PART 1: Practicing basic Linux commands

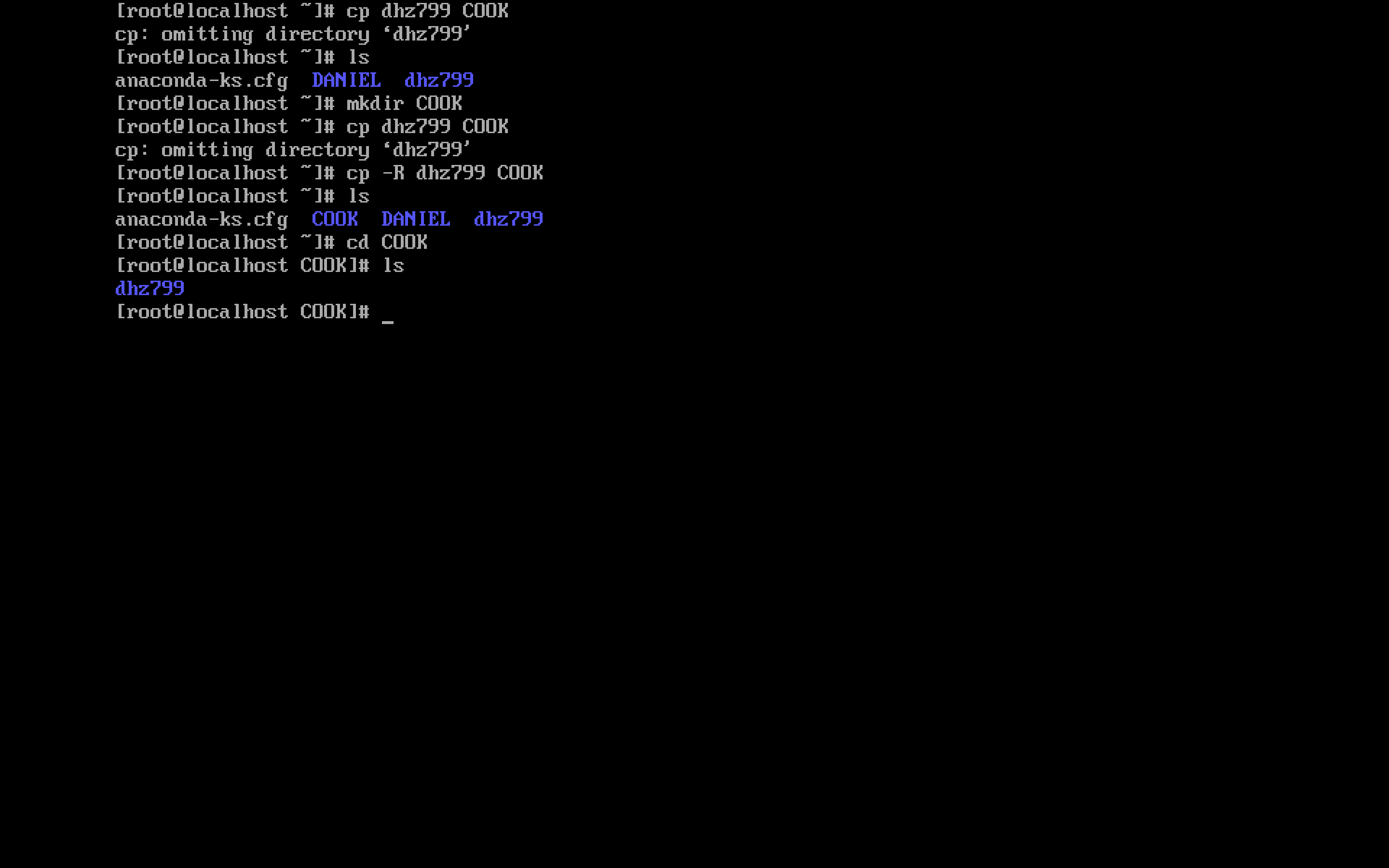
Created a folder named “DANIEL dhz799” under the root user’s home directory.



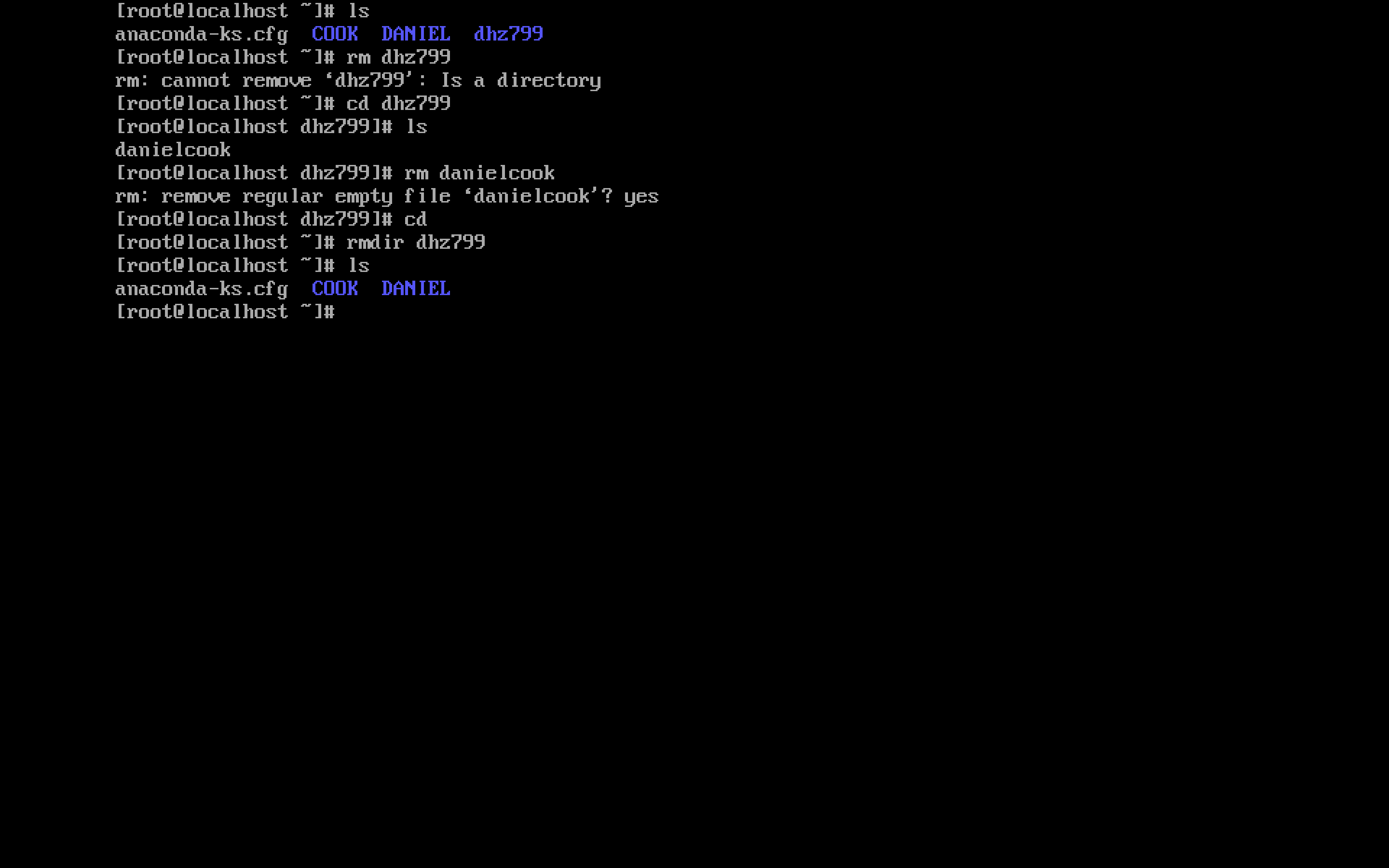
Created a file named “danielcook” in the “dhz799” folder.



Copied the “dhz799” folder with the contents of “danielcook” file into a folder called “COOK” into a subfolder.



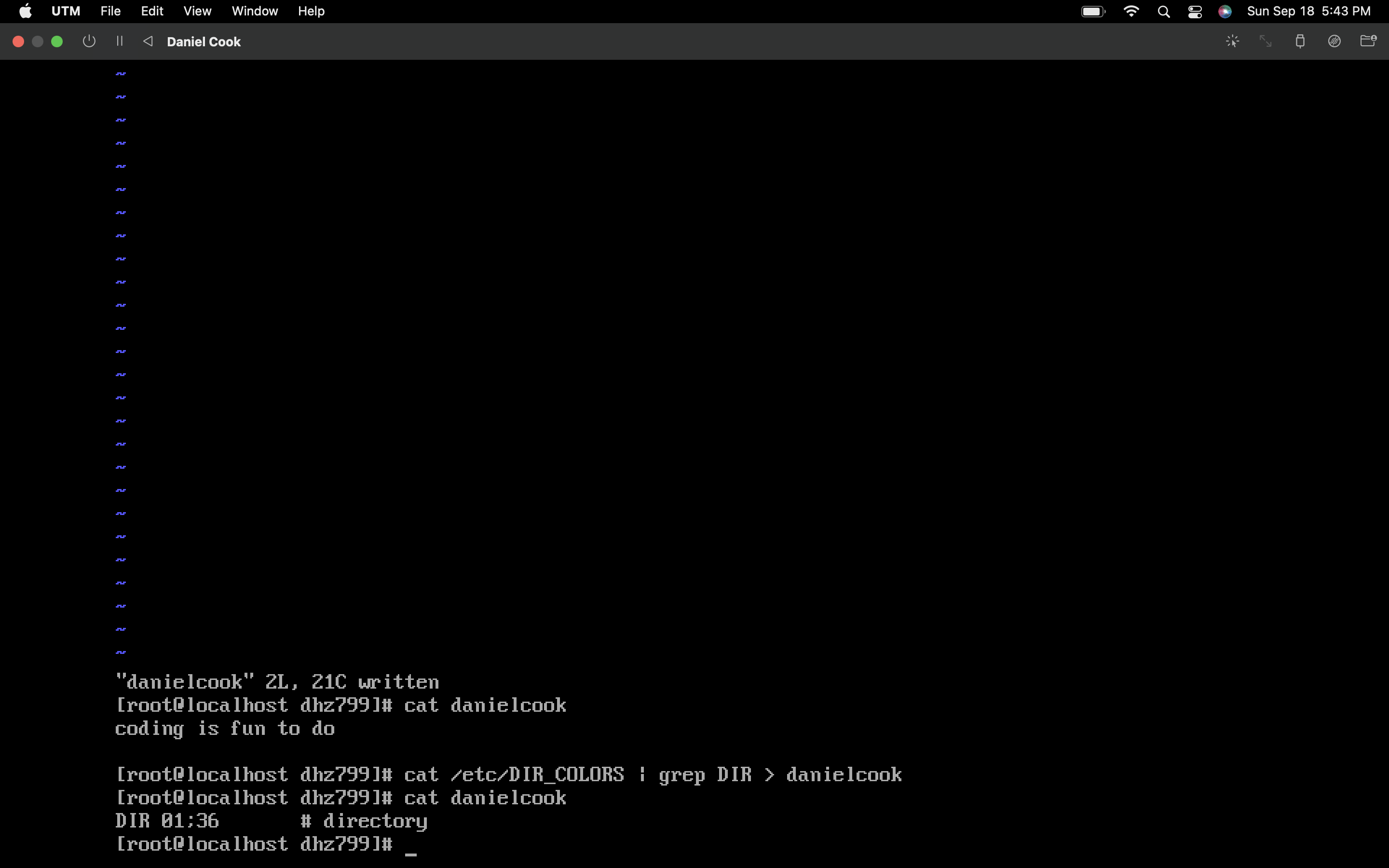
Removed the “dhz799” folder and all contents with single-line command.



Added a single-line text to file using text editor (vi). I commented “coding is fun to do.”

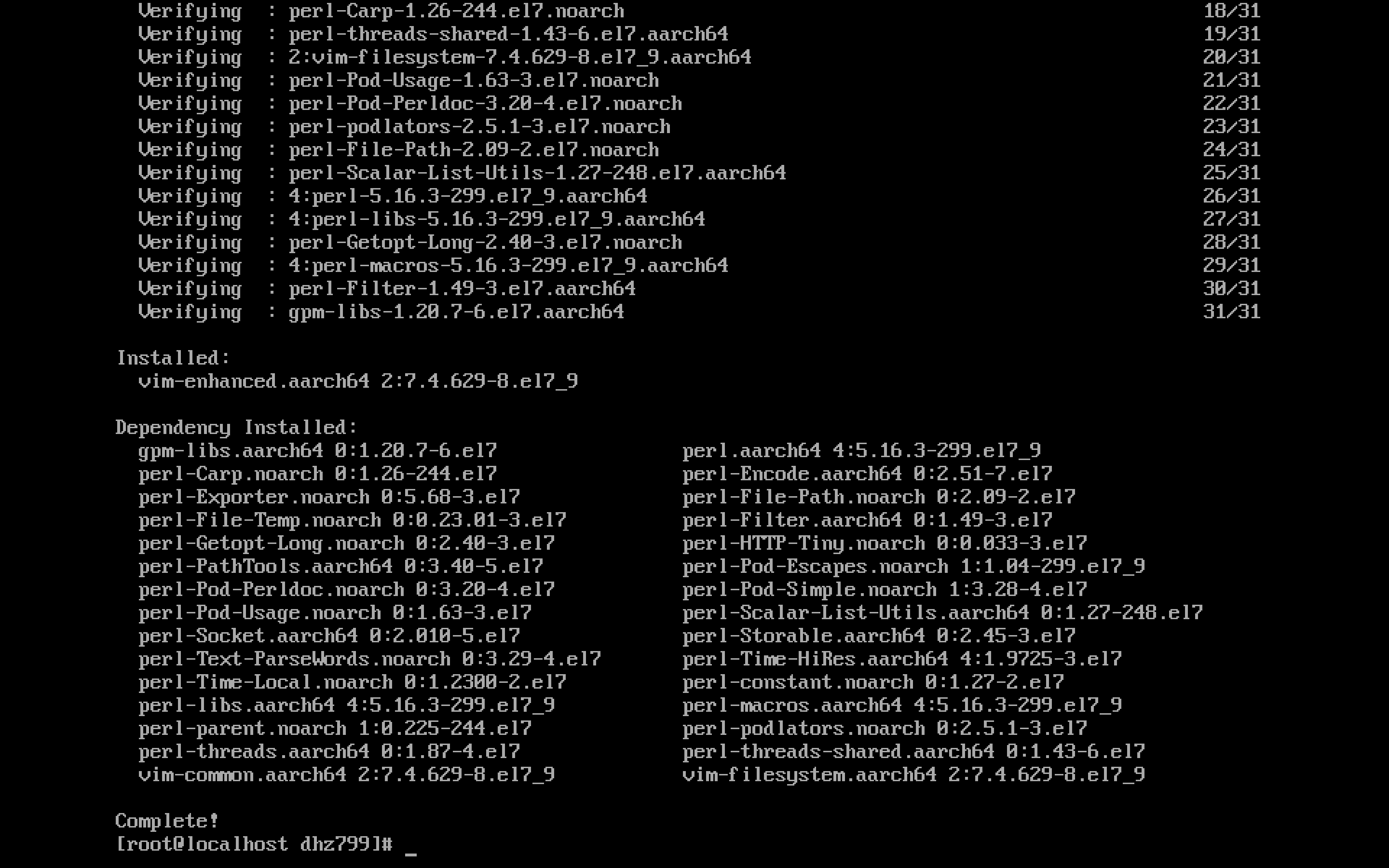


Pip the search line of /etc/DIR\_COLORS of the contents of “DIR 01;34” onto the file. Using the command # cat /etc/DIR\_COLORS | grep DIR > danielcook

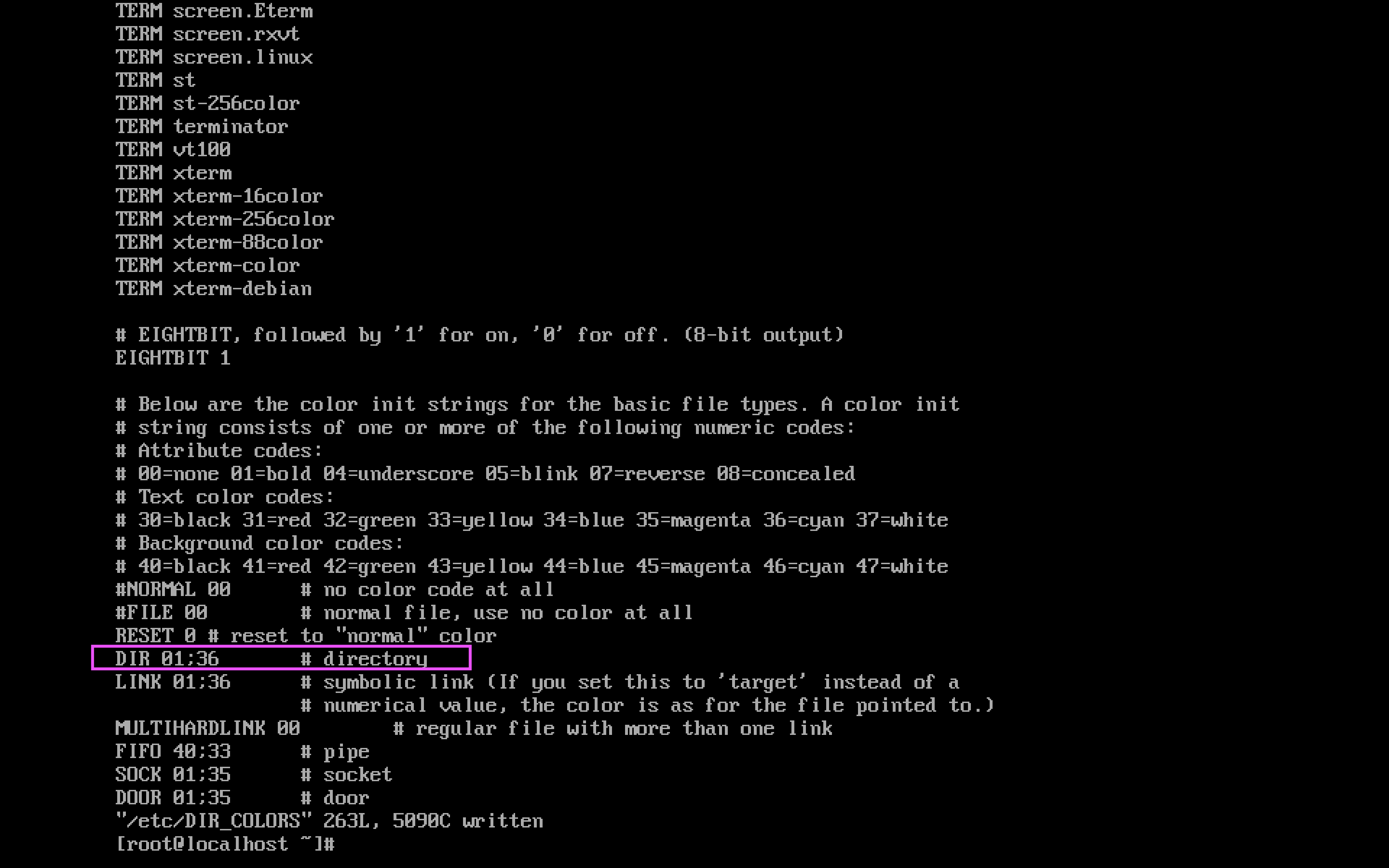


Installed Vim by using package manager with the command

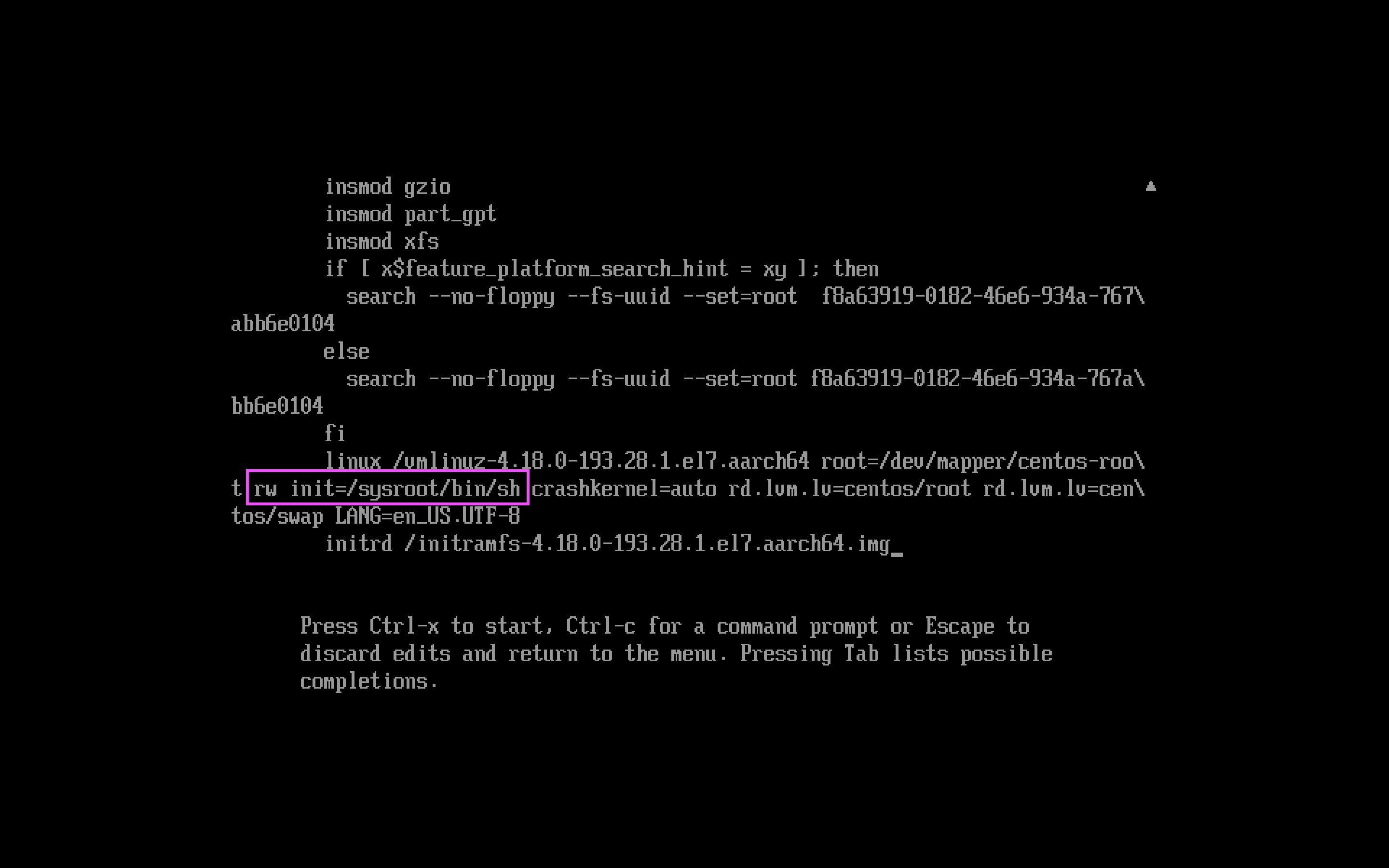
# yum install –y vim



Opened the file /etc/DIR\_COLORS using text editor. Modifying “DIR 01;34” to “DIR 01;36” changing the colors of the directories to cyan



PART 2: “Hacking” the root account

Changing the “ro” to “rw init=/sysroot/bin/sh”

Test Login

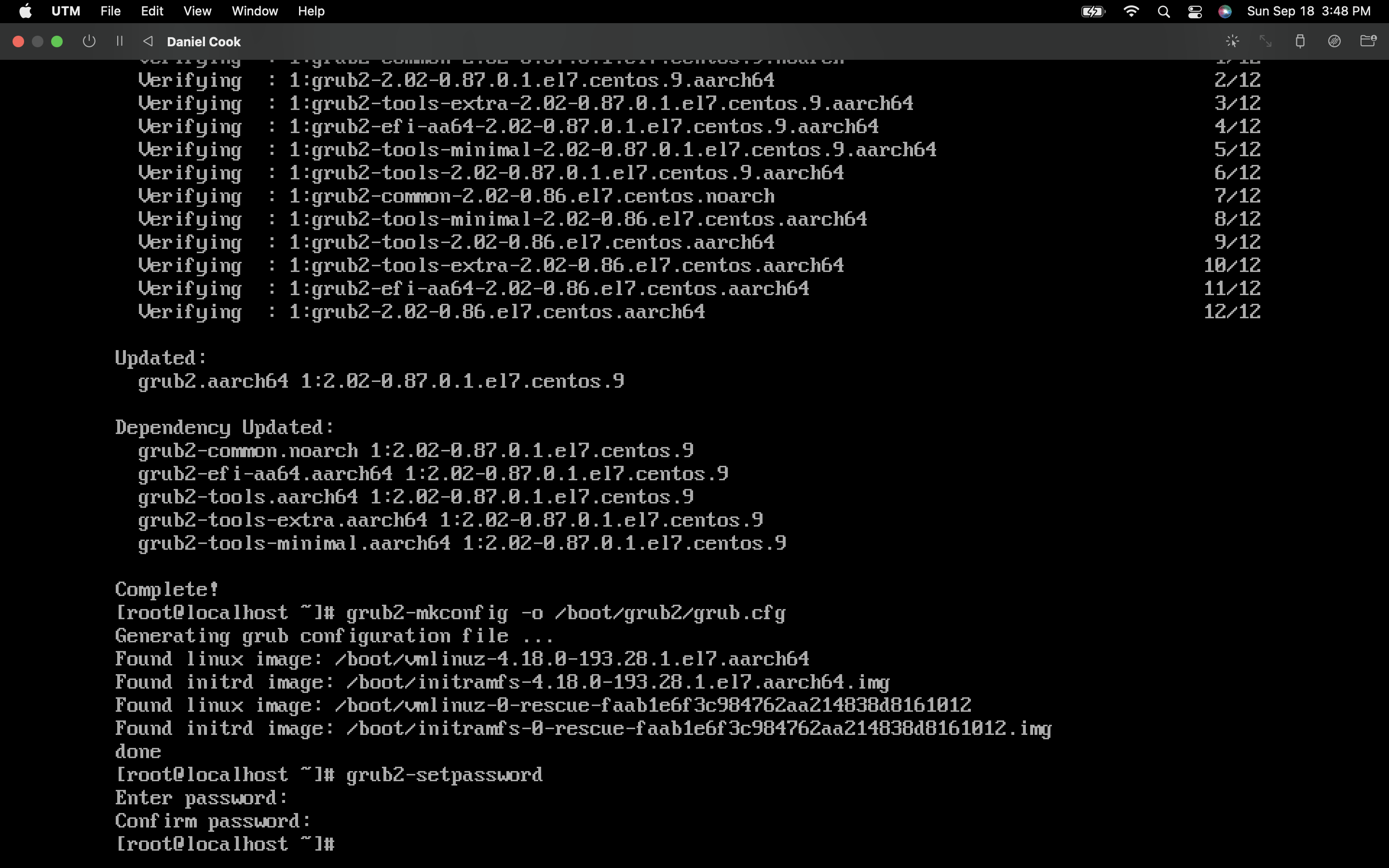
Question: briefly explain why having the access of bootloader could be utilized for changing/bypassing the root password protection of your Operating System (think of the booting process).

Bootloader is viable to prevent unauthorized users from accessing the media or using root privileges. It can authorize users to utilize the protection of the operating system. Preventing access to single-user mode and preventing access to GRUB console.

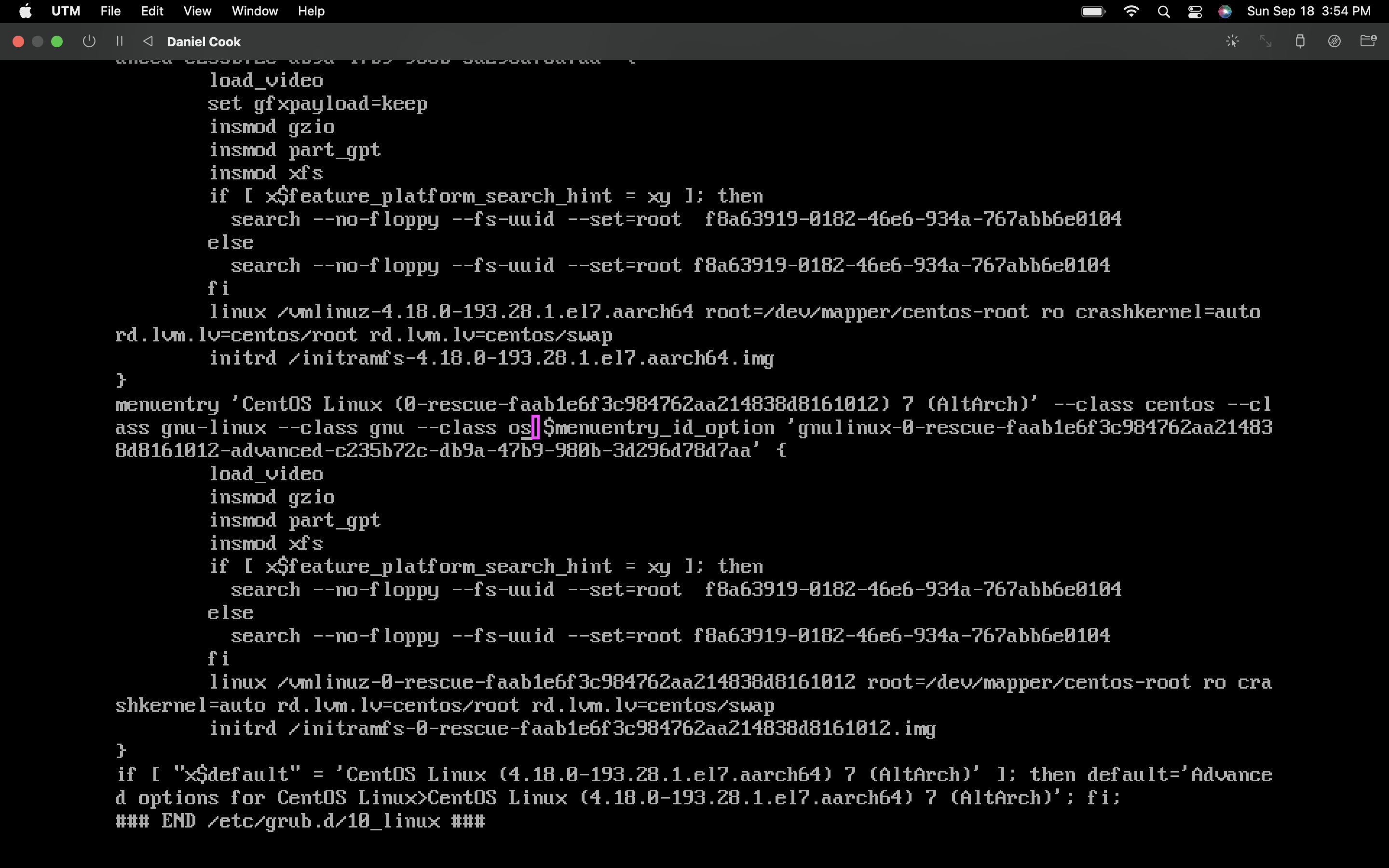
PART 3: Hardening the GRUB BOOTLOADER

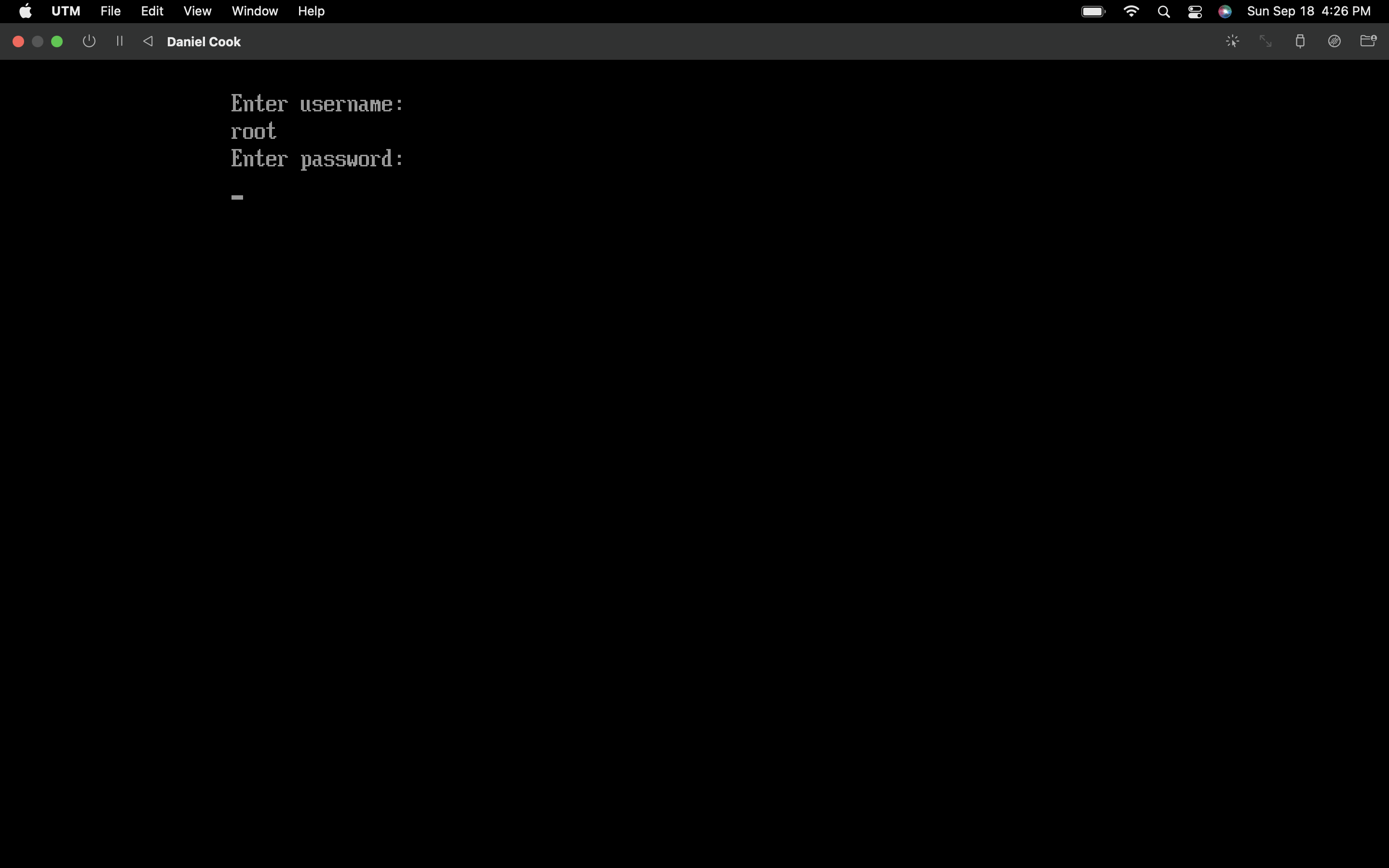
Installing it manually with command “yum install grub2 -y” and then update grub2’s configuration with command “grub2-mkconfig -o /boot/grub2/grub.cfg”. Using the following command

# grub2-setpassword



Open the /boot/grub2/grub.cfg file with vi, locating the “menuentry” and “--unrestricted” and clearing “--unrestricked”



Bootloader asks for password

Question: We suppose that “—unrestricted” wasn’t removed from the first entry. If you can log in the OS through the second entry (assuming that you know the root password for the OS on the second entry), are you able to change the root user’s password for the OS on the first entry (like what we did in PART II)? Yes, why? No, why?

No, I don’t believe that is the case. If a password is set on grub2 (see lab 02), it will ask for a password when an OS is selected, or when someone intends to edit the setting of the OS entry.

Question: Based on your answer in 3.1, what do step 1 (making GRUB password) and step 2 (removing “—unrestricted”) protect respectively (e.g., what is the difference between only setting a password for GRUB and setting for both). Hint: the best way to find out the answer is to set a password for GRUB only and redo part II.

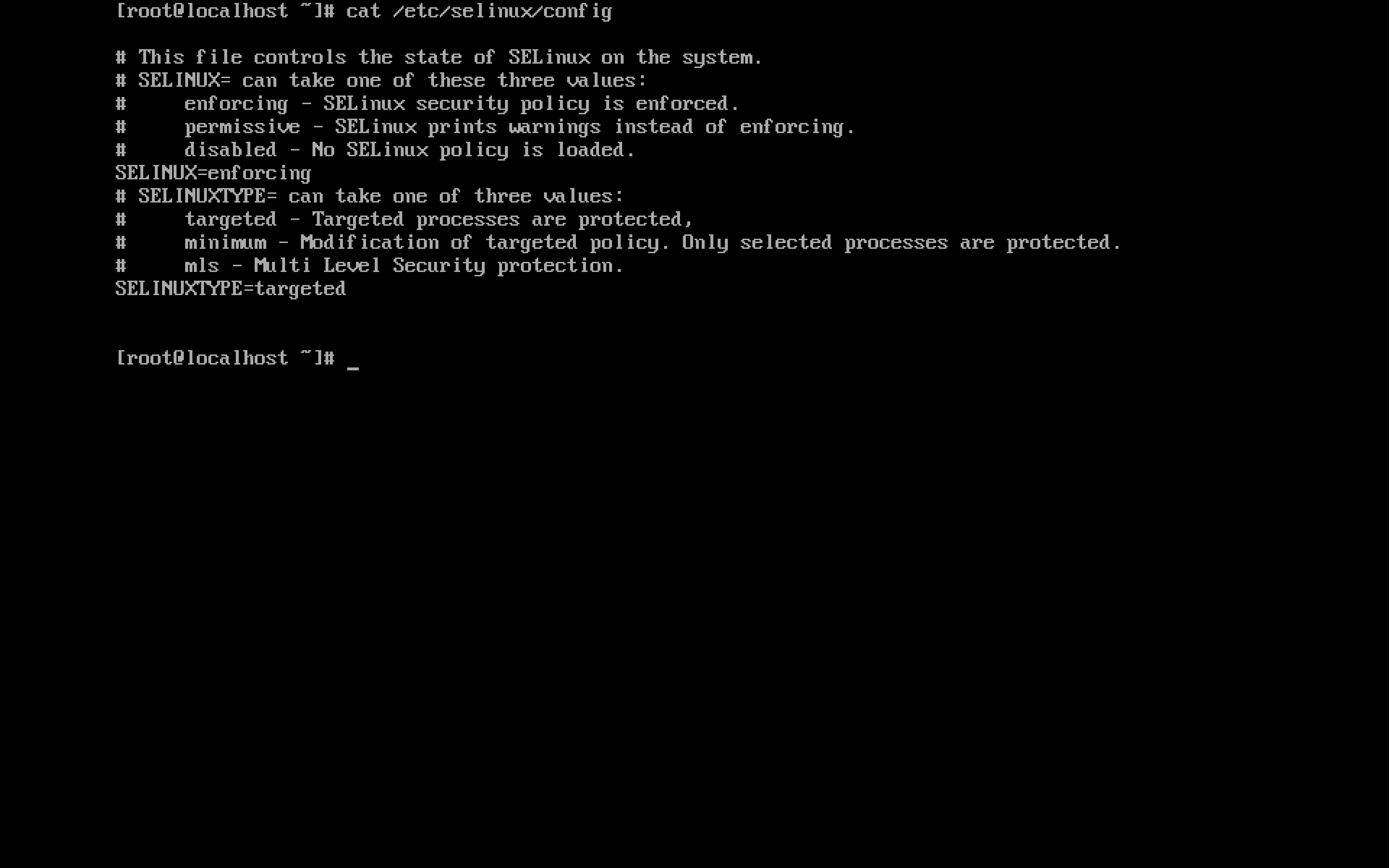
Setting the password shows in the bootloader can ensure that it's protected.

Question: According to the computer’s booting process, if the bootloader is hardened, does it mean that the computer is safe now? Briefly introduce what else we could do to bypass the bootloader’s password and how we can prevent it.

An unprotected BIOS can be utilized for booting the computer from an unauthorized bootloader stored on the attacker’s storage device (e.g., Flash drive or CD ROM) This ensures that its well put that intruders can’t attack from the computer.

PART 4: Enabling Security-Enhanced Linux

At the terminal command prompt, using command sestatus to check if SElinux is currently running on the enforcing mode.

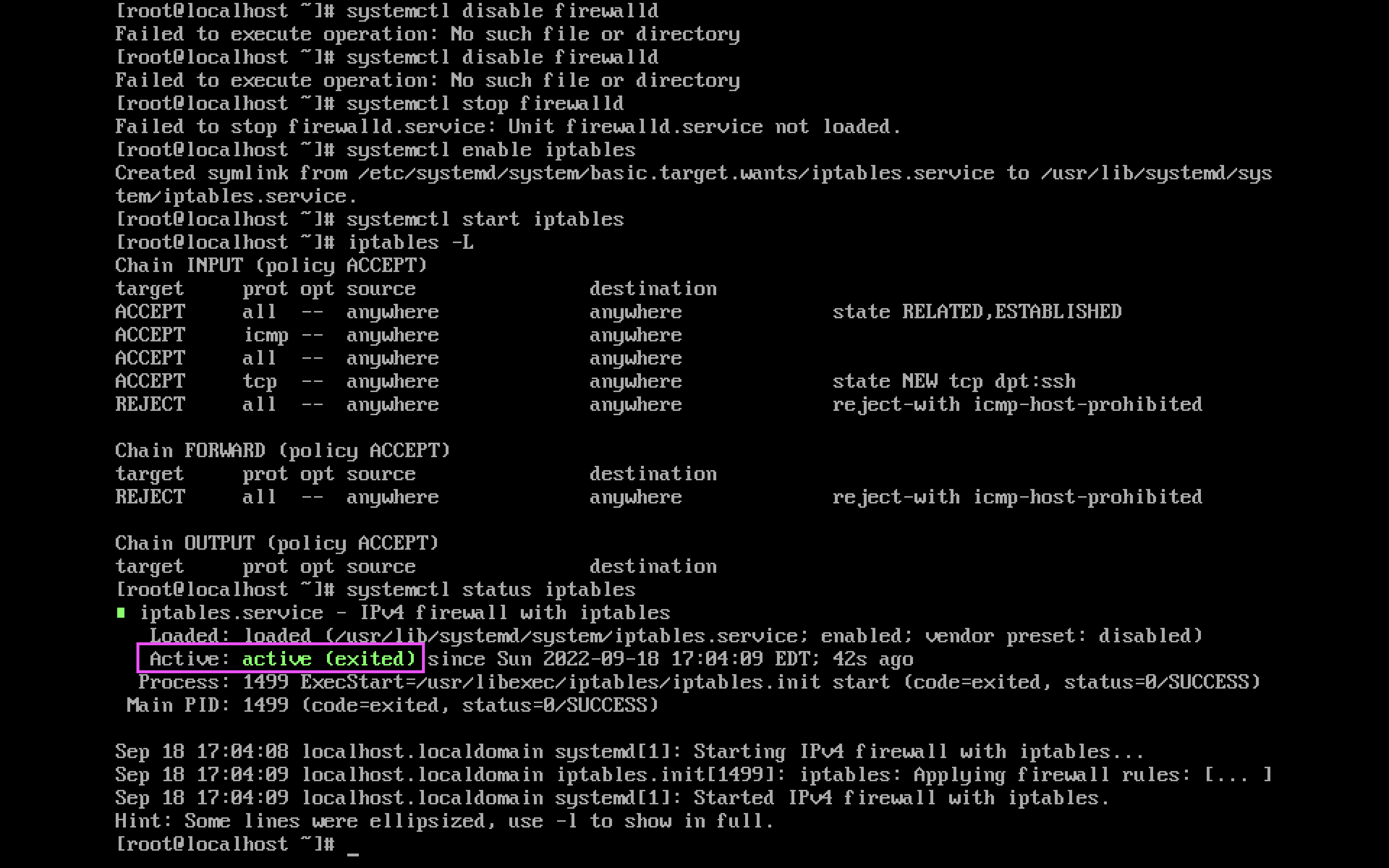


PART 5: Enable iptables firewall

Question: what is the difference between option “disable” and “stop”?

“Stop” stops the service of what is running temporarily, “disable” disables the service until enabling it.

Type in “systemctl status iptables” to confirm that iptables is activated. Checking the status.



Turning off “iptables” with the systemctl command.



Checking if the firewall is active or dead

