Laboratório - Fortaleça um sistema Linux

# Objetivos

=   Use uma ferramenta de auditoria de segurança para descobrir vulnerabilidades do sistema.

=   Implemente soluções recomendadas para proteger o sistema.

# Histórico/Cenário

A auditoria de um sistema em busca de possíveis configurações erradas ou serviços não protegidos é um aspecto importante da blindagem de um sistema. Lynis é uma ferramenta de auditoria de segurança de código aberto com um conjunto automatizado de scripts desenvolvidos para testar um sistema Linux. O Lynis executa uma verificação de integridade abrangente do seu sistema. Ele inclui um relatório detalhado de vulnerabilidades e ações recomendadas. Neste laboratório, você usará o Lynis para verificar sua VM e, em seguida, implementar soluções para proteger seu sistema.

# Recursos necessários

PC com o **CSE-LABVM** instalado no VirtualBox

# Instruções

## Parte 1: Instalação e atualização do Lynis.

### Etapa 1: Determine a versão do Lynis instalada.

a.     Inicie o **CSE-LABVM.**

b.     Clique duas vezes no ícone **Terminal** para abrir um terminal.

c.     Para determinar a versão mais recente fornecida pelo CISOfy, digite o seguinte comando no terminal.

cisco@labvm:~$ **sudo apt-cache policy lynis**

lynis:

  Installed: 3.0.6-100

  Candidate: 3.0.6-100

  Version table:

\*\*\* 3.0.6-100 500

        500 https://packages.cisofy.com/community/lynis/deb stable/main amd64 Packages

        500 https://packages.cisofy.com/community/lynis/deb stable/main i386 Packages

        100 /var/lib/dpkg/status

2.6.2-1 500

        500 http://archive.ubuntu.com/ubuntu focal/universe amd64 Packages

        500 http://archive.ubuntu.com/ubuntu focal/universe i386 Packages

d.     Avance para a próxima parte se você tiver a versão mais recente do Lynis.

Se o Lynis não estiver instalado ou a versão mais recente não estiver instalada, vá para a próxima etapa para instalar o Lynis.

### Etapa 2: Instalar o Lynis

O **Lynis** é uma ferramenta de segurança para sistemas que executam sistemas operacionais baseados em Unix, como Linux e macOS. O **lynis** será usado posteriormente em outra atividade para proteger um sistema Linux. O aplicativo **Lynis**é mantido pelo [CISOfy](https://cisofy.com/lynis/). Nesta etapa, adicionaremos o repositório de software e instalaremos o Lynis.

a.     Copie e cole o seguinte comando em um terminal para importar a chave do servidor de chaves CISOfy. Esta chave é necessária para verificar a integridade do seu download quando você baixa o **lynis**:

cisco@labvm:~$ sudo apt-key adv --keyserver keyserver.ubuntu.com --recv-keys 013baa07180c50a7101097ef9de922f1c2fde6c4

b.     Copie e cole o seguinte comando em um terminal para adicionar o repositório **lynis** mantido pelo CISOfy.

cisco@labvm:~$ echo "deb https://packages.cisofy.com/community/lynis/deb/ stable **main" | sudo tee /etc/apt/sources.list.d/cisofy-lynis.list**

c.     Execute uma atualização após adicionar um novo repositório. No prompt, digite **sudo apt-get update**.

d.     Use o comando **apt install** para instalar o Lynis, se ainda não estiver instalado.

cisco@labvm:~$ **sudo apt install lynis**

Reading package lists... Done

Building dependency tree

Reading state information... Done

The following NEW packages will be installed:

  lynis

0 upgraded, 1 newly installed, 0 to remove and 17 not upgraded.

Need to get 0 B/262 kB of archives.

After this operation, 1,681 kB of additional disk space will be used.

Selecting previously unselected package lynis.

(Reading database ... 205787 files and directories currently installed.)

Preparing to unpack .../lynis\_3.0.6-100\_all.deb ...

Unpacking lynis (3.0.6-100) ...

Setting up lynis (3.0.6-100) ...

Processing triggers for man-db (2.9.1-1) ...

e.    Faça uma atualização após a instalação para garantir que o Lynis instalado seja a versão mais recente. No prompt, digite **sudo apt-get upgrade**.

## Parte 2: Examine a versão atual do Lynis.

Mude para o diretório do Lynis e, em seguida, insira o comando **sudo lynis update info** para verificar as informações de atualização do Lynis. Digite **password** como senha para o comando sudo password. Esse comando verifica se essa é a versão mais recente e atualiza para a ferramenta utilizada no momento em que este laboratório estava sendo escrito. Se a versão instalada do Lynis não estiver atualizada, digite **sudo apt-get upgrade** no prompt.

cisco@labvm:~$ **sudo lynis update info**

[sudo] password for cisco: **password**

== Lynis ==

Versão: 3.0.6

  Status             : Up-to-date

  Release date       : 2021-07-22

  Project page       : https://cisofy.com/lynis/

  Source code        : https://github.com/CISOfy/lynis

  Latest package     : https://packages.cisofy.com/

2007-2021, CISOfy - https://cisofy.com/lynis/

## Parte 3: Execute a ferramenta Lynis.

a.     Insira o comando **sudo lynis --auditor cisco**. Você pode ou não precisar digitar a senha **password** novamente. A verificação levará cerca de um minuto para ser executada.

cisco@labvm:~$**sudo lynis --auditor cisco**

b.     Você deve receber saída para diversos recursos do sistema, começando com **Boot and services (inicialização e serviços)** e terminando com **Hardening (fortalecimento)**, **Testes personalizados** e **Plugins (fase 2)**. A próxima seção é sobre os resultados do **Lynis 3.0.6**. Seus resultados provavelmente incluem os dois **Warnings (avisos)** mostrados abaixo. Você também pode receber outros avisos. Além disso, haverá uma seção com uma lista de **Suggestions (sugestões)**, que lista 49 no exemplo de saída abaixo. Somente a primeira sugestão é exibida.

[Lynis 3.0.6]

################################################################################

  Lynis comes with ABSOLUTELY NO WARRANTY. This is free software, and you are

  welcome to redistribute it under the terms of the GNU General Public License.

  See the LICENSE file for details about using this software.

  2007-2021, CISOfy - https://cisofy.com/lynis/

  Enterprise support available (compliance, plugins, interface and tools)

################################################################################

[+] Initializing program

------------------------------------

  - Detecting OS...                                           [ DONE ]

  - Checking profiles...                                      [ DONE ]

<output omitted>

[+] Boot and services

------------------------------------

  - Service Manager                                           [ systemd ]

  - Checking UEFI boot                                        [ DISABLED ]

  - Checking presence GRUB2                                   [ FOUND ]

<output omitted>

[+] Hardening

------------------------------------

    - Installed compiler(s)                                   [ FOUND ]

    - Installed malware scanner                               [ NOT FOUND ]

    - Non-native binary formats                               [ NOT FOUND ]

[+] Custom tests

------------------------------------

  - Running custom tests...                                   [ NONE ]

[+] Plugins (phase 2)

------------------------------------

================================================================================

  -[ Lynis 3.0.6 Results ]-

  Warnings (2):

  ----------------------------

  ! 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 (49):

  ----------------------------

  \* Set a password on GRUB boot loader to prevent altering boot configuration (e.g. boot in single user mode without password) [BOOT-5122]

      https://cisofy.com/lynis/controls/BOOT-5122/

<output omitted>

================================================================================

Lynis 3.0.6

  Auditing, system hardening, and compliance for UNIX-based systems

  (Linux, macOS, BSD, and others)

  2007-2021, CISOfy - https://cisofy.com/lynis/

  Enterprise support available (compliance, plugins, interface and tools)

================================================================================

  [TIP]: Enhance Lynis audits by adding your settings to custom.prf (see /home/cisco/Downloads/lynis/default.prf for all settings)

cisco@labvm:~$

## Parte 4: Revise os resultados da sua análise e resolva quaisquer avisos.

a.      Role a página até a seção de **Resultados** na saída para a sua análise.

#### Perguntas:

Quantos avisos você recebeu?

Digite suas respostas aqui

Quantas sugestões você recebeu?

Digite suas respostas aqui.

b.     Você deve abordar os avisos. Escolha pelo menos um aviso e pesquise como corrigir esse problema. Você pode usar o link fornecido na saída de aviso como ponto de partida para lidar com um aviso. Mas você também pode precisar usar suas habilidades de pesquisa na Internet para rastrear informações adicionais.

#### Perguntas:

Qual aviso você está abordando?

Digite suas respostas aqui.

Qual é a sua solução?

Digite suas respostas aqui.

c.     Implemente a solução e execute o comando **sudo lynis --auditor cisco** novamente. Se o aviso escolhido não estiver mais listado na seção **Resultados**, parabéns! Você acabou de aumentar o fortalecimento da sua VM do Ubuntu. Se o aviso ainda estiver listado, veja se você pode descobrir mais informações para ajudá-lo a obter um relatório claro do Lynis no qual o aviso não é mais relatado.

Fim do documento