

---

# Linux System Hardening Report

## What is Lynis?

Lynis is open-source security auditing tool for Unix-based operating systems like Linux, macOS, and BSD variants. It scans your system for security vulnerabilities, misconfigurations, and weakness, providing suggestions for improvement and ultimately helping to harden your system against potential attacks.

## Why it is used?

- Audit for vulnerabilities and misconfiguration: Lynis scans our systems for weakness that attackers could potentially exploit.
- Harden your system: It provides recommendations and guidance to strength your system's security settings and reduce its attack surface.
- Ensure compliance: Lynis can assist in validating your system's compliance with security standards like PCI-DSS, HIPPA, and ISO/IEC 27001.
- Gain actionable insights: It generates detailed reports with warnings and suggestions, empowering you to improve your system's security posture.
- Enhanced penetration testing: Security professionals can utilize Lynis for reconnaissance, vulnerability identification, and hardening validation during penetration tests.
- Automate and customize: Lynis is lightweight, agentless, written in shell script, and supports customization through profiles, tests, and plugins.

## Objectives:

- Use a security auditing tool (Lynis) to discover system with vulnerabilities.
- Implement recommended solutions to harden the system.

## Environment:

- System: Ubuntu VM (cyber lab VM) in VM ware workstation.
  - Tool: Lynis Security Audit Tool Step-by-step Instructions.
-

---

## My System Hardening with Lynis

I had Initial Warnings before scanning

```
-[ Lynis 3.0.3 Results ]-  
  
Warnings (3):  
-----  
! Version of Lynis is very old and should be updated [LYNIS]  
  https://cisofy.com/lynis/controls/LYNIS/  
  
! Found one or more vulnerable packages. [PKGS-7392]  
  https://cisofy.com/lynis/controls/PKGS-7392/  
  
! iptables module(s) loaded, but no rules active [FIRE-4512]  
  https://cisofy.com/lynis/controls/FIRE-4512/
```

### Warning1

! Version of Lynis is very old and should be updated [LYNIS]

How did I clear these warnings?

Issue: our Lynis version is outdated, which means it might miss new vulnerabilities or give outdated advice.

Solution: I prefer to install Lynis from your distro:

Commands:      `sudo apt update`  
                 `sudo apt install --only-upgrade lynis`  
                 Or  
                 `sudo apt update`  
                 `sudo apt install lynis -y`  
                 `sudo lynis audit system`

`sudo apt update`: This command is used on Debian-based Linux systems (like Ubuntu, Kali, Linux Mint) to refresh the package list from the repositories.

- `sudo` gives admin/root permissions, which are required to modify system files (like the package cache).
- It checks for the latest versions of software packages available in your configured repositories (e.g., Ubuntu's online software servers).
- It does not install or upgrade anything, it just retrieves information about available updates.

`sudo apt upgrade`: This command is used to install the newest versions of all packages currently installed on your system — but only if the upgrade doesn't require removing or installing other packages.

- After you run `sudo apt update`, your system knows which packages are outdated.
  - Then, `sudo apt upgrade` downloads and installs those updates.
-

- 
- It only upgrades packages where it's safe to do so without changing dependencies.

`sudo apt install lynis -y`: This command tells your Linux system to:

1. Use apt — the package manager for Debian/Ubuntu systems
2. install lynis — install the Lynis security auditing tool
3. -y — automatically say "yes" to all prompts (non-interactive install)

`sudo lynis audit system`: This command runs a full security audit of your Linux system using Lynis.

## Warning 2

! Found one or more vulnerable packages [PKGS-7392]

Issue: Some installed packages have known vulnerabilities (CVEs) and should be patched.

Solution: Update package list and installed packages or Reviewed and updated packages using `apt upgrade` or checked with `apt list --upgradable`.

Commands: `sudo apt update`

`Sudo upgrade -y`

`Sudo full-upgrade -y`

`Sudo ./lynis audit system`

`sudo apt update`: This command updates the list of available packages and their versions from the repositories.

`sudo apt upgrade -y`: This upgrades all the installed packages on the system to their latest versions available in the repositories.

- -y: Automatically answers "yes" to any prompts.

`sudo apt full-upgrade -y`: This command performs the same action as `upgrade`, but also removes or installs packages as needed to complete the upgrade.

`sudo lynis audit system`: This command runs a full security audit of your Linux system using Lynis.

## Warning 3

! iptables module(s) loaded, but no rules active[Fire-4512]

Issue: our system is loaded the iptables firewall, but there are no rules defined. This means your system might be wide open to attacks.

Solution: Configured appropriate firewall rules using `ufw` or `iptables`.

1. use `ufw` (uncomplicated Firewall) and set basic rules:

Commands: `sudo apt install ufw -y`

`Sudo ufw default deny incoming`

---

---

Sudo ufw default allowing outgoing

Sudo ufw enable

sudo apt install ufw -y: Installs UFW (Uncomplicated Firewall), a user-friendly interface for managing iptables (the built-in Linux firewall).

- -y: Automatically agrees to install.

sudo ufw default deny incoming: Sets the default policy to deny all incoming connections.

sudo ufw default allow outgoing: Sets the default policy to allow all outgoing connections.

sudo ufw enable: Activates the UFW firewall with the rules set above.

2.use iptables: iptables is a Linux firewall utility that manages network traffic rules using Netfilter, the Linux kernel's packet filtering framework.

In cybersecurity and system hardening, iptables is used to:

- Allow or block specific types of network traffic
- Prevent unauthorized access
- Limit exposure of services (like SSH, HTTP)

Commands:     sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT # HTTP

                  sudo iptables -A INPUT -p tcp --dport 443 -j ACCEPT # HTTPS

Or

Sudo apt update

Sudo apt upgrade

Sudo reboot

sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT:

- -A INPUT: Appends a rule to the INPUT chain (incoming traffic).
- -p tcp: Applies to TCP protocol (used by web traffic).
- --dport 80: Matches packets targeting port 80 (HTTP).
- -j ACCEPT: Allows the traffic.

Allows inbound HTTP traffic on port 80 (used by websites that don't use encryption).

sudo iptables -A INPUT -p tcp --dport 443 -j ACCEPT:

- Same as above, but for port 443, which is used for HTTPS (secure web traffic).

Allows inbound HTTPS traffic, which is encrypted and more secure than HTTP.

---

---

## I fixed all warnings after performing the Lynis scan

```
-----  
=====
```

```
-[ Lynis 3.0.3 Results ]-  
  
Great, no warnings  
  
Suggestions (61):  
-----  
* This release is more than 4 months old. Check the website or GitHub to see if there is an update available  
  https://cisofy.com/lynis/controls/LYNIS/  
  
* Install libpam-tmpdir to set $TMP and $TMPDIR for PAM sessions [DEB-0280]  
  https://cisofy.com/lynis/controls/DEB-0280/
```

Successfully resolved 3 major warnings identified by Lynis.

Improved system hardening by applying firewall rules, updating packages, and considering boot security.

Final scan showed "Great, no warnings" – system is in a hardened state.

### Summary:

- Lynis Version: up-to-date
- Vulnerable Packages: Updated
- iptables Rules & Firewall: Secured

### References:

- <https://cisofy.com/lynis/controls/LYNIS/>
- <https://cisofy.com/lynis/controls/PKGS-7392/>
- [https:// cisofy.com/lynis/controls/FIRE-4512/](https://cisofy.com/lynis/controls/FIRE-4512/)
- <https://github.com/CISOfy/lynis>
- <https://help.ubuntu.com/community/UFW>

### Author:

Hardening conducted by: Priyanka H S

Security audit via lynis 3.0.3 on ubuntu Cyber-LABVM