

# 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

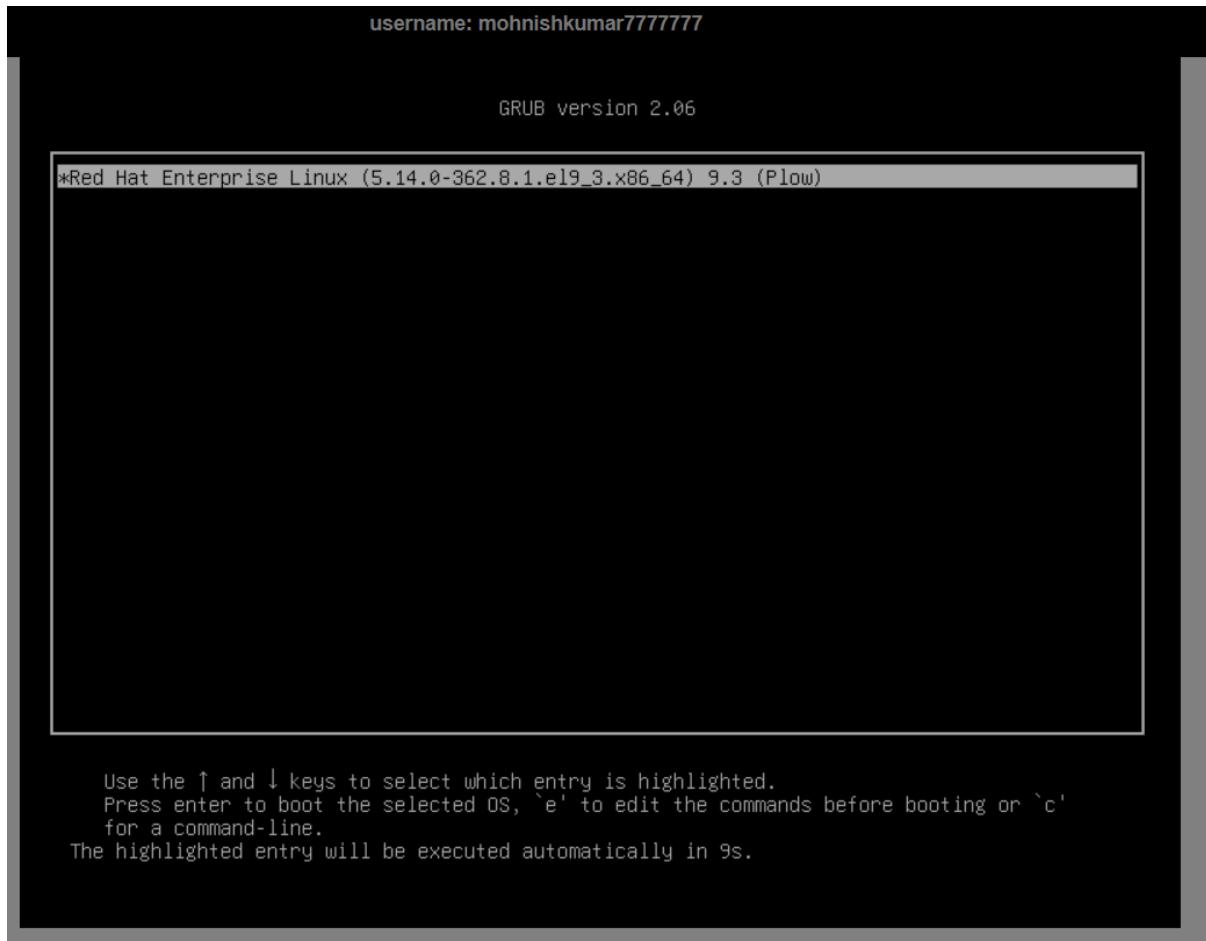
- **Physical or Console Access:** Direct physical access to the machine or console access (e.g., through a virtual machine console or remote management interface like iDRAC/iLO) is required to interact with the bootloader.
- **System Reboot:** The ability to reboot the target machine is necessary to 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:

```
username: mohnishkumar7777777

GRUB version 2.06

load_video
set gfxpayload=keep
insmod gzio
linux ($root)/vmlinuz-5.14.0-362.8.1.el9_3.x86_64 root=UUID=aec1c1e8-3576-4eb2-ab62-f62984e6\
55a2 console=tty0 console=ttyS0,115200n8 no_timer_check net.ifnames=0 crashkernel=1G-4G:192M\
,4G-64G:256M,64G-:512M
initrd ($root)/initramfs-5.14.0-362.8.1.el9_3.x86_64.img $tuned_initrd
-
Minimum Emacs-like screen editing is supported. TAB lists completions. Press Ctrl-x
or F10 to boot, Ctrl-c or F2 for a command-line or ESC to discard edits and return
to the GRUB menu.
.
```

After Edit in Kernel Boot Manager:

```
username: mohnishkumar7777777
```

```
GRUB version 2.06
```

```
load_video
set gfxpayload=keep
insmod gzio
linux ($root)/vmlinuz-5.14.0-362.8.1.el9_3.x86_64 root=UUID=aec1c1e8-3576-4eb2-ab62-f62984e6\55a2_115200n8 no_timer_check net.ifnames=0 crashkernel=1G-4G:192M,4G-64G:256M,64G-:512M rd\break;_
initrd ($root)/initramfs-5.14.0-362.8.1.el9_3.x86_64.img $tuned_initrd
```

```
.
```

```
Minimum Emacs-like screen editing is supported. TAB lists completions. Press Ctrl-x or F10 to boot, Ctrl-c or F2 for a command-line or ESC to discard edits and return to the GRUB menu.
```

### 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/`.

```

username: mohnishkumar7777777

[ 1.884334] Console: switching to colour dummy device 80x25
[ 1.884573] [drm] Found bochs VGA, ID 0xb0c0.
[ 1.884575] [drm] Framebuffer size 16384 kB @ 0xfd000000, mmio @ 0xfebd0000.
[ 1.884854] [drm] Initialized bochs-drm 1.0.0 20130925 for 0000:00:02.0 on mi
nor 0
[ 1.886284] fbcon: bochs-drmdrmfb (fb0) is primary device
[ 1.889059] Console: switching to colour frame buffer device 128x48
[ 1.890906] bochs-drm 0000:00:02.0: [drm] fb0: bochs-drmdrmfb frame buffer device
[ 1.993744] ata1: found unknown device (class 0)
[ 1.994192] ata1.00: ATAPI: QEMU DVD-ROM, 2.5+, max UDMA/100
[ 1.995179] scsi 0:0:0:0: CD-ROM           QEMU      QEMU DVD-ROM    2.5+ PQ: 0 ANSI: 5
[ 2.017367] scsi 0:0:0:0: Attached scsi generic sg0 type 5
[ 2.025038] sr 0:0:0:0: [sr0] scsi3-mmc drive: 4x/4x cd/rw xa/form2 tray
[ 2.025041] cdrom: Uniform CD-ROM driver Revision: 3.20
[ OK ] Finished dracut initqueue hook.
[ OK ] Reached target Preparation for Remote File Systems.
[ OK ] Reached target Remote Encrypted Volumes.
[ OK ] Reached target Remote File Systems.
  Starting dracut pre-mount hook...
[ OK ] Finished dracut pre-mount hook.
  Starting File System Check on /dev/disk/by-uuid/aec1c1e8-3576-4eb2-ab62-f62984e655a2...
[ OK ] Finished File System Check on /dev/disk/by-uuid/aec1c1e8-3576-4eb2-ab62-f62984e655a2.
  Mounting /sysroot...
[ 2.539807] SGI XFS with ACLs, security attributes, scrub, quota, no debug enabled
[ 2.543095] XFS (vda4): Mounting V5 Filesystem
[ 2.596660] XFS (vda4): Ending clean mount
[ OK ] Mounted /sysroot.
[ OK ] Reached target Initrd Root File System.
  Starting Mountpoints Configured in the Real Root...
[ OK ] Finished Mountpoints Configured in the Real Root.
[ OK ] Reached target Initrd File Systems.
[ OK ] Reached target Initrd Default Target.
  Starting dracut mount hook...
[ OK ] Finished dracut mount hook.
  Starting dracut pre-pivot and cleanup hook...
[ 2.654627] dracut-pre-pivot[551]: Warning: Break before switch_root
  Starting Dracut Emergency Shell...

Generating "/run/initramfs/rdsosreport.txt"

Entering emergency mode. Exit the shell to continue.
Type "journalctl" to view system logs.
You might want to save "/run/initramfs/rdsosreport.txt" to a USB stick or /boot
after mounting them and attach it to a bug report.

switch_root:#

```

#### 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
```

```

username: mohnishkumar7777777

switch_root:/# mount -o remount,rw /sysroot
switch_root:/# [ 65.768474] xfs filesystem being remounted at /sysroot supports timestamps until 2038 (0x7fffffff)
```

#### 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
```

```
switch_root:/#  
switch_root:/# chroot /sysroot  
sh-5.1# _
```

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
```

```
sh-5.1# passwd --stdin root  
Changing password for user root.  
MohanishK  
passwd: all authentication tokens updated successfully.  
sh-5.1#
```

### 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
```

```
sh-5.1# touch /.autorelabel  
sh-5.1#
```

```
sh-5.1# touch /.autorelabel  
sh-5.1# nano /etc/ssh/sshd_config_
```

```

GNU nano 5.6.1                               /etc/ssh/sshd_config
# $OpenBSD: sshd_config,v 1.104 2021/07/02 05:11:21 dtucker Exp $

# This is the sshd server system-wide configuration file. See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/local/bin:/usr/bin:/usr/local/sbin:/usr/sbin

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented. Uncommented options override the
# default value.

# To modify the system-wide sshd configuration, create a *.conf file under
# /etc/ssh/sshd_config.d/ which will be automatically included below
Include /etc/ssh/sshd_config.d/*.conf

# If you want to change the port on a SELinux system, you have to tell
# SELinux about this change.
# semanage port -a -t ssh_port_t -p tcp #PORTNUMBER
#
#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
PermitRootLogin yes
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

```

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

```

username: mohnishkumar7777777

Red Hat Enterprise Linux 9.3 (Plow)
Kernel 5.14.0-362.8.1.el9_3.x86_64 on an x86_64

Activate the web console with: systemctl enable --now cockpit.socket

server login: root
Password:

```

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