Cyber Security lab VM Ware Workstation

Lynis Hardening System

What is Lynis?

Lynis is a security auditing tool for systems based on UNIX like Linux, macOS, BSD, and others. It performs an **in-depth security scan** and runs on the system itself. The primary goal is to test security defenses and **provide tips for further system hardening**. It will also scan for general system information, vulnerable software packages, and possible configuration issues. Lynis was commonly used by system administrators and auditors to assess the security defenses of their systems. Besides the "blue team," nowadays penetration testers also have Lynis in their toolkit.

We believe software should be **simple**, **updated on a regular basis**, and **open**. You should be able to trust, understand, and have the option to change the software. Many agree with us, as the software is being used by thousands every day to protect their systems.

Goals

The main goals of Lynis include:

- Automated security auditing
- Compliance testing (e.g. ISO27001, PCI-DSS, HIPAA)
- Vulnerability detection

The software (also) assists with:

- Configuration and asset management
- Software patch management
- System hardening
- Penetration testing (privilege escalation)
- Intrusion detection

Audience

Typical users of the software:

- System administrators
- Auditors
- Security officers
- Penetration testers
- Security professionals

Why is Lynis Used?

Lynis is used for:

System hardening – improving the security of the system.

Vulnerability scanning – finding outdated packages, weak configurations, and missing protections.

Compliance checking – helpful for preparing systems to meet security standards like ISO27001, PCI-DSS, etc.

My System Hardening with Lynis

I had Intitial Warnings before scanning

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Issue: our Lynis version is outdated, which means it might miss new vulnerabilities or give outdated advice.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

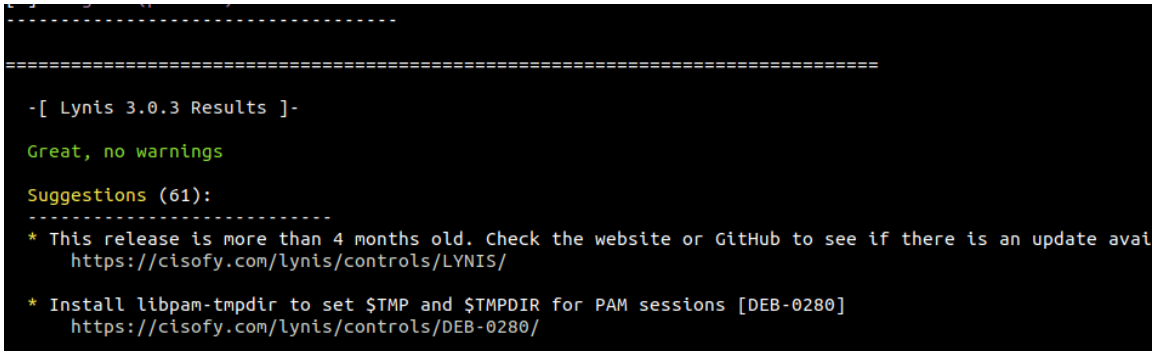
Allows inbound HTTP traffic on port 80 (used by websites that don't use encryption).

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



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.