Fastest Way to Gain Root Access in RHCSA7 Exam

Finnbarr P. Murphy

(fpm@fpmurphy.com)

Time is at a premium during the RHCSA exam. Every minute you can save on a task is a minute as it can be applied to some other task. If you have to reboot the operating system, that is wasting time as you cannot be doing anything useful in terms of task completion during the reboot.

One critical task is to require you to gain root access to the installed and running operating system. This is typically the first thing you need to do in the exam. There are many blogs and write-ups on how to do this by modifying the Linux kernel command line in GRUB including Certdepot and the RHEL7 System Administration Guide.

Typically they all require you to disable SELinux and break out of the early boot process via the following arguments on the kernel command line:

```
rd.break enforcing=0
```

and then relabel the entire operating system during a reboot via

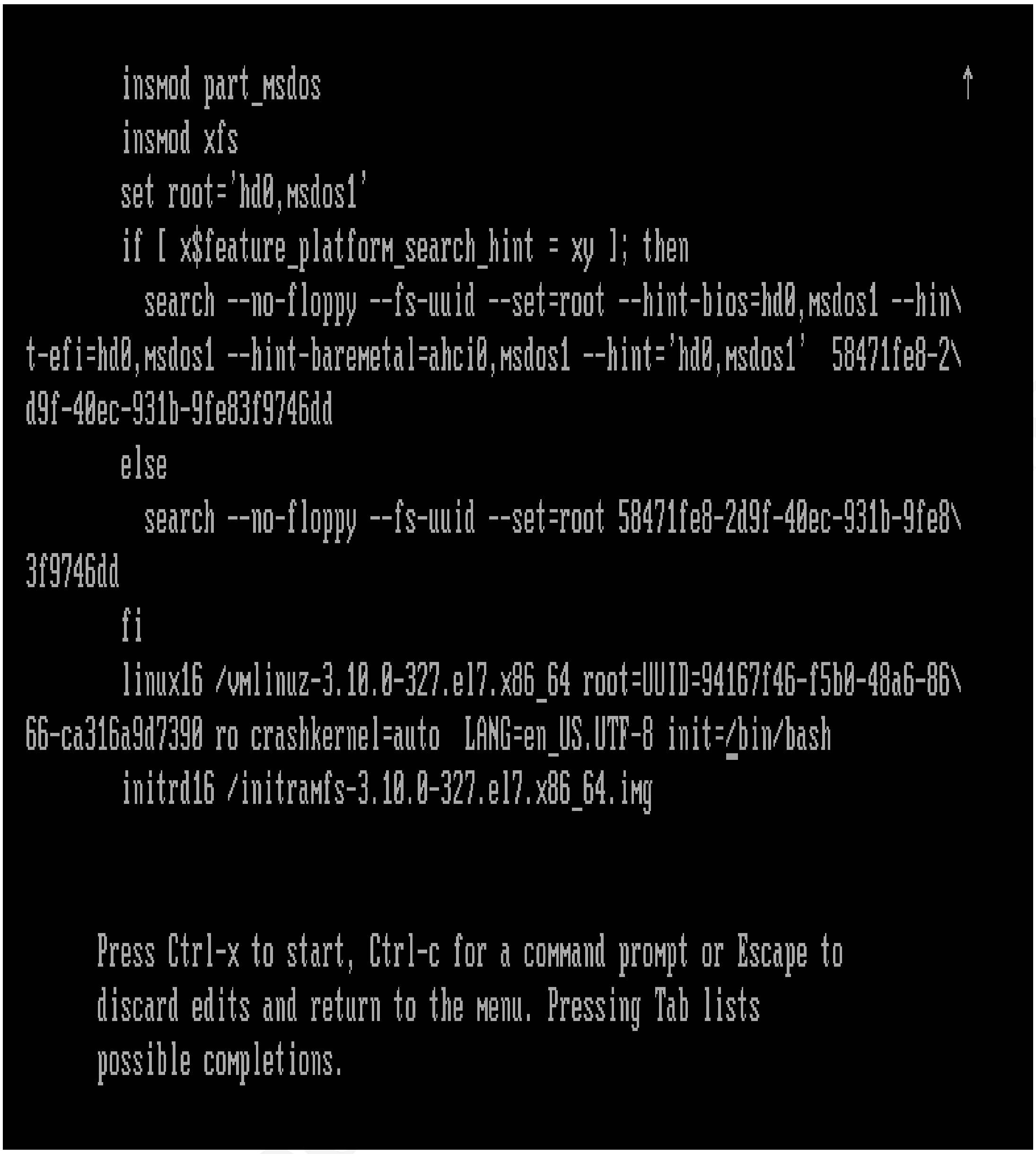
```
# touch /.autorelabel
```

This is wasteful because of the time lost by rebooting and there is the slight possibility that the relabeling may take several minutes or longer to complete.

By the way, *rd.break* is not a GRUB command; it is a Dracut argument which tells Dracut to drop into a shell. The version of GRUB is also different than in previous versions of RHEL. It is what was formerly know as GRUB2. It is a seriously over-engineered and complex multiboot loader which uses a completely different command syntax than GRUB Legacy.

The method I demonstrate here does not require a second reboot and relabels only */etc/shadow* since this is the only file whose security content is incorrect after you change the password for *root*. The net result of using this method is several minutes of time saved during the RHCSA exam.

First get to the GRUB command line by rebooting the operating system and add *init=/bin/bash* to the end of the GRUB command which starts with *linux16* in the case of non-UEFI firmware or *linuxefi* in the case of UEFI-enabled firmware. By the way, *linux16* means load the binary in 16-bit mode. UEFI does not have a 16–bit mode; hence the different GRUB commands. Do not bother removing the existing *rhgb* or *quiet* arguments unless you run into a problem while booting.

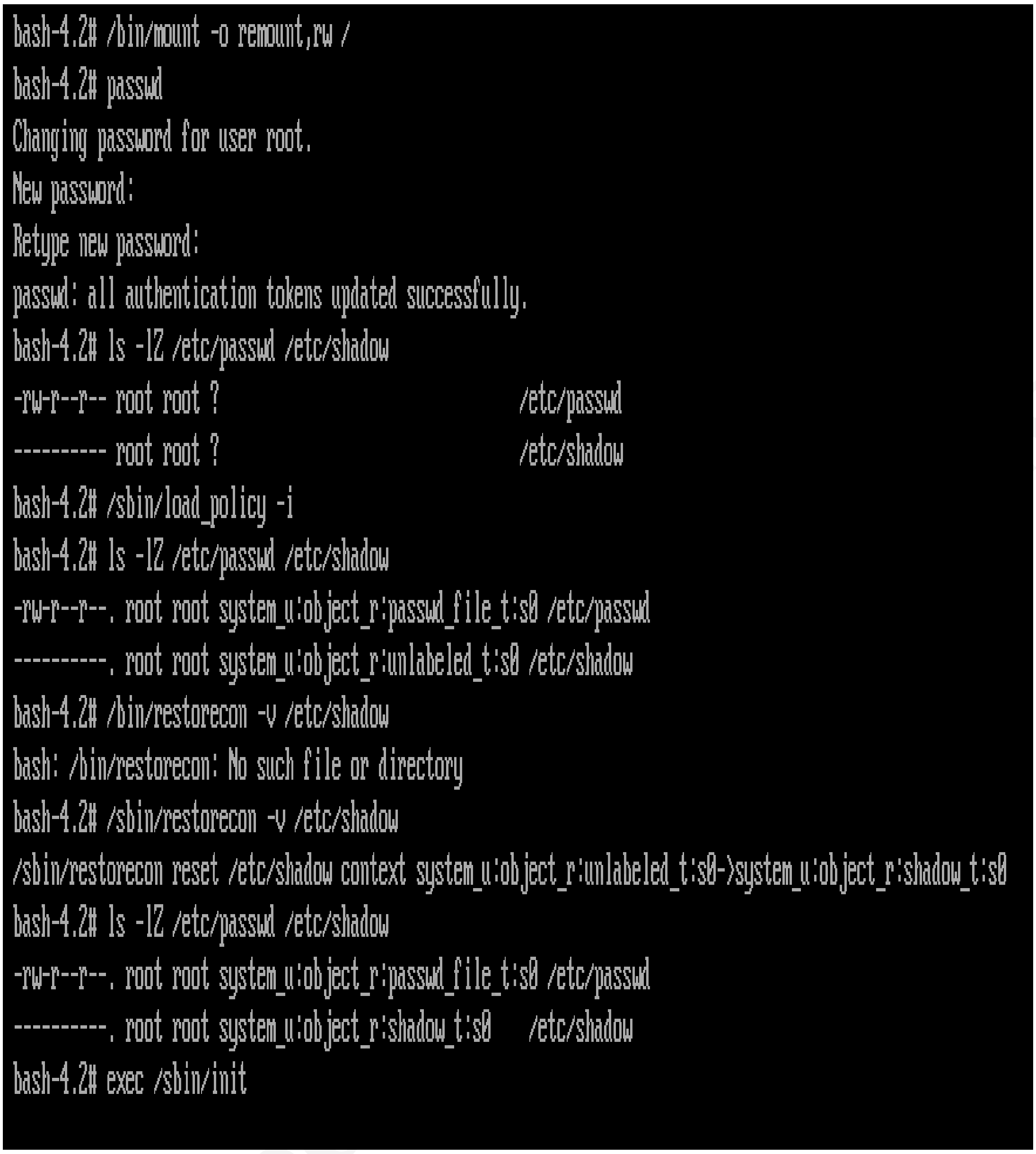


```
        insmod part_msdos                                                    ↑
        insmod xfs
        set root='hd0,msdos1'
        if [ x$feature_platform_search_hint = xy ]; then
          search --no-floppy --fs-uuid --set=root --hint-bios=hd0,msdos1 --hin\
t-efi=hd0,msdos1 --hint-baremetal=ahci0,msdos1 --hint='hd0,msdos1'  58471fe8-2\
d9f-40ec-931b-9fe83f9746dd
        else
          search --no-floppy --fs-uuid --set=root 58471fe8-2d9f-40ec-931b-9fe8\
3f9746dd
        fi
        linux16 /vmlinuz-3.10.0-327.el7.x86_64 root=UUID=94167f46-f5b0-48a6-86\
66-ca316a9d7390 ro crashkernel=auto  LANG=en_US.UTF-8 init=/bin/bash
        initrd16 /initramfs-3.10.0-327.el7.x86_64.img



      Press Ctrl-x to start, Ctrl-c for a command prompt or Escape to
      discard edits and return to the menu. Pressing Tab lists
      possible completions.
```

Then, as usual, press Ctrl-X to resume GRUB and the boot process. You will end up as *root* in a *bash* shell where you can change the root password, load the SELinux policy, relabel */etc/shadow* and load the full operating system without rebooting a second time.



```
bash-4.2# /bin/mount -o remount,rw /
bash-4.2# passwd
Changing password for user root.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
bash-4.2# ls -lZ /etc/passwd /etc/shadow
-rw-r--r-- root root ?                              /etc/passwd
---------- root root ?                              /etc/shadow
bash-4.2# /sbin/load_policy -i
bash-4.2# ls -lZ /etc/passwd /etc/shadow
-rw-r--r--. root root system_u:object_r:passwd_file_t:s0 /etc/passwd
----------. root root system_u:object_r:unlabeled_t:s0 /etc/shadow
bash-4.2# /bin/restorecon -v /etc/shadow
bash: /bin/restorecon: No such file or directory
bash-4.2# /sbin/restorecon -v /etc/shadow
/sbin/restorecon reset /etc/shadow context system_u:object_r:unlabeled_t:s0->system_u:object_r:shadow_t:s0
bash-4.2# ls -lZ /etc/passwd /etc/shadow
-rw-r--r--. root root system_u:object_r:passwd_file_t:s0 /etc/passwd
----------. root root system_u:object_r:shadow_t:s0    /etc/shadow
bash-4.2# exec /sbin/init
```

The command */sbin/load_policy -i* loads the current security policy into the kernel. The command */sbin/restorecon* restores the correct security context (*shadow_t*) to */etc/shadow*. As shown above, you can use *ls -lZ* to display a file’s SELinux contexts, etc.

This is a critical RHCSA7 exam task. If you cannot take control of the RHEL7 operating system through a reboot at the beginning of the exam and change the root password, you will fail the entire exam. You need to repeatedly practice this task until you can do it reliably in about 3 minutes or less.