Laboratório — Blindagem de um sistema Linux

Objetivos

Demonstrar a utilização de uma ferramenta de auditoria de segurança para blindar um sistema Linux.

Contexto/cenário

A auditoria de um sistema para possíveis configurações incorretas ou serviços desprotegidos é um aspecto importante da blindagem do sistema. O Lynis é uma ferramenta de auditoria de segurança de código aberto com um conjunto automatizado de scripts desenvolvidos para testar um sistema Linux.

Recursos necessários

- Um PC com o Ubuntu 16.04 Desktop LTS instalado no VirtualBox ou numa máquina virtual VMware.

Passo 1: Abrir uma janela de terminal no Ubuntu.

a. Inicie uma sessão no Ubuntu utilizando as seguintes credenciais:

Utilizador: **cisco**

Palavra-passe: **password**

b. Clique no ícone do terminal para abrir uma janela de terminal.

Passo 2: A ferramenta Lynis

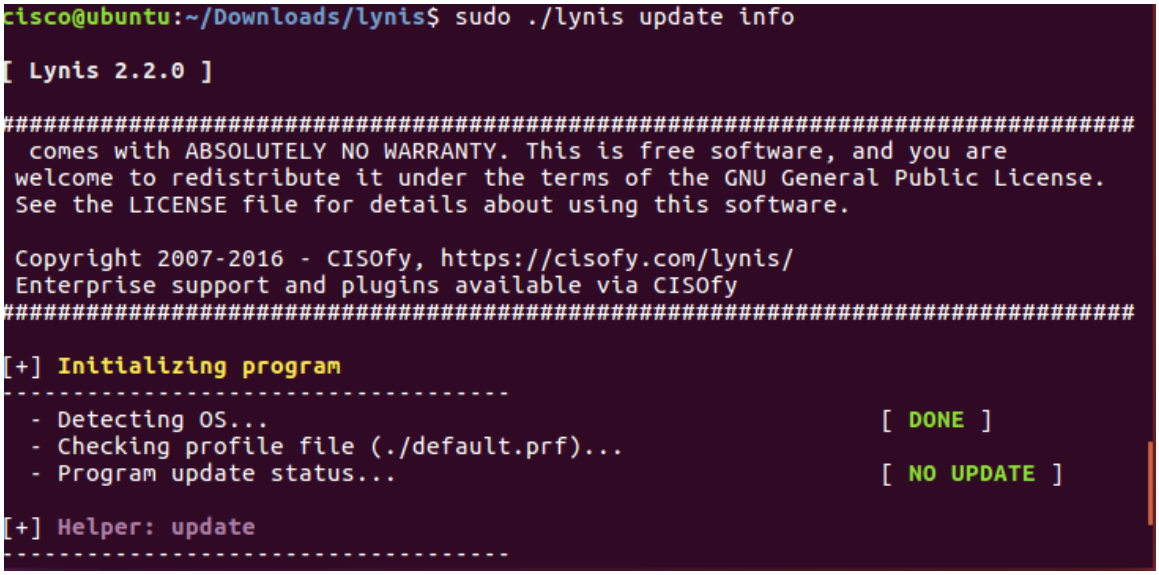
a. No prompt de comandos, introduza o seguinte comando para mudar para o diretório do lynis:

```
cisco@ubuntu:~$ cd Downloads/lynis/
```

```
cisco@ubuntu:~$ cd Downloads/lynis/
cisco@ubuntu:~/Downloads/lynis$
```

b. No prompt de comandos, introduza o seguinte comando e introduza a palavra-passe **password** quando lhe for pedida:

```
cisco@ubuntu:~/Dowloads/lynis$ sudo ./lynis update info
```

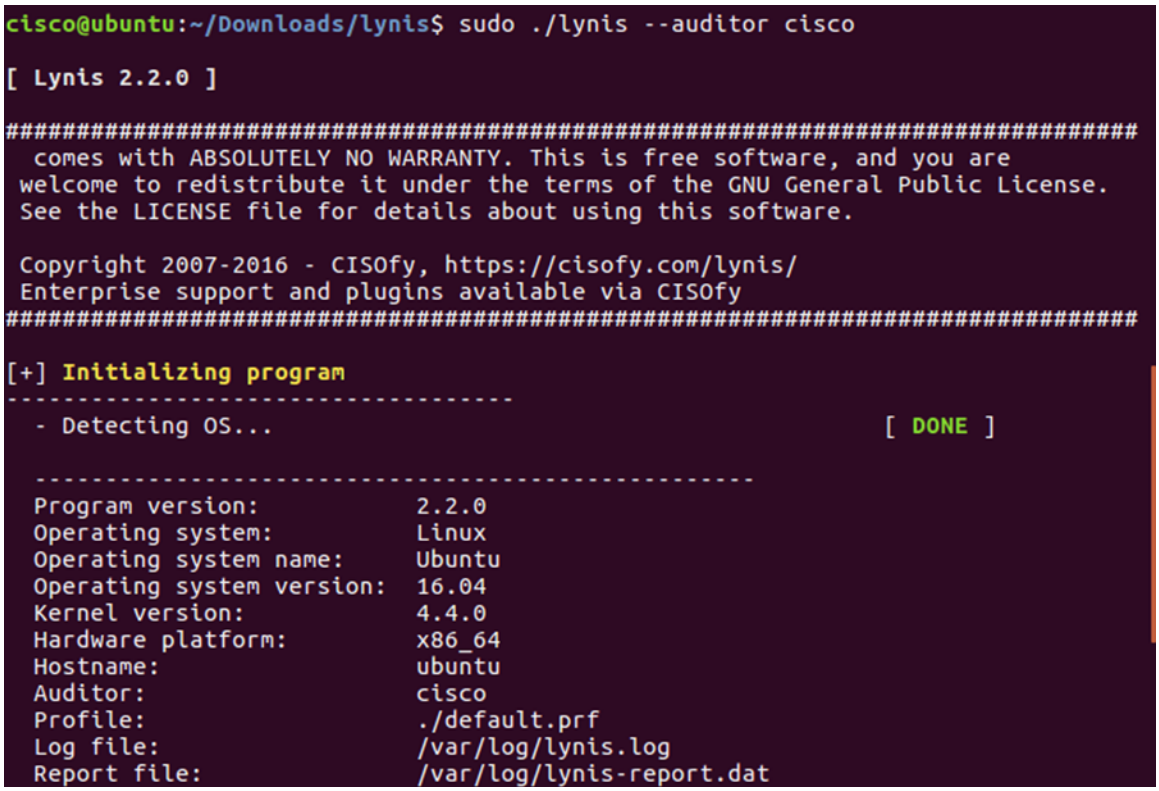


Este comando verifica se esta é a versão mais recente da ferramenta e as atualizações para a ferramenta à data de escrita deste laboratório.

Passo 3: Executar a ferramenta

a. Introduza o seguinte comando no terminal e pressione **Enter**:

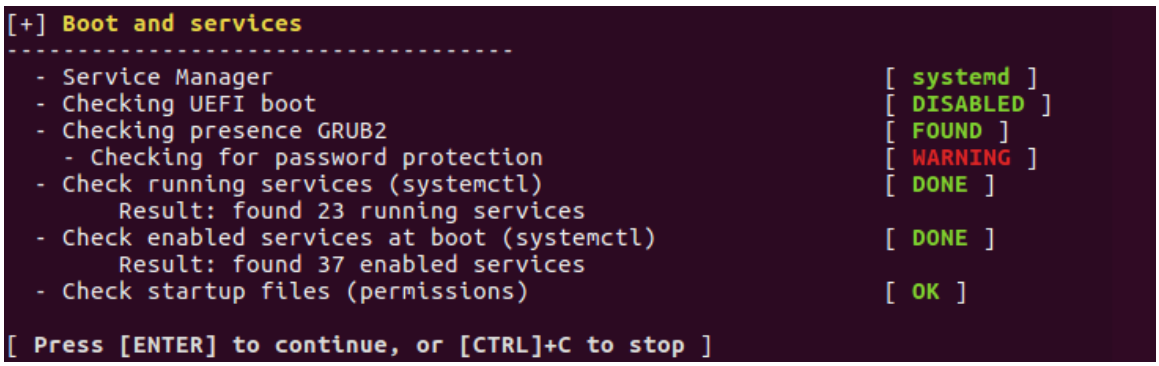
```
cisco@ubuntu:~/Downloads/lynis$ sudo ./lynis --auditor cisco
```



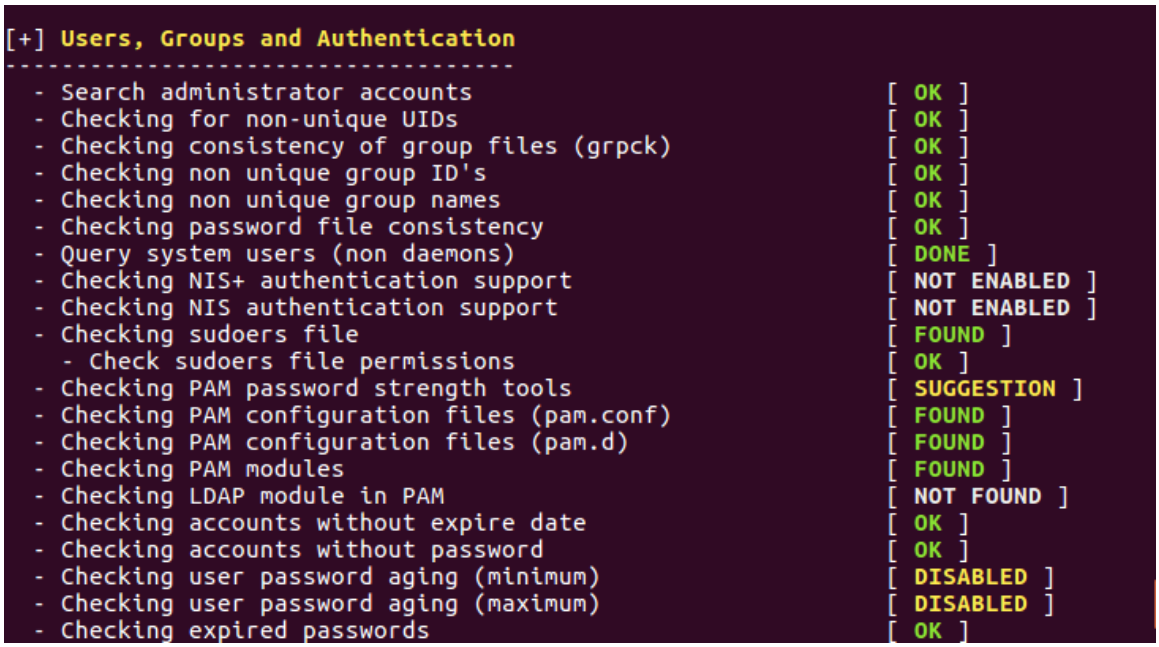
Conforme mostrado em cima, a ferramenta começará a auditar usando o utilizador **cisco** como o auditor.

Nota: Irá receber **alertas** (warnings).

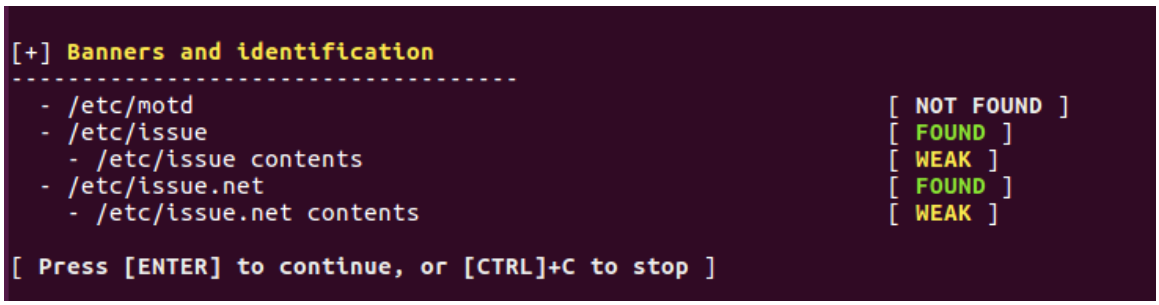
b. Para continuar com cada passo da auditoria pressione **Enter**. Irá receber alertas conforme mostrado em baixo.



c. Irá receber sugestões, conforme mostrado em baixo.



d. Irá receber uma notificação sobre uma qualquer configuração que seja fraca conforme mostrado em baixo.



e. Irá receber sugestões detalhadas de melhorias de segurança, bem como um resumo final que fornece a localização onde pode encontrar o ficheiro de log.

Passo 4: Analisar os Resultados

a. Faça Scroll para cima até à seção de resultados depois da ferramenta ter concluído a sua execução.

Quantos Alertas (Warnings) recebeu? _____

Quantas sugestões recebeu? _____

b. Percorra as sugestões e selecione uma. Pesquise uma sugestão que possa implementar para resolver o problema.

Qual é a sugestão que optou por seguir?

_____

_____

Qual é a sua solução sugerida?

_____

_____

SKUs

Lynis: https://cisofy.com/lynis/