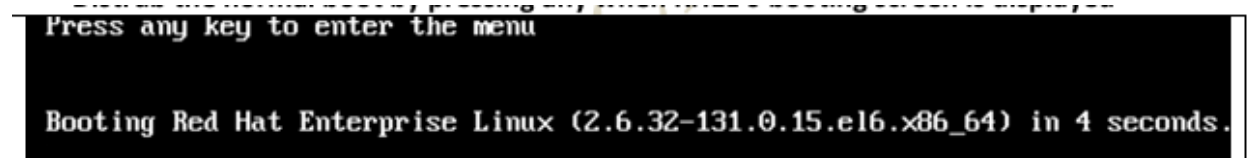


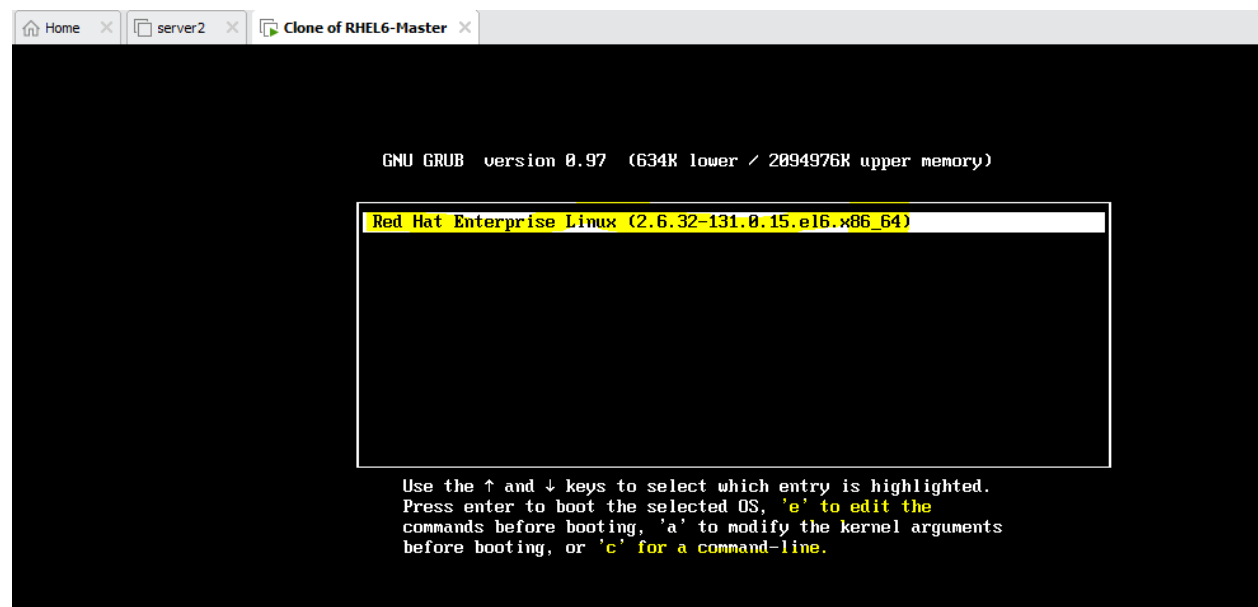
## Recovering the lost password in RHEL 6

To recover the password the steps are

Disturb the normal boot by pressing any when RHEL 6 booting screen is displayed



You will be inside the menu like the following



```
GNU GRUB version 0.97 (634K lower / 2894976K upper memory)

root (hd0,0)
kernel /vmlinuz-2.6.32-131.0.15.el6.x86_64 ro root=/dev/mapper/ug_mas
initrd /initramfs-2.6.32-131.0.15.el6.x86_64.img

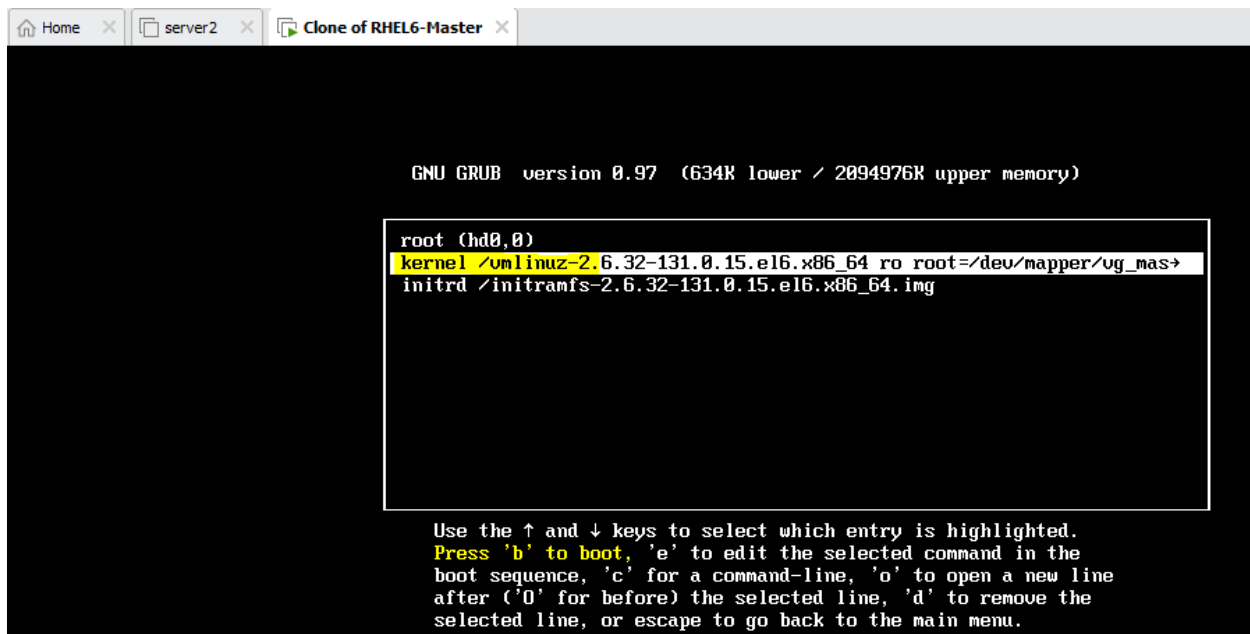
Use the ↑ and ↓ keys to select which entry is highlighted.
Press 'b' to boot, 'e' to edit the selected command in the
boot sequence, 'c' for a command-line, 'o' to open a new line
after ('O' for before) the selected line, 'd' to remove the
selected line, or escape to go back to the main menu.
```

Move the cursor to 2nd line (line of Kernel) and press 'e' to edit the kernel parameter

```
[ Minimal BASH-like line editing is supported. For the first word, TAB
lists possible command completions. Anywhere else TAB lists the possible
completions of a device/filename. ESC at any time cancels. ENTER
at any time accepts your changes.]

<shkernel=auto rhgb quiet 1
```

Type "1" after the line to boot in maintenance level and press enter to continue

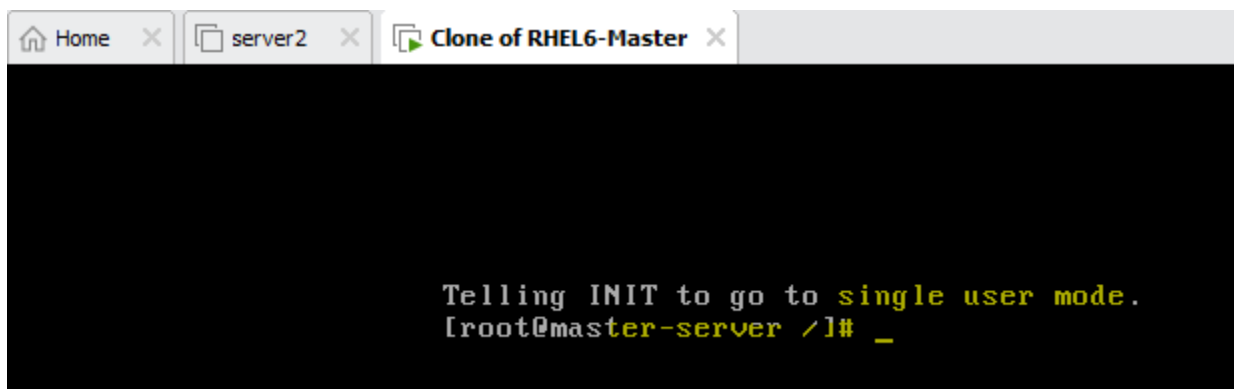


```
GNU GRUB version 0.97 (634K lower / 2094976K upper memory)

root (hd0,0)
kernel /vmlinuz-2.6.32-131.0.15.el6.x86_64 ro root=/dev/mapper/ug_mas
initrd /initramfs-2.6.32-131.0.15.el6.x86_64.img

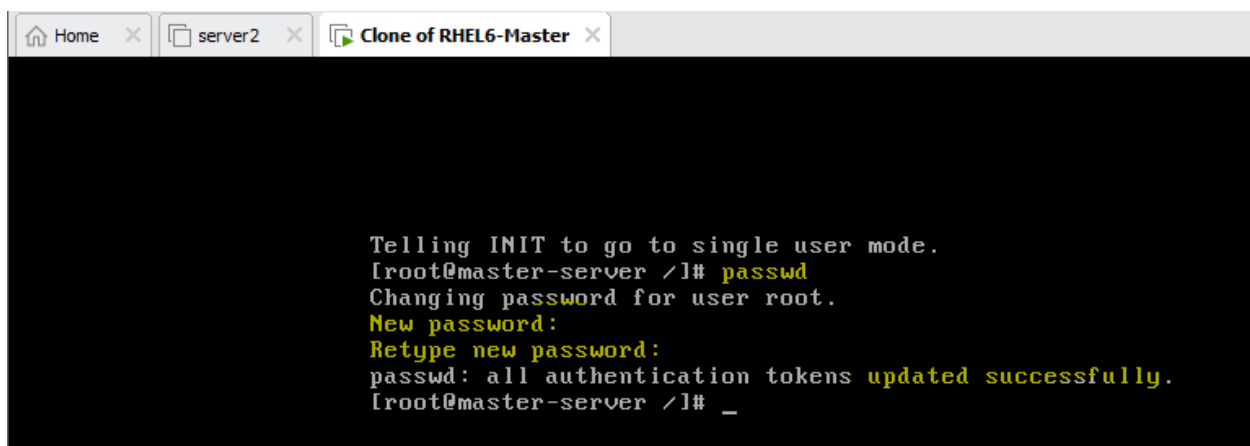
Use the ↑ and ↓ keys to select which entry is highlighted.
Press 'b' to boot, 'e' to edit the selected command in the
boot sequence, 'c' for a command-line, 'o' to open a new line
after ('O' for before) the selected line, 'd' to remove the
selected line, or escape to go back to the main menu.
```

Now, type “b” to boot it in single user mode. Then you will be in single user mode



```
Telling INIT to go to single user mode.
[root@master-server /]# _
```

Now without being prompted for password you will be logged in the single user mode

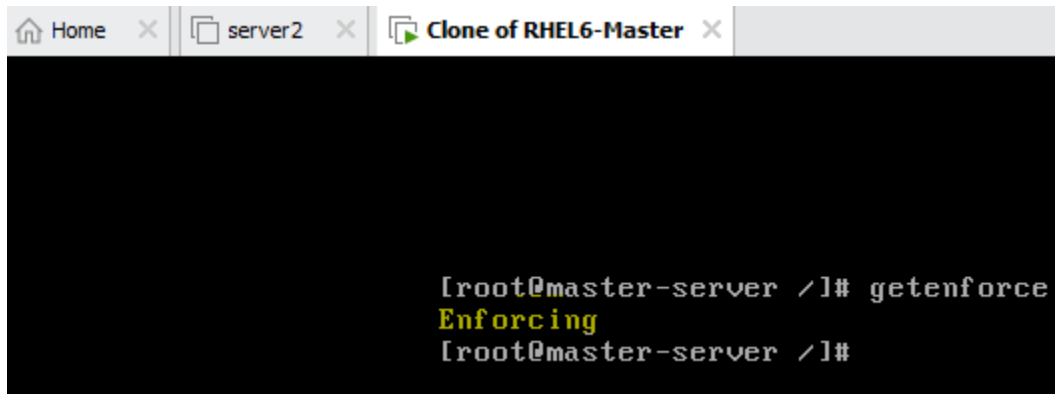


```
Telling INIT to go to single user mode.
[root@master-server /]# passwd
Changing password for user root.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
[root@master-server /]# _
```

Note: if you are facing error while changing the password. Follow the below process.

To change the password use command #passwd, but as you can see it will not work because of SELinux.

Check the SELinux mode by using #getenforce command

A terminal window titled 'Clone of RHEL6-Master' showing the command 'getenforce' being executed. The output is 'Enforcing'.

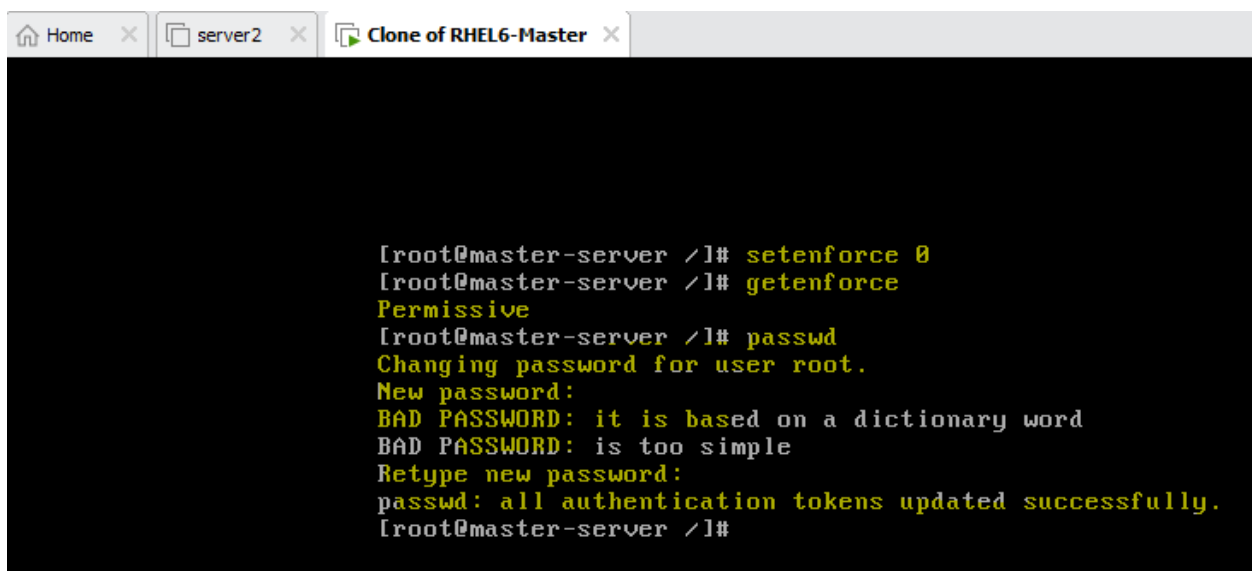
```
[root@master-server /]# getenforce
Enforcing
[root@master-server /]#
```

As we can see that SELinux is in Enforcing mode, change it to Permissive and then try changing the password

Change the SELinux Mode to Permissive, using

#setenforce 0

Now try changing the password using #passwd command

A terminal window titled 'Clone of RHEL6-Master' showing a sequence of commands: 'setenforce 0', 'getenforce' (output: 'Permissive'), and 'passwd'. The 'passwd' command prompts for a new password, which is rejected as being based on a dictionary word and too simple. It then prompts to retype the password, which is accepted, and finally shows 'all authentication tokens updated successfully'.

```
[root@master-server /]# setenforce 0
[root@master-server /]# getenforce
Permissive
[root@master-server /]# passwd
Changing password for user root.
New password:
BAD PASSWORD: it is based on a dictionary word
BAD PASSWORD: is too simple
Retype new password:
passwd: all authentication tokens updated successfully.
[root@master-server /]#
```

Okay, Now we are successfully changed the password, now just type exit or reboot, to reboot the system and try the new password for root.

