

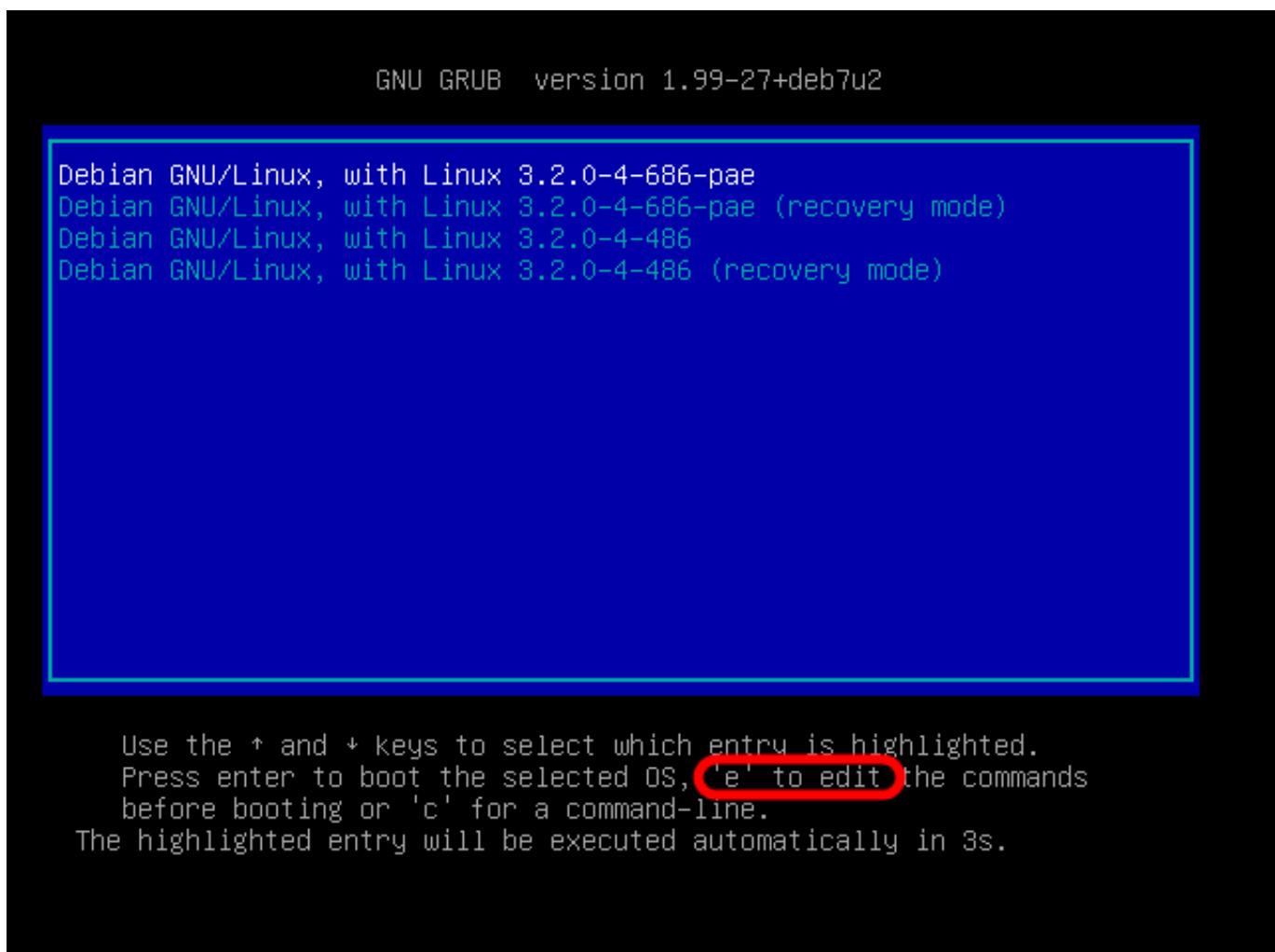
Zaboravljena zaporka za poslužitelj



Ponekad, najčešće nakon godišnjeg odmora, dogodi se da zaboravimo administratorsku lozinku za poslužitelj kojeg dulje vrijeme nismo koristili. Obično je nismo zapisali negdje na sigurno mjesto, ili u KeePass i slične *password managere*.

Iako smo na portalu već pisali kako riješiti problem zaboravljenih lozinaka, dodat ćemo još jedan način. No prvo, ponovimo kako to većina radi...

Poslužitelj moramo restartati, a nakon što se pojavi GRUB-ov izbornik, na tipkovnici odaberite slovo "e" (*edit mode*). Nemojte pritiskati tipku Enter.



Pronađite liniju koja počinje sa `linux/boot/vmlinuz-X.X.X..`, te na kraju linije ubacite razmak (`space`) i upišite `"init=/bin/bash"` (bez navodnika):

GNU GRUB version 1.99-27+deb7u2

```
setparams 'Debian GNU/Linux, with Linux 3.2.0-4-686-pae'

load_video
insmod gzio
insmod part_msdos
insmod ext2
set root='(hd0,msdos2)'
search --no-floppy --fs-uuid --set=root d5f912e5-0c2c-46e1-81fe-b6ab\de361512
echo 'Loading Linux 3.2.0-4-686-pae ...'
linux /boot/vmlinuz-3.2.0-4-686-pae root=UUID=d5f912e5-0c2c-46e1-81f\de-b6abde361512 ro quiet
echo 'Loading initial ramdisk ...'
initrd /boot/initrd.img-3.2.0-4-686-pae
```

Minimum Emacs-like screen editing is supported. TAB lists completions. Press Ctrl-x or F10 to boot, Ctrl-c or F2 for a command-line or ESC to discard edits and return to the GRUB menu.

GNU GRUB version 1.99-27+deb7u2

```
setparams 'Debian GNU/Linux, with Linux 3.2.0-4-686-pae'

load_video
insmod gzio
insmod part_msdos
insmod ext2
set root='(hd0,msdos2)'
search --no-floppy --fs-uuid --set=root d5f912e5-0c2c-46e1-81fe-b6ab\de361512
echo 'Loading Linux 3.2.0-4-686-pae ...'
linux /boot/vmlinuz-3.2.0-4-686-pae root=UUID=d5f912e5-0c2c-46e1-81f\de-b6abde361512 ro quiet init=/bin/bash_
echo 'Loading initial ramdisk ...'
initrd /boot/initrd.img-3.2.0-4-686-pae
```

Minimum Emacs-like screen editing is supported. TAB lists completions. Press Ctrl-x or F10 to boot, Ctrl-c or F2 for a command-line or ESC to discard edits and return to the GRUB menu.

Nakon što ste to upisali, za *boot* pritisnite Ctrl+X.

Kad se poslužitelj digne i dobijete naredbenu liniju, treba napraviti remount direktorija root (/), na takav način da je omogućeno i čitanje i pisanje:

```
# mount -w -o remount /

-w -      (i) čitanje (i) pisanje

-o - dodatne opcije
remount - ponovno mountanje uređaja s dodatnim opcijama (u ovom slučaju writeable).
```

Slijedi izmjena zaporke korisnika root pomoću naredbe *passwd*:

```
# passwd
```

```
root@(none):/# mount -w -o remount /
root@(none):/# passwd
Enter new UNIX password:
Retype new UNIX password: _
```

Prilično je jednostavno, no postoje i drugi načini. Ovdje mislimo uglavnom na razne Live CD-ove, koji osim promjene lozinke omogućavaju i druge operacije koje bi nam inače bilo teško napraviti iz ograničenog shella kojeg dobijemo prethodnim načinom.

U ovom primjeru ćemo demonstrirati izravno editiranje datoteke /etc/shadow, što nije preporučljivo, ali nekada sistemski alati ne mogu pomoći. Primjerice, datoteka je oštećena i format nije prepoznat, pa naredba *passwd* ne radi.

Koristit ćemo jedan od mnogih rescue diskova (Knoppix, The Trinity Rescue Kit, System Rescue CD). U primjeru koristili smo System Rescue CD (http://www.sysresccd.org/SystemRescueCd_Homepage [1]), sa grafičkim sučeljem.

Poslužitelj pokrećemo sa bootabilnog CD ili USB uređaja, te bez previše razmišljanja možete odabratи prvu opciju s izbornika.

SYSTEM-RESCUE-CD 4.6.0 (www.sysresccd.org)

- 1) SystemRescueCd: default boot options**
- 2) SystemRescueCd: all files cached to memory (docache)
- 3) SystemRescueCd: framebuffer console in high resolution
- 4) SystemRescueCd: do not ask for keyboard, use US keymap
- 5) Boot an existing Linux system installed on the disk
- 6) SystemRescueCd: alternative kernel with default boot option
- 7) SystemRescueCd: directly start the graphical environment
 - A) Run system tools from floppy disk image... >
 - B) Standard 32bit kernel (rescue32) with more choice... >
 - C) Standard 64bit kernel (rescue64) with more choice... >
 - D) Alternative 32bit kernel (altker32) with more choice... >
 - E) Alternative 64bit kernel (altker64) with more choice... >
- *) Boot from first hard disk**
- *) Boot from second hard disk**

Automatic boot in 59 seconds...

Press [TAB] to edit options or <F2>,<F3>,<F4>,<F5>,<F6>,<F7> for help

Boot standard kernel with default options (should always work). You should use this entry if you don't know which one to use. You can press [TAB] and add extra boot options after rescue32 or/and rescue64 if required

Nakon odabira tipkovnice sljedeći prozor daje nam kratke upute kako što mountati i kako pokrenuti grafičko sučelje. Odabrali smo rad iz grafičkog sučelja sa naredbom: "**startx**". Prilikom pokretanja grafičkog sučelja odmah se pokreće terminal i spajanje na mrežu.

```
===== SystemRescue-Cd ----- 4.6.0 ====== tty1/6 ==
http://www.sysresccd.org/

* Type net-setup eth0 to specify ethernet configuration.
* If your PC is on an ethernet local network, you can configure by hand:
  - ifconfig eth0 192.168.x.a (your static IP address)
  - route add default gw 192.168.x.b (IP address of the gateway)
* To be sure there is an ssh server running, type /etc/init.d/sshd start.
  You will need to create an user or to change the root password with passwd.
* Available console text editors : nano, vim, qemacs, zile, joe.
* Web browser in the console: elinks www.web-site.org.
* Ntfs-3g : If you need a full Read-Write NTFS access, use Ntfs-3g.
  Mount the disk: ntfs-3g /dev/sda1 /mnt/windows
* Graphical environment :
  Type startx to run the graphical environment
  X.Org comes with the XFCE environment and several graphical tools:
  - Partition manager:...gparted
  - Web browsers:.....midori
  - Text editors:.....gvim and geany
```

```
root@sysresccd /root % startx_
```

```
Disk /dev/loop0: 325 MiB, 340746240 bytes, 665520 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk /dev/sda: 22.2 GiB, 23824007168 bytes, 46531264 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x0003ac74

Device      Boot   Start     End   Sectors  Size Id Type
/dev/sda1            2048 2930687 2928640  1.4G 82 Linux swap / Solaris
/dev/sda2 *         2930688 3934207 1003520 490M 83 Linux
/dev/sda3         3934208 19558399 15624192  7.5G 83 Linux
/dev/sda4         19560446 46530559 26970114 12.9G  5 Extended
/dev/sda5         19560448 35182591 15622144  7.5G 83 Linux
/dev/sda6         35184640 37136383 1951744   953M 83 Linux
/dev/sda7         37138432 46530559 9392128   4.5G 83 Linux

root@sysresccd /root %
```

Sa "**fdisk -l**" pregledamo particije našeg sustava koje trebamo za mount, tj. tražimo root particiju koja je se u našem primjeru nalazi na uređaju "/dev/sda2". Kreiramo jednu privremenu točku za mount, primjerice privremeno, s "mkdir privremeno". Nakon kreiranja ukucamo "mount /dev/sda2 privremeno".

```
Disk /dev/loop0: 325 MiB, 340746240 bytes, 665520 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk /dev/sda: 22.2 GiB, 23824007168 bytes, 46531264 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x0003ac74

Device      Boot   Start     End   Sectors  Size Id Type
/dev/sda1            2048 2930687 2928640  1.4G 82 Linux swap / Solaris
/dev/sda2 *         2930688 3934207 1003520 490M 83 Linux
/dev/sda3         3934208 19558399 15624192  7.5G 83 Linux
/dev/sda4         19560446 46530559 26970114 12.9G  5 Extended
/dev/sda5         19560448 35182591 15622144  7.5G 83 Linux
/dev/sda6         35184640 37136383 1951744   953M 83 Linux
/dev/sda7         37138432 46530559 9392128   4.5G 83 Linux

root@sysresccd /root % mkdir privremeno
root@sysresccd /root % mount /dev/sda2 privremeno/
```

Nakon što smo mountali disk, odlazimo do **/etc** (**cd privremeno/etc**) direktorija gdje se nalazi

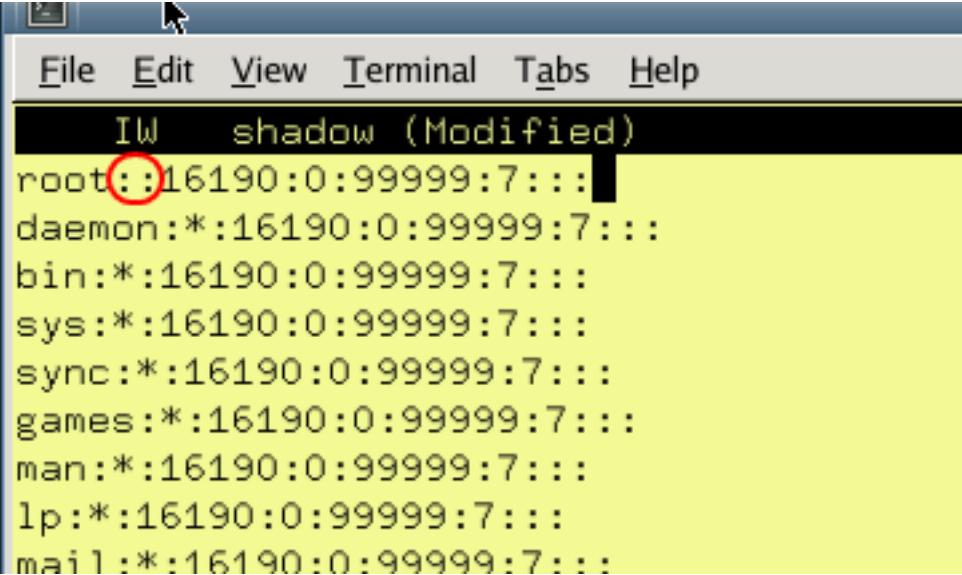
shadow datoteka. U njoj ćemo obrisati rootovu zaporku, tako da ćemo izbrisati pripadajući enkriptirani niz znakova.

Ono što je važno kod editiranje shadow datoteke za korisnika root je brisanje sadržaja između prve dvotočke (":") do sljedeće dvotočke (ni manje ni više, kako ne bi narušili strukturu datoteke!):



```
File Edit View Terminal Tabs Help
Iw shadow
root:$6$HMLiuUoh$4Dpsy00FyF4JuEix7H1X0/oRLDYN9t9mdg6/b1QttbfTbPv8/j1bgXc3iuNHElb1Fwsj0D4YsoZVHBELRNg$161
daemon:*:16190:0:99999:7:::
bin:*:16190:0:99999:7:::
sys:*:16190:0:99999:7:::
sync:*:16190:0:99999:7:::
games:*:16190:0:99999:7:::
man:*:16190:0:99999:7:::
lp:*:16190:0:99999:7:::
mail:*:16190:0:99999:7:::
news:*:16190:0:99999:7:::
uucp:*:16190:0:99999:7:::
proxy:*:16190:0:99999:7:::
www-data:*:16190:0:99999:7:::
backup:*:16190:0:99999:7:::
list:*:16190:0:99999:7:::
irc:*:16190:0:99999:7:::
gnats:*:16190:0:99999:7:::
nobody:*:16190:0:99999:7:::
libuuid:!:16190:0:99999:7:::
Debian-exim:!:16190:0:99999:7:::
statd:*:16190:0:99999:7:::
sshd:*:16190:0:99999:7:::
ftp:*:16190:0:99999:7:::
```

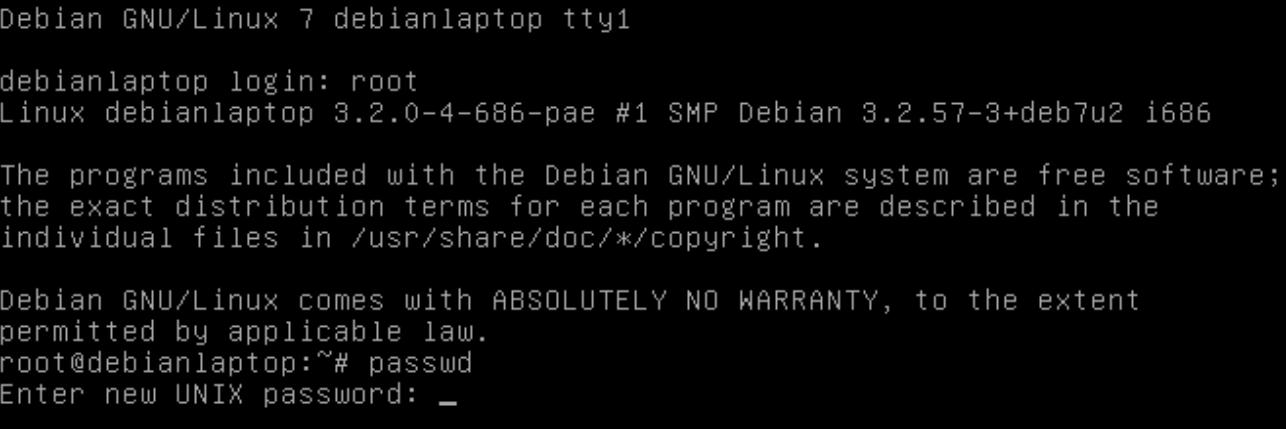
Nakon brisanja tog niza znakova, shadow datoteka treba izgledati ovako:



```
File Edit View Terminal Tabs Help
Iw shadow (Modified)
root:::16190:0:99999:7:::
daemon:*:16190:0:99999:7:::
bin:*:16190:0:99999:7:::
sys:*:16190:0:99999:7:::
sync:*:16190:0:99999:7:::
games:*:16190:0:99999:7:::
man:*:16190:0:99999:7:::
lp:*:16190:0:99999:7:::
mail:*:16190:0:99999:7:::
```

Ukoliko je datoteka oštećena (u smislu da su neke linije spojene i slično), popravite i to. Snimite datoteku i napravite reboot računala. Izvadite CD ili USB uređaj s kojeg ste pokretali računalo.

Nakon što se računalo normalno starta, prijavite se kao korisnik root. Sustav će tražiti zaporku, ali ona ne postoji, pa samo stisnite Enter. Obavezno odmah promijenite zaporku i možete nastaviti s normalnim radom.



```
Debian GNU/Linux 7 debianlaptop tty1

debianlaptop login: root
Linux debianlaptop 3.2.0-4-686-pae #1 SMP Debian 3.2.57-3+deb7u2 i686

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
root@debianlaptop:~# passwd
Enter new UNIX password: _
```

sri, 2015-09-30 10:43 - Zdravko Rašić**Kuharice:** [Linux](#) [2]

Kategorije: [Operacijski sustavi](#) [3]

Vote: 5

Vaša ocjena: Nema Average: 5 (1 vote)

Source URL: <https://sysportal.carnet.hr/node/1570>

Links

[1] http://www.sysresccd.org/SystemRescueCd_Homepage

[2] <https://sysportal.carnet.hr/taxonomy/term/17>

[3] <https://sysportal.carnet.hr/taxonomy/term/26>