Assignment #1

NES 595, Fall 2018, Dr. Ahmad T. Al-Hammouri

**Due date: Tuesday 2/10/2018 at 11:55pm.**

Student Names & IDs :

صلاح حافظ بني حمد

محمد علي السلامين

Group #: 13

**Objectives:**

* To learn how to harden a Linux operating system during the boot process.

**Part I. Booting with single-user mode:**

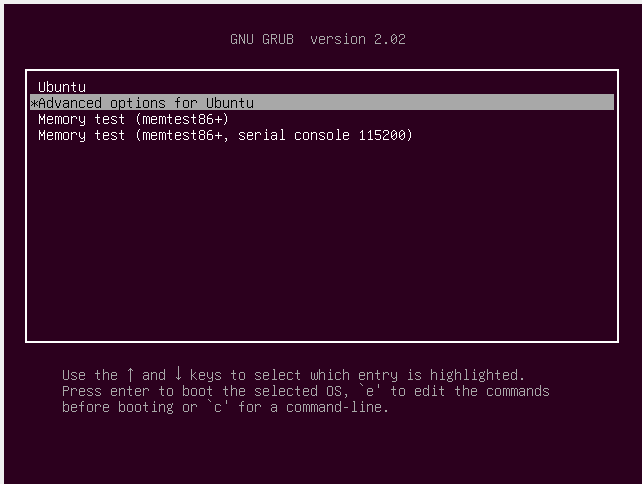
1. Boot into your Linux machine in **single-user mode**.

**Question 1.** Document/List, here, all steps to successfully boot in this mode. (*Be specific of changes*.)

When the grub loader opens choose advanced options for Ubuntu

And click “e”

Edit the command of the line started with “boot” word ,then instead of “quiet splash”,  
write “/bin/bash"



**Question 2.** What is the user name you are logging in onto the machine? What is the command to check for the user name? *Provide an appropriate screenshot*.

**root**

**command : whoami**

***C:\Users\mystro\Desktop\q2.PNG***

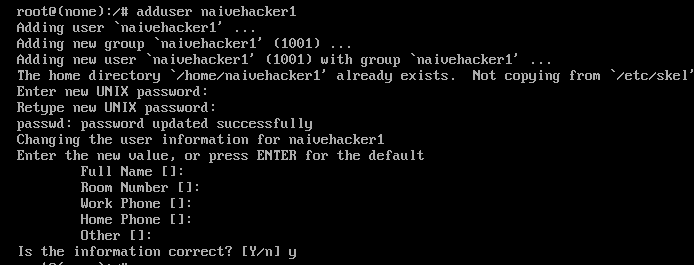
**Question 3.** What is *usually* the single-user-mode boot used for?

To get into the root , usually for maintenance such as forgetting password

1. On the command line prompt, add a new user, naivehacker1.

**Question 4.** What is the command? *Provide* *an appropriate screenshot of the command and its effect.*

adduser naivehacker1



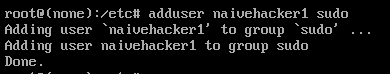
1. Edit the /etc/sudoers file. Make sure there is the following **exact** line. If not, just add it.

%sudo ALL=(ALL:ALL) ALL

1. Add naivehacker1 to the sudo group.

**Question 5.** What is the command? *Provide* *an appropriate screenshot of the command and its effect.*

adduser naivehacker1 sudo

****

**Question 6.** What is the purpose of adding a normal user to sudo group, or to sudoers file?

To give him the ability to use sudo command , which is allowed for the members in sudo group

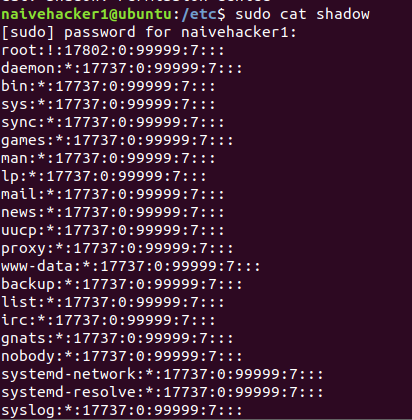
1. **Exit** single-user mode, and let the systems boot normally. Then, log in onto the machine with the newly added user naivehacker1.
2. Try to list the contents of the most **sensitive** and **confidential** file on the system, shadow, with the command cat /etc/shadow.

**Question 7.** *Provide a screenshot of the output*.

C:\Users\mystro\Desktop\q7.PNG

1. Now, try the previous step with the command sudo cat /etc/shadow.

**Question 8.** *Provide a screenshot of the output*.



1. Configure the boot loader (GRUB) to use a password.

**Question 9.** Document/List, here, all steps to configure a boot loader password.

First enter these commands

cd /etc/grub.d

grub-mkpasswd-pkdf2

then it will ask for password , and it will compute the hash

then copy the hash and then edit the file 40\_custom in grub.d directory

and then add the hash into it

then enter this command

sudo update-grub

**Question 10.** What is the benefit of adding a boot loader password?

When we add a password for the boot loader , no one can enter the single user mode

unless he knows the password.

**Part II. Booting using a live CD:**

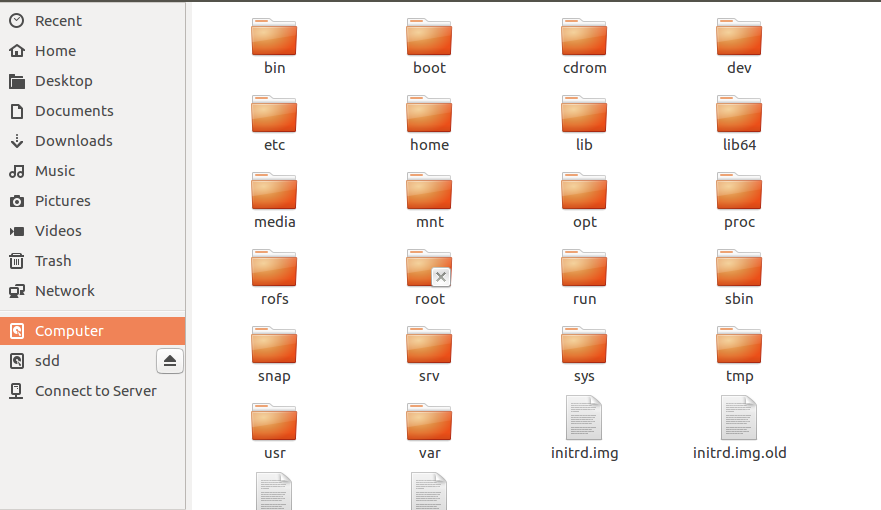
1. Completely power off your Linux machine.
2. Download the Ubuntu 16 *desktop* image (.iso file) appropriate to your environment, i.e., 32- or 64-bit, from http://de.releases.ubuntu.com/16.04. (**This needs to be performed on your alternative operating system, i.e., the host operating system**.)
3. If your Linux machine is deployed as a virtualized environment (e.g., with VirtualBox or VMware), attach the iso image file as a virtual optical drive (and tick the “Live CD/DVD” option). In the System configuration tab, make sure the Optical drive has a higher boot order than the Hard Disk. Then, go to step 5.
4. If your Linux machine runs as a dual boot operating system right on the physical hardware, you need to burn the iso image on a physical CD/DVD, or put it on a USB flash drive. You then need to enter the BIOS configuration, and make sure the CD (or, USB) has a higher boot sequence order than the Hard Disk.
5. Start the machine and let it boot off and run from the CD. **Do not choose to install Ubuntu**.
6. Once you logged in, click on the left menu bar on the disk icon to mount it (it is the volume with size of several gigabytes). To make sure the volume was correctly mounted, issue the command ls /media. There must be a second directory other than cdrom.

**Question 11.** How many Linux file systems are now there, i.e., how many different etc, home, boot, root etc. directories are there? *Provide* *an appropriate screenshot to defend your answer.*

*For cdrom directory*



For drive



1. Change to the second directory inside /media, i.e., not cdrom. Then, following the directory structure, change into the etc directory inside.
2. Edit the passwd file. **The last line must be the one starting with** naivehacker1. Add the following line at the end of file:

naivehacker2:x:1010:1010:,,,:/home/naivehacker2:/bin/bash

1. Edit the shadow file. **The last line must be the one starting with** naivehacker1. Add the following line at the end of file:

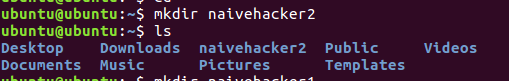
naivehacker2:U6aMy0wojraho:17587:0:99999:7:::

**Question 12.** What is the difference between the passwd and shadow files?

The passwd file contains passwords of the system files, while shadow file contains those passwords hashed.

1. Edit the group file, and add naivehacker2 to the sudo group just after the existent naivehacker1. (They must be separated by a comma.)
2. Following the directory structure starting from /media, change into the home directory inside.
3. Inside, create a new directory named naivehacker2.

**Question 13.** What is the command? *Provide* *an appropriate screenshot of the command and its effect.*



1. Change the permissions of this newly created directory to give *full access* to it to *everyone*.

**Question 14.** What is the command? *Provide* *an appropriate screenshot of the command and its effect.*





1. Power off the machine, remove the iso image from the virtual drive, and then start the machine.
2. Log in onto the machine with the newly added user naivehacker2 supplying no password!!! (I.e., select the user and just hit enter.)
3. Try to list the contents of the most **sensitive** and **confidential** shadow file on the system with the command sudo cat /etc/shadow. (No password is required!!!)

**Question 15.** *Provide a screenshot of the output*.

**Question 16.** If the Linux operating system is running on the hardware directly (i.e., no virtualization), what should you do to prevent an attacker getting hold of your computer from booting into your operating system via a Live CD?

**We could add a password on the hyper visor.**

**Part III. Installing Linux with full disk encryption:**

1. Perform a new Linux operating system install. When prompted during the guided process, you **must choose to encrypt the disk**. (To speed up things, you may choose to make a *bare-minimum* install.)

**Question 17.** Can you boot into this new system in single-boot mode and add an arbitrary user (as in Part I above) *without supplying the correct password you used to encrypt the disk during the installation process*?

**No**

**Question 18.** Can you boot into this new system using a Live CD and add an arbitrary user (as in Part II above) *without supplying the correct password you used to encrypt the disk during the installation process*?

**no**

**Question 19.** By using disk encryption, is an operating system and its data protected against all threats? *Defend your answer*.

**No , because there’s no system that 100% secure there’s always a way to get in!**

**Deliverables:**

Answer all questions (1–19) above, provide/paste the required *appropriate* screenshots, and upload the file to the elearning via the provided link. Do **NOT** send it via e-mail or a message from within the elearning *even before the deadline* ***because it will be deleted tacitly***.