Project Report: Gaining Root Access by Resetting Password on RHEL 9.3

Author: Mohanish K

Date: July 10, 2025

System: Red Hat Enterprise Linux (RHEL) 9.3 (Plow)

Web Documentation: Link

1. Objective

The primary objective of this project is to demonstrate the procedure for resetting the root user's password on a Red Hat Enterprise Linux 9.3 system. This process is a critical system administration skill, typically required when the root password is lost or forgotten, effectively locking administrators out of the system. By following these steps, we can regain administrative access without reinstalling the operating system.

2. Prerequisites

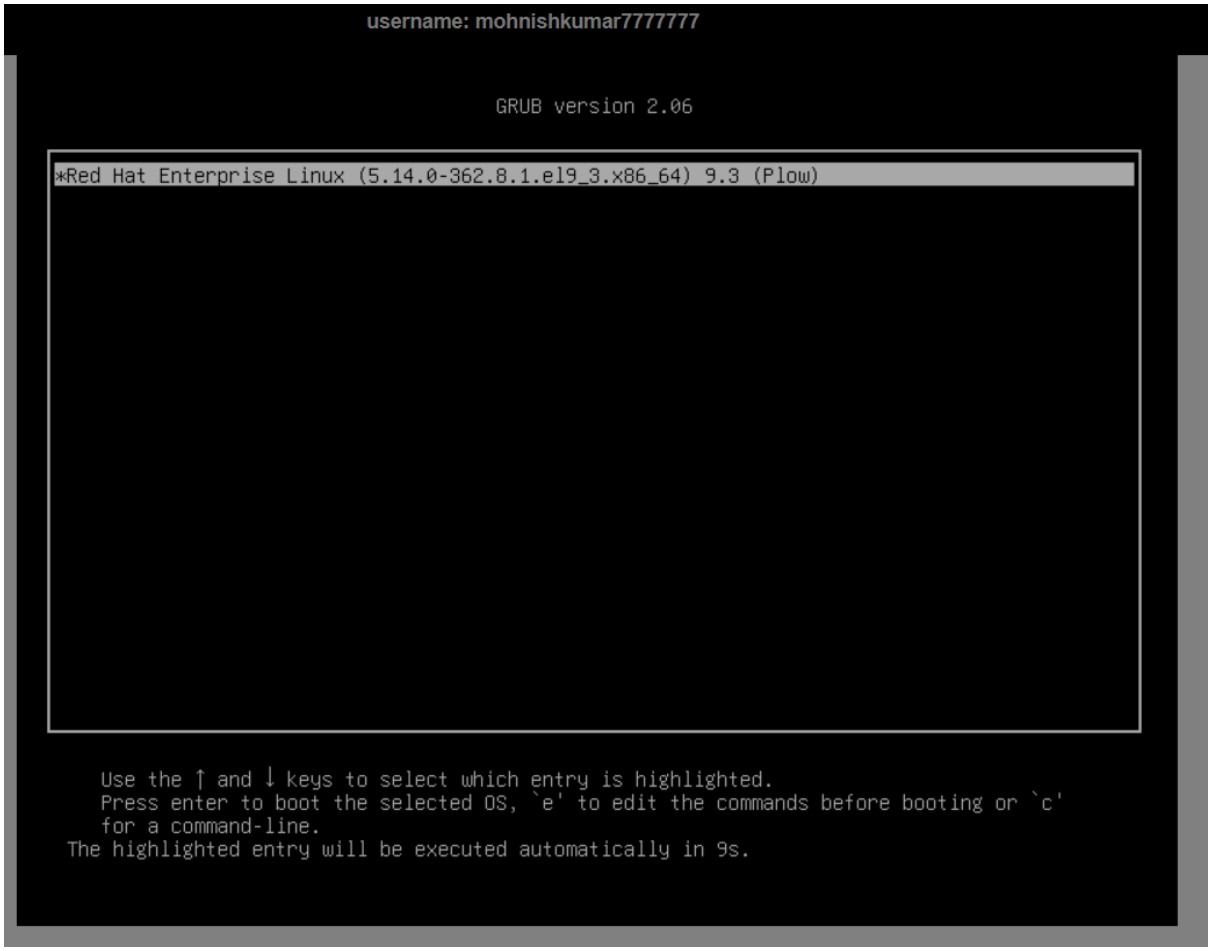
- **Physical or Console Access:** Direct physical access to the machine or console access (e.g., through a virtual machine console or remote management interface like iDRAC/iLO) is required to interact with the bootloader.
- **System Reboot:** The ability to reboot the target machine is necessary to interrupt the boot process.
- **Operating System:** A functioning Red Hat Enterprise Linux 9.3 installation.

3. Procedure

The process involves interrupting the boot sequence, modifying the kernel boot parameters to enter an emergency shell, and then using system commands to change the password.

Step 1: Reboot the System and Interrupt GRUB

First, reboot the Linux machine. As it starts up, watch for the GRUB bootloader menu. Once it appears, use the arrow keys to highlight the desired kernel (usually the default one) and press the e key to edit the boot parameters.



Step 2: Modify Kernel Boot Parameters

After pressing e, you will see the GRUB editor. Use the arrow keys to navigate to the line that starts with linux. Go to the end of this line and add the parameter rd.break. This parameter instructs the system to break the boot process before control is handed over from the initial RAM disk (initramfs) to the actual system, landing you in an emergency shell.

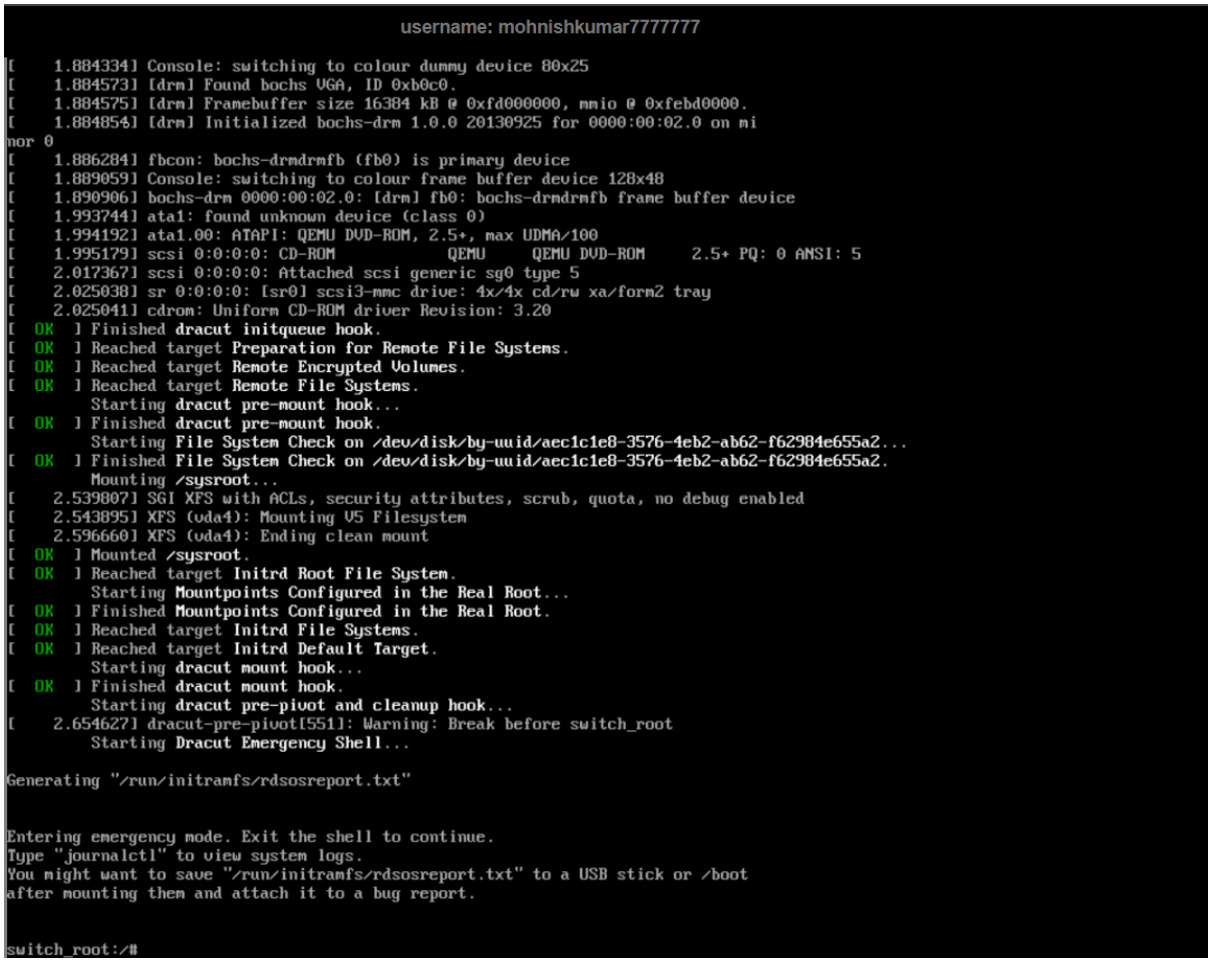
Once the parameter is added, press Ctrl+x to boot with these modified parameters.

Kernel Boot Manager:

After Edit in Kernel Boot Manager:

Step 3: Access the Emergency Shell

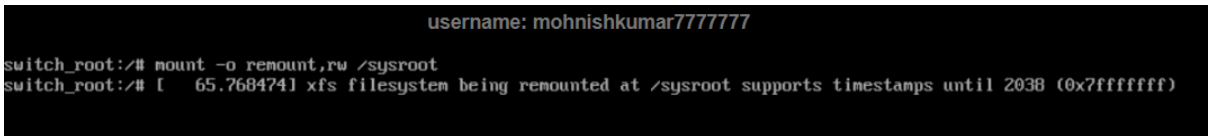
The system will boot and then stop at the emergency shell, presenting a prompt like switch_root:/#. At this point, the actual root filesystem is mounted in read-only mode under /sysroot/.



Step 4: Remount the Filesystem with Read-Write Permissions

To change the password, we need to be able to write to the filesystem. Remount the /sysroot directory with read-write permissions using the following command:

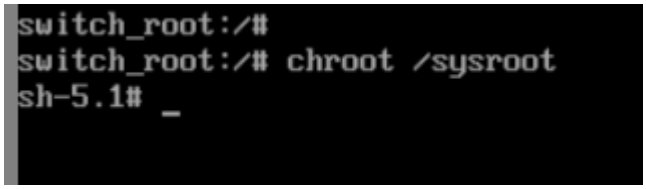
mount -o remount,rw /sysroot



Step 5: Enter the chroot Environment

Now, change the root of your environment to the system's actual root directory. This allows you to run commands as if you were in the fully booted operating system.

chroot /sysroot



The command prompt will change to sh-5.1#, indicating you are now in the chrooted environment.

Step 6: Change the Root Password

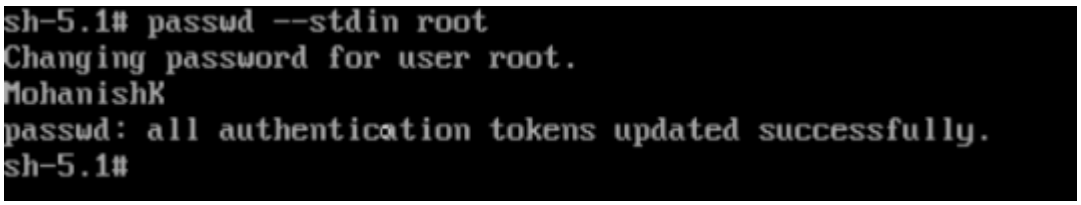
You can now change the root password using the passwd command.

passwd root

You will be prompted to enter and confirm the new password. In the provided screenshot, the --stdin option was used to pipe the password directly, which is also a valid method.

passwd --stdin root

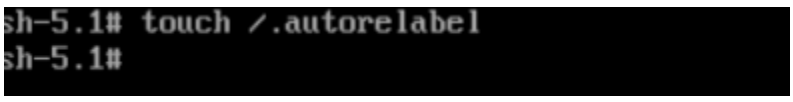
MohanishK

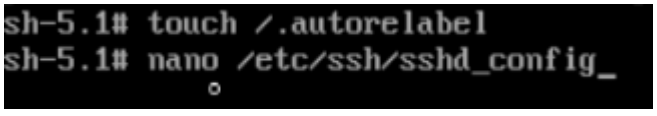


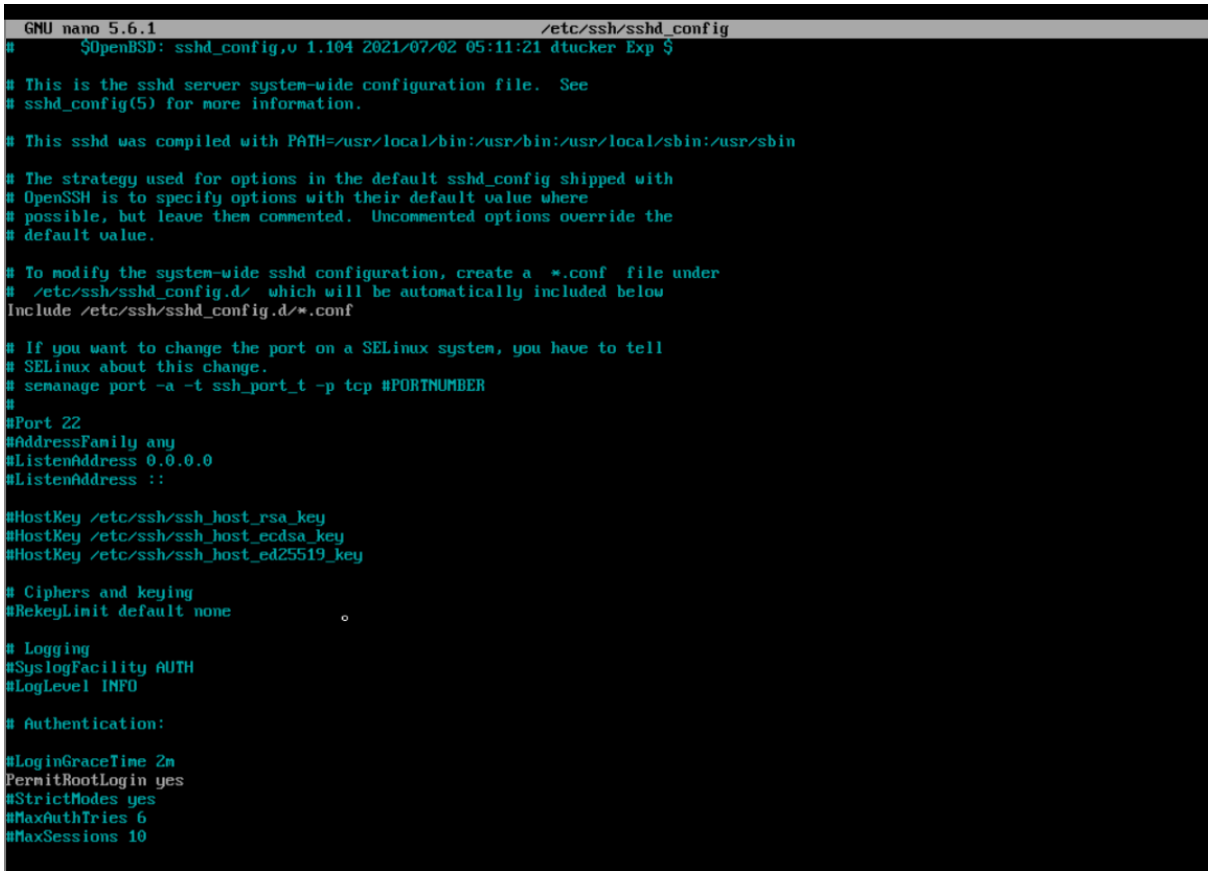
Step 7: Update SELinux Context (Crucial Step)

Because the password file (/etc/shadow) was modified outside of the normal SELinux context, we must instruct SELinux to relabel all files on the next boot. This prevents potential login issues. Create an empty file named .autorelabel in the root directory:

touch /.autorelabel







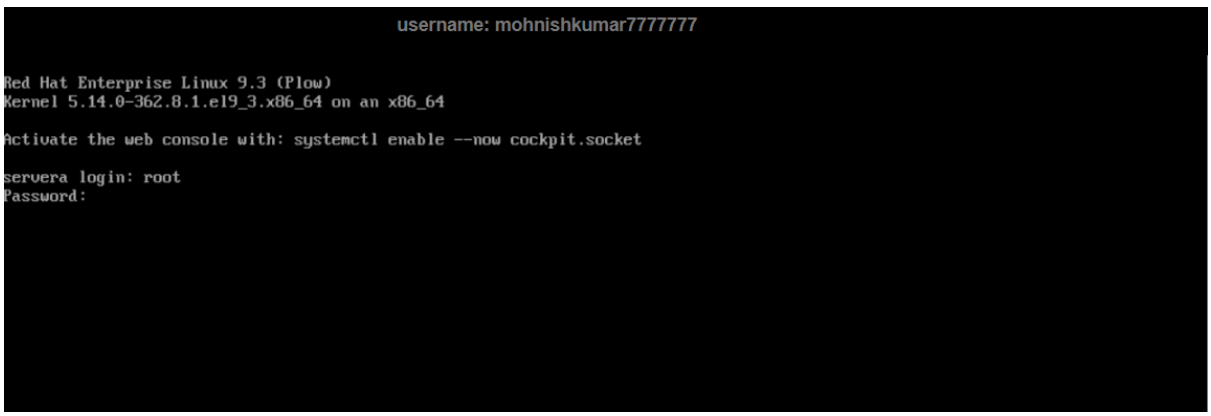
Line Number 40 → PermitRootLogin yes

Step 8: Exit and Reboot

Finally, exit the chroot environment and then exit the emergency shell to let the system reboot.

exit

exit



The system will now reboot. During this boot, SELinux will perform a full relabeling of the filesystem, which may take some time. Once it is complete, the system will reboot one final time, and you will be able to log in as the root user with your new password.

4. Conclusion

This project successfully demonstrated the standard procedure for resetting a forgotten root password on a Red Hat Enterprise Linux system. By interrupting the GRUB bootloader and using a chroot environment, we were able to securely change the password and restore administrative access. This process underscores the importance of physical security, as anyone with console access can potentially perform these actions.

Made with ❤️ for Cybersecurity Excellence ~Mohanish.K