Linux System Hardening Report

What is lynis?

Lynis is an 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 weaknesses, providing suggestions for improvement and ultimately helping to harden your system against potential attacks.

Why it is used?

- Audit for vulnerabilities and misconfigurations: Lynis scans your system for weaknesses that attackers could potentially exploit.
- Harden your system: It provides recommendations and guidance to strengthen 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, HIPAA, and ISO/IEC 27001.
- Gain actionable insights: It generates detailed reports with warnings and suggestions, empowering you to improve your system's security posture.
- Enhance 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 vulnerabilities.
- Implement recommended solutions to harden the system.

Environment:
- System: Ubuntu VM (cyberLABVM) in VirtualBox
- Tool: Lynis Security Audit ToolStep-by-Step Instructions:

1. Launch Terminal:
   - Open your VM and start the terminal from your desktop.

2. Check Lynis Version:
   Commands:
   cd Downloads/lynis/ sudo ./lynis update info
   Expected Output:Version: 3.0.3
   Status: Up-to-date

3. Run the Lynis Audit:
   Command:
   sudo ./lynis --auditor cisco

4. Analyze Results:

   Warnings:

```
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/
```

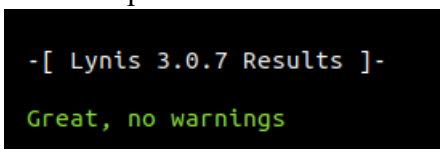
   Suggestions:
   Example: * Set a password on GRUB boot loader [BOOT-5122] Solutions Implemented.

   Warning 1: Outdated Lynis Version Commands:
   cd /opt sudo git clone https://github.com/CISOfy/lynis
   cd lynis
   sudo ./lynis audit system

   Warning 2: Vulnerable Packages Commands:
   sudo apt-get update sudo apt-get upgrade sudo apt-get dist-upgrade sudo reboot

   Warning 3: iptables Rules Not Active
   Commands:
   sudo apt install ufw -y
   sudo ufw default deny incoming
   sudo ufw default allow outgoing
   sudo ufw allow ssh
   sudo ufw enable
   Re-Run Lynis:
   sudo ./lynis --auditor cisco

Final Output:



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://github.com/CISOfy/lynis- https://help.ubuntu.com/community/UFW

Author:

Hardening conducted by: Neha M N

Security audit via Lynis 3.0.3 on Ubuntu Cyber-LABVM