

## **Linux-Basics für Hacker**

Einstieg in die Hacking-Grundlagen mit Kali Linux:  
Netzwerke, Scripting und Security

» Hier geht's  
direkt  
zum Buch

# **DIE LESEPROBE**

# Die Grundlagen



Hacker sind Macher, das liegt in ihrem Wesen. Sie wollen Dinge anfassen und mit ihnen herumspielen. Sie möchten etwas erschaffen und (manchmal auch) kaputtmachen. Nur wenige von ihnen wollen dicke Wälzer voller IT-Theorie lesen, bevor sie mit dem loslegen, was sie am meisten lieben: Hacken. Angesichts all dessen soll dieses Kapitel Ihnen einige grundlegende Fertigkeiten vermitteln, damit Sie den Einstieg in Kali finden ..., und zwar jetzt!

Sie werden in diesem Kapitel keines der Konzepte in aller Ausführlichkeit kennenlernen, sondern gerade so viel erfahren, dass Sie mit Linux, dem Betriebssystem der Hacker, herumspielen und es erkunden können. Tiefergehende Diskussionen erwarten Sie dann in späteren Kapiteln.

## 1.1 Einführende Begriffe und Konzepte

Bevor Sie mit der Reise durch die wunderbare Welt von *Linux Basics für Hacker* beginnen, möchte ich Ihnen einige Begriffe vorstellen, die einige der später in diesem Kapitel diskutierten Konzepte näher erklären.

- **Binärdateien (Binaries)** – Dieser Begriff bezieht sich auf Dateien, die ausgeführt werden können, also vergleichbar den ausführbaren Programmdateien unter Windows. Im Allgemeinen befinden sich die Binärdateien im Verzeichnis `/usr/bin` oder `/usr/sbin` und umfassen Dienstprogramme wie `ps`, `cat`, `ls` und `ifconfig` (Sie werden im Laufe dieses Kapitels mehr über diese vier Programme erfahren) ebenso wie Anwendungen wie das Wi-Fi-Hacking-Tool `aircrack-ng` und das Intrusion-Detection-System (System zum Erkennen von Angriffen) `Snort`.
- **Case Sensitivity** – Anders als in Windows achtet Linux auf Groß- und Kleinschreibung, ist also case-sensitiv. Das bedeutet, dass `Desktop` sich von `desktop` und auch von `DeskTop` unterscheidet. Jede dieser Varianten würde einen anderen Datei- oder Verzeichnisnamen repräsentieren. Viele, die eher an eine Windows-Umgebung gewöhnt sind, finden das frustrierend. Falls Sie die Fehlermeldung »File or directory not found« erhalten und sich sicher sind, dass die Datei oder das Verzeichnis existiert, sollten Sie die Groß-/Kleinschreibung überprüfen.

- **Verzeichnis (Directory)** – Hiermit ist dasselbe gemeint wie ein Ordner unter Windows. Ein Verzeichnis bietet eine Möglichkeit, Dateien zu organisieren, und dies normalerweise auf hierarchische Weise.
- **Home** – Jeder Benutzer hat ein eigenes */home*-Verzeichnis. Das ist im Allgemeinen die Stelle, an der Dateien, die Sie erzeugen, standardmäßig gespeichert werden.
- **Kali** – Kali Linux ist eine Linux-Distribution, die speziell für Penetrationstests geschaffen wurde. Darin sind Hunderte von Tools vorinstalliert, sodass Sie diese nicht selbst zeitaufwendig suchen, herunterladen und installieren müssen.
- **root** – Wie fast alle Betriebssysteme hat Linux einen Administrator- oder *Super-user*-Zugang, der für die Benutzung durch eine vertrauenswürdige Person gedacht ist, die auf dem System fast alles machen kann. Dazu gehören Dinge wie das Neukonfigurieren des Systems, das Hinzufügen von Benutzern und das Ändern von Passwörtern. Unter Linux wird dieser Zugang *root* genannt. Als Hacker oder Pentester werden Sie den *root*-Zugang oft benutzen, um sich selbst Kontrolle über das System zu verschaffen. Tatsächlich ist es für viele Hacker-Tools erforderlich, den *root*-Zugang zu benutzen.
- **Skript** – Hierbei handelt es sich um eine Abfolge von Befehlen, die interpretiert und direkt ausgeführt werden. Viele Hacking-Tools sind einfach nur Skripte. Skripte können mit dem *bash*-Interpreter oder anderen Skriptsprachen-Interpretern ausgeführt werden, wie Python, Perl oder Ruby. Python ist momentan der beliebteste Interpreter bei Hackern.
- **Shell** – Dies ist eine Umgebung und ein Interpreter für das Ausführen von Befehlen unter Linux. Die am weitesten verbreitete Shell ist die *bash* – die sogenannte *Bourne again*-Shell. Andere beliebte Shells sind die *C-Shell* und die *Z-Shell*. Ich werde in diesem Buch ausschließlich die *bash* verwenden.
- **Terminal** – Dies ist eine Kommandozeilenschnittstelle, auch *Command Line Interface* oder *CLI* genannt.

Jetzt haben Sie also die grundlegenden Begriffe kennengelernt und werden nun beginnen, systematisch die wichtigsten Linux-Fertigkeiten zu entwickeln, die Sie brauchen, um ein Hacker oder Pentester zu werden. In diesem ersten Kapitel werde ich mir mit Ihnen zusammen den Einstieg in Kali Linux anschauen.

## 1.2 Eine Tour durch Kali

Nach dem Start von Kali begrüßt Sie ein Login-Bildschirm. Melden Sie sich mit dem Benutzernamen *kali* und dem Standard-Passwort *kali* an (falls Sie dieses Passwort vorhin geändert haben, nehmen Sie natürlich hier dieses neue Passwort). Sie sollten nun Zugang zu Ihrem Kali-Desktop haben. Sie werden im Folgenden zwei der grundlegendsten Aspekte des Desktops kennenlernen: die Terminalschnittstelle und die Dateistruktur.

## 1.2.1 Das Terminal

Der erste Schritt für die Benutzung von Kali besteht darin, das *Terminal* zu öffnen. Dabei handelt es sich um die Kommandozeilenschnittstelle (auch Command Line Interface oder CLI), die in diesem Buch benutzt wird. Klicken Sie auf dieses Icon, um das Terminal zu starten. Es sollte ungefähr so aussehen wie in Abbildung 1.1.

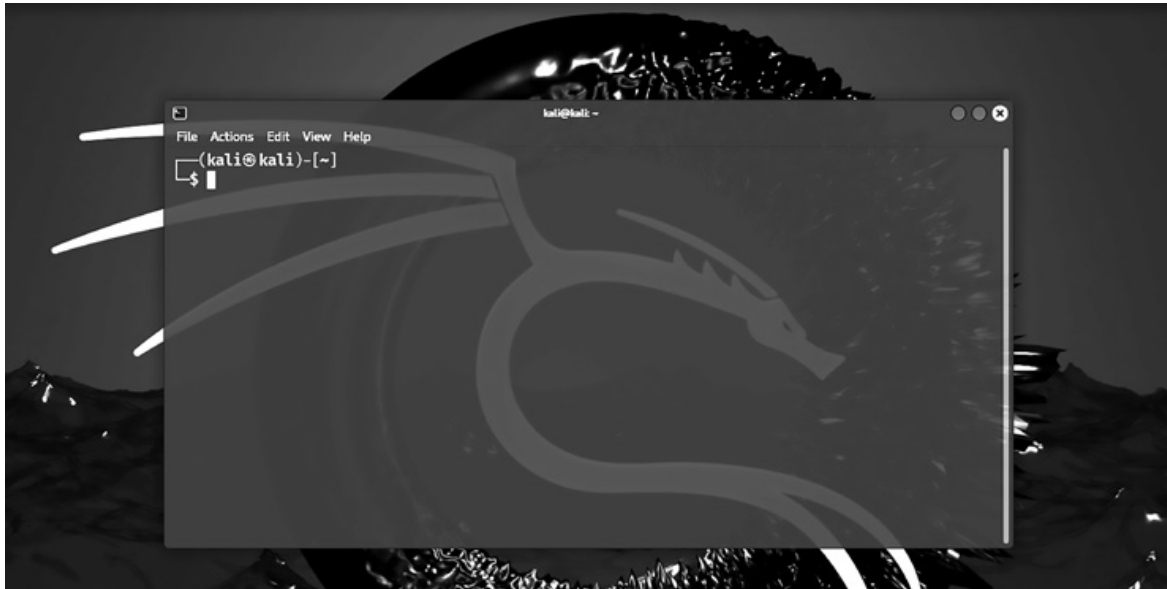


Abb. 1.1: Das Kali-Terminal

Dieses Terminal öffnet die Kommandozeilenumgebung, die sogenannte *Shell*, die es Ihnen erlaubt, Befehle auf dem darunter liegenden Betriebssystem auszuführen und Skripte zu schreiben. Linux besitzt viele unterschiedliche Shell-Umgebungen. Die beliebteste ist die *bash*, die in vielen Linux-Distributionen standardmäßig eingestellt ist.

Um Ihr Passwort zu ändern, können Sie den Befehl `passwd` verwenden.

## 1.2.2 Das Linux-Dateisystem

Die Linux-Dateisystemstruktur unterscheidet sich ein wenig von der unter Windows. Linux besitzt kein physisches Laufwerk (wie das Laufwerk C:) als Basis für das Dateisystem, sondern verwendet stattdessen ein logisches Dateisystem. An der Spitze der Dateisystemstruktur liegt `/`, das oft als *root* oder *Wurzel* des Dateisystems bezeichnet wird, so, als würde man einen auf dem Kopf stehenden Baum vor sich sehen (Abbildung 1.2). Beachten Sie jedoch, dass das nichts mit dem *root*-Benutzer zu tun hat. Diese Bezeichnungen mögen zunächst verwirrend sein, lassen sich aber leicht auseinanderhalten, wenn Sie sich erst einmal an Linux gewöhnt haben.

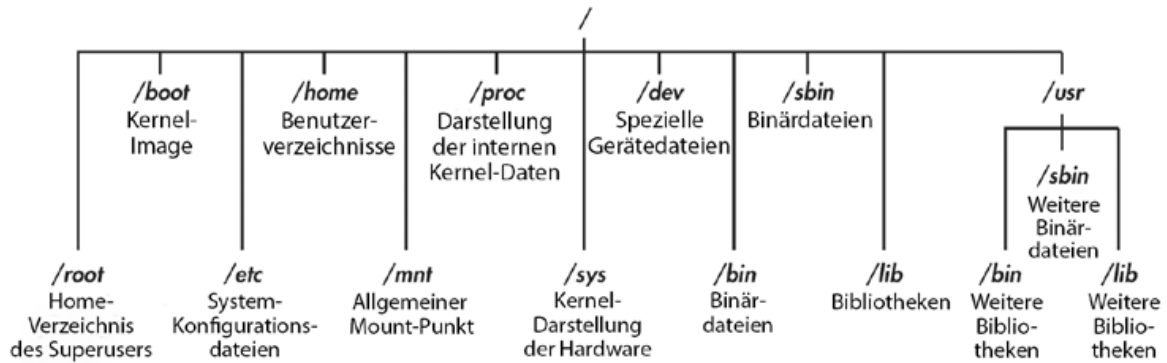


Abb. 1.2: Das Linux-Dateisystem

Die Wurzel (/) des Dateisystems befindet sich an der Spitze des Baums. Die im Folgenden aufgeführten Verzeichnisse sind die wichtigsten Unterverzeichnisse, die Sie kennen sollten:

- **/root** – Das Home-Verzeichnis des allmächtigen root-Benutzers
- **/etc** – Enthält im Allgemeinen die Linux-Konfigurationsdateien – Dateien, die kontrollieren, wann und wie Programme starten
- **/home** – Das Home-Verzeichnis der Benutzerin oder des Benutzers
- **/mnt** – Die Stelle, an der andere Dateisysteme an dieses Dateisystem angehängt bzw. »gemountet« sind
- **/media** – Die Stelle, an der CD- und USB-Geräte normalerweise an das Dateisystem angehängt bzw. »gemountet« sind
- **/bin** – Hier befinden sich die *Binärdateien* oder *Binaries* (diese sind äquivalent zu den ausführbaren Dateien in Windows oder den Anwendungen in macOS)
- **/lib** – Die Stelle, an der Sie die *Bibliotheken* oder *Libraries* finden (gemeinsam genutzte Programme, die vergleichbar mit den Windows-DLLs sind)

Sie werden im Verlauf des Buchs noch eine Menge Zeit mit diesen wichtigen Verzeichnissen verbringen. Um von der Kommandozeile aus durch das Dateisystem navigieren zu können, ist es jedenfalls wichtig, diese Verzeichnisse zu verstehen.

Wichtig ist außerdem, dass Sie sich nicht als root anmelden sollten, wenn Sie einfach nur Routineaufgaben erledigen wollen, da jeder, der Ihr System hackt (ja, auch Hacker sind manchmal Opfer von Hackerangriffen), wenn Sie als root angemeldet sind, sofort root-Rechte erhält und damit Ihr System »besitzt«. Melden Sie sich als normaler Benutzer an, wenn Sie normale Anwendungen starten, im Web surfen, Tools wie Wireshark ausführen wollen usw. Für die Übungen, die Sie in diesem Buch durchführen, ist es in Ordnung, als root angemeldet zu bleiben.

## 1.3 Grundlegende Befehle unter Linux

Schauen Sie sich zu Beginn einige grundlegende Befehle an, die Ihnen helfen, den Einstieg unter Linux zu finden und loszulegen.

### 1.3.1 Sich selbst finden mit `pwd`

Anders als beim Arbeiten mit einer grafischen Oberfläche, einem sogenannten Graphical User Interface oder GUI, wie in Windows oder macOS, ist es auf der Kommandozeile unter Linux nicht immer offensichtlich, in welchem Verzeichnis Sie sich gerade befinden. Um zu einem neuen Verzeichnis zu navigieren, müssen Sie normalerweise wissen, wo Sie gerade sind. Der Befehl `pwd` zum Ausgeben des Arbeitsverzeichnisses (*print working directory*) liefert Ihnen Ihren momentanen Ort innerhalb der Verzeichnisstruktur zurück.

Geben Sie in Ihrem Terminal `pwd` ein um festzustellen, wo Sie sich gerade befinden:

```
kali> pwd
/home/kali
```

Linux gibt in diesem Fall `/home/kali` zurück und sagt mir damit, dass ich gerade im Verzeichnis des Benutzers *kali* bin. Da Sie sich beim Start von Linux ebenfalls als *kali* angemeldet haben, sollten Sie sich auch im Verzeichnis des Benutzers *kali* befinden, das zwei Ebenen unter der Wurzel der Dateisystemstruktur (`/`) liegt.

Sind Sie in einem anderen Verzeichnis, liefert `pwd` stattdessen diesen Verzeichnisnamen zurück.

### 1.3.2 Ihr Login mit `whoami` prüfen

Unter Linux wird der »allmächtige« Superuser oder Systemadministrator als `root` bezeichnet und besitzt alle Systemberechtigungen, um Benutzer anzulegen, Passwörter zu ändern, Berechtigungen zu ändern usw. Natürlich wollen Sie nicht, dass jede beliebige Person das Recht hat, solche Änderungen vorzunehmen – es soll jemand sein, der vertrauenswürdig ist und sich mit dem Betriebssystem angemessen auskennt. Als Hacker müssen Sie normalerweise all diese Rechte haben, um die notwendigen Programme und Tools auszuführen (viele Hacker-Tools funktionieren nur, wenn Sie `root`-Rechte haben), sodass Sie sich als `root` anmelden sollten.

Falls Sie vergessen haben, ob Sie als `root` oder als ein anderer Benutzer angemeldet sind, können Sie mit dem Befehl `whoami` herausfinden, wer Sie sind:

```
kali> whoami
kali
```

Wäre ich als ein anderer Benutzer angemeldet gewesen, z.B. mit meinem persönlichen Zugang, hätte `whoami` stattdessen meinen Benutzernamen zurückgeliefert:

```
kali> whoami
OTW
```

Denken Sie außerdem daran, und ja, man kann das nicht oft genug sagen, dass Sie sich nicht als `root` anmelden sollten, wenn Sie nur Routineaufgaben ausführen, da ansonsten jeder, der Ihr System hackt (ja, auch Hacker werden manchmal gehackt), sonst automatisch `root`-Rechte erhält.

### 1.3.3 Durch das Linux-Dateisystem navigieren

Das Navigieren des Linux-Dateisystems vom Terminal aus ist eine ausgesprochen wichtige Linux-Fertigkeit. Um irgendetwas tun zu können, müssen Sie in der Lage sein, sich durch die Dateistruktur zu bewegen, um Anwendungen, Dateien und Verzeichnisse zu finden, die in anderen Verzeichnissen liegen. In einem grafischen System können Sie die Verzeichnisse sehen, doch in einer Kommandozeilenschnittstelle ist die Struktur vollkommen textbasiert und Sie brauchen Befehle, um durch das Dateisystem zu navigieren.

#### Verzeichnisse wechseln mit `cd`

Um vom Terminal aus Verzeichnisse zu wechseln, verwenden Sie den Befehl `cd` (für *change directory*). So wechseln Sie z.B. in das Verzeichnis `/etc`, in dem sich Konfigurationsdateien befinden:

```
kali> cd /etc
kali:/etc>
```

Der Prompt ändert sich zu `kali:/etc`, wodurch signalisiert wird, dass Sie nun im Verzeichnis `/etc` sind. Sie können dies bestätigen, indem Sie `pwd` eingeben:

```
kali:/etc> pwd
/etc
```

Um sich in der Dateistruktur eine Ebene nach oben zu bewegen (in Richtung der Wurzel der Dateistruktur oder `/`), verwenden Sie `cd`, gefolgt von zwei Punkten (`..`):

```
kali:/etc> cd ..
kali> pwd
/
```

Dies bringt Sie eine Ebene nach oben von */etc* in das Wurzelverzeichnis (*/*). Sie können so viele Ebenen nach oben gehen, wie Sie wollen. Verwenden Sie dazu einfach so viele Punkte-Paare, wie Sie Ebenen hinaufwandern wollen:

- Mit `..` gehen Sie eine Ebene nach oben.
- Mit `../..` bewegen Sie sich zwei Ebenen nach oben.
- Mit `../../..` würden Sie drei Ebenen nach oben wandern usw.

Um z.B. zwei Ebenen nach oben zu gehen, geben Sie `cd` ein, gefolgt von zwei Gruppen aus doppelten Punkten, die durch einen Schrägstrich getrennt sind:

```
kali> cd ../../
```

Sie können sich außerdem von einer beliebigen Stelle in die Wurzelebene begeben, indem Sie `cd /` eintippen, wobei `/` die Wurzel des Dateisystems repräsentiert.

### Den Inhalt eines Verzeichnisses mit `ls` auflisten

Um den Inhalt eines Verzeichnisses (die Dateien und Unterverzeichnisse) zu sehen, benutzen Sie den Befehl `ls` (*list*). Das ist vergleichbar mit dem `dir`-Befehl in Windows.

```
kali> ls
Debian          Music           usr
Desktop        Picture         Videos
Documents      Public
Downloads      Templates
```

Dieser Befehl listet sowohl die Dateien als auch die Verzeichnisse auf, die in diesem Verzeichnis enthalten sind. Sie können den Befehl auch bei einem ganz bestimmten Verzeichnis einsetzen, also nicht nur an dem, in dem Sie sich gerade befinden. Dazu geben Sie nach dem Befehl den entsprechenden Verzeichnisnamen an. So zeigt z.B. `ls /etc` den Inhalt des */etc*-Verzeichnisses an.

Um weitere Informationen über die Dateien und Verzeichnisse zu bekommen, wie etwa ihre Zugriffsberechtigungen, Eigentümer, Größen und Daten der letzten Änderung, setzen Sie hinter den Befehl `ls` den Schalter (auch *Flag* genannt) `-l` (für *long*). Oft wird dies als *langes Listing* bezeichnet. Versuchen Sie es einmal:

```
kali> ls -l
total 32
drw-r--r-- 1 kali kali 4096 Dec 5 11:15 Debian
drw-r--r-- 2 kali kali 4096 Dec 5 11:15 Desktop
drw-r--r-- 3 kali kali 4096 Dec 9 13:10 Documents
```

```
drw-r--r-- 18  kali kali 4096 Dec 9 13:43 Downloads
--schnippschnapp--
drw-r--r-- 1   kali kali 4096 Dec 5 11:15 Videos
```

Wie Sie sehen, liefert `ls -l` Ihnen bedeutend mehr Informationen, wie etwa, ob ein Objekt eine Datei oder ein Verzeichnis ist, die Anzahl der Links, den Eigentümer, die Gruppe, seine Größe, wann es erzeugt oder modifiziert wurde sowie seinen Namen.

Ich nutze den Schalter `-l` eigentlich immer, wenn ich ein Verzeichnis unter Linux auflisten lasse, aber das müssen Sie am Ende selbst für sich entscheiden. Sie werden in Kapitel 5 mehr über `ls` erfahren.

Manche Dateien unter Linux sind verborgen und lassen sich mit einem einfachen `ls` oder `ls -l` nicht auflisten. Um solche verborgenen Dateien anzeigen zu lassen, fügen Sie den Schalter `-a` hinzu:

```
kali> ls -la
```

Falls Sie eine Datei vermissen, die Sie eigentlich zu sehen erwarten, lohnt es sich, das Flag `a` einzusetzen. Sie können mehrere Flags miteinander kombinieren, wie Sie das hier mit `-la` gemacht haben, und müssen sie nicht einzeln als `-l -a` angeben.

### 1.3.4 Hilfe bekommen

Nahezu alle Befehle, Anwendungen oder Dienstprogramme haben unter Linux jeweils eigene Hilfedateien, in denen Sie Hinweise zur Benutzung erhalten. Falls ich z.B. Hilfe für die Verwendung des besten Wi-Fi-Cracking-Tools `aircrack-ng` bräuchte, könnte ich einfach den Befehl `aircrack-ng`, gefolgt vom Befehl `--help`, eingeben:

```
kali> aircrack-ng --help
```

Beachten Sie hier den doppelten Bindestrich. Die Konvention unter Linux besteht darin, einen doppelten Bindestrich (`--`) vor Optionen einzusetzen, die aus einem kompletten Wort bestehen, wie etwa `help`. Vor Optionen, die nur einen einzigen Buchstaben umfassen, wie `-h`, reicht ein einfacher Bindestrich (`-`).

Wenn Sie diesen Befehl eingeben, sollten Sie eine kurze Beschreibung des Tools sowie Hinweise zu seiner Benutzung erhalten. In manchen Fällen können Sie sowohl `-h` als auch `-?` verwenden, um zur Hilfedatei zu gelangen. Falls ich z.B. Hilfe

zur Benutzung des besten Portscanners nmap haben möchte, gebe ich Folgendes ein:

```
kali> nmap -h
```

Obwohl viele Anwendungen alle drei Optionen (`-- help`, `-h` und `-?`) unterstützen, gibt es leider keine Garantie, dass das immer so ist. Sollte also eine der Optionen nicht funktionieren, versuchen Sie es mit einer der anderen.

### 1.3.5 Das Handbuch aufrufen

Neben der Hilfe besitzen die meisten Befehle und Anwendungen ein Handbuch (Manual Pages) mit weiteren Informationen, wie etwa einer Beschreibung und einer Synopsis des Befehls oder der Anwendung. Sie können sich eine der sogenannten *Manpages* anschauen, indem Sie vor dem Befehl, dem Dienstprogramm oder der Anwendung `man` angeben. Um z.B. die Manpage für `aircrack-ng` zu öffnen, geben Sie Folgendes ein:

```
kali> man aircrack-ng
NAME
    aircrack-ng - a 802.11 WEP / WPA-PSK key cracker
SYNOPSIS
    aircrack-ng [options] <.cap / .ivs file(s)>
DESCRIPTION
    aircrack-ng is an 802.11 WEP and WPA/WPA2-PSK key cracking program. It
    can recover the WEP key once enough encrypted packets have been
    captured with airodump-ng. This part of the aircrack-ng suite
    determines the WEP key using two fundamental methods. The first method
    is via the PTW approach (Pyshkin, Tews, Weinmann). The main advantage
    of the PTW approach is that very few data packets are required to crack
    the WEP key. The second method is the FMS/KoreK method. The FMS/KoreK
    method incorporates various statistical attacks to discover the WEP
    key and uses these in combination with brute forcing. Additionally, the
    program offers a dictionary method for determining the WEP key. For
    cracking WPA/WPA2 pre-shared keys, a wordlist (file or stdin) or an
    airolib-ng has to be used.
```

Hier wird das Handbuch für `aircrack-ng` geöffnet, in dem Sie deutlich mehr Informationen finden als mit der Hilfe. Sie können mithilfe der `[Enter]`-Taste durch diese Handbuchdatei scrollen bzw. mit den `[Bild↑]`- und `[Bild↓]`-Tasten seitenweise blättern; aber auch die Pfeiltasten lassen sich verwenden. Um die Manpage zu verlassen, drücken Sie `[Q]` (für *quit*) und Sie gelangen wieder zurück zum Befehlsprompt.