**Hardning the OS (debian)**

First I have installed Linux distribution of Debian version 11 and I have used the open source project Lynis to test the security of my OS which is basically a script you run on debian and it will give you the percentage of your OS , I will walk you throw the process how I installed Lynis and how I have harden my debian to have a secure OS

1. **Installing Lynis:**

* Download the Lynis package by executing the following command:

“wget <https://cisofy.com/files/lynis-3.0.8.tar.gz>”

* Extract the downloaded package using the following command:

“tar xvfz lynis-3.0.4.tar.gz”

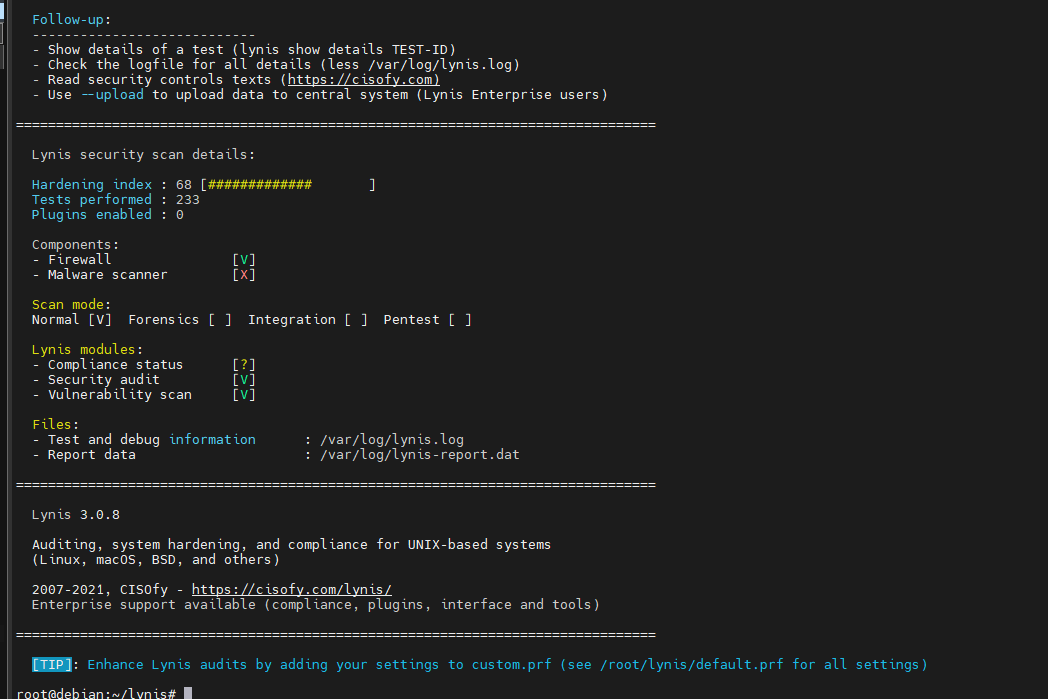
* Navigate into the lynis directory by running:

“cd lynis”

* To perform a system audit with Lynis, run the following command:

Lynis now initiate the security audit of my system and displayed the results in the terminal.

As the screenshot shows :



You can see that the rate of OS is 68% based on 233 tests performed

So now it’s our job to harden the OS and make it more secure.

1. **password protection with GRUB2:**

When I have run Lynis using the command “./lynis audit system” it output this weakness : “Checking for password protection [ NONE ]”. Which mean that my OS does not have password protection enabled for a specific component. To solve it you have to follow this steps:

* open the file /etc/default/grub use the following command : nano /etc/default/grub
* Find the line that starts with : “GRUB\_CMDLINE\_LINUX\_DEFAULT” and put this parameters in the first “splash grub.pbkdf2.sha512=1 ”
* Your file will look : GRUB\_CMDLINE\_LINUX\_DEFAULT="quiet splash grub.pbkdf2.sha512=1"
* Set a GRUB2 password using this command : grub-mkpasswd-pbkdf2
* Copy the generated password hash that shows in the terminal
* Update the GRUB configuration file use this command to open the file nano /etc/grub.d/40\_custom
* Add the this lines at the end of the file:

set superusers="username"

password\_pbkdf2 username generated\_password\_hash

The username must be replayed with your username

* Then save the file Ctrl+O and Ctrl+X
* Update GRUB2: update-grub

And after you complete all this steps it will show:



And the rate of OS will be 69%

**NOTE: all this steps must be done using the root privileges.**

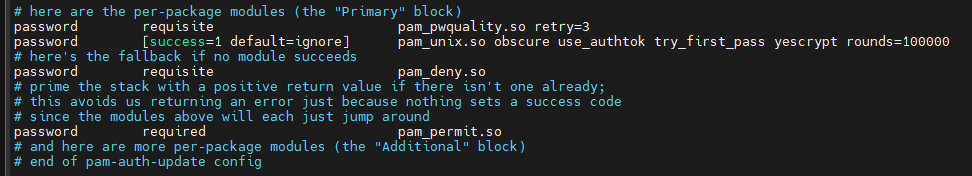
1. **Secure Authentication by configuring pam :**

* Configure a hashing method for the Password:

You just need to update the commn-password file which you can do it using a text editor:

You can just use this command: nano /etc/pam.d/common-password

And then look for the line where you find pam.unix.so and I update it like in the screenshot



* Configure password hashing rounds:

It’s the same file that must be configured just see the same command in the section before and put this parameter: rounds= (the number of rounds needed).

* Configure password aging (minimum, maximum):

Now I have updated the login.defs file to do it use this command :

nano /etc/login.defs and configure this parameters according to your need:

PASS\_MAX\_DAYS 100

PASS\_MIN\_DAYS 7

* Determining default umask for files :

Open the file that Lynis tool detected that must be update using a text editor and put in the end of the file: umask 027

1. **Set the permission of recommended files:**

After you run the script, you will in the result some files that you have to harden the permissions of them.

I used “chown” command to set the file owner and group ownership to “root”

And the “chmod” command to set correct permission (read and execute).

1. **Mount directories recommended**

Here after got the result of the lynis script. There is a number of directories you will be recommended to mount like /home /tmp /var

So let me show an example of those directories the way I mount it (/tmp):

* Create a new directory : mkdir /mnt/tmp\_mount
* Then I mounted the /mnt/tmp\_mount : mount /dev/sda /mnt/tmp\_mount
* Copy the content of /tmp to /mnt/tmp\_mount : cp –a /tmp/. /mnt/tmp\_mount/.
* Now we have to add the new entry to the /etc/fstab , add this line to the file

/dev/sdX1 /tmp ext4 defaults 0 2

* Finally mount the /tmp with the updated /etc/fstab : mount –a

1. **Configure the networking**

First I have to make sure that my OS at least have 2 working DNS servers

To do that you just have to configure /etc/resolv.conf file

* Open the file using : nano /etc/resolv.conf
* Append those to servers like a backup to the DNS server you will find aleady:

nameserver 8.8.8.8

nameserver 8.8.4.4

after this you can close any open port that you don’t need.

There are other things we have done to reduce the risk like installing malware scanner, IDS/IPS, accounting software, firewall, auto upgrade software and some other things….

I can’t write all the steps that we have did in order to harden the Debian OS that we have used to deploy our SOC in it, because it will be a too long.

But here is the percentage of our harden Debian 11 OS for now:

