Lab – Hardening a Linux System

Objectives

Demonstrate the use of a security auditing tool to harden a Linux system.

Background / Scenario

Auditing a system for potential misconfigurations or unprotected services is an important aspect of system hardening. Lynis is an open source security auditing tool with an automated set of scripts developed to test a Linux system.

Required Resources

- PC with Ubuntu 16.04 Desktop LTS installed in a VirtualBox or VMware virtual machine.

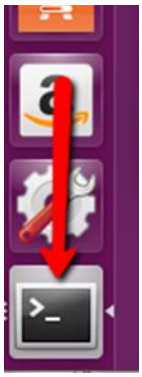
Step 1: Open a terminal window in Ubuntu.

a. Log in to Ubuntu using the following credentials:

User: **cisco**

Password: **password**

b. Click the terminal icon to open a terminal window.



Step 2: The Lynis Tool

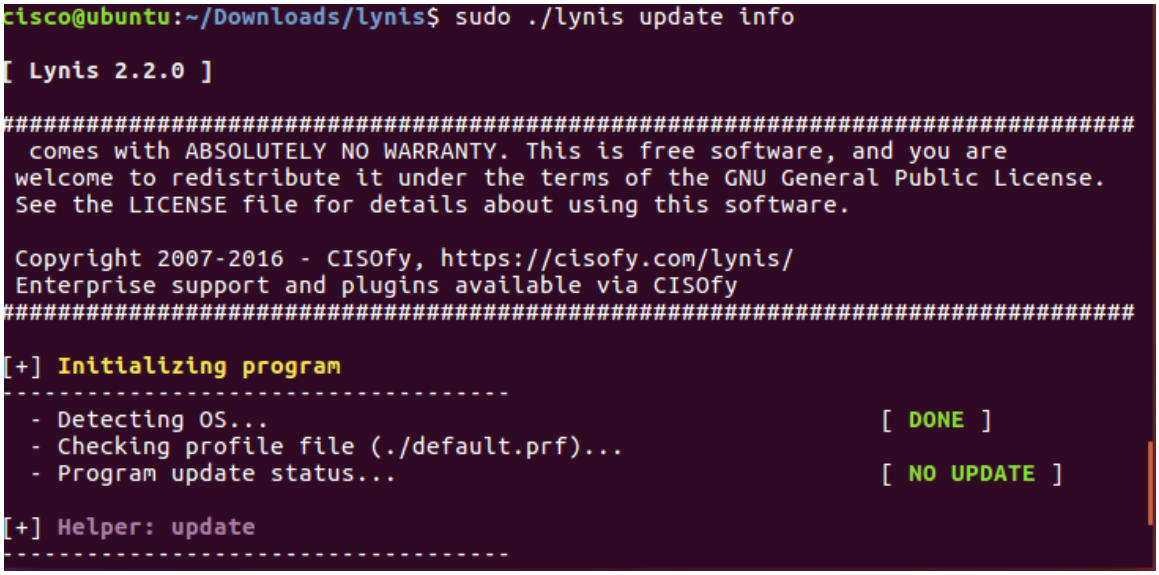
a. At the command prompt, enter the following command to change to the lynis directory:

```
cisco@ubuntu:~$ cd Downloads/lynis/
```

```
cisco@ubuntu:~$ cd Downloads/lynis/
cisco@ubuntu:~/Downloads/lynis$
```

b. At the command prompt, enter the following command and enter the password **password** when prompted:

```
cisco@ubuntu:~/Dowloads/lynis$ sudo ./lynis update info
```

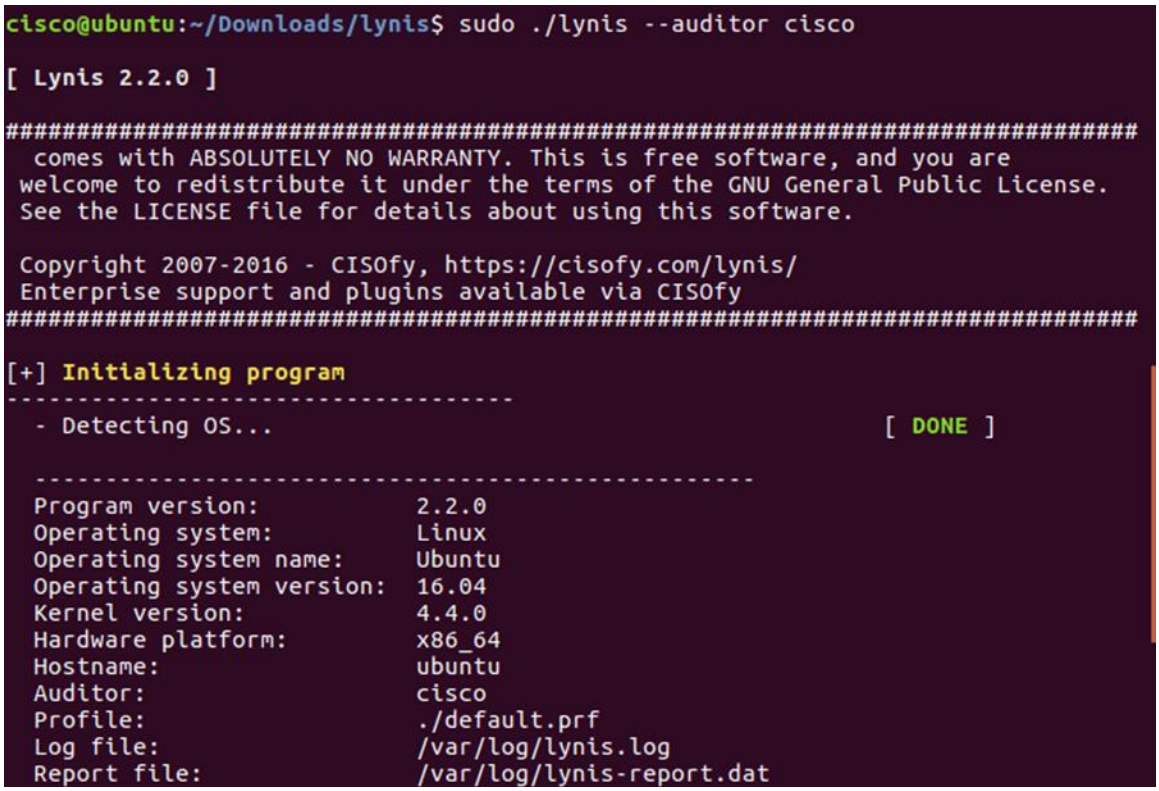


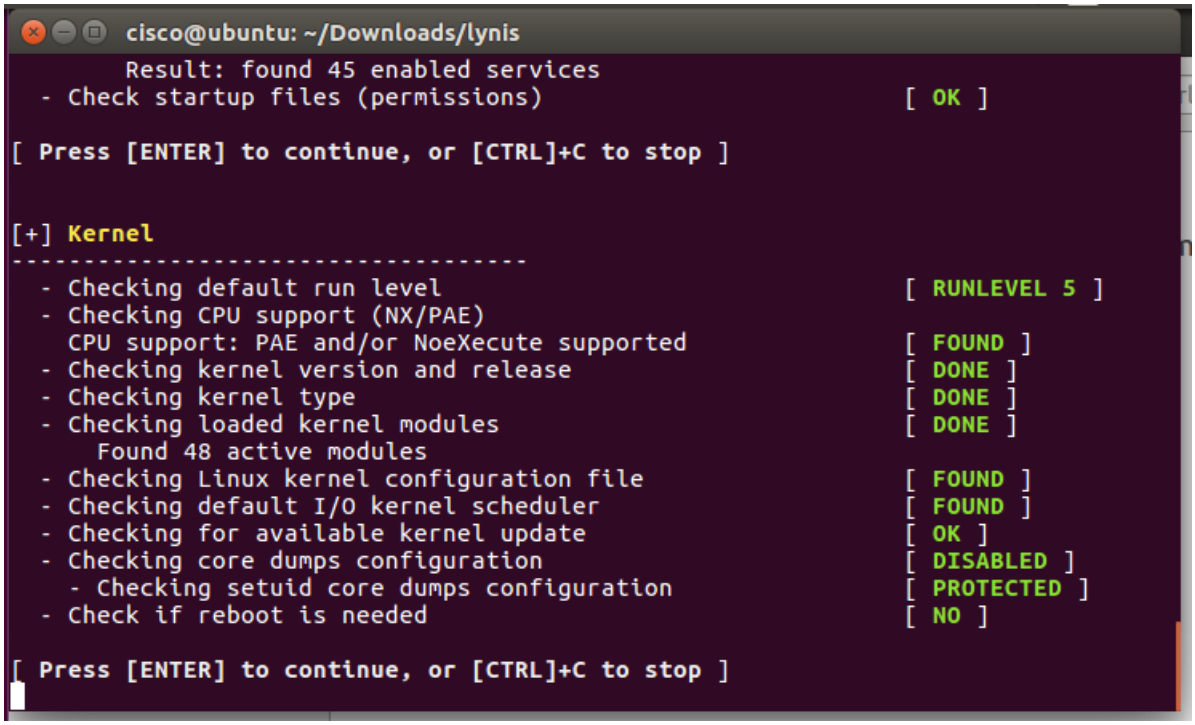
This command verifies that this is the latest version and updates for the tool at the time of writing of this lab.

Step 3: Run the Tool

a. Type the following command in terminal and press **Enter**:

```
cisco@ubuntu:~/Downloads/lynis$ sudo ./lynis --auditor cisco
```

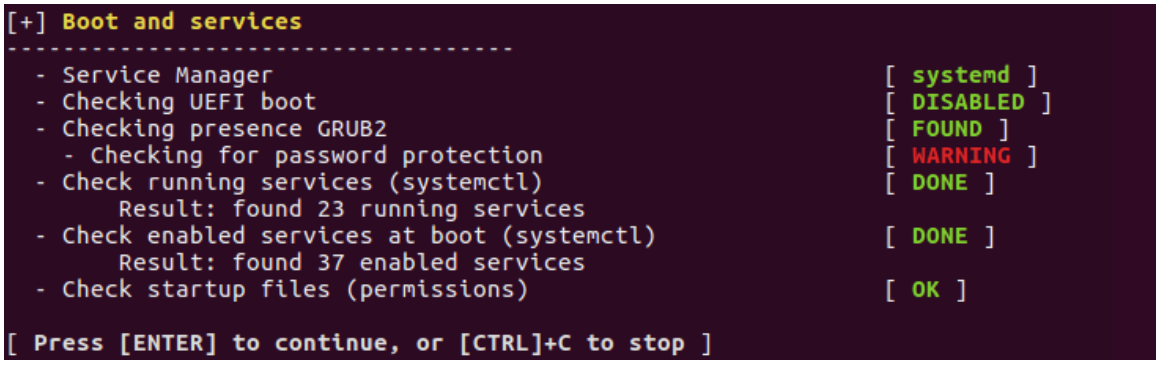




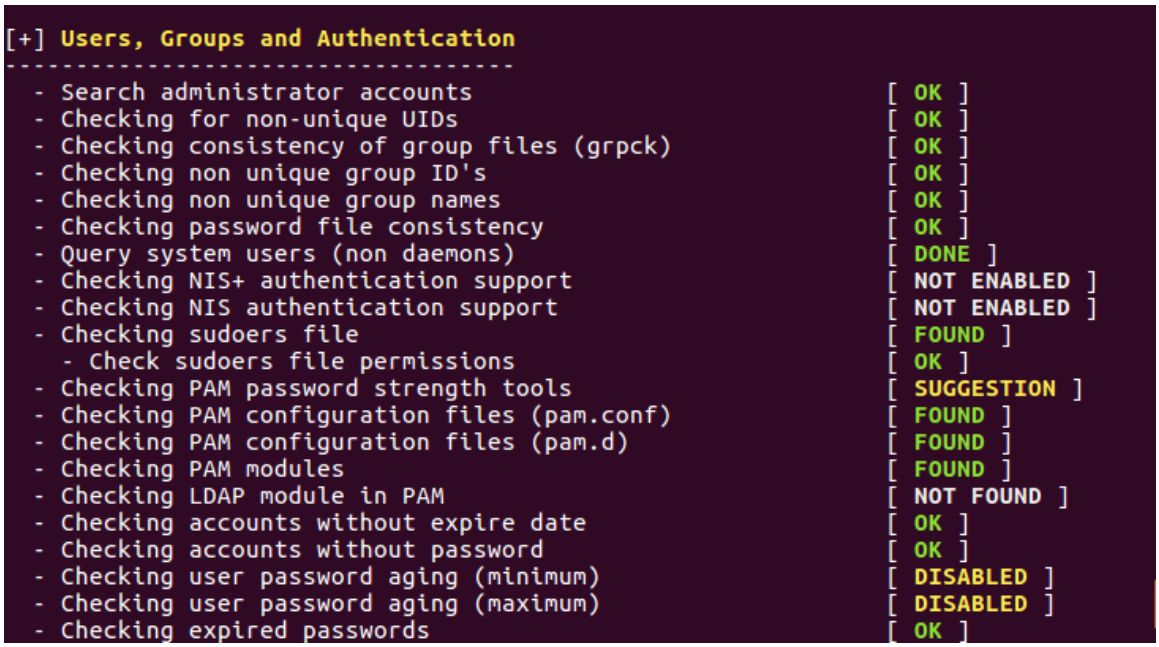
As displayed above, the tool will begin auditing using the user **cisco** as the auditor.

Notice: You will receive **warnings**.

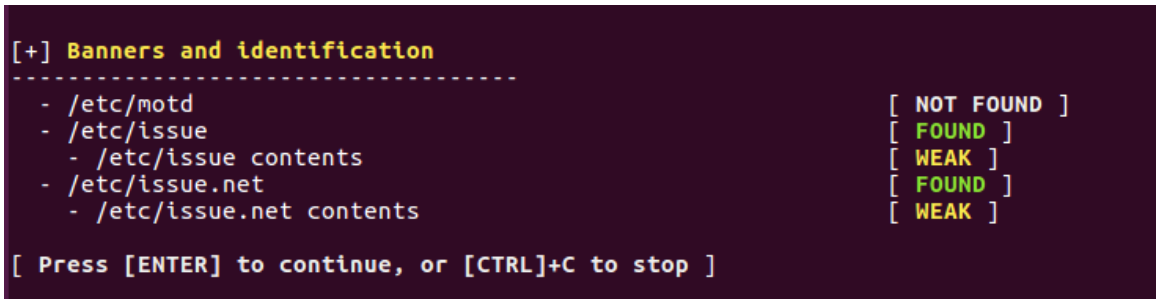
b. To continue with each stage of the audit press **Enter**. You will receive warnings as shown below.



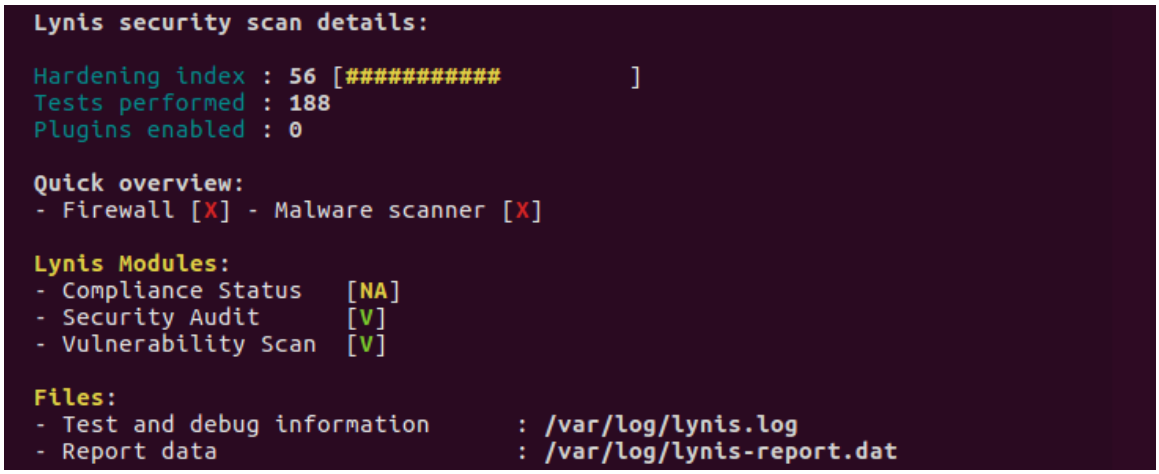
c. You will receive suggestions, as shown below.



d. You will receive a notification for any configuration that is weak as shown below:

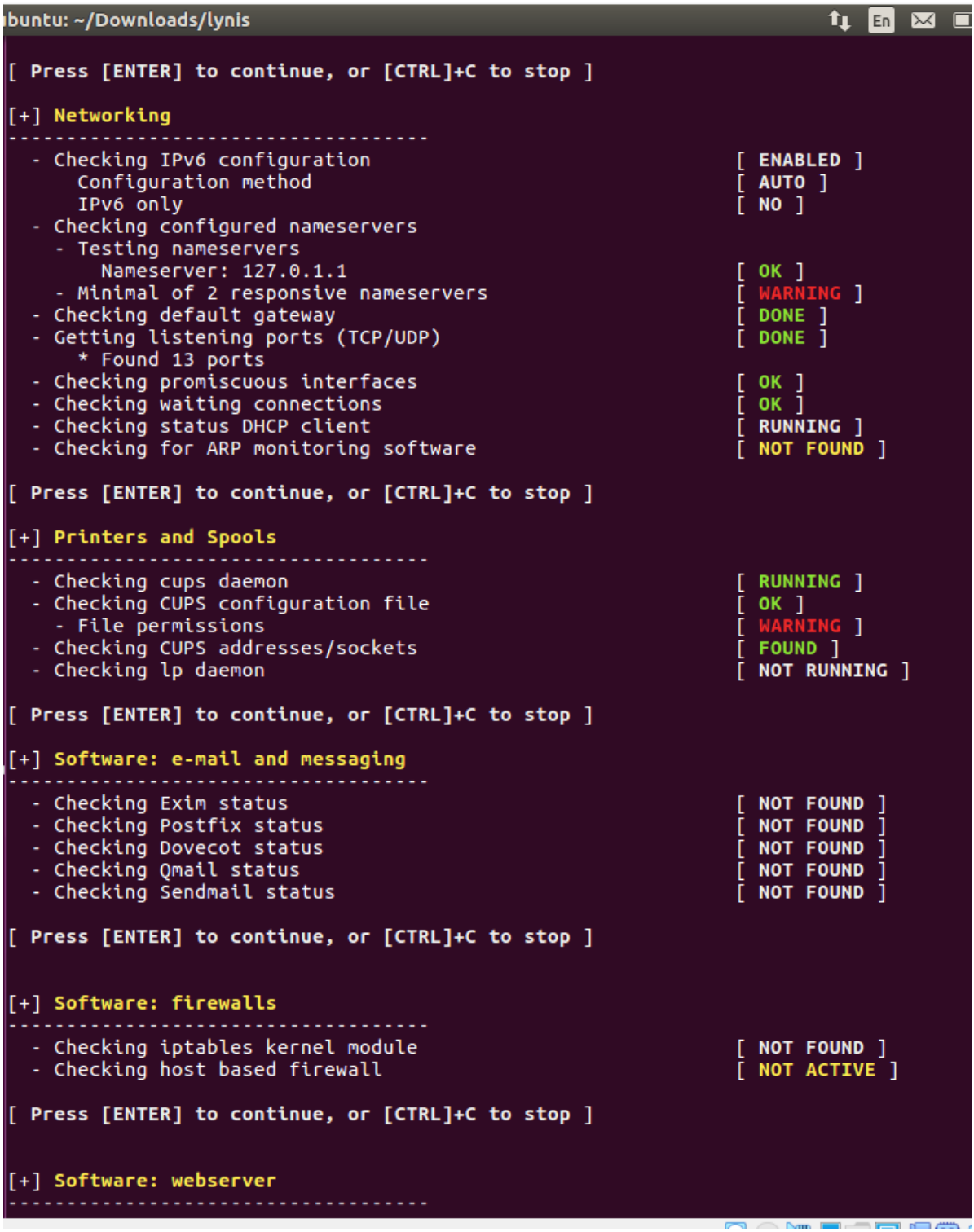


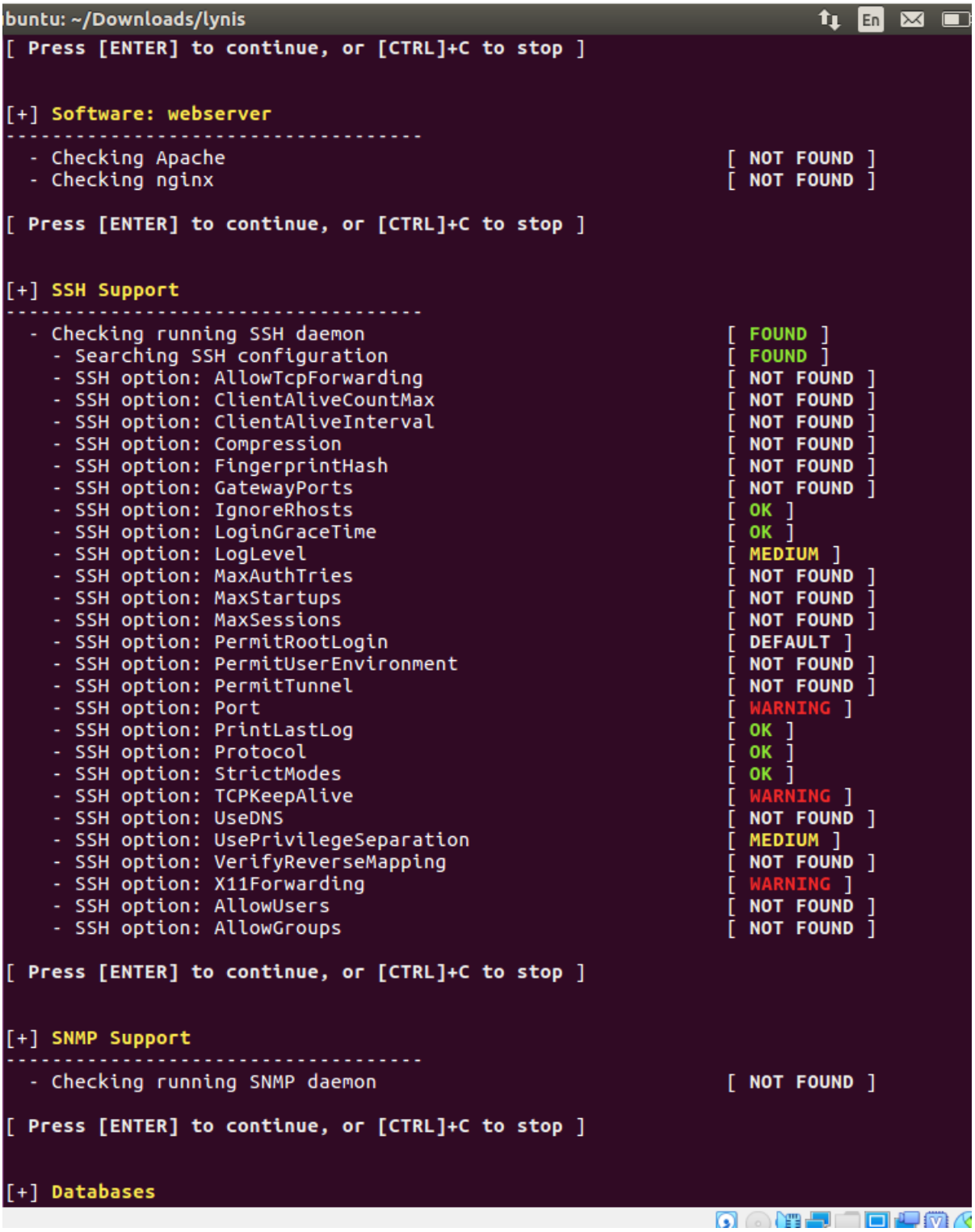
e. You will receive detailed security enhancement suggestions as well as a final summary which provides the location where you can find the log file.

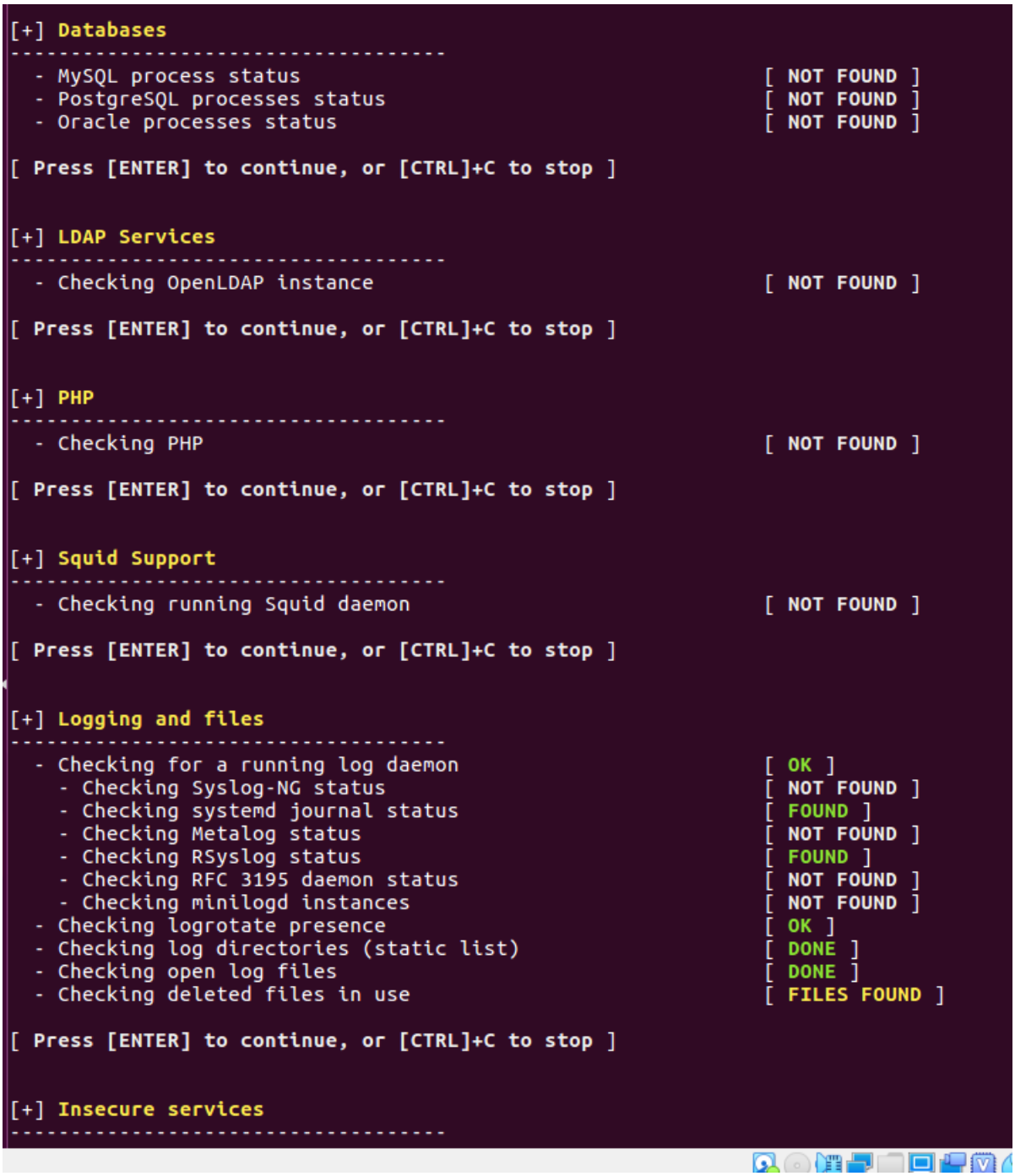


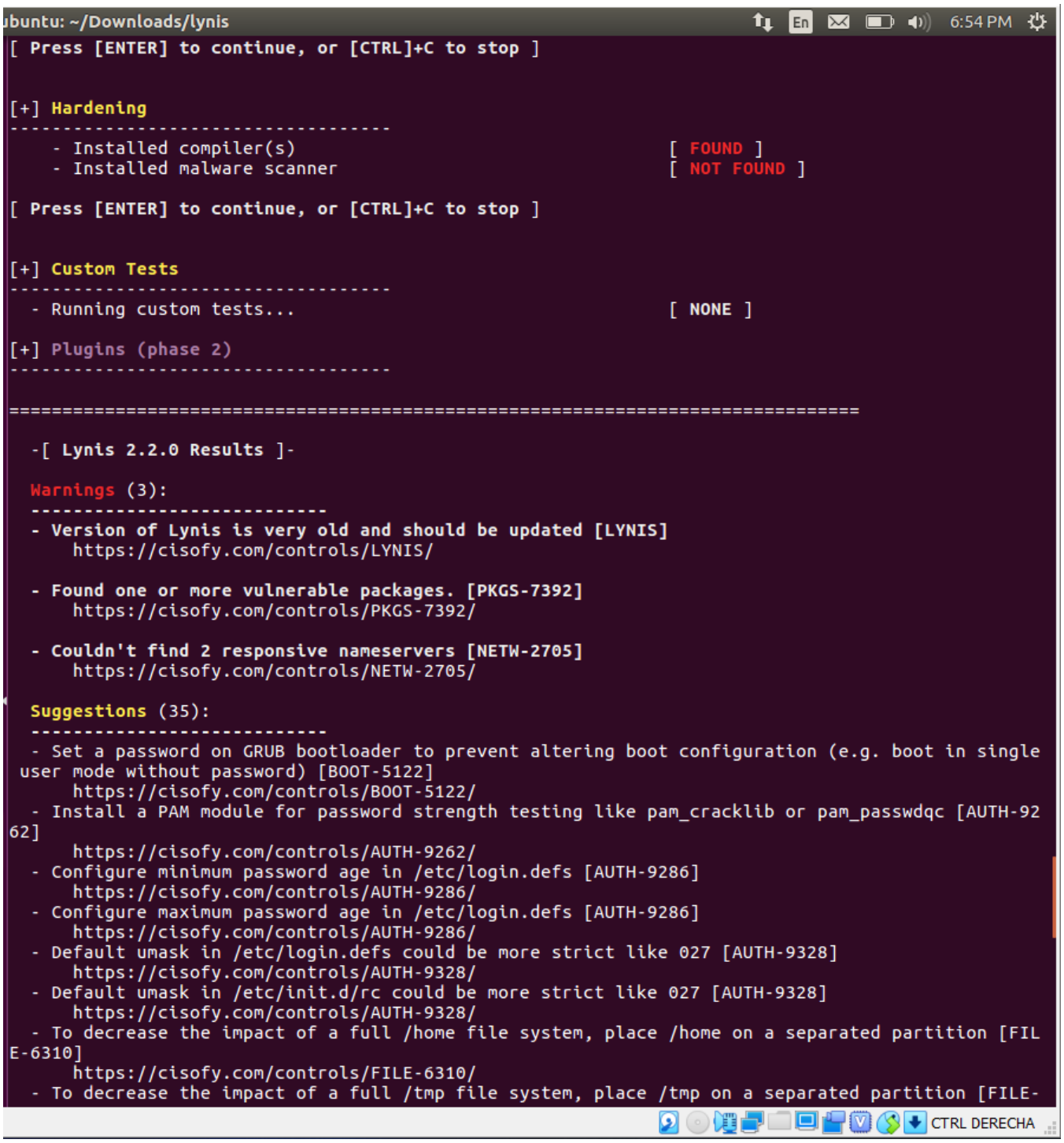
Step 4: Review Results

```
[+] Plugins (phase 1)
------------------------------------
 Note: plugins have more extensive tests, which may take a few minutes to complete

  - Plugins enabled                                          [ NONE ]

[+] Boot and services
------------------------------------
  - Service Manager                                          [ systemd ]
  - Checking UEFI boot                                       [ DISABLED ]
  - Checking presence GRUB2                                  [ FOUND ]
    - Checking for password protection                       [ WARNING ]
  - Check running services (systemctl)                       [ DONE ]
        Result: found 26 running services
  - Check enabled services at boot (systemctl)               [ DONE ]
        Result: found 45 enabled services
  - Check startup files (permissions)                        [ OK ]

[ Press [ENTER] to continue, or [CTRL]+C to stop ]

[+] Kernel
------------------------------------
  - Checking default run level                               [ RUNLEVEL 5 ]
  - Checking CPU support (NX/PAE)
    CPU support: PAE and/or NoeXecute supported              [ FOUND ]
  - Checking kernel version and release                      [ DONE ]
  - Checking kernel type                                     [ DONE ]
  - Checking loaded kernel modules                           [ DONE ]
      Found 49 active modules
  - Checking Linux kernel configuration file                 [ FOUND ]
  - Checking default I/O kernel scheduler                    [ FOUND ]
  - Checking for available kernel update                     [ OK ]
  - Checking core dumps configuration                        [ DISABLED ]
    - Checking setuid core dumps configuration               [ PROTECTED ]
  - Check if reboot is needed                                [ NO ]

[ Press [ENTER] to continue, or [CTRL]+C to stop ]

[+] Memory and processes
------------------------------------
  - Checking /proc/meminfo                                   [ FOUND ]
  - Searching for dead/zombie processes                      [ OK ]
  - Searching for IO waiting processes                       [ OK ]

[ Press [ENTER] to continue, or [CTRL]+C to stop ]

[+] Users, Groups and Authentication
------------------------------------
  - Search administrator accounts                            [ OK ]
  - Checking for non-unique UIDs                             [ OK ]
  - Checking consistency of group files (grpck)              [ OK ]
  - Checking non unique group ID's                           [ OK ]
```









a. Scroll up to the results section after the tool is finished running.

How many Warnings did you receive? 8

How many Suggestions did you receive? 35

Scroll through the suggestions and select one. You will research a suggestion that you can implement to address the issue.

Which suggestion are you addressing?

AUTH-9262

What is your suggested solution?

El sistema necesita comprobar la seguridad de las contraseñas para mantener su robustez, se soluciona implementando un módulo PAM como passwdqc o cracklib.

References

Lynis: https://cisofy.com/lynis/