

Praktische Datenverarbeitung

- **Einbruch in ein Linux System**
 - z.B. „root“-Passwort vergessen oder nicht mehr bekannt
- Voraussetzung:
 - Physikalischer Zugriff auf die Konsole
 - Remote Zugriff auf die Konsole (z.B. über ILO-, IPMI-Interface oder KVM-Switch)

„Hacking“

Aufwand max. 1 UE

Achtung ;-)

<ironic mode>

Für den unwahrscheinlichen Fall, dass Sie Ihr Passwort für das Login als „root“ vergessen haben sollten, finden Sie hier die Anleitung, wie Sie wieder in **Ihr** System kommen.

Die Methode setzt voraus, dass Sie Zugriff auf eine Konsole Ihres Systems haben.

</ironic mode>

~

Booten bis zum „grub“-Menü


Mit „e“ in den Editiermodus des GRUB wechseln

29.01.24 Horst Bräuner 2

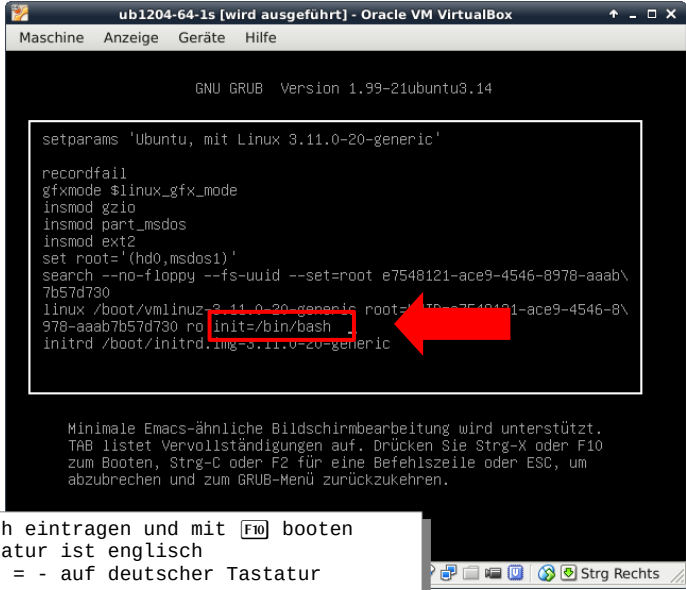
Als erstes unterbrechen Sie den Boot-Vorgang mit der ESC-Taste, sobald der Bootloader angezeigt wird.

Stellen Sie die Markierung mit den Pfeiltasten auf die Zeile, mit der Ihr System normalerweise startet. Das ist meist die erste Zeile.

Wechseln Sie mit „e“ in den Editiermodus des Bootloaders ...



Grub-Eintrag bearbeiten



29.01.24Horst Bräuner3

... und suchen Sie die Zeile mit in der „linux /boot/...“ gestartet wird. Das ist meist die Zeile über „initrd ...“.

Tragen Sie am Ende der Zeile „linux ...“ „init=/bin/bash“ ein. Damit starten Sie Ihr System in eine Shell. Denke Sie daran, dass die Tastaturbelegung vor dem Bootvorgang noch englisch ist. Das „=“ ist auf der „ß“-Taste und der „/“ ist auf der „-“Taste.

Booten Sie mit der F10-Taste den modifizierten Bootloader.

Wenn Sie das vorangestellte „ro“ durch „rw“ ersetzen versucht das System das Dateisystem mit Schreibrechten zu starten. Das kann, je nach Zustand und Linux-Variante, erfolgreich sein. Es ist jedoch nicht empfehlenswert.

~

Booten in die „bash“

ub1204-64-1s [wird ausgeführt] - Oracle VM VirtualBox


MaschineAnzeigeGeräteHilfe

```
[ 3.814435] sdd: unknown partition table
[ 3.815374] sd 5:0:0:0: [sdd] Attached SCSI disk
[ 4.132911] ata7: SATA link up 3.0 Gbps (SStatus 123 SControl 300)
[ 4.138339] ata7.00: ATA-6: UBOX HARDDISK, 1.0, max UDMA/133
[ 4.138339] ata7.00: 2097152 sectors, multi 128: LBA48 NCQ (depth 31/32)
[ 4.138339] ata7.00: configured for UDMA/133
[ 4.138545] scsi 6:0:0:0: Direct-Access    ATA        UBOX HARDDISK    1.0 PQ
: 0 ANSI: 5
[ 4.141340] sd 6:0:0:0: [sde] 2097152 512-byte logical blocks: (1.07 GB/1.00
GiB)
[ 4.142643] sd 6:0:0:0: [sde] Write Protect is off
[ 4.143358] sd 6:0:0:0: [sde] Write cache: enabled, read cache: enabled, does
n't support DPO or FUA
[ 4.146326] sd 6:0:0:0: Attached scsi generic sg5 type 0
[ 4.167451] sde: sde1 sde2
[ 4.168935] sd 6:0:0:0: [sde] Attached SCSI disk
Begin: Running /scripts/local-premount ... done.
[ 4.628242] EXT4-fs (sda1): mounted filesystem with ordered data mode. Opts:
(null)
Begin: Running /scripts/local-bottom ... done.
done.
Begin: Running /scripts/init-bottom ... done.
bash: cannot set terminal process group (-1): Inappropriate ioctl for device
bash: no job control in this shell
root@(none):/#
```



System bootet in ein „bash“ ohne Passwort-
Abfrage; **user = root**

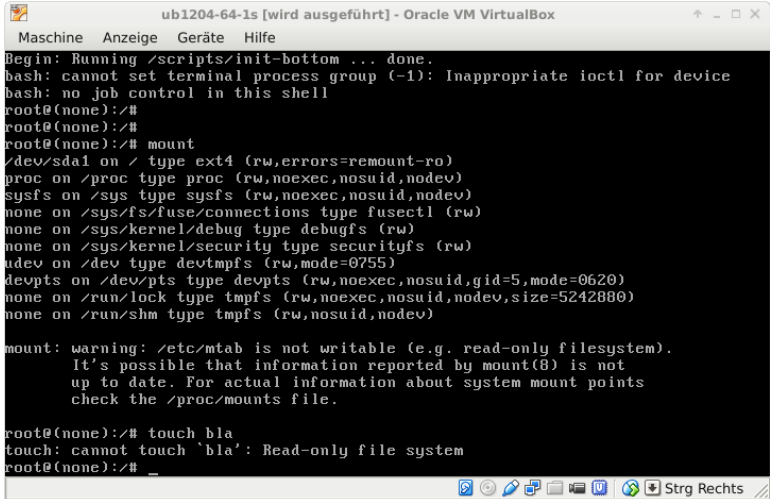
29.01.24Horst Bräuner4

Ihr System startet in eine „root“-Shell ohne nach einem Passwort zu fragen.



System = „read only“





System ist mit / = read only gestartet.

29.01.24

Horst Bräuner

5

Zur „Sicherheit“ ist Ihr System mit einem „Read only“-Dateisystem gestartet. Sie können also das „root“-Passwort nicht direkt ändern.

Falls Sie bei dem geänderten Boot-Prompt (init=/bin/bash) das vorangestellte „ro“ durch „rw“ zu ersetzt haben, versucht der Bootloader das System/Dateisystem bereits mit Schreibrechten zu starten.



root passwd ändern



```
ub1204-64-1s [wird ausgeführt] - Oracle VM VirtualBox
Maschine Anzeige Geräte Hilfe
udev on /dev type devtmpfs (rw,mode=0755)
devpts on /dev/pts type devpts (rw,noexec,nosuid,gid=5,mode=0620)
none on /run/lock type tmpfs (rw,noexec,nosuid,nodev,size=5242880)
none on /run/shm type tmpfs (rw,nosuid,nodev)


mount: warning: /etc/mtab is not writable (e.g. read-only filesystem).
It's possible that information reported by mount(8) is not
up to date. For actual information about system mount points
check the /proc/mounts file.

root@(none):/# touch bla
touch: cannot touch 'bla': Read-only file system
root@(none):/#
root@(none):/#
root@(none):/# mount -o remount /
[ 159.461627] EXT4-fs (sda1): re-mounted. Opts: errors=remount-ro
root@(none):/#
root@(none):/# touch bla
root@(none):/#
root@(none):/# passwd root
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
root@(none):/#
root@(none):/# _
```


/ „remounten“, damit /etc/shadow „schreibbar“
ist und anschließend root-Passwort ändern

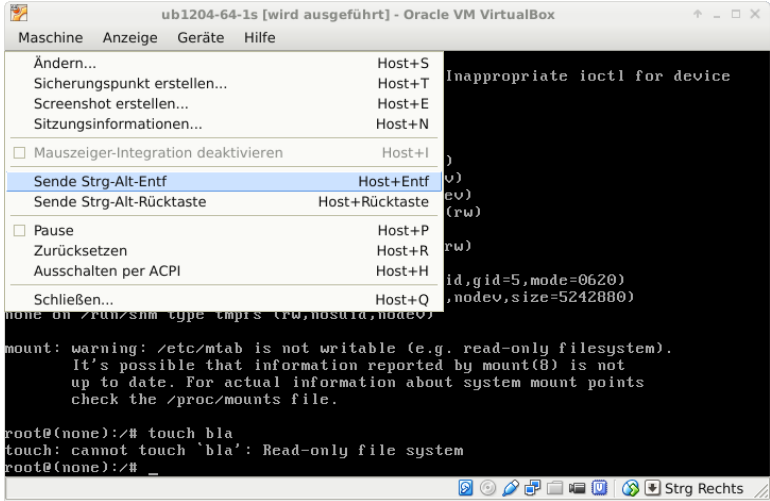
„mounten“ Sie das Dateisystem im „Read write“-Modus und setzen Sie mit „passwd“ Ihr neues Passwort für „root“.

```
root@(none):/# mount -o remount /
root@(none):/#
root@(none):/# passwd
```



reboot





System mit **Strg+Alt+Entf** (oder über Menü der VirtualBox) „sauber“ neu starten

29.01.24Horst Bräuner7

Dann starten Sie Ihr System neu, zum Beispiel mit der STRG-ALT-ENTF / CTRL-ALT-DELETE Tastenkombination.



Neues Passwort verwenden



```
ub1204-64-1s [wird ausgeführt] - Oracle VM VirtualBox
Maschine  Anzeige  Geräte  Hilfe

Ubuntu 12.04.4 LTS ubuserver1 tty1
ubuserver1 login: root
Password:
Last login: Sun Apr 27 19:31:50 CEST 2014 on tty1
Welcome to Ubuntu 12.04.4 LTS (GNU/Linux 3.11.0-20-generic x86_64)

* Documentation:  https://help.ubuntu.com/

System information disabled due to load higher than 1.0

root@ubuserver1:~# _
```

Mit geändertem Passwort als „root“ anmelden.

29.01.24Horst Bräuner8

Sie können sich dann ab sofort mit dem „neuen“ Passwort anmelden.

Die Änderungen im Boot-Loader wurden nur temporär durchgeführt. Sie müssen hier nichts rückgängig machen.

Nochmal: Dies ist die Anleitung, wie Sie in **IHR EIGENES SYSTEM** einbrechen können, falls Sie Ihr Passwort für „root“ vergessen haben.