

grml - Knoppix für Geeks

Michael Prokop <mika@grml.org>

27. Mai 2005



Agenda

- 1 grml? Die Theorie
 - grml?
 - grml unter der Haube. . .
 - Specials. . .
- 2 grml in der Praxis
- 3 Zukunft und Support

Was ist grml?

Was ist grml?

eine [Linux Live-CD](#) für x86

Und was noch?

- keine Installation notwendig (aber möglich)
- Zielgruppe: Systemadministratoren und Texttool-User -> Geeks :)
- Augenmerk auf "handicaped persons"
- basiert auf Knoppix und Debian
- "Merge the best of all the world" - das Schweizer Taschenmesser der Live-CDs

Was ist grml?

Was ist grml?

eine [Linux Live-CD](#) für x86

Und was noch?

- keine Installation notwendig (aber möglich)
- Zielgruppe: Systemadministratoren und Texttool-User -> Geeks :)
- Augenmerk auf "handicaped persons"
- basiert auf Knoppix und Debian
- "Merge the best of all the world" - das Schweizer Taschenmesser der Live-CDs

Was ist grml?

Was ist grml?

eine [Linux Live-CD](#) für x86

Und was noch?

- keine Installation notwendig (aber möglich)
- Zielgruppe: Systemadministratoren und Texttool-User -> Geeks :)
- Augenmerk auf "handicaped persons"
- basiert auf Knoppix und Debian
- "Merge the best of all the world" - das Schweizer Taschenmesser der Live-CDs

Was ist grml?

Was ist grml?

eine [Linux Live-CD](#) für x86

Und was noch?

- keine Installation notwendig (aber möglich)
- Zielgruppe: Systemadministratoren und Texttool-User -> Geeks :)
- Augenmerk auf "handicaped persons"
- basiert auf Knoppix und Debian
- "Merge the best of all the world" - das Schweizer Taschenmesser der Live-CDs

Was ist grml?

Was ist grml?

eine [Linux Live-CD](#) für x86

Und was noch?

- keine Installation notwendig (aber möglich)
- Zielgruppe: Systemadministratoren und Texttool-User -> Geeks :)
- Augenmerk auf "handicaped persons"
- basiert auf Knoppix und Debian
- "Merge the best of all the world" - das Schweizer Taschenmesser der Live-CDs

Was ist grml?

Was ist grml?

eine [Linux Live-CD](#) für x86

Und was noch?

- keine Installation notwendig (aber möglich)
- Zielgruppe: Systemadministratoren und Texttool-User -> Geeks :)
- Augenmerk auf "handicaped persons"
- basiert auf Knoppix und Debian
- "Merge the best of all the world" - das Schweizer Taschenmesser der Live-CDs

Warum grml?

Für was verwendet man grml?

- portable Arbeitsumgebung
- Systemadministration
- Security-Audits
- Netzwerk-Debugging
- Forensische Untersuchungen
- Testumgebung

Warum grml?

Für was verwendet man grml?

- portable Arbeitsumgebung
- Systemadministration
- Security-Audits
- Netzwerk-Debugging
- Forensische Untersuchungen
- Testumgebung

Warum grml?

Für was verwendet man grml?

- portable Arbeitsumgebung
- Systemadministration
- Security-Audits
- Netzwerk-Debugging
- Forensische Untersuchungen
- Testumgebung

Warum grml?

Für was verwendet man grml?

- portable Arbeitsumgebung
- Systemadministration
- Security-Audits
- Netzwerk-Debugging
- Forensische Untersuchungen
- Testumgebung

Warum grml?

Für was verwendet man grml?

- portable Arbeitsumgebung
- Systemadministration
- Security-Audits
- Netzwerk-Debugging
- Forensische Untersuchungen
- Testumgebung

Warum grml?

Für was verwendet man grml?

- portable Arbeitsumgebung
- Systemadministration
- Security-Audits
- Netzwerk-Debugging
- Forensische Untersuchungen
- Testumgebung

grml vs. Knoppix

	Knoppix	grml
Zielgruppe	Ein- und Umsteiger	Fortgeschrittene/Experten
Basis	Debian testing-experimental	Debian unstable
Software	KDE, OpenOffice,...	schlanke WM, >800 exkl. Apps
Entwicklung	geschlossen	offen (BTS, devel-blog)

grml und Debian

Wer Wissen hat, lasse andere ihr Licht daran entzünden...

- Laut <http://lwn.net/Distributions/> gibt es >400 Distributionen
- kommerzielle Anbieter: Release-Druck + Vendor-Lock-In
- Man **kann** nicht größer als 'Debian' sein:
 - Es gibt \geq 115 von Debian abgeleitete Distributionen
 - 960 Entwickler
 - >15.000 Pakete
 - "If you can't beat them - join them!"
- Mailinglisten, HowTos, Guidelines
- Ausgereiftes Paketmanagement
- öffentliches Bug-Tracking-System (BTS) seit 1994

Was steckt unter der Haube?

Aktuell

- Core: Debian unstable
- Add-Ons: grml-Pakete, Ubuntu + ausgesuchte externe Quellen
- Linux Kernel 2.6.11(.8) - Vanilla mit Patches
 - MPPE/MPCE
 - Reiser4
 - ... - grml.org/kernel/
- UnionFS: Schreibsupport auf Readonly-Medium
- SquashFS: bessere Komprimierung, schnellerer Buildprozess als bei cloop
- HW-Erkennung: hotplug + discover (+ hwinform)
- Device-System: udev

grml specials?

Spezialitäten

- zsh-lovers: grml.org/zsh/
- Skripte:
 - grml-mutt[ng]
 - grml-slrn
 - grml-nessus
 - grml-pptp-*
 - make_chroot_jail
 - ...

Was bringt grml mit?

Software

- Editoren: vim, emacs, joe, nano, ex-vi,...
- Internet: mutt[ng], slrn, centericq, irssi,...
- Datenrettung: gpart, recover, salvage-ntfs, scrounge-ntfs,...
- Netzwerk: nessus, nmap, hping, doscan,...
- Auditing: rats, pscan, bass, satan, smb-nat,...
- Datenbanken: mysql, postgresql, sqlite
- Serverdienste: subversion, apache/apache2,...

→ insgesamt 2244 Pakete

Features der zsh 1/3

Hashing:

```
% hash -d deb=/var/cache/apt/archives  
% cd ~deb  
% pwd
```

"Abkuerzung":

```
% ls -lah $(which vim)  
% ls -lah `which vim`  
% ls -lah =vim
```

Features der zsh 2/3

History-Completion:

```
% echo 123
% echo 321
% echo <cursor-up>
```

Global Alias:

```
% alias -g G='|grep'
% echo -e '123\n321' G 123
```

Features der zsh 3/3

"keephack" von Bart Schaefer:

```
% ls ~/ | keep  
% echo $kept
```

Sonstiges Wertvolles:

- Optionen: setopt ksh_option_print && setopt
- History-Sharing (setop sharehistory)
- Completion: compinstall
- vared VARIABLE # \$ vared PATH
- setopt autocd # \$ /tmp
- \$ ls **/*(.) # nur Dateien
- \$ whence -m '*vi*' # type + which -> vereint

zsh und die Tastatur 1/2

Wichtig! Was man oft braucht: mappen, konfigurieren

```
<tab>  -> Completion  
Alt-h   -> run-help  
Alt-<number>-<zeichen> -> x Zeichen einfuegen  
Alt-'   -> quote-line => ''  
Alt-$   -> spell-word(?)  
Alt-?   -> which-command  
Esc-.   -> insert-last-word to a key  
Strg-a  -> Anfang der Zeile  
Strg-b  -> ein Zeichen zurueck  
Strg-d  -> vervollstaendingen / EOF -> Shell beenden  
Strg-e  -> Ende der Zeile  
Strg-l  -> clear-screen
```

zsh und die Tastatur 2/2

Strg-_ -> Rueckgaengig (undo)
Strg-x+a -> Alias vervollstaendigen
Strg-x+e -> Wort vervollstaendigen
Strg-x+h -> Vervollstaendigung im Hilfe-Modus
Strg-x+? -> Vervollstaendigung im Debug-Modus
Strg-k -> kill-line
Strg-u -> ganze Zeile kopieren
Strg-w -> letztes Word loeschen
Strg-y -> yank (kill-ring einfuegen)

Generell:

```
$ man readline  
$ bindkey -L  
$ bindkey 'ctrl-v <keys>'
```

grml-Specials

Nützliche Sachen

- (x)say: Textoutput via Sound (text2speech)
- grml-mutt[ng]: Grundkonfiguration für Mailclient mutt[ng] erstellen
- grml-slrn: Grundkonfiguration für Newsreader slrn erstellen
- make_chroot_jail: minimales chroot erstellen
- `dpkg -L grml-scripts grml-sectools ...`

Utilities 1/3

Hardware-Informationen:

```
# sitar.pl --outfile=sitar.html --format=html  
# hwinfo | most  
# grml-hwinfo
```

Systeminformationen/Statistiken:

```
# bonnie++ ....  
# vmstat  
# dstat # 'vmstat -adDpsm 1' in bunt
```

Utilities 2/3

Informationen zu einem Device:

```
# hdparm -I /dev/hda  
# blktool /dev/hda class
```

lesspipe von Wolfgang Friebel:

```
% less \  
  /usr/share/grml-sectools/exploits/ramen.tar.gz  
% less \  
  /usr/share/grml-sectools/exploits/ramen.tar.gz:\br/>  Ramen/scan.sh
```

Utilities 3/3

Top 75 Security Tools (www.insecure.org/tools.html)

```
* nast, doscan, hping3,...
```

```
# xprobe2 $IPADDRESS
```

```
% amap $IP 22-80
```

```
% sudo /etc/init.d/apache2 start
```

```
% mkdir ~/public_html
```

```
% echo welcome > ~/public_html/index.html
```

grml2hd - grml auf die Festplatte installieren

Das Installationsprogramm

- keine speziellen (Linux-)Kenntnisse notwendig(!)
- nur wenige Abfragen:
 - Dateisystem
 - Username
 - Passwort für root + User

Welcome to grml2hd 0.4.2!

grml2hd can install grml to your harddisk.

The grml team doesn't take responsibility for any loss of data!
grml2hd requires at least 2.7 GiB of free space on your
harddisk.

Make sure you have the latest version of grml2hd!
Additional information and updates are available at:
<http://grml.org/grml2hd/>

Please give us feedback to improve the installer!
<http://grml.org/contact/> contact (at) grml.org

< OK >

grml2hd
Congratulations!
You have a harddisk installation of GRML now.
Enjoy.
< OK >

```
grml2hd /dev/hda5 -mbr /dev/hda 2.72s user 79.23s system 18% cpu 7:11.88 total  
grml has logged on pts/4 from :7.0.  
grml has logged on pts/5 from :7.0.  
root@grml ~ #
```

grml-terminalserver

grml übers Netzwerk booten

- via PXE
- via Diskette + Netzwerk

grml im Einsatz

Und nun schauen wir uns das System einmal im Einsatz an.

grml in der Zukunft. . .

- Erweiterung der Dokumentation
- grml2hd: vollautomatische Installation
- "Choose the Debian way of life"

Support?

Kostenfrei

- Mailingliste
- IRC (#grml)

Kostenpflichtig

- Remastering / speziell angepasste CDs
- Systemadministration
- IT-Consulting + Security

Das Ende...

Feedback

Danke für die Aufmerksamkeit!
Feedback ist willkommen!
Bei grml fehlt noch etwas? Melden!

Kontakt

Michael Prokop <mika@grml.org>
<http://michael-prokop.at/>
<http://grml.org/>