Linux para Ingeniería:

Recuperación del Sistema: Resset a Password

Luis Garreta

luis.garreta@javerianacali.edu.co

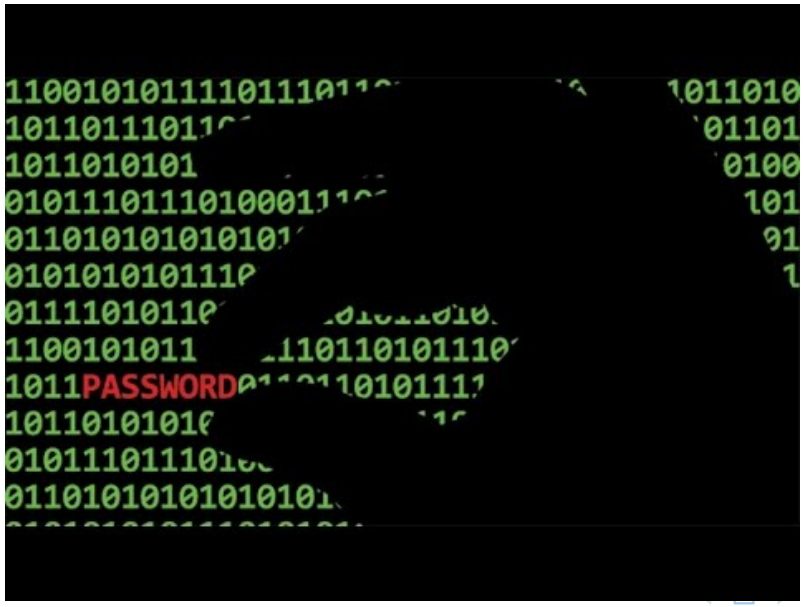
Ingeniería de Sistemas y Computación
Pontificia Universidad Javeriana – Cali

6 de abril de 2018

Why resseting passwords?

There are many reasons you might want to reset a password:

- Someone cracked your system and change the root password
- Someone gave you a computer with Ubuntu installed on it but not the password for the user account.
- You just installed Ubuntu and forgot what password you selected during the installation process.
- You have too many passwords in your life and can't keep track of them all.



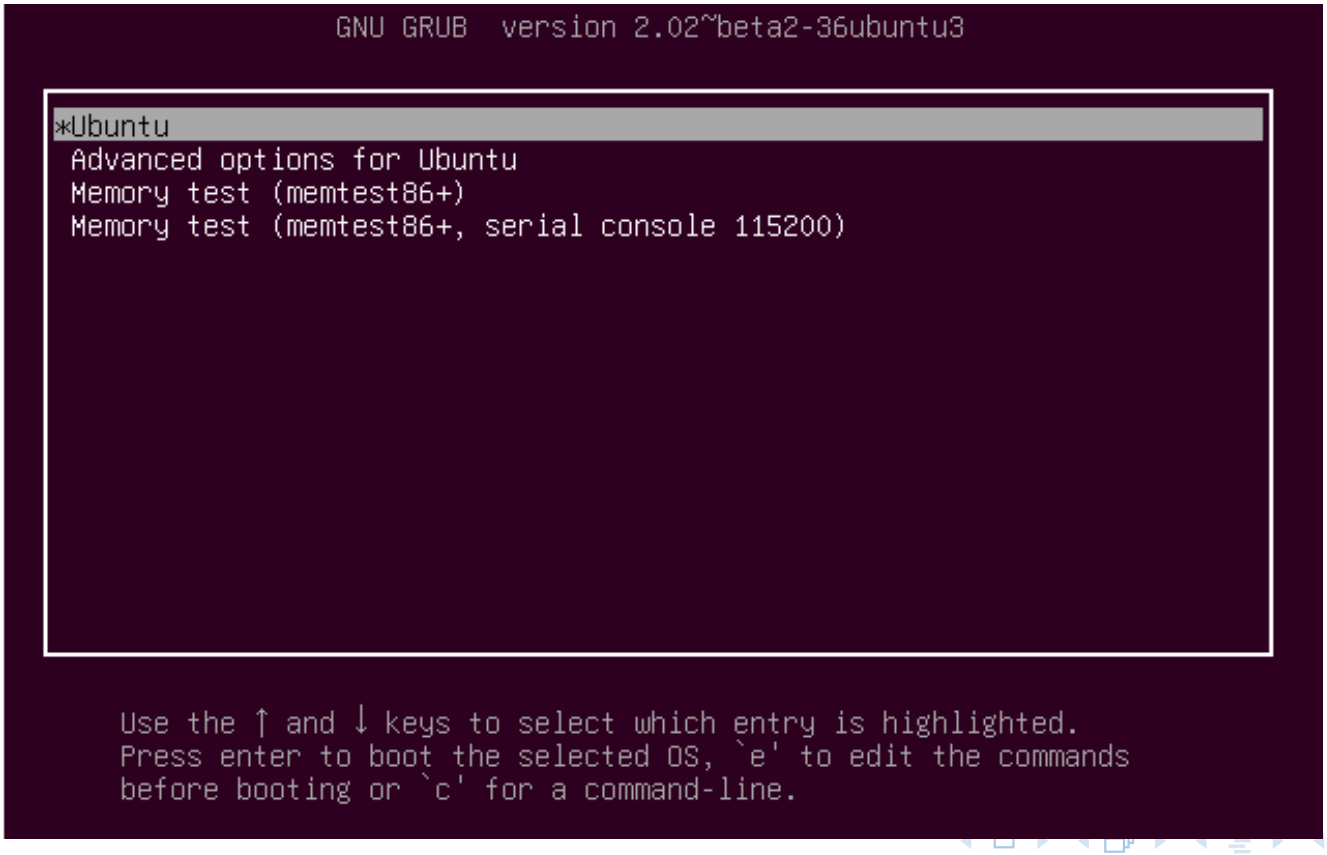
Methods

- Modify Grub Menu
- Using a System Rescue CD/USB

- Modify the Grub Menu

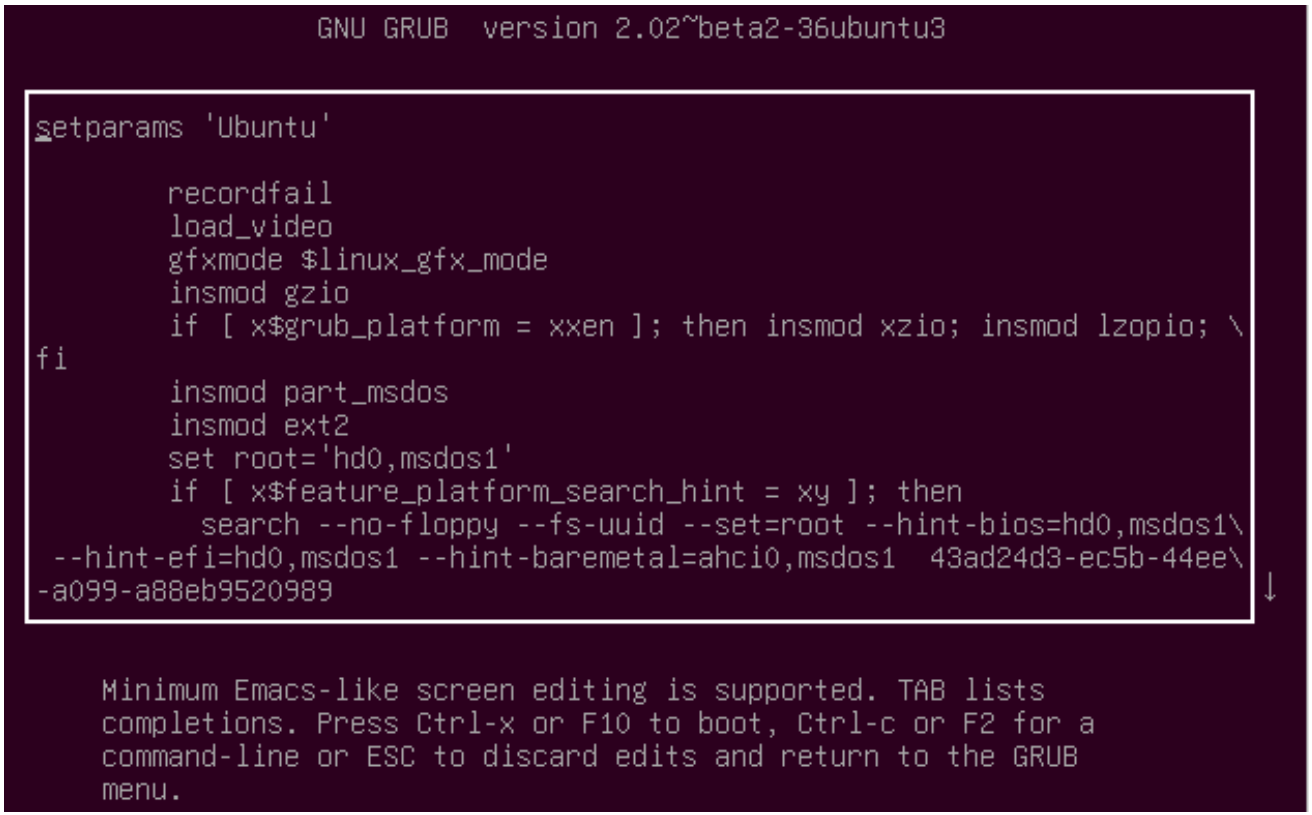
Reboot to Grub Menu

- In the first step you need to reboot your Ubuntu 16.04 Linux box to Grub's menu.
- If the Ubuntu 16.04 is the only installation available keep pressing SHIFT after you start your computer until GRUB's menu appears:



Edit Grub Menu

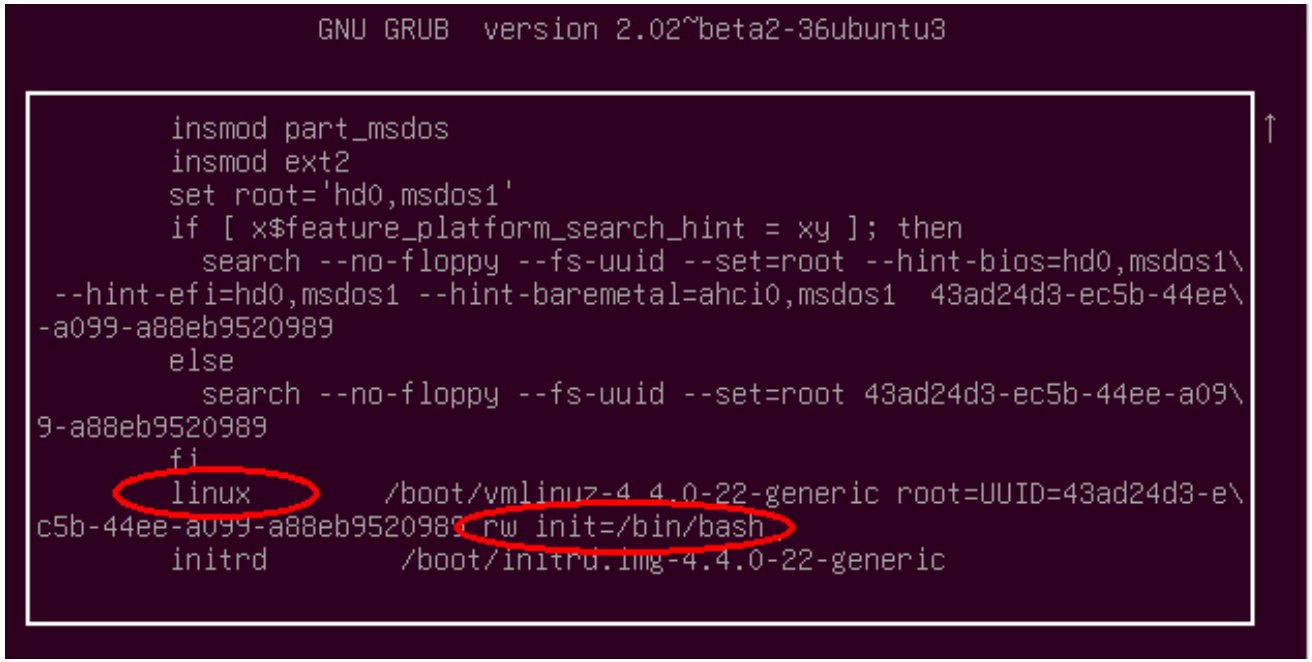
- Once you reboot to Grub menu, select the first menu item or the menu item you normally use to boot your Ubuntu system and **press e** to edit:



Alter boot menu

Once in the Grub's boot menu edit mode use navigation arrows to locate a line starting with **linux** and edit it to include:

read-write mode rw and init=/bin/bash



- For example:

```
linux     /boot/vmlinuz-4-4.0-22-generic root=UUID=43ad24d3-e\
c5b-44ee-a099-a88eb9520989 ro  quiet splash $vt_handoff
```

- CHANGE TO:

```
linux     /boot/vmlinuz-4-4.0-22-generic root=UUID=43ad24d3-e\
c5b-44ee-a099-a88eb9520989 rw init=/bin/bash
```

- Once ready press CTRL+x or F10 to boot.

Resetting root's password

- If all went well you should now see root shell command line and your root partition should be mounted with read/write flags. To confirm run:

```
root@(none):/# mount | grep -w /
/dev/sda1 on / type ext4 (rw,relatime,data=ordered)
root@(none):/# _
```

- Now we are ready to reset root's password. To do so, simply run passwd command with no arguments. When prompted enter your new root password:

```
root@(none):/# mount | grep -w /
/dev/sda1 on / type ext4 (rw,relatime,data=ordered)
root@(none):/# passwd
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
root@(none):/# _
```

- All done. Your root's password is now reset.

Troubleshooting

```
Enter new UNIX password:
Retype new UNIX password:
passwd: Authentication token manipulation error
passwd: password unchanged
```

Your root partition is mounted read-only. Try:

```
# mount -o remount,rw /
```

to resolve this issue.

```
[ end Kernel panic - not syncing: Attempted to kill init! exit code=0x0007f00
```

Make sure that you removed splash boot option when editing grub's menu item.

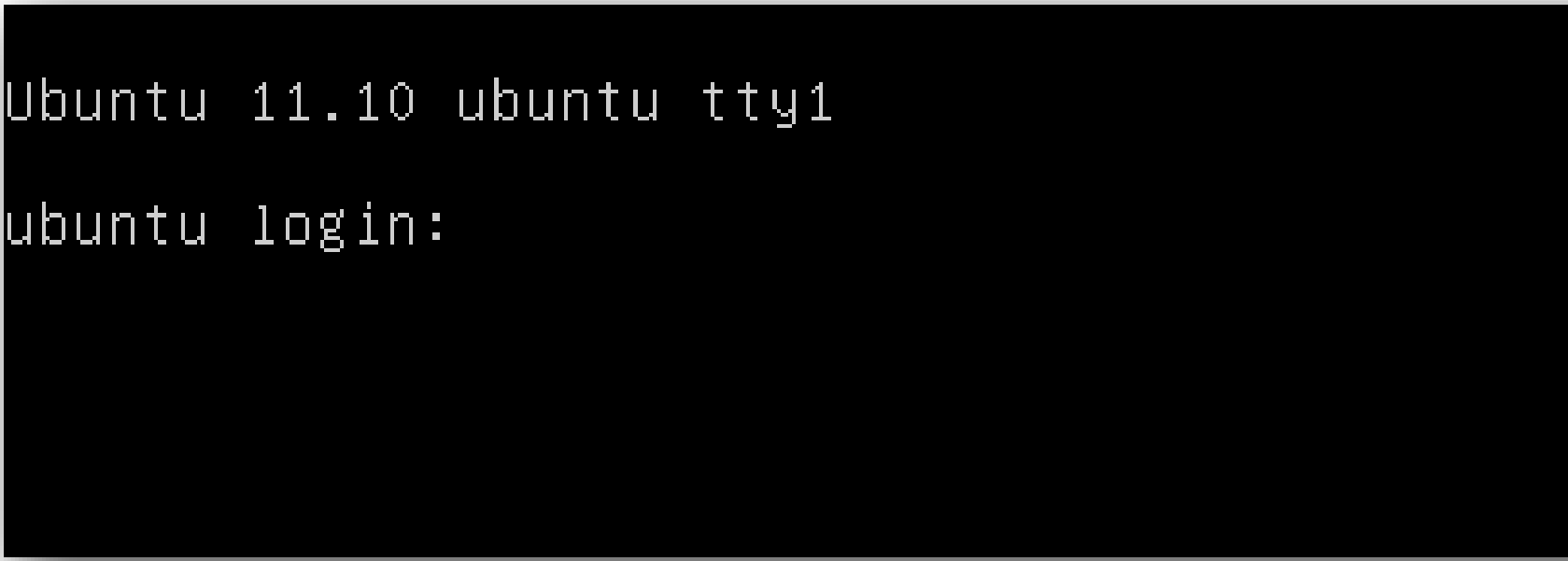
Reset a lost password using SytemRescueCD or FLash USB

Step 1: Boot the Ubuntu from the Rescue CD/USB

- Reboot your system and press the key to select the boot options
  - The key depends of the type of machine (ESC for dell, F10 for HP, ...)

Step 2: Open Terminal Window

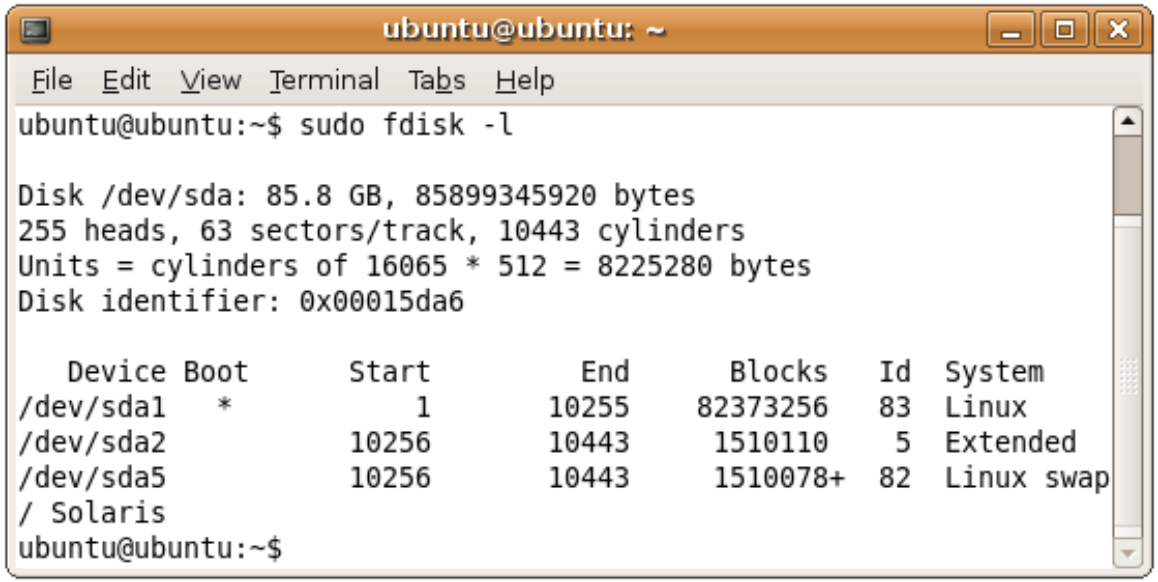
- Press Ctrl-Alt-F1 or open a graphical terminal
- Log-in with your normal user



Step3: Find the device of the root filesystem (/)

- Type in the following command to see the current filesysten:

```
$ sudo fdisk -l
```



Step 4: Mount the root filesystem

- Normally the first filesystem, /dev/sda1
- But, if not, you have to mount the others filesystems until you find it.

```
$ cd /mnt
$ mkdir ubuntu
$ mount -t ext4 /dev/sda1 ubuntu
```

- If you have a separate boot partition mount that too.

```
$ mount -t ext2 /dev/sda1 /mnt/ubuntu/boot
```

Step 5: Mount dev, proc, and sys subsystems

- Now in order to have a functional chroot, we need the **proc, dev and sys** subsystems to be mounted onto the chroot.
- This is the tricky bit.

```
$ mount -t proc none /mnt/ubuntu/proc
$ mount -o bind /dev /mnt/ubuntu/dev
$ mount -o bind /sys /mnt/ubuntu/sys
```

- In the case of the **sys** and **dev** dirs, we need to reference the exact same mountpoints as the host so we use the -o bind option.

Step 6: Optional name resolution

- Last thing, we want to have functional network name resolution so we copy over the host's /etc/resolv.conf to
- Copy over the host's /etc/resolv.conf to /mnt/ubuntu/etc/resolv.conf

Step 7: Chroot your system

- A chroot on Unix operating systems is an operation that changes the apparent root directory for the current running process and its children.
- A program that is run in such a modified environment cannot name (and therefore normally cannot access) files outside the designated directory tree.

```
$ chroot /mnt/ubuntu /bin/bash
```

Step 8: Recover passwords

- The options are:
  - Create a new user with and add it to the sudo

```
$ passw
```

  - Change the passwoird of an existing user and add it to the sudo

```
passwd user
```

  - Change the root password (Be cautious)

Exit from chroot and unmount the root partition

- You can exit from the chroot shell in the same way as any other shell, for example using the exit command:

```
exit
```

  or by pressing control-D.

- Unmount the root partition

```
umount /mnt/ubuntu
```

- Reboot the system

```
Reboot
```

Sources

- https://linuxconfig.org/how-to-reset-lost-root-password-on-ubuntu-16-04-xenial-xerus-linux
- http://www.microhowto.info/howto/reset_a_forgotten_root_password_using_a_live