CSI Linux Password Reset

Contents

Oops, it seems like you've hit a minor bump on your CSI Linux journey – you've forgotten your login password. Don't worry, it's a common occurrence, especially when you haven't been engaging with CSI Linux for a while. Here's the exciting part: you don't have to start all over by reinstalling the whole operating system. Far from it! CSI Linux has got you covered with user-friendly solutions for password recovery. So, let's turn this little hurdle into an opportunity to learn more about the flexibility and resilience of CSI Linux! Ready to get back on track? Let's dive right in!

The default username is "**csi**" and the password is "**csi**"

Either before you forget or after you do, here are two suggestions to make sure you can keep in the system. Here's a step-by-step guide:

1. Now, create a new user by typing `adduser newuser` (replace 'newuser' with your desired username). You will be prompted to enter a password and other details for this new user.

   ```
   adduser newuser
   ```

2. After creating the new user, let's add them to the sudo group with:

   ```
   usermod -aG sudo newuser
   ```

But wait, there's more! If you have access to the system via a sudoer user, you can change the root password with a few simple commands. Here's how:

1. In the Terminal, type `sudo su` and press enter. This command will switch you to the root user.

   ```
   sudo su
   ```

2. Now, use the `passwd` command to change the root password. You will be prompted to enter the new password and then confirm it.

   ```
   passwd
   ```

Reset Password Locally on System.

Resetting a password from recovery or Grub in Linux refers to the process of regaining access to a Linux system when the user's password has been forgotten or lost. This is accomplished by leveraging special features or modes in the Linux boot process, such as recovery mode or the Grand Unified Bootloader (Grub).

> **Recovery Mode:** In many Linux distributions, there's an option in the boot menu called 'recovery mode' which boots the system into a basic state where only essential services are started. The recovery mode also provides root access, thereby bypassing normal user authentication. Once in the recovery mode, you can use root privileges to reset a forgotten user password.
>
> **Grub:** The Grub bootloader is what loads Linux (or other operating systems) when your computer starts. By interrupting the Grub boot process, you can temporarily modify the boot parameters and instruct the system to start with a bash shell instead of the regular login screen. This gives you root access, allowing you to reset any user password.

These methods do not require any external tools or media and can be accomplished with just the built-in features of the Linux system. They provide powerful recovery capabilities, but they also illustrate the importance of physical security, as anyone with physical access to a system can potentially use these methods to gain access.

Method 1: Recovery Mode

Step 1: Boot into recovery mode

Switch the computer on. Go to the grub menu. Generally, it appears automatically – if not, then hold down the shift key or press Esc key until the boot menu appears.

- **Oracle VirtualBox or VMware**: you must hold down the shift key when the logo of Oracle or VMware appears.

- **Other**: As the computer restarts, repeatedly press and hold the Shift key. This action should bring up the GRUB 2 menu.

In the grub menu, select the "Advanced …":

In here, you'll see the option to go to recovery mode:

It will bring you to a black screen with several lines of output displayed in a flash. Wait for a few seconds here.

Step 2: Drop to root shell prompt.

Now you'll be presented with different options for recovery mode. Here you need to choose "Root – Drop to root shell prompt". Just press the enter key to select this option.

You'll see that when you select the root shell prompt option, an option to enter commands appears at the bottom. This is your root shell prompt, and this is where you'll use the commands to reset the password.

Step 3: Remount the root with write access.

You need to have write access to the root partition. By default, it has read-only access. Use the command below to remount it with write access:

```
mount -rw -o remount /
```

Step 4: Reset username or password.

Here, you'll be given root access. Use the following command to list all the users available:

```
ls /home
```

Based on this command, choose the "username" for which you want to reset or (say) hack the password. Now, use the following command to reset the password for the selected "username":

```
passwd username
```

It prompts for a new password. Enter the new password twice.

When you start typing the password, nothing is displayed on the screen. This is perfectly normal and a security feature in Linux systems. Just blindly type the password and press enter.

You have just successfully reset the password. Now exit the root shell prompt:

```
exit
```

When you exit, you'll be back at the recovery mode menu. Select the normal boot option here.

There will be a warning about graphics mode compatibility. Don't worry. A complete reboot will fix any issues with this.

You should now be able to log in with the new password.

Method 2: Reset CSI Linux Password via Grub

Step 1: Initiate Grub Screen

Reboot your computer. Hold the shift key to trigger the grub screen (if it doesn't appear automatically). Press 'E' at the grub prompt to proceed to edit the grub screen.

Step 2: Edit Grub Settings

Locate the line starting with 'linux', change the 'ro' to 'rw' and append 'init=/bin/bash' at the end of that line.

Step 3: Save Changes and Boot

Press 'ctrl-x' to save your changes and initiate the boot process.

Now your system will boot into the Linux kernel with read-write permissions and instead of loading a graphical user interface, you'll land at the bash shell.

Step 4: Transition to Passwordless Root Shell

Your system has now booted up to a passwordless root shell.

Step 5: Identify Username

Type in the 'ls /home' command to list all users if you're unsure of your username.

Step 6: Reset Password

Type in the 'passwd' command followed by your username to initiate the password reset process.

Set your new password when prompted.

Step 7: Exit Terminal and Reboot

Once you've set the new password, exit the terminal by typing 'exit'. Reboot your computer by typing 'shutdown -r now' or simply 'reboot' in the terminal.

Possible Troubleshoot:

While entering the new password you might be prompted with Authentication token manipulation error like this:

```
passwd username
```

Enter new UNIX password: Retype new UNIX password: passwd: Authentication token manipulation error passwd: password unchanged.

The reason for this error is that the file system is mounted with read access only. Change the access and remount the file system in the following manner:

```
mount -rw -o remount /
```

Now try to reset the password again. It should work now.

As you can see, it is extremely easy to change CSI Linux password even if you've forgotten it. It will barely take a few minutes.

Your password should be changed now.

Resetting Password Using a Bootable System

Resetting a password using a bootable disk involves using a specially created disk or USB drive to gain access to a computer system when the original password is forgotten or inaccessible. The bootable disk contains a separate operating system or utility that bypasses the password security measures on the target system. By booting from the disk, the user can access the system's files and settings and reset the password to regain access.

- **Oracle VirtualBox:** Once the virtual machine window opens, click on the "Machine" menu at the top of the window. From the dropdown menu, select "Settings". In the Settings window, navigate to the "System" tab. Under the "Motherboard" section, you will find the "Boot Order" options. To change the boot sequence, you can modify the order of boot devices by clicking on the arrows or using the "+" and "-" buttons. Arrange the boot devices in the desired order. For example, if you want to prioritize booting from a CD/DVD, you can move it to the top of the list. You can also enable or disable boot devices by checking or unchecking the checkboxes next to each device. Once you have made the desired changes, click "OK" to save the settings.

- **VMware**: In the Virtual Machine Settings window, navigate to the "Options" tab. Under the "Advanced" category, select "Boot Options". Check the box for "Specify boot sequence."

- **KVM** (Kernel-based Virtual Machine): Right-click on the selected virtual machine and choose "Open". In the virtual machine window, click on the "Boot Options" tab or a similar option related to boot settings. In the boot options section, you'll see a list of available boot devices or boot order. Use the provided interface to rearrange the boot order according to your preferences. Typically, you'll have options like hard drive, CD/DVD drive, network boot, etc. Use the arrow buttons or drag-and-drop to change the order. Once you have adjusted the boot sequence as desired, click "Apply" or "OK" to save the changes.

- **Xen**: Xen is a popular open-source hypervisor that allows for running multiple virtual machines on a single physical machine. The process of accessing the boot menu or configuration options in Xen can vary depending on the specific Xen implementation and the management tool being used. Commonly, you would access the Xen management console or use tools like xl or xm to interact with the virtual machine.

- **Hardware-based:** Accessing the boot menu on laptops and PCs can vary depending on the manufacturer and the specific model. Here are some common methods to access the boot menu. If you're unsure about the specific key or method for your laptop or PC, you can try the following general approaches:

    a. **F12** Method: Restart your laptop/PC and press the F12 key repeatedly when the manufacturer logo appears.
    b. **Esc** Method: Restart your laptop/PC and press the Esc key repeatedly when the manufacturer logo appears.
    c. **Del** Method: Restart your laptop/PC and press the Del key repeatedly when the manufacturer logo appears.
    d. **F10** Method: Restart your laptop/PC and press the F10 key repeatedly when the manufacturer logo appears.

It's important to note that the exact steps and key combinations may vary depending on the specific virtualization platform, version, and configuration you are using. Always consult the documentation or support resources for your particular system or software for accurate instructions on accessing the boot menu or configuring virtual machines.

Method 1: Boot from an External Drive, USB, or .iso Image

Step 1: Insert your bootable device or disc

Insert the bootable USB or disc into the USB on your computer.

Step 2: Boot from the device or disc

Restart your computer and access your BIOS settings. Set your boot order to boot first from the device or disc.

Step 3: Choose 'Try CSI Linux without installing'

In the grub menu, choose 'Try CSI Linux without installing'. This will load CSI Linux from your bootable device.

Step 4: Open terminal and identify the partition

Open the terminal and use 'fdisk -l' to list the partitions and identify the partition where CSI Linux is installed.

Step 5: Mount the CSI Linux partition

Once booted into the external Linux system, open a Terminal. Use the `fdisk -l` command to list all disk partitions and identify the one that has your Linux system.

When you have identified it (for example, /dev/sda1), you will need to mount it. If you don't have a /mnt directory already, create one with `sudo mkdir /mnt`. Then, mount your Linux partition with `sudo mount /dev/sda1 /mnt`.

Step 6: Chroot into your system

Use the command 'chroot /mnt' to get a root shell of your system.

Step 7: Change the password

Use 'passwd username' to change the password of the specific user.

Method 2: Reset CSI Linux Password via Triage Drive

Step 1: Create a Bootable External Drive

Firstly, you need to create a bootable external drive or USB. You can use the CSI Linux 2023 Triage Drive dd image. Here is the link for your reference:

> http://downloads.csilinux.com/Setting%20up%20the%20CSI%20Linux%202021.1%20Bootable%20Image.pdf.

For Windows users, you can follow the process in these tutorials:

> https://youtu.be/uFDvxlnFE6w

Before proceeding, test your drive to ensure everything has copied correctly:

> https://youtu.be/BsUSFjaPRUw

Step 2: Boot from the External Linux Hard Drive

Start your computer and immediately access the BIOS/UEFI settings or boot screen.

Step 3: Mount the Linux Partition

Once booted into the external Linux system, open a Terminal. Use the `fdisk -l` command to list all disk partitions and identify the one that has your Linux system.

Once you have identified it (for example, /dev/sda1), you will need to mount it. If you don't have a /mnt directory already, create one with `sudo mkdir /mnt`. Then, mount your Linux partition with `sudo mount /dev/sda1 /mnt`.

Step 4: Chroot into Your Mounted Linux System

Use the command `sudo chroot /mnt` to access your mounted Linux system.

Step 5: Reset the Password

Use the `passwd` command followed by the username of the account you want to reset. For example, if your username was 'username', you would type `passwd username`. You'll be prompted to enter a new password and confirm it.

Step 6: Unmount the Partition and Reboot

Exit from the chroot environment by typing `exit`. Unmount the partition with `sudo umount /mnt`.

Reboot your computer. This time, make sure it boots from the internal drive (you may need to adjust the boot order again in the BIOS/UEFI settings).

Step 7: Boot Back into CSI

After reboot, you should now be able to log into your CSI Linux system with the new password you set.

Your password should be changed now.

Build or Re-build a CSI Linux Workstation

Building or rebuilding a system from a trusted image, also known as a "golden image," involves creating a standardized and pre-configured system image that serves as a template for deploying multiple systems. Here's a summary of what it means to build or rebuild a system from a trusted image:

Building or rebuilding systems from a trusted image offers numerous benefits, including simplified deployment, improved system consistency, reduced configuration errors, and enhanced security. It is commonly used in enterprise environments to streamline system provisioning and maintain a consistent infrastructure across a large number of machines.

Method 1: Image and Restore the System

Step 1: Download the CSI Linux Triage Image

Firstly, you need to create a bootable external drive or USB. You can use the CSI Linux 2023 Triage Drive dd image. Here is the link for your reference:

> http://downloads.csilinux.com/Setting%20up%20the%20CSI%20Linux%202021.1%20Bootable%20Image.pdf.

For Windows users, you can follow the process in these tutorials:

> https://youtu.be/uFDvxlnFE6w

Before proceeding, test your drive to ensure everything has copied correctly:

> https://youtu.be/BsUSFjaPRUw

Step 2: Reboot to Verify

Reboot your system to verify that the image was copied correctly. Ensure your system's BIOS/UEFI settings are set to boot from the external drive.

Step 3: Using Clonezilla to Restore from the External Drive with Clonezilla

Clonezilla is a free and open-source disk imaging/cloning program. You will need your CSI Triage drive, a USB with Clonezilla installed, and an internal drive to restore the system to. Let's assume the internal drive is /dev/sda and the triage drive is /dev/sdb. Here's how to use it:

1. First, boot from a drive or disc that has Clonezilla installed. This could be the same external drive you just created, or it could be a separate drive or disc.

2. Choose Language and Keyboard Layout. Once Clonezilla is running, you will need to choose your language and keyboard layout.

3. On the main menu, select "Start Clonezilla", and then choose "device-device" to clone from one drive to another.

4. In the expert mode menu, select the "disk_to_local_disk" option to clone the entire external drive to an internal drive.

5. Select the Source and Target Disks. Choose the source disk (the external drive) and the target disk (the internal drive). Be very careful to get these the right way around, as the target disk will be overwritten.

6. Set Advanced Options. In the expert mode options, you should find an option like "-icds" or "Skip checking/repairing source file system." Check this option to skip the size check on the destination disk.

7. Follow the rest of the prompts to continue setting other options as per your requirements. Then begin the Cloning Process. Once you've set all the necessary options, you can start the cloning process.

8. Reboot the System and Verify

Video for reference: https://youtu.be/tQuS1Suonxo

After the system image is restored, reboot your system. Make sure your BIOS/UEFI settings are set to boot from the internal drive. You should then be able to log in with the credentials that were valid at the time the image was created.

Build "Golden Image" of a CSI Linux Workstation

Method 1: Image the System with Clonezilla

Step 1: Using Clonezilla to Restore to the External Drive with Clonezilla

Clonezilla is a free and open-source disk imaging/cloning program. You will need your CSI Triage drive, a USB with Clonezilla installed, and an internal drive to restore the system to. Let's assume the internal drive is /dev/sda and the triage drive is /dev/sdb. Here's how to use it:

1. First, boot from a drive or disc that has Clonezilla installed. This could be the same external drive you just created, or it could be a separate drive or disc.

2. Choose Language and Keyboard Layout. Once Clonezilla is running, you will need to choose your language and keyboard layout.

3. On the main menu, select "Start Clonezilla", and then choose "device-device" to clone from one drive to another.

4. In the expert mode menu, select the "disk_to_local_disk" option to clone the entire external drive to an internal drive.

5. Select the Source and Target Disks. Choose the source disk (the internal drive) and the target disk (the external drive). Be very careful to get these the right way around, as the target disk will be overwritten.

6. Use Basic options.

7. Follow the rest of the prompts to continue setting other options as per your requirements. Then begin the Cloning Process. Once you've set all the necessary options, you can start the cloning process.

8. Reboot the System and Verify

Video for reference: https://youtu.be/tQuS1Suonxo

Bonus: Possible Keyring Issue After Password Change

There is a keyring feature in CSI Linux that is used for keeping passwords locked and safe.

When you reset the forgotten password, the keyring remains unlocked, and you may see an error message like this.

Enter Password to Unlock Your Login Keyring CSI Linux

Open the Passwords and Keys application and here, delete the Login passwords.

When you try to use Google Chrome again in CSI Linux, it will ask you to create a new keyring. Use the new login password as the keyring password.

If resetting Linux passwords is this easy, isn't this a security risk?

That's a fair question. One of the main advantages of Linux over Windows is its security. But if "anyone" can reset the password, how come CSI Linux or other Linux distributions can be considered secure?

Let me explain a few things here. The main security risk is if someone hacks into your account from a remote location via the internet. That's not happening here.

If anyone has physical access to your computer, the data in your computer is already at risk. Unless the entire disk is encrypted, anyone can "steal" your data using a live USB without even entering your installed operating system. However, if you have disk or volume encryption, you should have setup up an emergency account to reset your password or just reset it to factory default.

Welcome Back!