

## 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*.

lako smo na portalu već pisali kako riješiti problem zaboravljene lozinke, 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.

Debian GNU/Linux, with Linux 3.2.0-4-686-pae Debian GNU/Linux, with Linux 3.2.0-4-686-pae (recovery mode) Debian GNU/Linux, with Linux 3.2.0-4-486 (recovery mode) Debian GNU/Linux, with Linux 3.2.0-4-486 (recovery mode) Use the t and t keys to select which entry is highlighted. Press enter to boot the selected OS, ('e' to edit the commands before booting or 'c' for a command-line. The highlighted entry will be executed automatically in 3s.

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):





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





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 (<u>http://www.sysresccd.org/SystemRescueCd\_Homepage</u> [1]), sa grafičkim sučeljem.

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



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 op	tion
(T) = (T + T) + (T + T)	nt 👘
7) Systemnescueta: alrectly start the graphical environment	
<ul><li>A) Run system tools from floppy disk image</li></ul>	>
<ul> <li>A) Run system tools from floppy disk image</li> <li>B) Standard 32bit kernel (rescue32) with more choice</li> </ul>	>
<ul> <li>A) Run system tools from floppy disk image</li> <li>B) Standard 32bit kernel (rescue32) with more choice</li> <li>C) Standard 64bit kernel (rescue64) with more choice</li> </ul>	>
<ul> <li>A) Run system tools from floppy disk image</li> <li>B) Standard 32bit kernel (rescue32) with more choice</li> <li>C) Standard 64bit kernel (rescue64) with more choice</li> <li>D) Alternative 32bit kernel (altker32) with more choice</li> </ul>	>
<ul> <li>A) Run system tools from floppy disk image</li> <li>B) Standard 32bit kernel (rescue32) with more choice</li> <li>C) Standard 64bit kernel (rescue64) with more choice</li> <li>D) Alternative 32bit kernel (altker32) with more choice</li> <li>E) Alternative 64bit kernel (altker64) with more choice</li> </ul>	
<ul> <li>A) Systemnescueca: arrectly start the graphical environmer</li> <li>A) Run system tools from floppy disk image</li> <li>B) Standard 32bit kernel (rescue32) with more choice</li> <li>C) Standard 64bit kernel (rescue64) with more choice</li> <li>D) Alternative 32bit kernel (altker32) with more choice</li> <li>E) Alternative 64bit kernel (altker64) with more choice</li> <li>*) Boot from first hard disk</li> </ul>	

Automatic boot in 59 seconds...

Press ITAB1 to edit options or <P2>,<P3>,<P4>,<P5>,<P6>,<P7> 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.

	======================================
	http://www.sysresccd.org/
	lype net-setup etho to specify ethernet configuration.
	It your PL is on an ethernet local network, you can configure by nand:
	- ITCONTIG ETNU 192.100.X.a (your static iP address)
	To be sure there is an esh server running, tune /etc/init d/schd start
	You will need to create an user or to change the root password with passwd.
	Available console text editors : nano, vim, gemacs, 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.Urg comes with the XFCE environment and several graphical tools:
	- Partition manager:gparted
	- Meb browsers:milori
	- Text editorsgvim and yeany
rc	oot@susresccd /root % startx





Sa "**fdisk -I**" 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".

<u>F</u> ile <u>E</u> dit <u>V</u> i	ew <u>T</u> er	minal T <u>a</u> bs	<u>H</u> elp							
root@sysresccd /root % fdisk -l										
)isk /dev/loop0: 325 MiB, 340746240 bytes, 665520 sectors										
Jnits: sectors of 1 * 512 = 512 bytes										
Sector size (logical/physical): 512 bytes / 512 bytes										
I/O size (ı	ninimu	m∕optimal	l): 512 by	ytes / 512	2 bytes	3				
Disk /dev/s	sda: 2	2.2 GiB,	238240071	168 bytes,	46531	.264	4 sectors			
Units: sec	tors c	of 1 * 512	2 = 512 by	ytes						
Sector size	∋ (log	ical/phys	sical): 51	12 bytes /	′ 512 k	oyte	35			
I/O size (r	ninimu	m/optimal	l): 512 by	ytes / 512	2 bytes	6				
Disklabel 1 Disk identi	type:	dos	74							
Disk ident:	1+1er:	0x0003ac	C74							
Device	Boot	Start	End	Sectors	Size	Id	Туре			
/dev/sda1		2048	2930687	2928640	1.4G	82	Linux swap / Solaris			
/dev/sda2	ж	2930688	3934207	1003520	490M	83	Linux			
/dev/sda3		3934208	19558399	15624192	7.5G	83	Linu×			
/dev/sda4	/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@sysre:	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!):

Ele Cdt V/ew Terminal Tabs Help           IV         Source         Cnl -26         9:03         6tral=6         H. Source           root:         \$\$\$55K1L1UoN\$4DPsyOOFyF4JUaEix7H1XO/dRLDYn9t9mdg67b10ttbfFtbPv8/j1bqXc31ukHELbiFusj0D4Yac2VHBELRHg/s1           daemon:*:16190:0:99999:7:::         \$\$yo:*:16190:0:99999:7:::         \$\$yo:*:16190:0:99999:7:::           syo::*:16190:0:99999:7:::         \$\$yo:*:16190:0:99999:7:::         \$\$yo:*:16190:0:99999:7:::           amar:*:16190:0:99999:7:::         \$\$yo:*:16190:0:99999:7:::         \$\$yo:*:16190:0:99999:7:::           upu::         \$\$xi:16190:0:99999:7:::         \$\$yo:*:16190:0:99999:7:::           backwp:*:16190:0:99999:7:::         \$\$yo:*:16190:0:99999:7:::           backwp:*:16190:0:99999:7:::         \$\$yo:*:16190:0:99999:7:::           backwp:*:16190:0:99999:7:::         \$\$yo:*:16190:0:99999:7:::           backwp:*:16190:0:99999:7:::         \$\$yo:*:16190:0:99999:7:::           ist:*:16190:0:99999:7:::         \$\$yo:*::           backup:*:16190:0:99999:7:::         \$\$yo:*::							
Nu         Standon         Sciu         2         Chi         28         9403         Chi         14         Bone how           roti t(555KHL ULON14DPsy00FyF4JU&E1x7H1X0/dRLDYn919mdg67bl0ttbFFtbPv8/j1bqXc31uWHELbiFusj004Yso2VHEELBHg/11         daemoni*1(15190:019999917:::         sj004Yso2VHEELBHg/11           ubin:*161400:019999917:::         sy1:*161400:019999917:::         sy1:*161400:019999917:::         sy1:*16190:019999917:::           games:*161400:019999917:::         mani**1616100:019999917:::         sy1:*161400:019999917:::         sy1:*161400:019999917:::           up:*1161400:019999917:::         mani**1616100:019999917:::         sy1:*161400:019999917:::         sy1:*161400:019999917:::           up:*1161400:019999917:::         backup:*1161900:019999917:::         sy1:*:         sy1:*:         sy1:*:           sy1:*16190:019999917:::         sy1:*:         sy1:*:         sy1:*:         sy1:*:         sy1:*:           syn:*:         sy1:*:         sy1:*:         sy1:*:         sy1:*:         sy1:*:         sy1:*:	<u>F</u> ile	<u>E</u> dit	<u>V</u> iew	<u>T</u> erminal	Tabs	Help	
<pre>root:@stStKHLLUOHSt4DPsyDOFyF47UsE1x7H1X0/dRLDYn9t9mdg67b10ttbfFtbPv8/j1bqXc31uWHELbiFwsj0D4Yso2VHEELBHg/11 deamon:#:116190:0199999:7::: sync:#:16190:0199999:7::: games:#:16190:0199999:7::: games:#:16190:0199999:7::: news:#:16190:0199999:7::: news:#:16190:0199999:7::: news:#:16190:0199999:7::: proxyt::16190:0199999:7::: proxyt::16190:0199999:7::: backup:#:16190:0199999:7::: backup:#:16190:0199999:#:16190:#: backup:#:16190:0199999:#:16190:#: backup:#:16190:#: backup:#:1</pre>		IW	shad	nω			Row 2 Col 28 9:03 Ctrl-K H for help
<pre>daemon**16190:0:99999:77:::     sys:*16190:0:99999:77:::     sys:*16190:0:99999:77:::     games*16160:0:99999:77:::     games*16160:0:99999:77:::     lp:*16190:0:99999:77:::     lp:*16190:0:99999:77:::     ucp:*116190:0:99999:77:::     backup:*16190:0:99999:77:::     backup:*16190:0:99999:77:::     backup:*16190:0:99999:77:::     backup:*16190:0:99999:77:::     lp:*16190:0:99999:77:::     lp:*16190:0:999999:77:::     lp:*16190:0:99999:77:::     lp:*16190:0:99999:77:::     lp:*16190:0:99999:77:::     lp:*16190:0:99999:77:::     lp:*17:*17:*17:*17:*17:*17:*17:*17:*17:*17</pre>	root	:\$6\$	5KMLi	UoN\$4DF	svOOP	vF4JU	UaEix7H1XQ/dRLDYn9t9mdg67b1QttbfFtbPv8/j1bqXc31uWMELbiFwsj0D4YsoZVHBELRHg/:161
bin*:16190:0:99999:7::: sync:*:16190:0:99999:7::: sync:*:16190:0:99999:7::: man*:16190:0:99999:7::: lp:*:16190:0:99999:7::: news:*:16190:0:99999:7::: up:*:16190:0:99999:7::: proxy:*:16190:0:99999:7::: backup:*:16190:0:99999:7::: backup:*:16190:0:99999:7::: backup:*:16190:0:99999:7::: lb::*:16190:0:99999:7::: backup:*:16190:0:99999:7::: lb::*:16190:0:99999:7::: lb::*:16190:0:99999:7::: lb::*:16190:0:99999:7::: lb::*:16190:0:99999:7::: nbbcdy:*:16190:0:99999:7:::	daem	on:*	:1619	0:0:999	999:7:	::	
<pre>sys:*:16190:0:99999:7::: games:*:16190:0:99999:7::: games:*:16190:0:99999:7::: hp:*:16190:0:99999:7::: hp:*:16190:0:99999:7::: news:*:16190:0:99999:7::: upc:*:16190:0:99999:7::: proxy:*:16190:0:99999:7::: backup:*:16190:0:99999:7::: backup:*:16190:0:99999:7::: hs:*:*:16190:0:99999:7::: hs:*:*:16190:0:99999:7::: hs:*:*:16190:0:99999:7::: hs:*:*:16190:0:99999:7::: hs:*:*:16190:0:99999:7::: hs:*:*:16190:0:99999:7::: hs:*:*:16190:0:99999:7::: hs:*:*:16190:0:99999:7::: hs:*:*:16190:0:99999:7::: hs:*:*:16190:0:99999:7:::</pre>	bin:	*:16	190:0	:999999:	:7:::		
<pre>sync:*:16190:0:99999:7::: games:*:16190:0:99999:7::: hp:*:16190:0:99999:7::: mail:*:16190:0:99999:7::: news:*:16190:0:99999:7::: uucp:*:16190:0:99999:7::: uucp:*:16190:0:99999:7::: backup:*:16190:0:99999:7::: backup:*:16190:0:99999:7::: backup:*:16190:0:99999:7::: hs:*::16190:0:99999:7::: hs:*::16190:0:9999:7::: hs:*::16190:0:99999:7::: hs:*::16190:0:9999:7::: hs:*::16190:0:999:9::15: hs:*::16190:0:999:9::15: hs:*::16190:0:999:9::15: hs:*::16190:0:999:9::15: hs:*:16190:0:999:15: hs:*:16190:0:999:15: hs:*:16190:0:999:15: hs:*:16190:0:999:15: hs:*:16190:0:999:15: hs:*:16190:17::1111 hs:*:16190:17::1111 hs:*:16190:17::1111 hs:*:16190:17::11111 hs:*:16190:17::1111 hs:*:16190:17::1111 hs:*:16190:17::1111 hs:*:16190:17::1111 hs:*:16190:17::1111 hs:*:16190:17::1111 hs:*:11111 hs:*:111111 hs:*:11111 hs:*:11111 hs:*:11111 hs:*:111111 hs</pre>	sys:	*:16	190:0	:99999:	7:::		
<pre>games ** 16190 0:99999;7::: hon:*16190 0:99999;7::: lp:*16190 0:99999;7:: mews:*16190 0:99999;7:: uoup:*16190 0:99999;7:: proxy:*16190 0:99999;7:: backup:*16190 0:99999;7:: backup:*16190 0:99999;7:: ls:**16190 0:99999;7:: inc:*16190 0:99999;7:: ls:**16190 0:99999;7:: ls:**16190 0:99999;7:: lb:***16190 0:99999;7:: nobody:*16190 0:99999;7:: lb:udi:**16190 0:99999;7::</pre>	sync	:*:1	5190:	0:99999	9:7:::		
<pre>man:*:16190:0:99999:7::: 1p:*:16190:0:99999:7::: mail:*:16190:0:99999:7::: uucp:*:16190:0:99999:7::: proxy:*:16190:0:99999:7::: backup:*:16190:0:99999:7::: backup:*:16190:0:99999:7::: backup:*:16190:0:99999:7::: 1ic:*:16190:0:99999:7::: ncbady:*:16190:0:99999:7::: lic::*:16190:0:99999:7::: lic::*:16190:0:9999:7::: lic::*:16190:0:99999:7::: lic::*:16190:0:9999:7::: lic::*:16190:0:999:7::: lic::*:170:170:170:170:170:170:170:170:170:170</pre>	game	s:*:	16190	:0:9999	99:7::	:	
<pre>lp:#id:90:0:99999:7::: mews:#id:90:0:99999:7::: mews:#id:90:0:99999:7::: proxy:#id:90:0:99999:7::: proxy:#id:90:0:99999:7::: backup:#id:90:0:99999:7::: backup:#id:90:0:99999:7::: id::#id:90:0:99999:7::: id::#id::#id:90:0:99999:7::: id::#id::#id:90:0:99999:7::: id::#id::#id::#id::#id::#id::#id::#i</pre>	man:	*:16	190:0	:999999:	:7:::		
<pre>mail:*:16190:0:99999:7::: uucp:*:16190:0:99999:7::: uucp:*:16190:0:99999:7::: backup:*:16190:0:99999:7::: backup:*:16190:0:99999:7::: backup:*:16190:0:99999:7::: irc:*:16190:0:99999:7::: irc:*:16190:0:99999:7::: nobady:*:16190:0:99999:7::: nobady:*:16190:0:99999:7::: libuid:::16190:0:99999:7::: </pre>	lp:*	:161	90:0:	99999:7	7:::		
<pre>news:*:16190.0:99999:7::: uucp:*:16190.0:99999:7::: proxy:*:16190.0:99999:7::: backup:*:16190.0:99999:7::: 1st:*:16190.0:99999:7::: 1st:*:16190.0:999997::: nobody:*:16190.0:999997::: nobody:*:16190.0:999997::: 1buudi::16190.0:999997:::</pre>	mail	:*:1	5190:	0:99999	9:7:::		
uucp:*:16190.0:99999:7::: www-data:*:16190.0:99999:7::: www-data:*:16190.0:99999:7::: list:*:16190.0:99999:7::: irc:*:16190.0:99999:7::: mobdy:*:16190.0:99999:7::: nobdy:*:16190.0:99999:7:::	news	:*:1	5190:	0:99999	9:7:::		
<pre>proxy:*16190:0:99999:7::: backup:*16190:0:99999:7::: backup:*16190:0:99999:7::: inc:*16190:0:99999:7::: gnats:*16190:0:99999:7::: nobody:*16190:0:99999:7::: lbouid:*16190:0:99999:7:::</pre>	uucp	:*:1	5190:	0:99999	9:7:::		
<pre>www-data:*:16190:0:99999:7::: backup:*:16190:0:99999:7::: irc:*:16190:0:99999:7::: irc:*:16190:0:99999:7::: nobody:*:16190:0:99999:7::: libuuid::16190:0:99999:7::: libuuid::16190:0:99999:7::: </pre>	prox	y:*:	16190	:0:9999	99:7::	2	
backup:*:16190:0:99999:7::: list:*:16190:0:99999:7::: gmats:*:16130:0:99999:7::: nobody:*:16190:0:99999:7::: libuuid::16190:0:99999:7:::	ωωω-	data	:*:16	190:0:9	99999:	7:::	
<pre>list:*:iti0:00:99999:7::: gnats:*:16190:0199999:7::: nobody:*:16190:0199999:7::: libuid::1:16190:0199999:7::: libuid::1:16190:0199999:7::: </pre>	back	up:*	:1619	0:0:999	999:7:		
<pre>1rc:#ib19010:99999:f::: nobody:#i16190:0:99999:f::: 1bouid::16190:0:99999:f::: 1bouid::16190:0:99999:f::: </pre>	list	:*:1	5190:	0:99999	9:7:::		
gnats:*1101000199999977777 nobody:*1619000199999977777 libuuid:1161900019999977777	irc:	*:16	190:0	:999999:			
libuuid:!:16190:0:999999:7:::	gnat	s:*:	16190	:0:9999	99:7::	÷	
1100010:::16190:0:99999:7:::	nobo	ay:*	1619	0101999	999:7:		
Debies	11bu	u10:	::161	90:0:99	19999:1		
	Deb1	an-e	16400	:10190:	0.999		
Blatter (10120-00-2020) (11:1)	stat	u.*:	1019U	4P 0P04	10749-	Artual	IPucPEISENa4EuropoiafonM000k7bNuTVP2 709 IKu&Puu0pouE4467kC+6 u0tilo2Po1465(u)
2+	ftn:	* 16	10011	-000000	7	WO UCI	orversionworkersholdigtphotockshnvirr2.5555KyAPwwqpSwE4AC5KCt6.V6t11pzRE14SE/yN.:

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



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 normalo 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: <u>Operacijski sustavi</u> [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