[Introduction 1](#_Toc1060857779)

[1 Using Oracle’s Troubleshooting to bypass GRUB (Method 1) 2](#_Toc272742329)

[1.1 Installing Oracle ISO and inserting into and booting CD Drive 2](#_Toc256927591)

[1.2 Accessing Oracle recovery 3](#_Toc477760412)

[1.3 Accessing Grub2 config file 5](#_Toc73522327)

[1.4 Disabling Grub login 6](#_Toc2004088085)

[1.4 Resetting grub password 8](#_Toc1186298230)

[1.5 Re-enabling Grub password 8](#_Toc295040386)

[2 Recovering GRUB password through digital forensics (Method 2) 9](#_Toc983423927)

[2.1 Creating a forensic image 10](#_Toc891477974)

[2.2 Converting image format 11](#_Toc1594592988)

[2.3 Using FTK imager to extract GRUB hash 13](#_Toc218031745)

[2.4 Brute forcing GRUB hash to get password for GRUB 16](#_Toc308314188)

[3 Root password Recovery 18](#_Toc47684697)

[3.1 Accessing emergency mode 18](#_Toc1245144731)

[3.2 Remounting 20](#_Toc507090384)

[3.3 Changing password 20](#_Toc195972497)

[Conclusion 21](#_Toc1231960399)

# Introduction

What happens when you lose your grub password and root password?

In this report we will show you 2 methods of what you can do to recover your GRUB password, and to recover your root password.

AND

Why you technically should not be able to recover them.

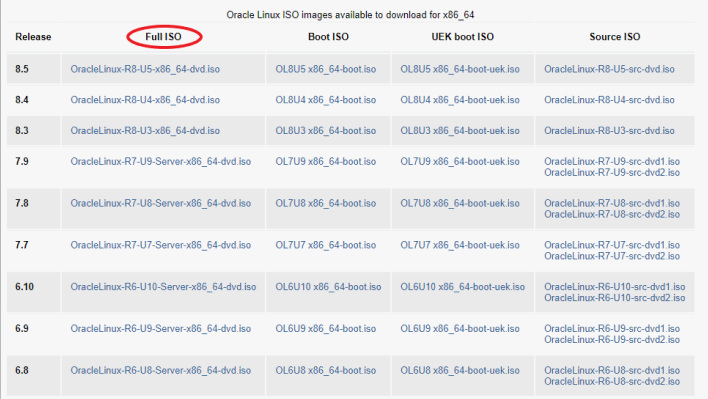
# 1 Using Oracle’s Troubleshooting to bypass GRUB (Method 1)

|  |
| --- |
| This method will require the user to use Red Hat Linux (ISO). The boot order must be configured to boot the newly insert ISO. This will allow the user to access the rescue menu, where users can configure the GRUB2 configuration file to remove the GRUB login.  \*If the GRUB locked system is a physical machine, you will need to format a thumb drive as a bootable USB. |

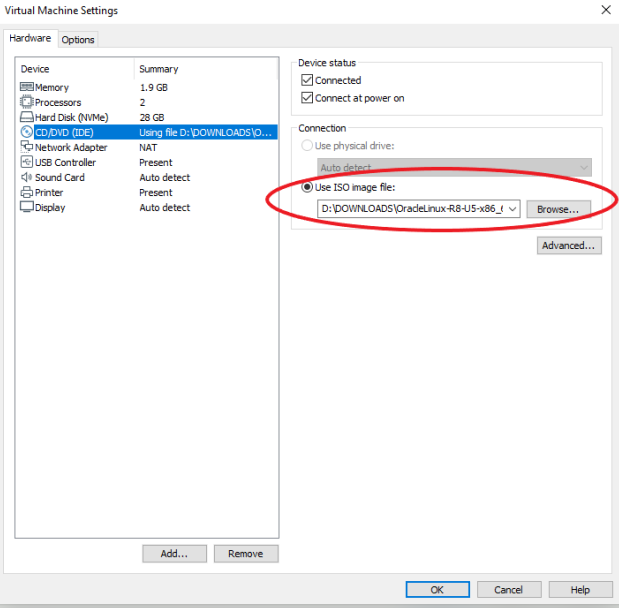
## 1.1 Installing Oracle ISO and inserting into and booting CD Drive

1. First, you will need to download an Oracle ISO, you can download it [here](https://yum.oracle.com/oracle-linux-isos.html)

* Download from the FULL ISO column. As for the release version, choose a version closest to your Linux Oracle VM

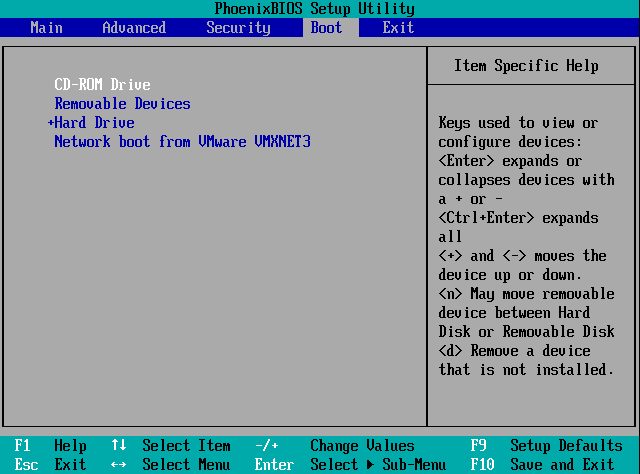


1. Edit the settings of your VM, in your VM player. Go to the hardware tab and look for CD/DVD(IDE) section and check “Use ISO image file". Click browse and select the ISO image file you downloaded just now (Ensure that “Connect at power on” is ticked)

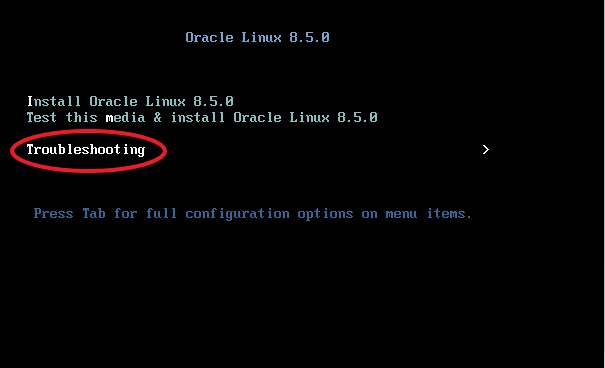


## 1.2 Accessing Oracle recovery

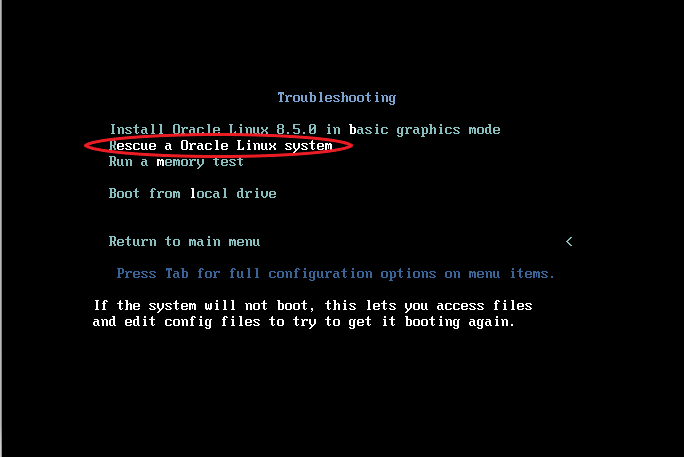
1. Configure the Boot order by restarting the VM, and as it is booting up quickly press F2 multiple times (\*If you are not in the Setup Utility like the one shown in the image below, please restart and try again)
2. Go to the boot tab and move “CD-ROM Drive” with your “+” key, to the top and save it by entering “F10”
3. This will boot up the OS from the ISO you inserted into the CD-ROM drive rather than the hard drive where the GRUB Locked system is located at.



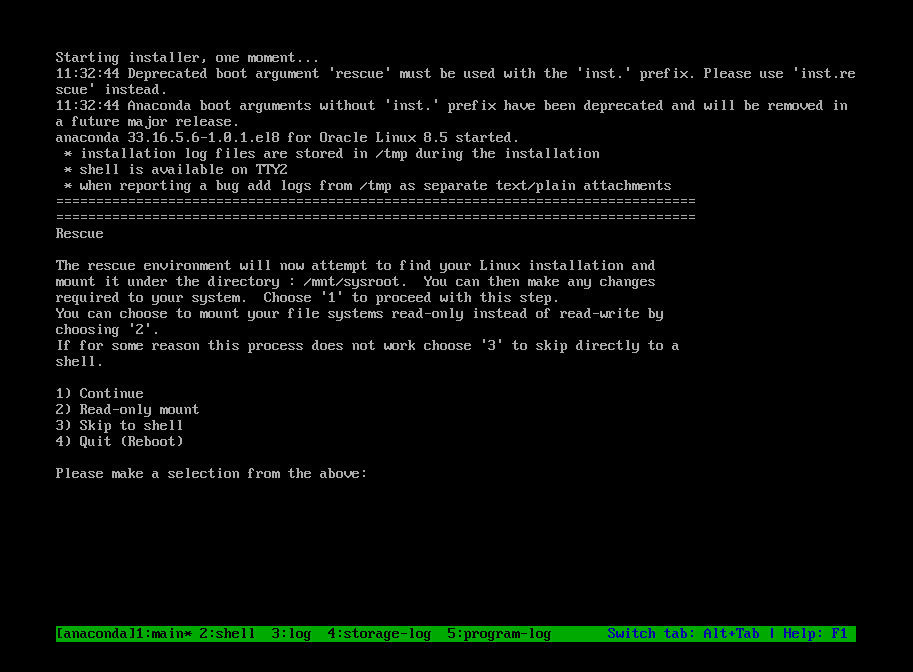
* You will be redirected to the setup menu after saving and exiting the setup utility. Using your arrow keys, select “Troubleshooting”



* On the troubleshooting menu, select “Rescue an Oracle Linux system”



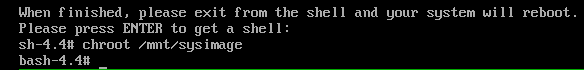
* You should then see a menu like the image below, enter “1” to proceed, and then press Enter for the shell to appear.



## 1.3 Accessing Grub2 config file

* Enter the following command in the shell to mount root partition

*chroot /mnt/sysimage*



* Configure the Grub 2 file with the following command

*nano /etc/grub2.cfg*

\*If you are more comfortable with other text editors such as vi /vim, you may use them by replacing the word “nano” from the command line with your desired text editor, however it is strongly recommended to use nano due to its simplicity

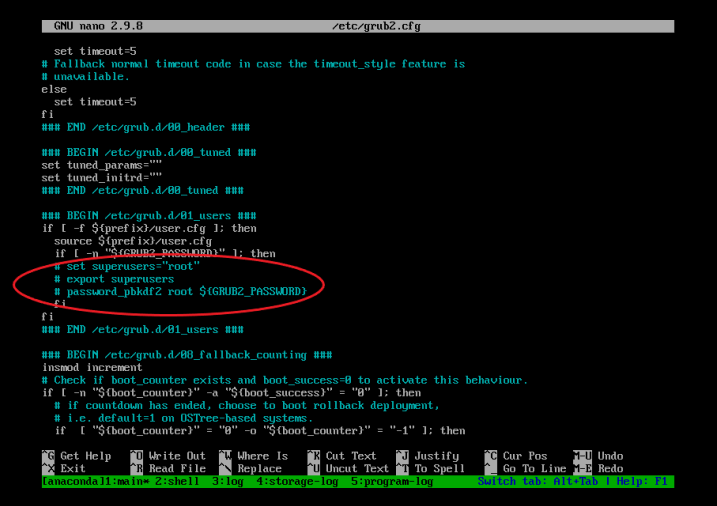
## 1.4 Disabling Grub login

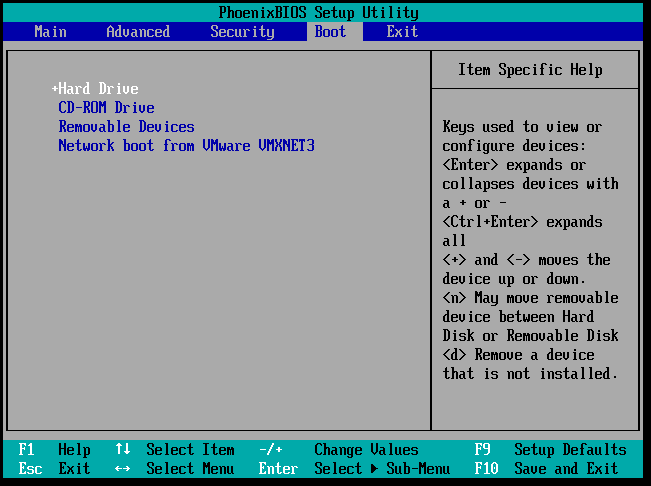
* You should now be in the grub2.cfg, head down the file and find the user credentials section and comment the following 3 lines, by adding a *#* at the start of each line

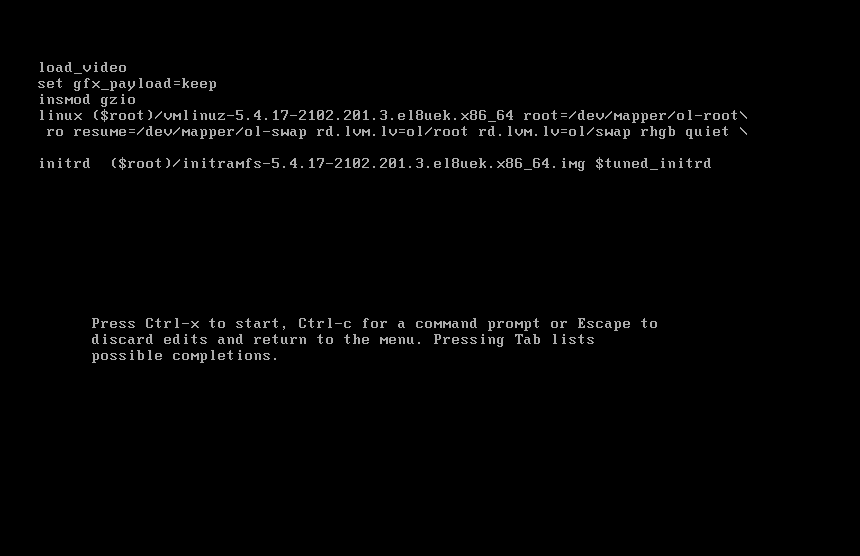
*set superuser**=”root”*

*export superusers*

*password\_pbkdf2 root ${GRUB2\_PASSWORD}*



* + Exit out of the file by pressing the “ctrl” and “x” button on your keyboard simultaneously. If prompted to save changes click “Y” on your keyboard
  + Exit out of the bash shell by typing *exit.*
  + Exit out of shell by typing *exit* again.
  + Configure the boot order by restarting the VM, and as it is booting up quickly press F2 multiple times.
  + Go to the boot tab and move “Hard Drive” back to the top with your “+” key and save it, this will boot the Hard Drive where the unlocked Grub system.
  + SUCCESS! You should now be able to access your grub parameter without the password to reset your root password. (Go to page 18, Chap 3 for the instructions on how to reset your root password)

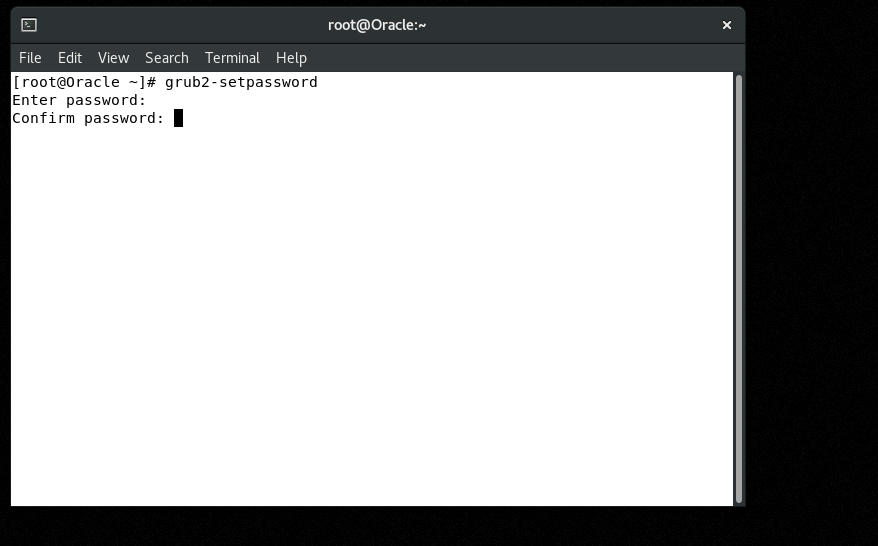


## 1.4 Resetting grub password

1. Once you reset your root password, log in to your root account with your new password
2. Open your command prompt
3. Reset your Grub password with the following command

*grub2-setpassword*

* Enter a password, and enter it once more to confirm password



## 1.5 Re-enabling Grub password

1. Now we can re enable the grub login by editing the grub2.cfg file by typing this command in the terminal

*nano /etc/grub2.cfg*

1. Uncomment out the 3 lines that was commented previously by removing the #, as shown in the following image



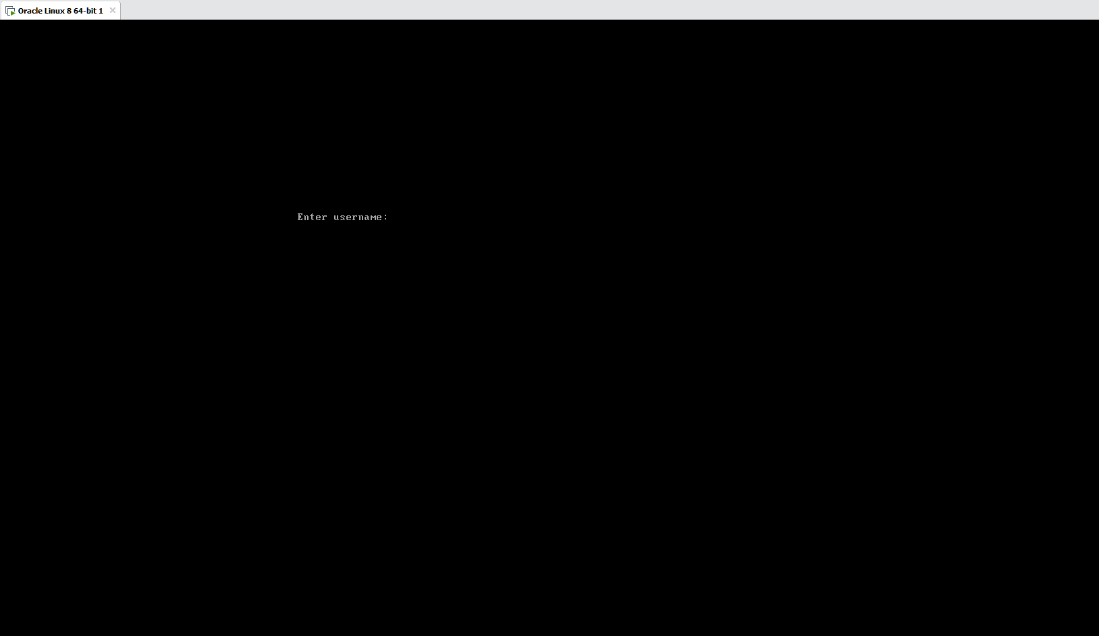
1. Exit out of the file by pressing the “ctrl” and “x” button on your keyboard simultaneously. If prompted to save changes, click “Y” on your keyboard

* Success! You have re-enabled your grub password; you will have to enter your Grub login username and password when you try to access the grub parameters. Enter *root* as your grub login username and use the password you reset at step 1.4 just now.
* You can now reset your root password, head over to page 18 of this document for the steps to reset your root password

# 2 Recovering GRUB password through digital forensics (Method 2)

|  |
| --- |
| For this to work, the GRUB password must be brute-forcible, which means the password must be able to be cracked.  The other technique would be to remove the /boot/grub/user.cfg in the raw file and convert the raw file back to a vmdk file. (Which removing the file can also be done via SSH with root permissions) |
| You may skip to “Using FTK imager to extract GRUB hash” if the OS is on the hard drive itself. However, you will need to extract the image file from your hard drive through another computer. (https://www.digitalforensics.com/blog/how-to-make-the-forensic-image-of-the-hard-drive/) |

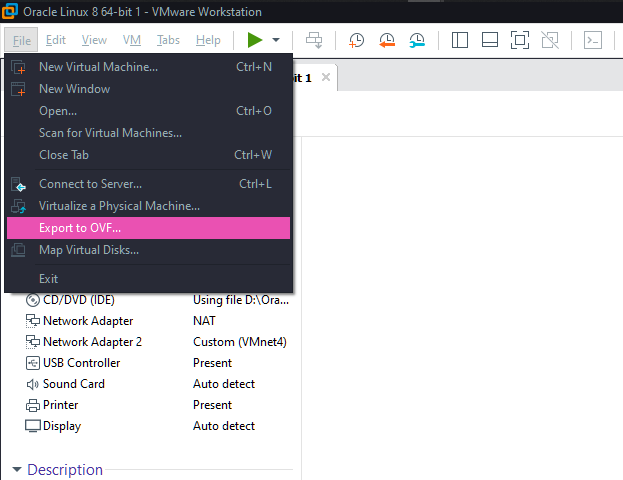
GRUB locked system:



## 2.1 Creating a forensic image

1. Click on Export to OVF... and save the file to your HDD (recommended)

* You should get 3 files: (.mf .ovf .vmdk)
* We will be converting the vmdk file to a raw file.



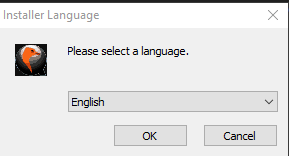
## 2.2 Converting image format

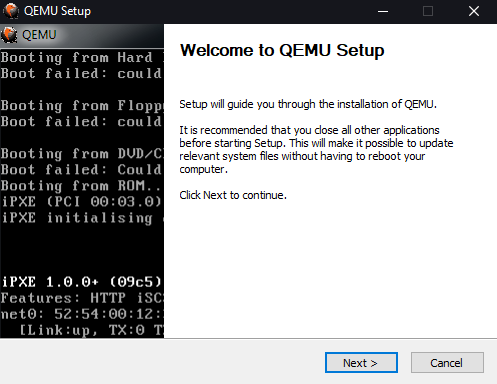
1. To convert the image to a raw format, we will use the following tool:

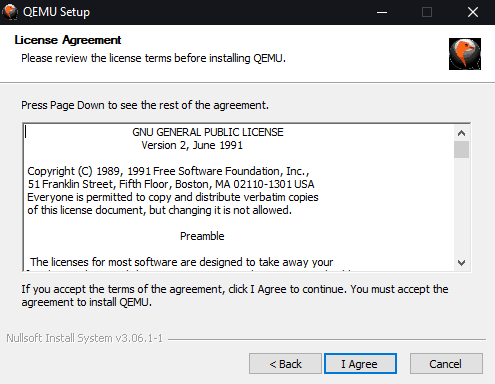
* ***Qemu-img***

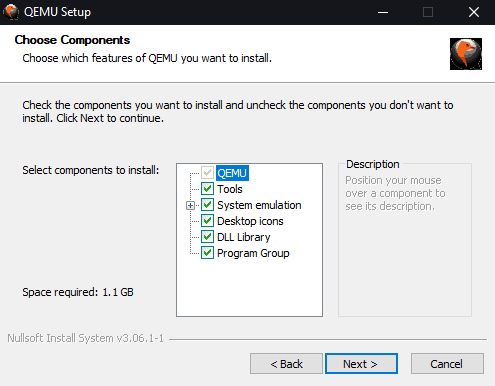
|  |
| --- |
| <https://www.qemu.org/download/#windows> |

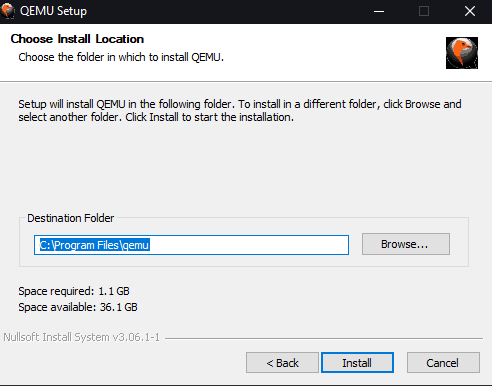
1. Run the installer:







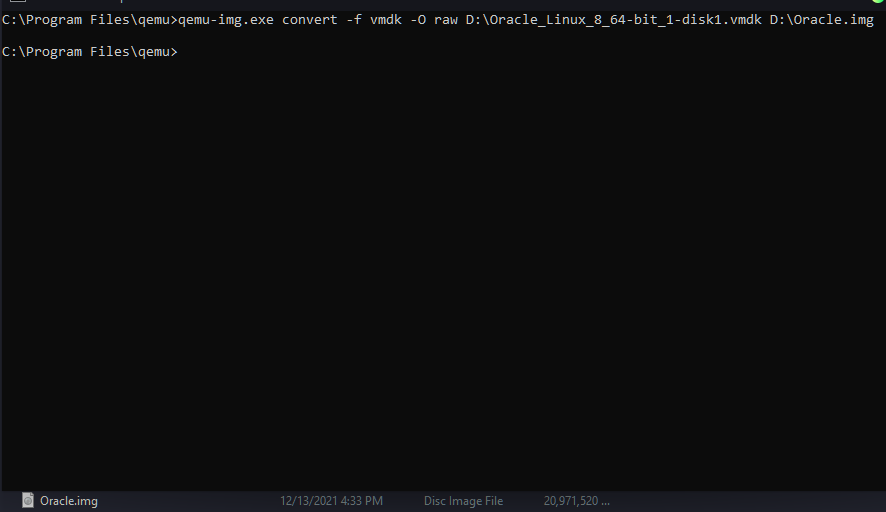




1. Open command prompt and type:

*cd "C:\Program Files\qemu"*

*qemu-img.exe convert -f vmdk -O raw <vmdk> <destination>*

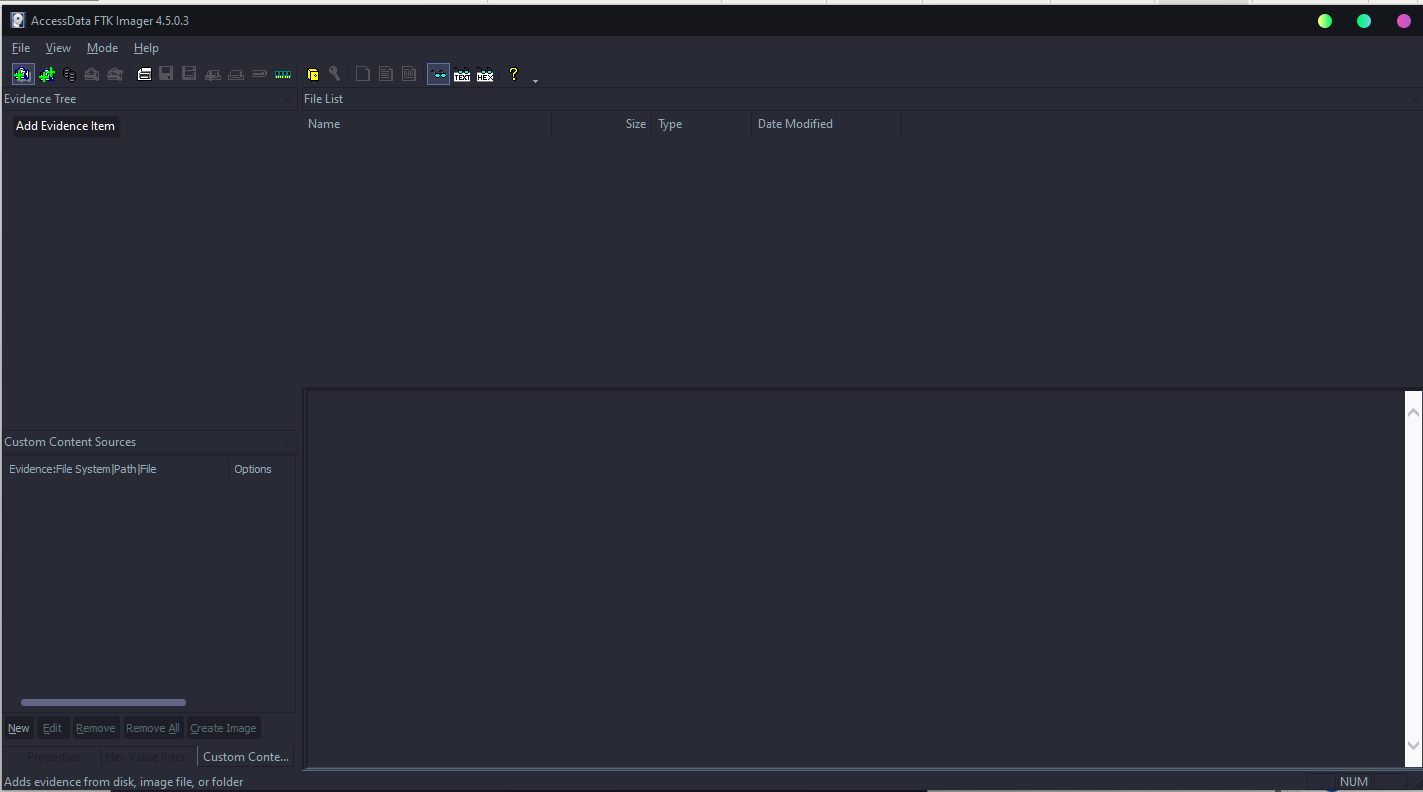


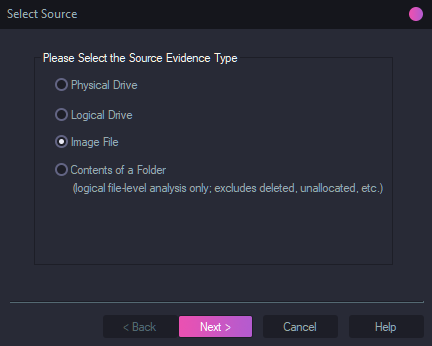
## 2.3 Using FTK imager to extract GRUB hash

1. This software will allow you to view most of the raw image file’s file.

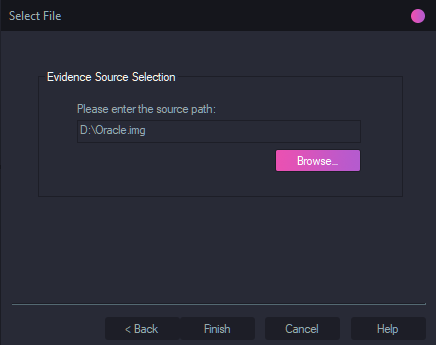
*FTK imager*

|  |
| --- |
| <https://www.exterro.com/ftk-imager> |

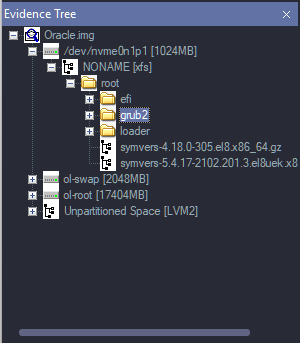
1. Click add evidence item:
2. Select Image File and click Next:



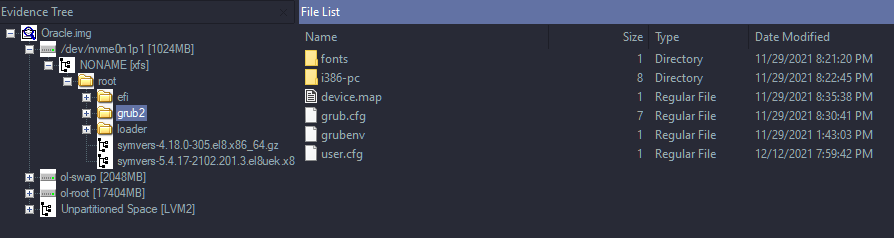
1. Add your raw image file and click finish:



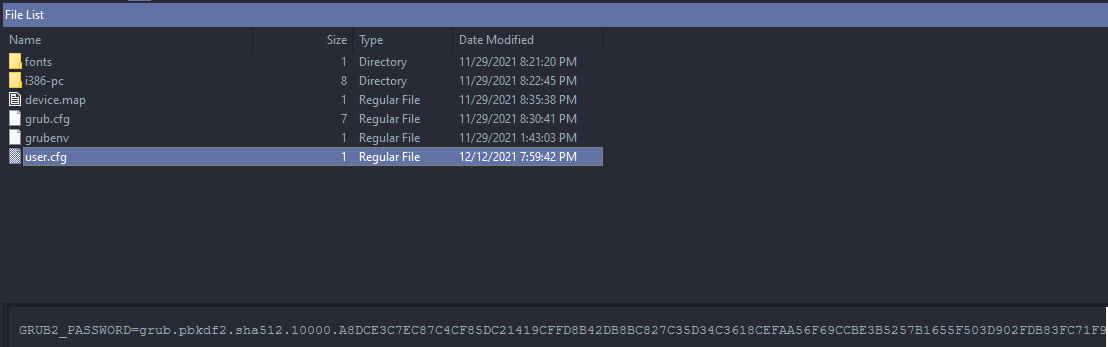
1. Now expand /dev/nvme0n1p1 in the image file, you should see grub2:



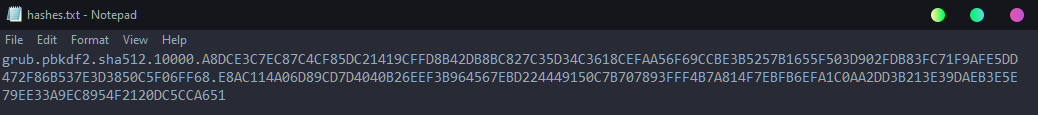
1. Click on grub2:



1. Click on user.cfg, this is the GRUB hash of the system:



1. Save the hash into a text file:



## 2.4 Brute forcing GRUB hash to get password for GRUB

* Now all that is left is to brute-force the hash using hashcat it to get the password. This activity may be very resource-intensive, it is recommended to close any processes that are not necessary and have sufficient cooling for your computer.
* Hashcat:

|  |
| --- |
| <https://hashcat.net/hashcat/> (hashcat binaries) |

1. First, for hashcat to run properly, the –m option will need to be provided. The option provided will specify what type of hash hashcat will brute force. (<https://hashcat.net/wiki/doku.php?id=example_hashes>)



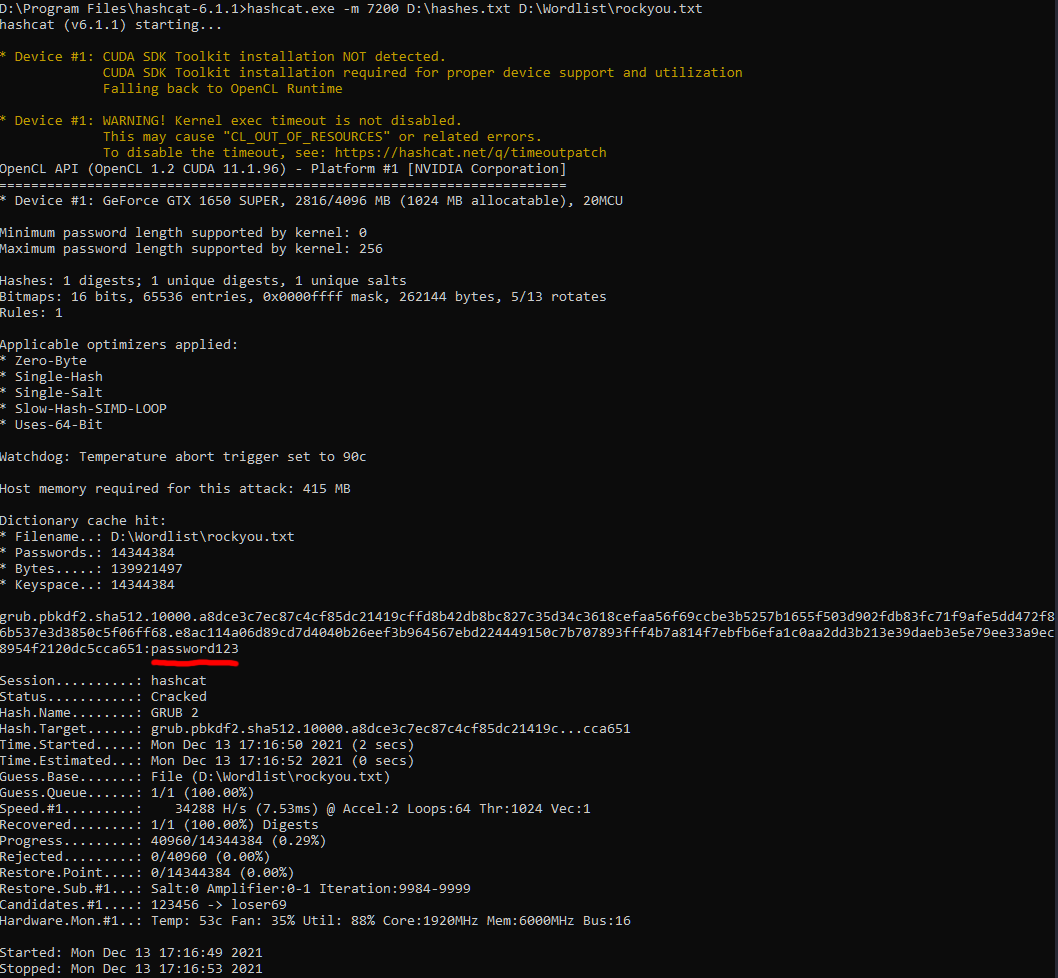
1. Secondly, hashcat will need a wordlist to brute force the hash. Rockyou.txt will be used:

* (<https://github.com/praetorian-inc/Hob0Rules/blob/master/wordlists/rockyou.txt.gz>)

1. Now we can brute force the hash:

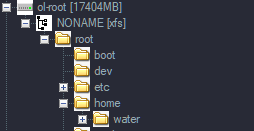
* Type:

*Hashcat.exe -m 7200 <hashes> <wordlist>*

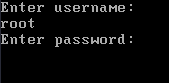


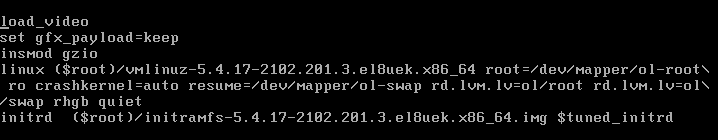
* Since the password was simple, it cracked instantly.

1. Now that the password is found, a username will be needed. This can be found through the /home folder in FTK imager or simply guessing “root” as the username:



1. Now log in to the grub:





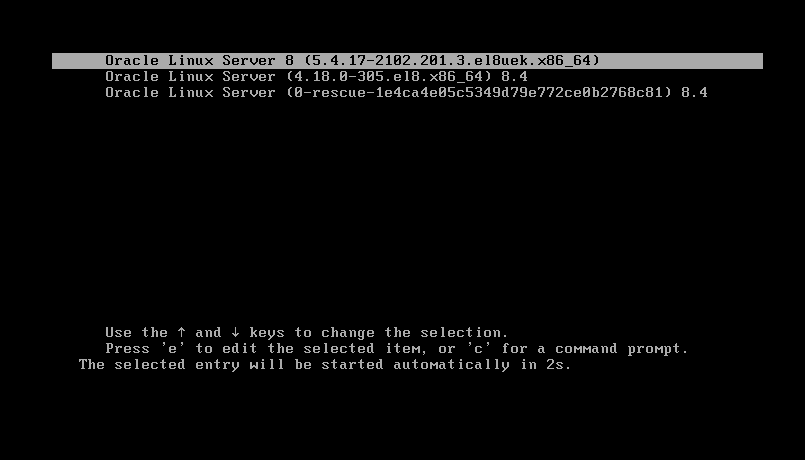
* Now we can reset the root account password

# 3 Root password Recovery

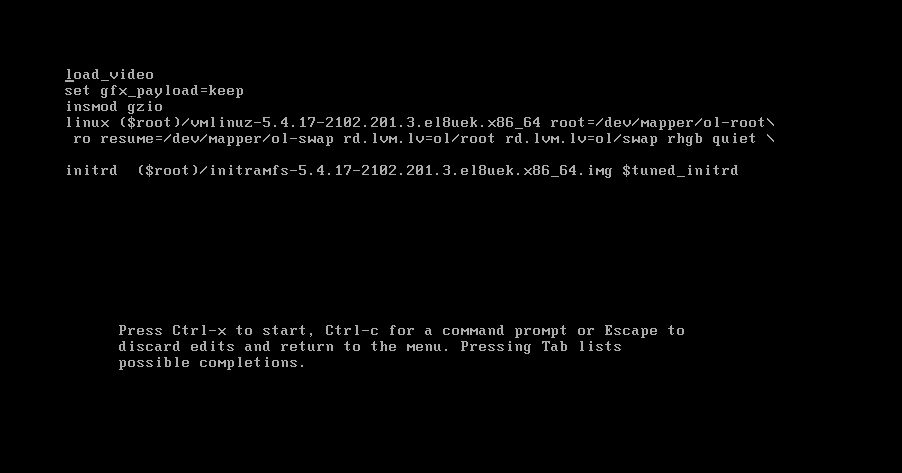
|  |
| --- |
| After disabling or recovering GRUB password with either method 1 or 2. Users can now proceed to recover their Root account, by accessing the emergency mode, remounting the mount point and changing the password |

## 3.1 Accessing emergency mode

1. If you have recovered your grub Password with method 2, log in to the GRUB. If you have bypassed GRUB with method 1, Restart the VM, while the GRUB boot menu is displayed (as shown below), quickly press “E” to interrupt the grub boot process



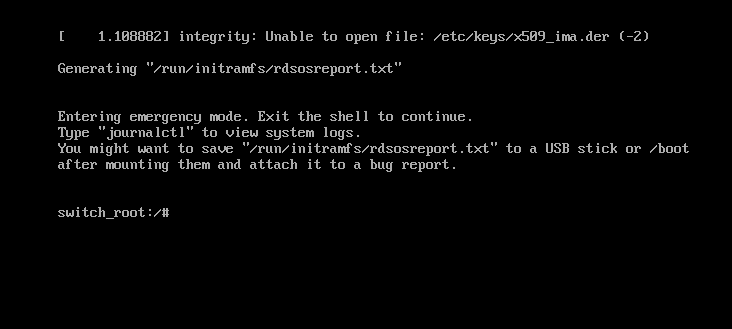
1. You should see the set parameters of the grub bootloader (as shown below)



1. Add the parameter *”rd.break”* after the Linux line (as shown below)



1. Press Crtl –x on your keyboard, this will resume the boot process
2. You will now be directed to the emergency mode CLI



## 3.2 Remounting

1. Remount /sysroot to read, write mode by typing the following command:

*mount –o remount,rw /sysroot*

1. Change current root mount to /sysroot by typing the following command:

*chroot /sysroot*

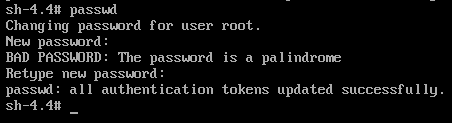
* These two steps are important before attempting to change the root password, because your Oracle VM is booted up from the ram disk, so if you attempt to change the root password before changing the root mount it will only be applied to the temporary files.

## 3.3 Changing password

1. You can now change the root password with the following command

*passwd*

1. Type in your new password. You may be prompted with a “BAD PASSWORD” warning. Simply retype the new password again to confirm the password or use a more complex password (as show below)



1. Exit the shell and reboot the system with the 2 following commands

*exit*

*Init 6*

* Your VM should be rebooted, and you would be able to login to your root account with the password.

# Conclusion

From method 1, we can see that the BIOS was easily accessible which allowed us to change the boot order to recover the GRUB locked system, this is a security vulnerability, which can easily be prevented via **configuring a password for the computer BIOS/UEFI**.

From method 2, we can see the importance of encrypting your hard drives, just by exporting the OS, we are able to extract files which completely bypasses the need of password to login to the user, which is why it is necessary to **encrypt sensitive parts of a hard drive** and **use strong passwords** to prevent potential brute forcing of the system.

So, in theory, you could potentially patch the system and follow every procedure to ensure that it would be impossible or incredibly hard to recover the root/GRUB password, but perfecting security can be extremely hard, even if all the steps (password for BIOS, strong passwords, encrypted hard drive) were done, there would still be vectors to exploit to recover the root password. Which is why we must accept the risk and ensure that only certain individuals have access to the system.

When recovering root password, we can see the importance of **having password protection for Grub**. Because without password protection for Grub, unauthorized users can have access to the root account by simply interrupting the grub boot process and resetting the root account password.