What’s Lynis ?

Lynis is a very complete security tool to perform an audit of our Linux system.

How does it work?

Lynis scans the software installed on the system for security problems. Along with security-related information, it will also look for general system information, installed packages, and configuration errors.

Lynis allows us to evaluate the current security defense of our server, thus knowing what security measures are applied and which are pending to decide if we have to take additional steps.

Download and Instill Lynis in CentOS

Step 1: Update the CentOS

**sudo yum install epel-release -y**

**sudo yum update -y**

**sudo shutdown -r now**

Step 2: Install Lynis in CentOS

**sudo yum install lynis -y**

Download and Install Lynis in Ubuntu

Step 1: Update Ubuntu

**sudo apt update**

**sudo apt-get upgrade**

**sudo shutdown -r now**

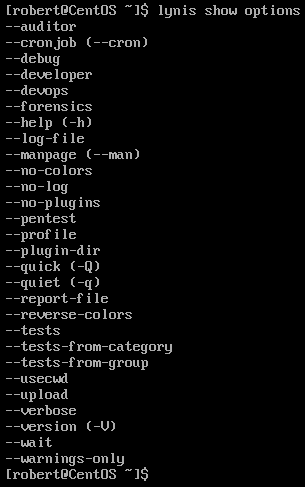
Step 2: Install Lynis in Ubuntu

**apt-get install lynis**

If we run the lynis command alone, we can see some of the available options



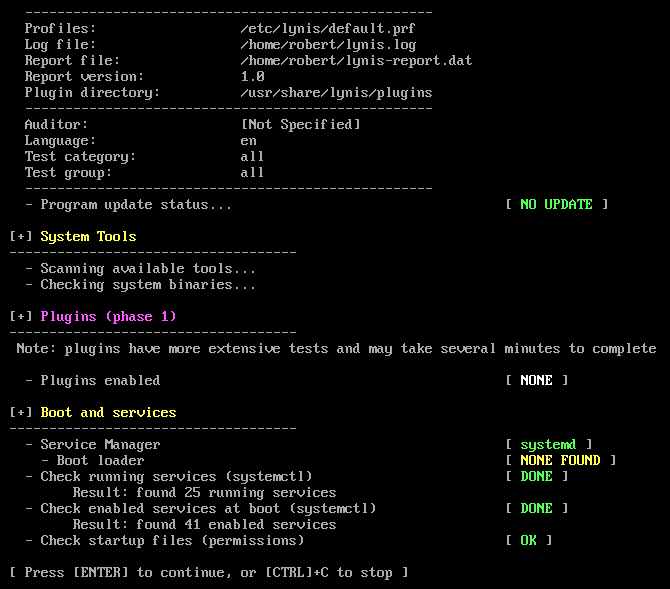
By running ‘**lynis show options**’ we can see more parameters



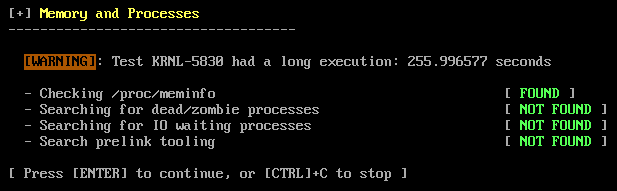
To run lynis type the following command : **lynis audit system**

To run lynus and wait for user input before procedding to the next scan : **lynis audit system –wait**

Once executed, we can first see a summary of our system.



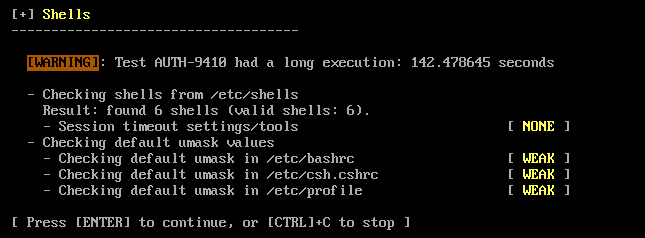
This section analyzes the boot loader detected in our system, the services that we start when we start and different aspects of the kernel.

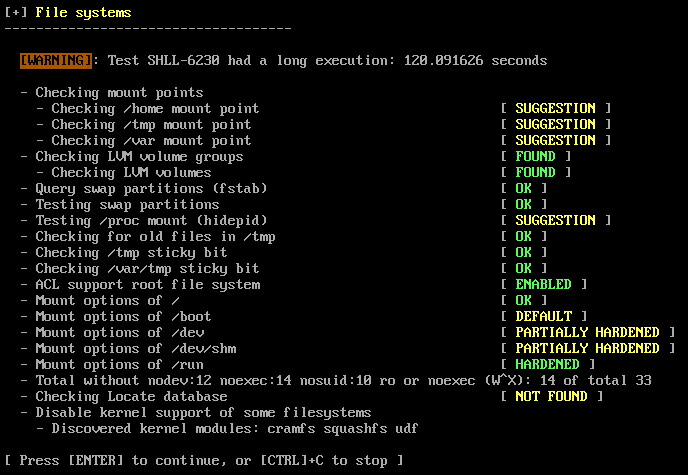
This represent the information about memory and the processes that run in the server. 

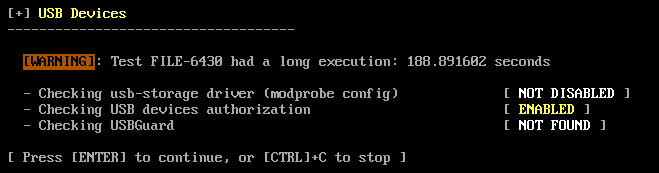
this section displays the users, groups and authentication created on the system.

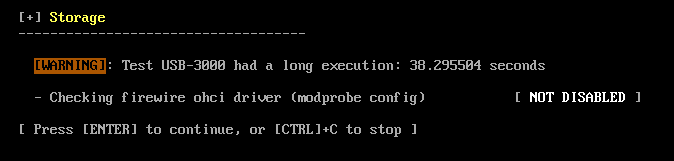


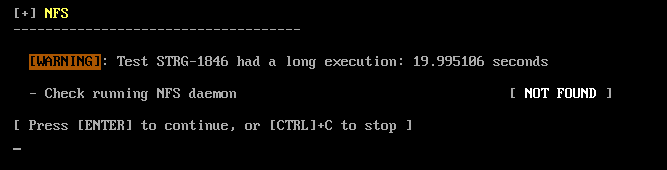
This analyze the system shells or shields, the file system and the support for mass storage.



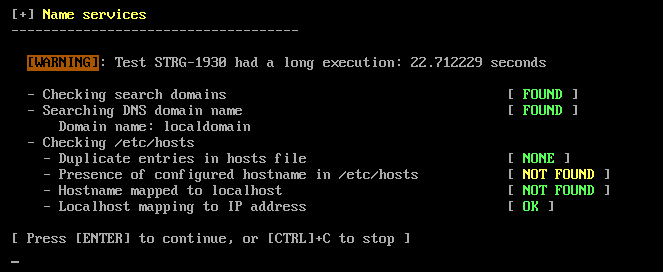


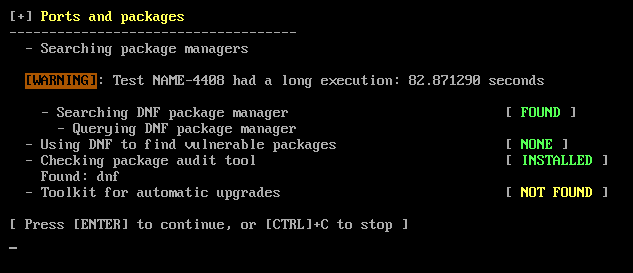






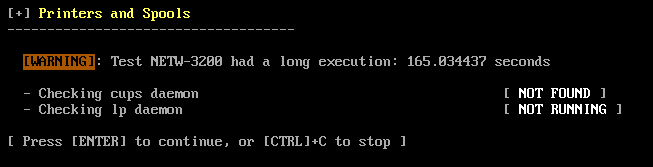
This section analyzes the domain name services (if any) and the package manager of the distribution.

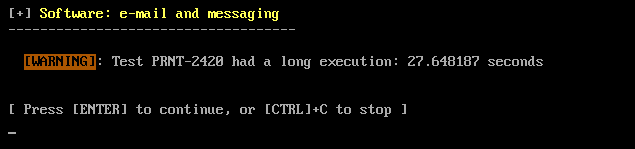


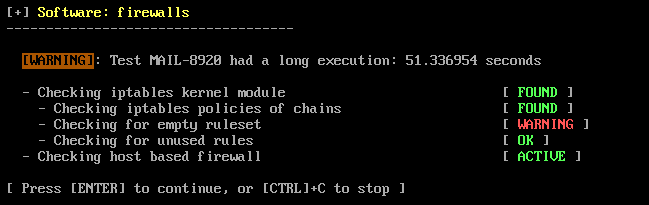


Printers, networks, email servers and firewall status.

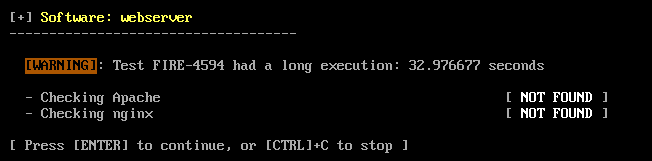


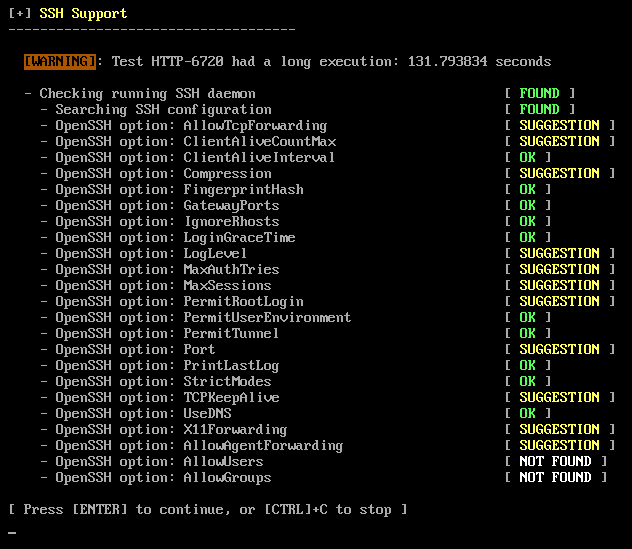


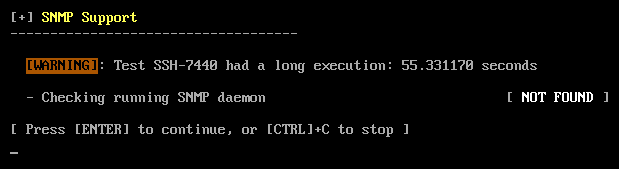


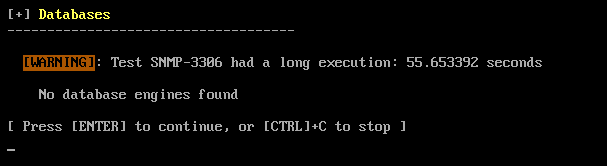


web servers, SSH server, SNMP and system databases.

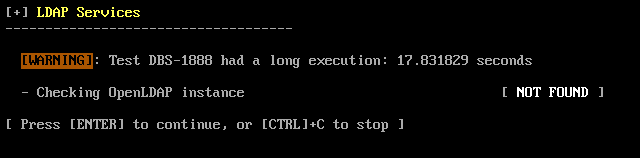


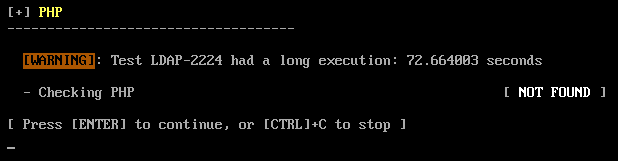


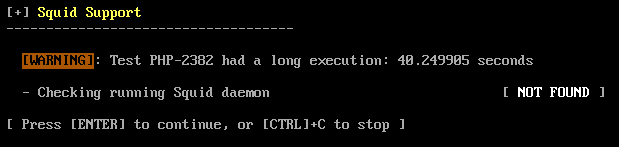


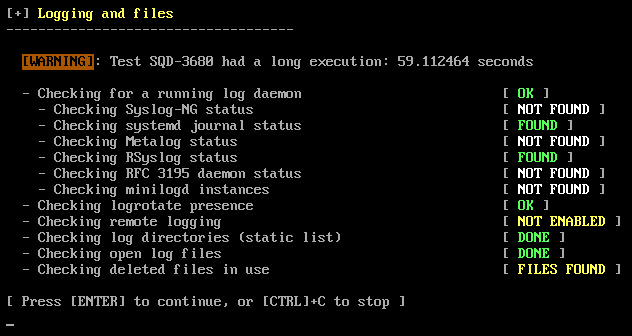


This section analyzes LDAP services, PHP program, Squid server and system logging data.

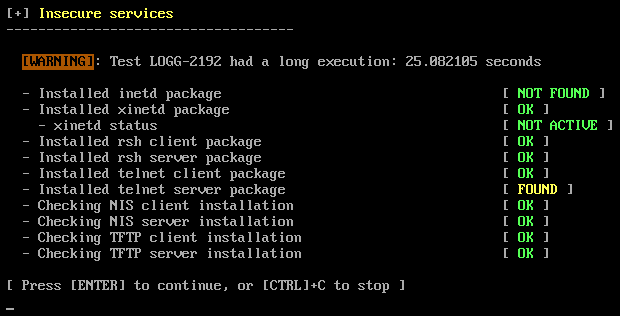


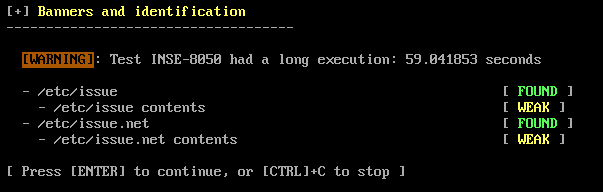


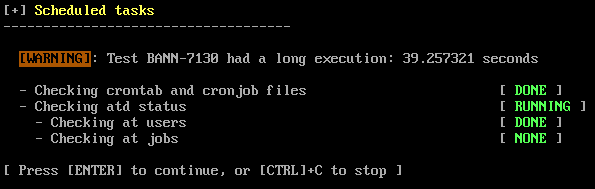




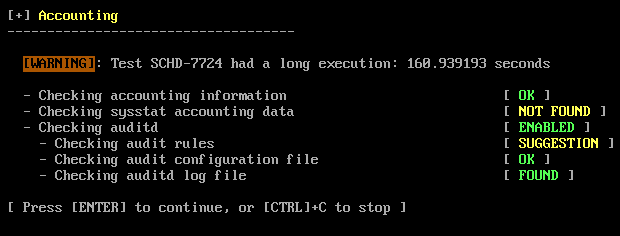
This section analyzes the status of inetd, banners and identification and scheduled tasks.

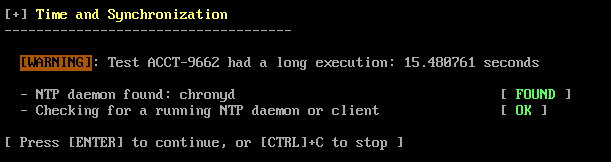


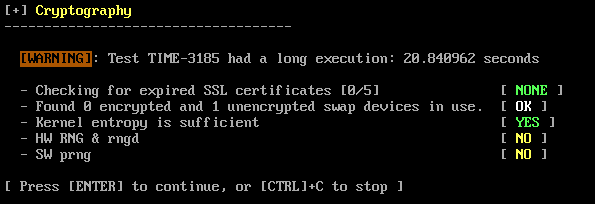


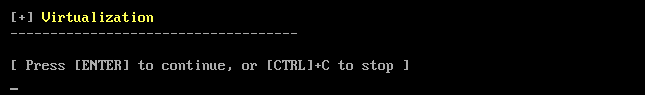


This section analyzes our account information along with the status of the time and synchronization server. Also, the cryptography of the system and the aspects related to virtualization.

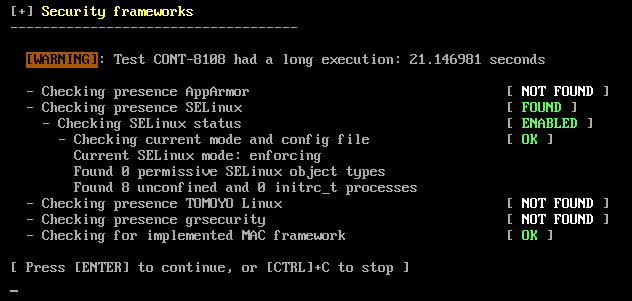


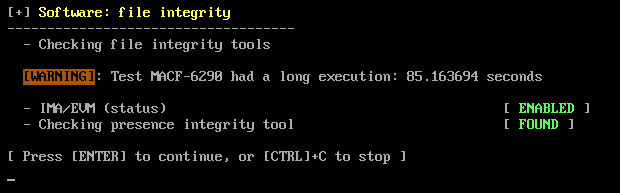


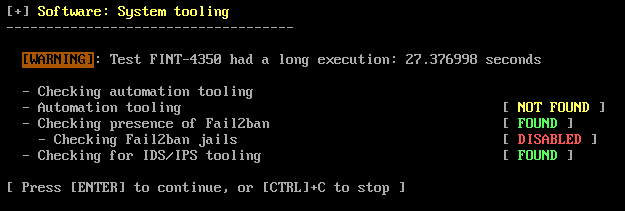


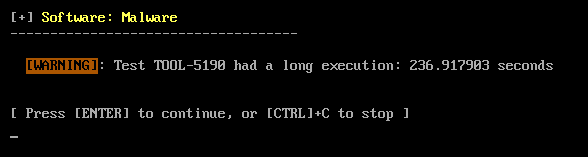


This section analyzes various security aspects such as security frameworks, file integrity, and malware scanners.

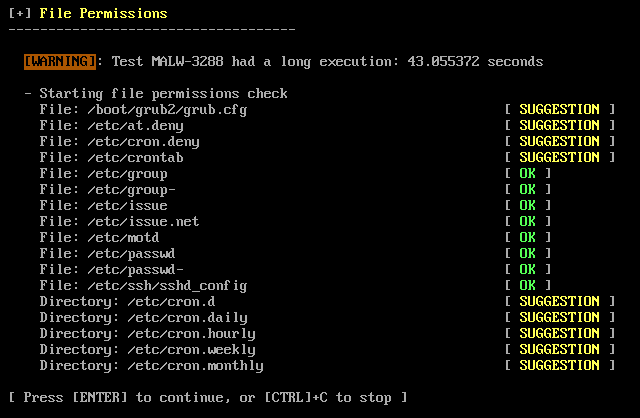


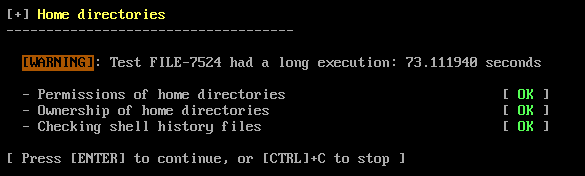






This section analyzed the file permissions in the system.

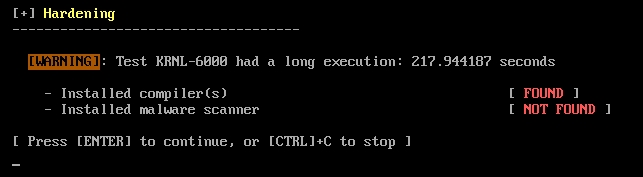




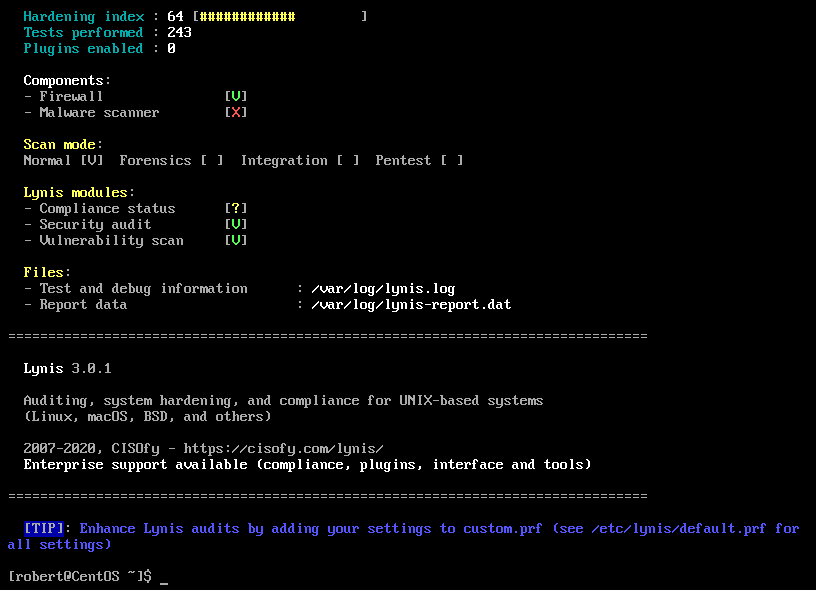
This section analyzes the kernel ipv4 net filtering



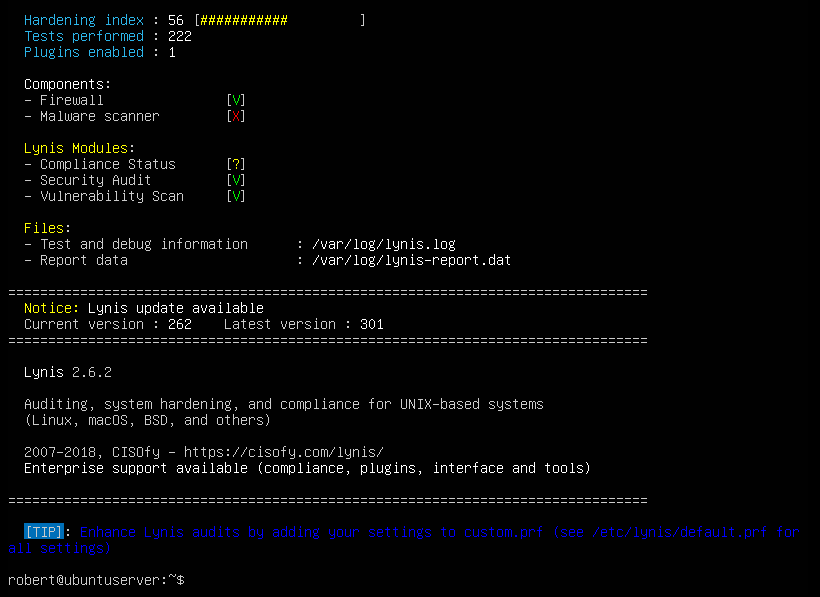
This analyze the security level of the system.



Once the scan is completed, it will us a summary of all the errors, warnings and suggestions detected.



# Ubuntu Scan Summary



Comparing the scan from CentOS and Ubuntu, I can say that they gave me similar result on both of my installed servers. The summary suggest that I do not have a malware scanner installed in neither server. Thus, a malware scanner must be installed to strength the security defense on both systems. In the ubuntu scan summary a “notice” suggestion appeared at the end of the summary. Claiming that Lynis has an update available. Overall, both server had similar results.

# Script to check the health of a server

**#!bin/bash**

**sudo lynis update release**

If there is an update for lynis, I want the software to scan the server with the latest version of lynis.

**sudo lynis audit system -Q**

It runs the scan without waiting for user inputs, except on errors.

to create a daily scan report of your system, you must set up a cron job for it. Run the following command in the shell.

**crontab -e**

Add the following cron job with the --cronjob option so that the scan will run fully automated.

**30 22 \* \* \* /home/user/script**

**lynis-report.dat**

Here we will have a report of the analysis from the health of our server.

**lynis.log**

In this file we will find each of the checks carried out (log).