerhalb des Praktikums) den Artikel von Bruce Schneier über sichere Passwörter.

`https://www.schneier.com/blog/archives/2014/03/choosing_secure_1.html`

Aufgabe 1 (Shell Kommandozeile)

Wir werden in der Kommandozeile mit der Bourne Again Shell arbeiten (`bash`). Falls Sie unter `stl-s-stud` die Kornshell eingetragen haben, haben Sie auf den ISL–Rechnern ebenfalls die Kornshell (`ksh`). In diesem Falle geben Sie nach dem Öffnen eines Terminalfensters einfach (`bash`) ein. Sie können das automatisieren, indem Sie das Kommando (`bash`) in

`${HOME}/.kshrc`

eintragen.

Die `bash` Shell hält einige Features parat, um das Editieren der Kommandozeile zu vereinfachen. Finden Sie diese in den folgenden Aufgaben heraus und ordnen Sie die richtigen Tastenkombinationen zu.

(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
`[Alt]+f`	`[Alt]+b`	`[Strg]+l`	`[Strg]+w`	`[Strg]+k`	`[Strg]+e`	`[Strg]+a`	`[Strg]+d`

a) Cursor an den Anfang der Zeile

b) Cursor ans Ende der Zeile

c) Löschen des Zeichens unter dem Cursor

d) Löschen des Rests der Zeile

e) Wortweises Weiterbewegen des Cursors

f) Wortweises Rückwärtsbewegen des Cursors

g) Lösche bis zum Anfang des Wortes

h) Lösche Bildschirm

Legen Sie die Datei `.inputrc` in ihrem Homeverzeichnis an mit dem Inhalt:

```
C-p: history-search-backward
```

Dann können Sie nach dem nächsten bash-Start die letzte Befehlszeile mit einem vorgegebenen Anfang sehr leicht durch das Drücken der Tastenkombination `[Strg]+p` finden.

Beispiel:

```
$ cc -O2 -Wall -pedantic -o test test.c
$ cc[[Strg]+p]
```

ergibt die komplette cc–Zeile. Weitere Features, die das Tippen erleichtern, finden sich in der Manualpage der `bash` unter *Commands for Moving, Commands for Manipulating the History, Commands for Changing Text, Killing and Yanking, Completing.*

Eine ähnliche Funktion hat das Ausrufezeichen.

```
$ !cc
```

führt das letzte Kommmando aus, das mit `cc` beginnt.

Aufgabe 2 (C Programm)

Das Kommando `date` gibt das aktuelle Datum mit Uhrzeit aus.

Schreiben Sie ein C–Programm, das die gleiche Ausgabe erzeugt.

a) mit Hilfe von `time()`, gefolgt von `ctime()`

b) mit Hilfe von `time()`, gefolgt von `localtime()` und `strftime()`

Es sind zwei Compiler auf dem System vorhanden (cc und gcc).

Überprüfen Sie, dass Ihr Programm mit beiden Compilern funktioniert.

Falls Sie Informationen zu den C–Funktionen benötigen, hilft Ihnen das `man`–Kommando:

```
man 3 time

man 3 strftime
```

Aufgabe 3 (Kryptoschlüssel erzeugen)

Erzeugen Sie sich einen RSA–Kryptoschlüssel mit 2048 Bit.

```
$ ssh-keygen -t rsa -b 2048
Generating public/private rsa key pair.

Enter file in which to save the key (/export/home_pm/dweber/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:

Your identification has been saved in /export/home_pm/dweber/.ssh/id_rsa.
Your public key has been saved in /export/home_pm/dweber/.ssh/id_rsa.pub.

The key fingerprint is:
3d:96:a1:ab:cf:9a:ff:d6:f2:de:e6:10:d5:60:e5:d4 dweber@stl-s-studwork
```

Fügen Sie diesen Key zu der Datei

```
${HOME}/.ssh/authorized_keys
```

hinzu.

Jetzt können Sie sich ohne Passworteingabe zwischen `isl`–Rechnern einloggen. Wenn Sie sich ohne Passworteingabe vom `stl-s-stud.htwsaar.de` zum `isl-c-01.htwsaar.de` verbinden wollen, müssen Sie den Key auf dem `stl-s-stud` erzeugen und in der `authorized_keys` eines `isl`–Rechners eintragen.

Hinweis: Vorgang zum Einloggen in das ISL–Netz

von zu Hause oder vom HTW-WLAN aus:

```
$ ssh -l stl-login-name stl-s-stud.htwsaar.de
The authenticity of host 'stl-s-stud.htwsaar.de (134.96.216.212)' can't be
established.
RSA key fingerprint is 00:c3:5b:21:6a:c0:ad:3f:03:37:1c:e0:88:bf:82:7b.
No matching host key fingerprint found in DNS.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'stl-s-stud.htwsaar.de' (RSA) to the list of
known hosts.
Passwort: ********
Last login: Fri Apr 17 11:03:02 2015 from pd9e08fd4.dip0.
$ ssh isl-c-01
The authenticity of host 'isl-c-01 (134.96.216.81)' can't be established.
RSA key fingerprint is 04:5d:22:aa:dc:d6:67:27:8e:a7:db:10:2e:03:7e:5e.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'isl-c-01,134.96.216.81' (RSA) to the list of
known hosts.
Password: ********
Last login: Fri Apr 17 16:55:49 2015 from :0 FreeBSD 10.1-STABLE (ISL-C-07)
#0 r281529: Tue Apr 14 18:35:24 CEST 2015
stl-login-name@isl-c-01(1)$
```