sudo lynis audit system

The first section of the audit detects the version of Linux, kernel release, and other system details.

Text

Description automatically generated

Areas that need to be looked at are highlighted in amber (suggestions) and red (warnings that should be addressed).

Below is an example of a warning. Lynis has analyzed [the postfix](http://www.postfix.org/) mail server configuration and flagged something to do with the banner. We can get more details of exactly what it found and why it might be an issue later.

Text

Description automatically generated

Below, Lynis warns us that the firewall isn’t configured.

Text

Description automatically generated

Scroll through your results to see what Lynis flagged. At the bottom of the audit report, you’ll see a summary screen.

Graphical user interface, text

Description automatically generated

The “Hardening Index” is your exam score. We got 56 out of 100, which isn’t great. There were 222 tests performed and one Lynis plugin is enabled. If you go to the Lynis Community Edition plugin [download page](https://cisofy.com/lynis/#download) and subscribe to the newsletter, you’ll get links to more plugins.

There are many plugins, including some for auditing against standards, such as [GDPR](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679), [ISO27001](https://www.iso.org/isoiec-27001-information-security.html), and [PCI-DSS](https://www.pcisecuritystandards.org/pci_security/glossary).

A green V represents a check mark. You might also see amber question marks and red X’s.

We have green check marks because we have a firewall and malware scanner. For test purposes, we also installed [rkhunter](http://rkhunter.sourceforge.net/), a rootkit detector, to see whether Lynis would discover it. As you can see above, it did; we got a green check mark next to “Malware Scanner.”

The compliance status is unknown because the audit didn’t use a compliance plugin. The security and vulnerability modules were used in this test.

Two files are generated: a log and data file. The data file, located at “/var/log/lynis-report.dat,” is the one we’re interested in. It will contain a copy of the results (without the color highlighting) that we can see in the terminal window. These come in handy to see how your hardening index improves over time.

If you scroll backward in the terminal window, you’ll see a list of suggestions and another of warnings. The warnings are the “big ticket” items, so we’ll look at those.

Text

Description automatically generated

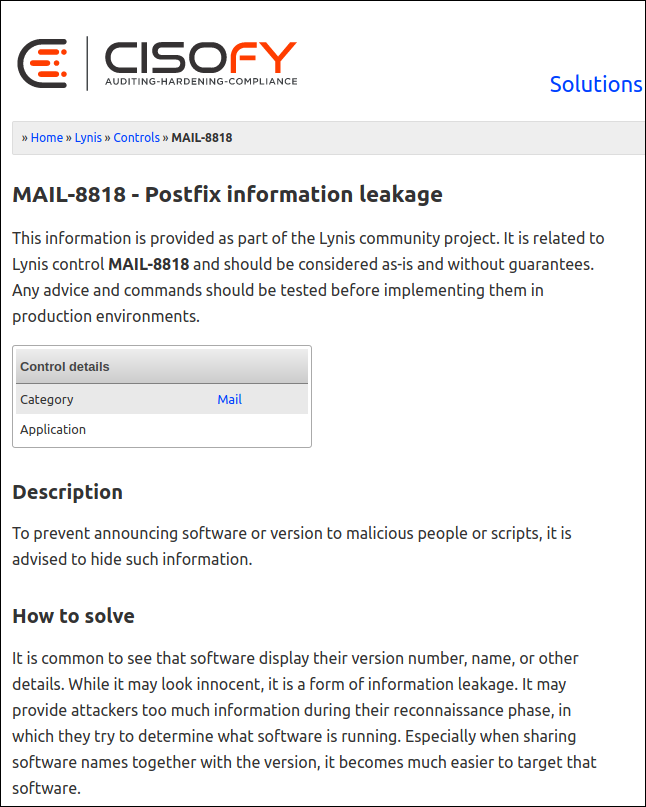
These are the five warnings:

* **“Version of Lynis is very old and should be updated”:** This is actually the newest version of Lynis in the Ubuntu repositories. Although it’s only 4 months old, Lynis considers this very old.  If you really want the latest version you can [clone the project from GitHub](https://github.com/CISOfy/lynis) and keep it synchronized.
* **“No password set for single mode”:** Single is a recovery and maintenance mode in which only the root user is operational. No password is set for this mode by default.
* **“Couldn’t find 2 responsive nameservers”:** Lynis tried to [communicate with two DNS servers](https://www.howtogeek.com/122845/htg-explains-what-is-dns/), but was unsuccessful. This is a warning that if the current DNS server failed, there’d be no automatic roll-over to another.
* **“Found some information disclosure in SMTP banner”:** Information disclosure happens when applications or network equipment give away their make and model numbers (or other info) in standard replies. This can give threat actors or automated malware insight into the types of vulnerability to check for. Once they’ve identified the software or device they’ve connected to, a simple lookup will find the vulnerabilities they can try to exploit.
* **“iptables module(s) loaded, but no rules active”:** The Linux firewall is up and running, but there are no rules set for it.

**Clearing Warnings**

Each warning has a link to a webpage that describes the issue and what you can do to remedy it. Just hover your mouse pointer over one of the links, and then press Ctrl and click it. Your default browser will open on the webpage for that message or warning.

The page below opened for us when we Ctrl+clicked on the link for the fourth warning we covered in the previous section.



You can review each of these and decide which warnings to address.

The web page above explains that the default snippet of information (the “banner”) sent to a remote system when it connects to the postfix mail server configured on our Ubuntu computer is too verbose. There’s no benefit to offering too much information—in fact, that’s often used against you

The web page also tells us the banner resides in “/etc/postfix/main.cf.” It advises us that it should be trimmed back to only show “$myhostname ESMTP.”

We type the following to edit the file as Lynis recommends:

sudo gedit /etc/postfix/main.cf

We locate the line in the file that defines the banner.

Graphical user interface, text, application

Description automatically generated

We edit it to show only the text Lynis recommended.

Graphical user interface, text, application

Description automatically generated

We save our changes and close gedit. We now need to restart the postfix mail server for the changes to take effect:

sudo systemctl restart postfix

Now, let’s run Lynis once more and see if our changes have had an effect.



The “Warnings” section now only shows four. The one referring to postfix is gone.

Text

Description automatically generated

One down, and just four more warnings and 50 suggestions to go!