Lab – Hardening a Linux System

1. Objectives

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

1. 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.

1. Required Resources

* PC with Ubuntu 16.04 Desktop LTS installed in a VirtualBox or VMware virtual machine.
  1. Open a terminal window in Ubuntu.
     1. Log in to Ubuntu using the following credentials:

User: **cisco**

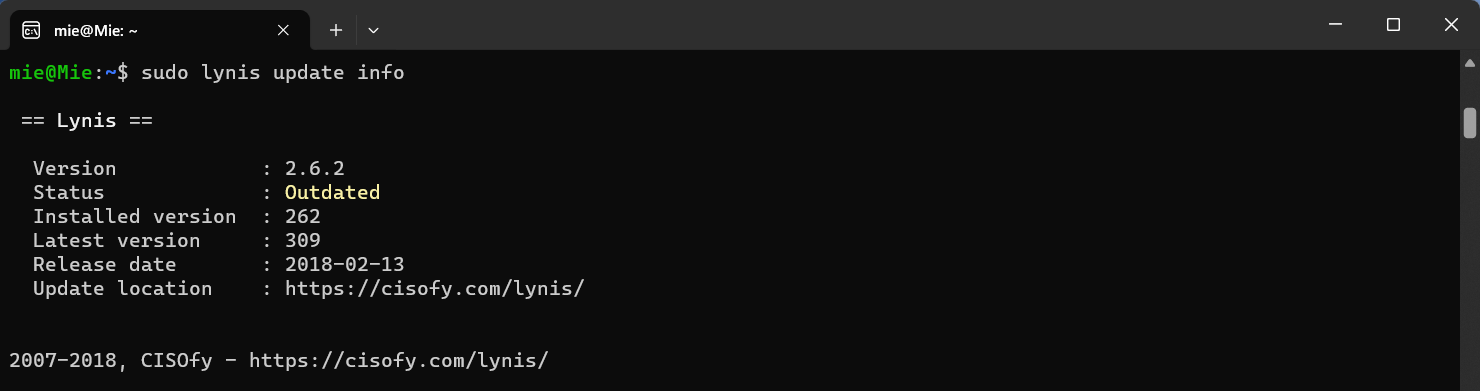
Password: **password**

* + 1. Click the terminal icon to open a terminal window.
  1. The Lynis Tool
     1. At the command prompt, enter the following command to change to the lynis directory:

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

* + 1. At the command prompt, enter the following command and enter the password **password** when prompted:

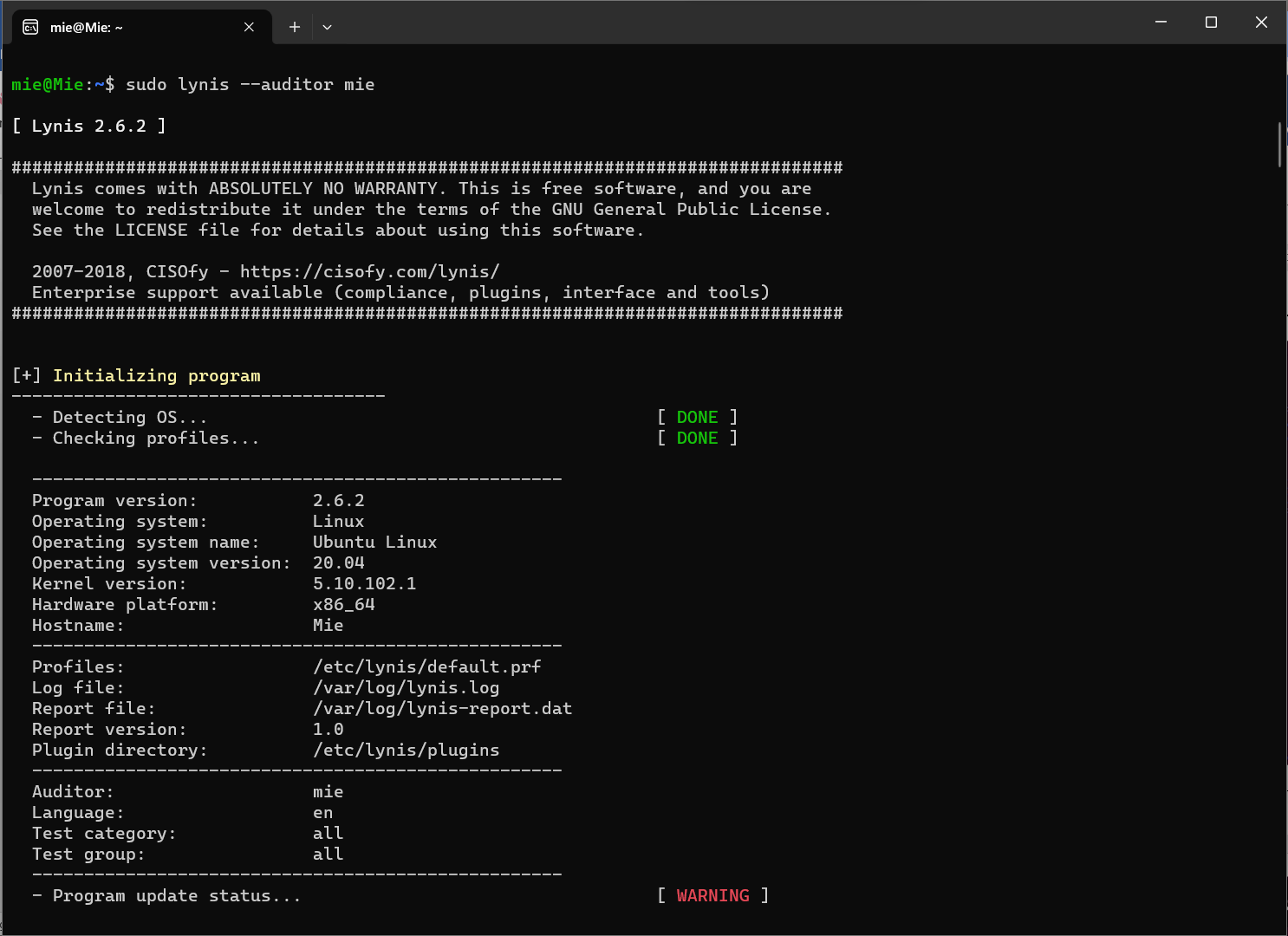
cisco@ubuntu:~/Dowloads/lynis$ **sudo ./lynis update info**



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

* 1. Run the Tool
     1. Type the following command in terminal and press **Enter**:

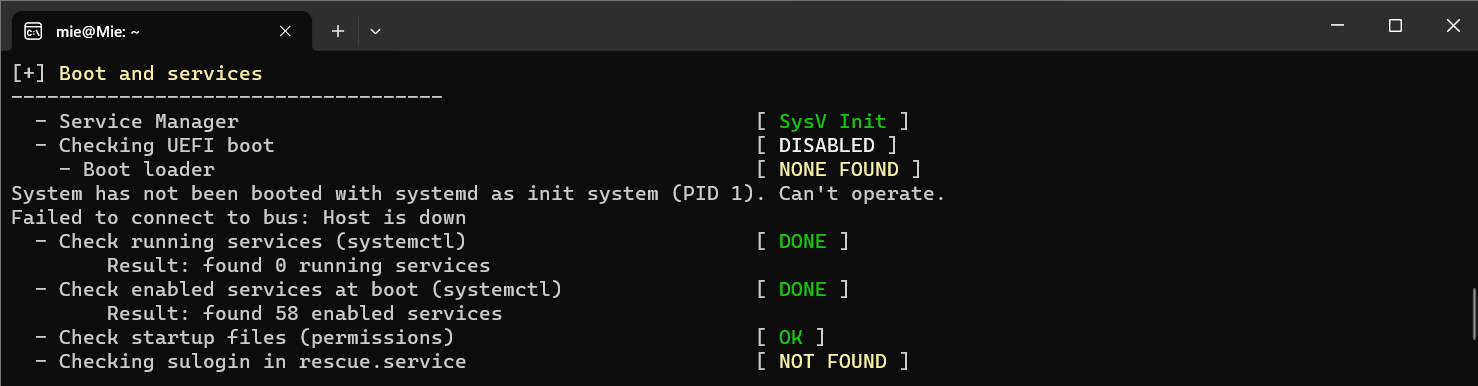
cisco@ubuntu:~/Downloads/lynis$ **sudo ./lynis --auditor cisco**



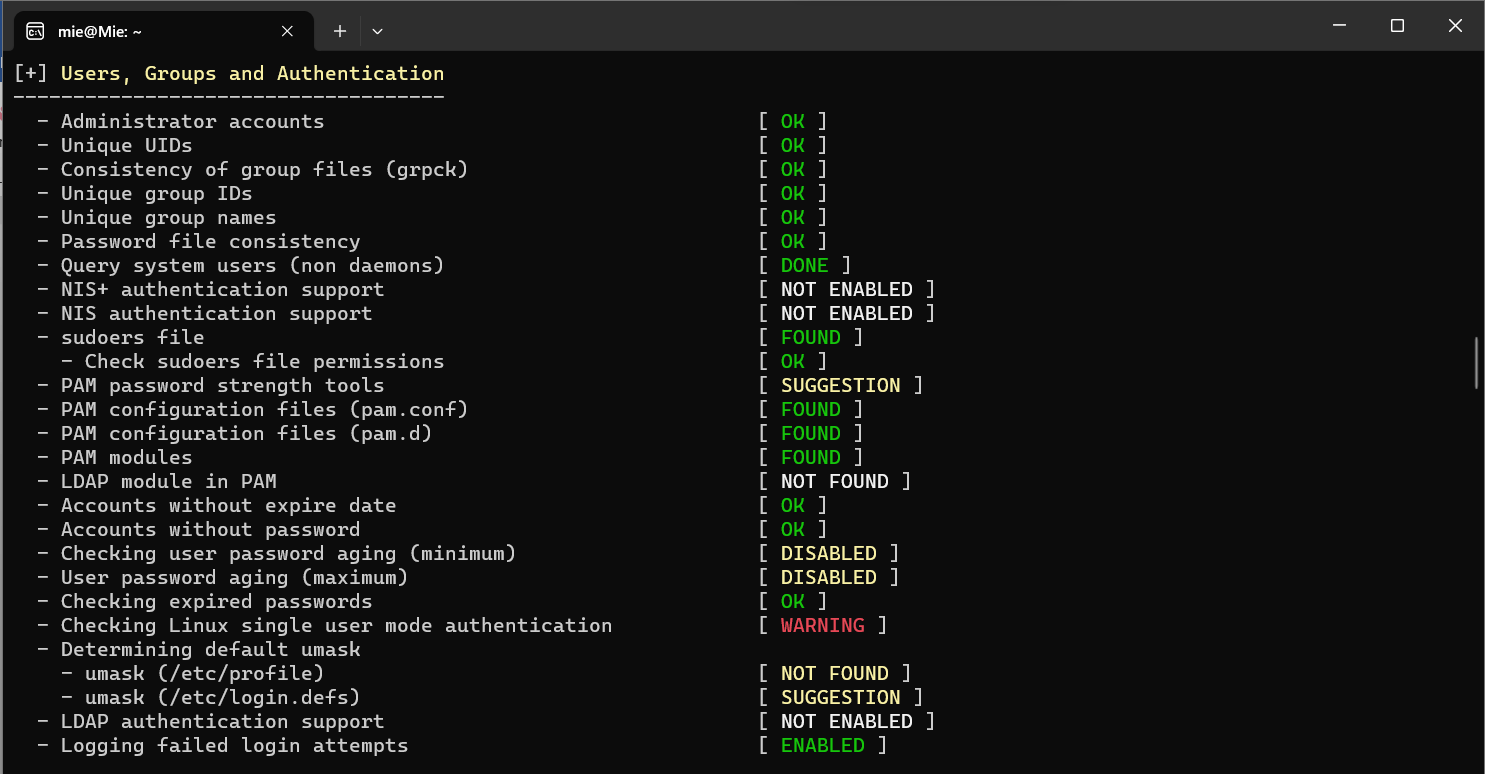
As displayed above, the tool will begin auditing using the user **cisco** as the auditor.

Notice: You will receive **warnings**.

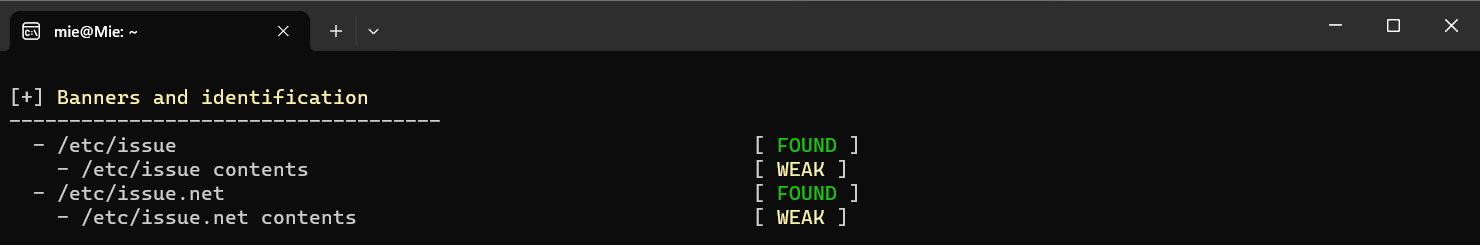
* + 1. To continue with each stage of the audit press **Enter**. You will receive warnings as shown below.



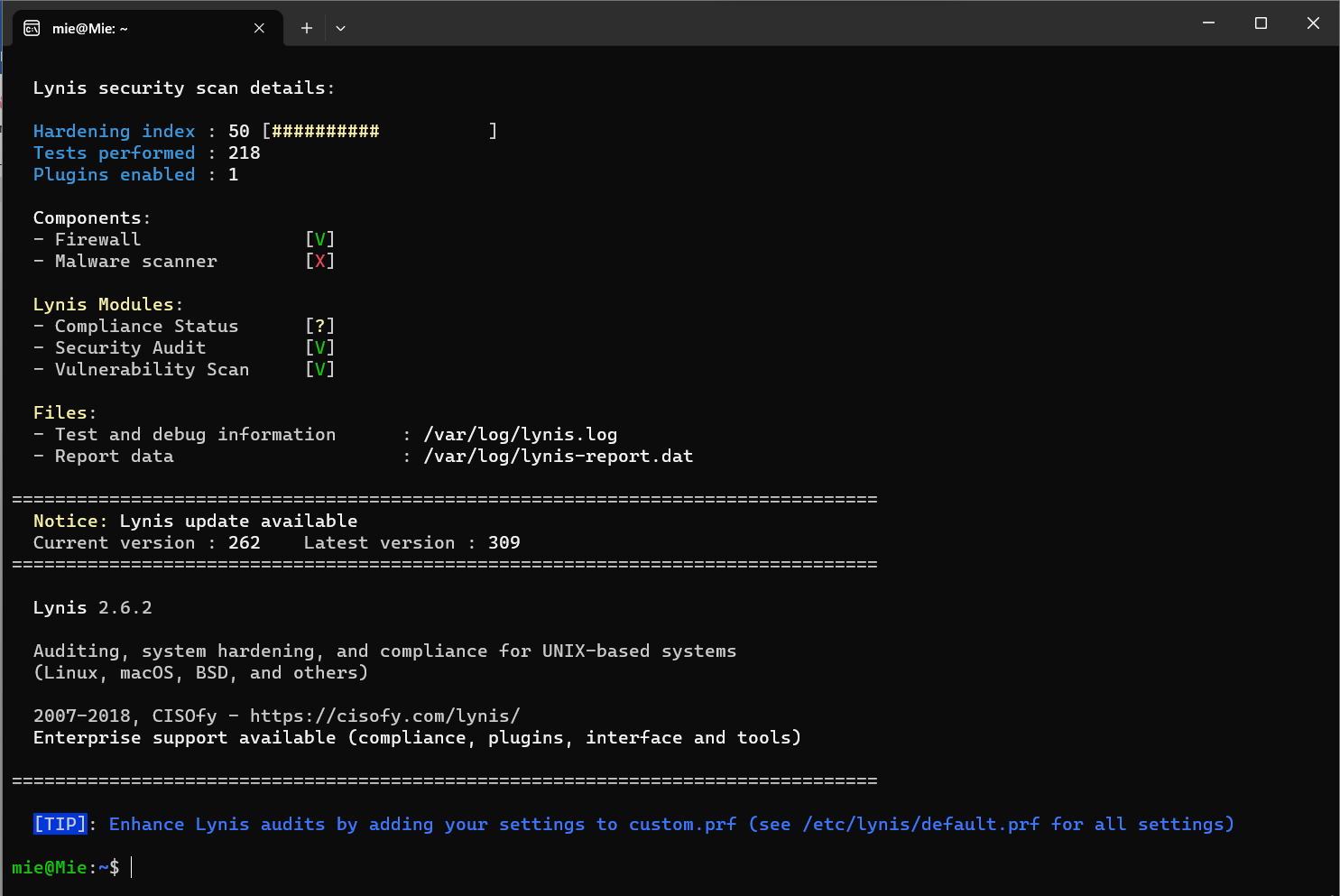
* + 1. You will receive suggestions, as shown below.



* + 1. You will receive a notification for any configuration that is weak as shown below:



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



* 1. Review Results
     1. Scroll up to the results section after the tool is finished running.

How many Warnings did you receive?

*Trả lời: 6 cảnh báo*

How many Suggestions did you receive?

*Trả lời: 33 đề xuất*

* + 1. 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?

*Trả lời: Install libpam-tmpdir to set $TMP and $TMPDIR for PAM sessions [CUST-0280]*

What is your suggested solution?

*Trả lời: cài đặt gói, giúp thiết lập các biến môi trường và cho các phiên PAM. Điều này có thể cải thiện tính bảo mật và cách ly các thư mục tạm thời được sử dụng bởi các ứng dụng và dịch vụ khác nhau trên hệ thống của bạn ‘libpam-tmpdir’ ‘$TMP’ ‘$TMPDIR’*

**References**

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