Laboratório – Blindagem de um sistema Linux

Objetivos

Demonstre o uso de uma ferramenta de auditoria de segurança para endurecer um sistema Linux.

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.

Recursos necessários

- PC com Ubuntu 16.04 Desktop LTS instalado em um VirtualBox ou em uma máquina virtual VMware.

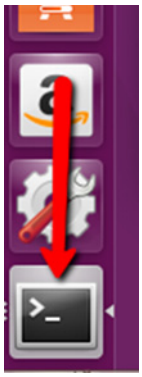
Passo 1: Abra uma janela de terminal no Ubuntu.

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

Usuário: **cisco**

Senha: **password**

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



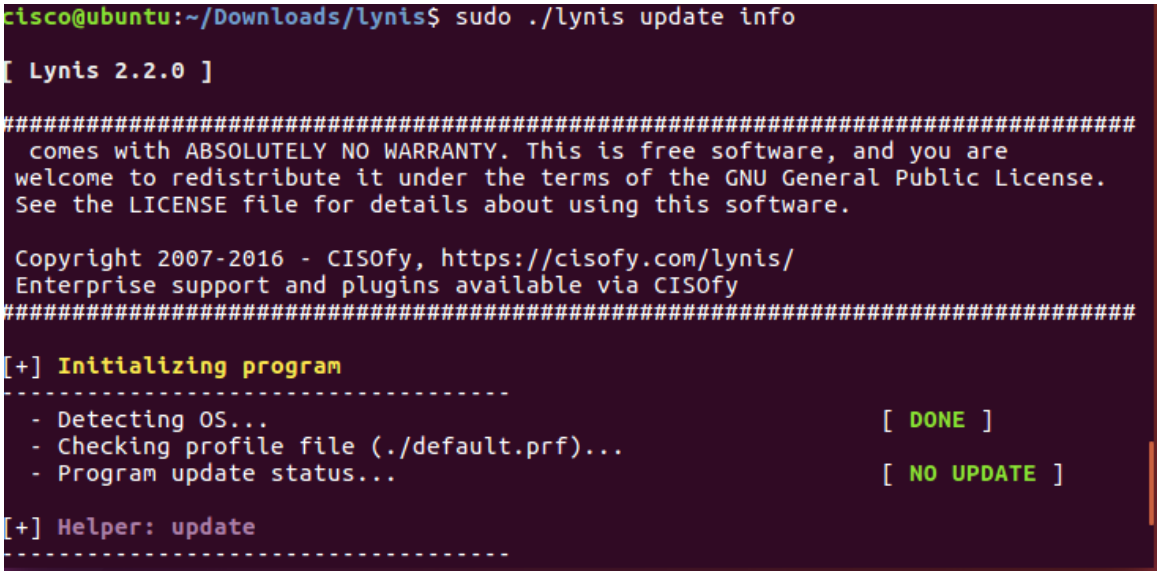
Passo 2: A ferramenta Lynis

a. No command prompt (prompt de comando), digite o seguinte comando para mudar para o diretório lynis:

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

b. No command prompt (prompt de comando), digite o seguinte comando e digite a senha **password** quando solicitado:

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

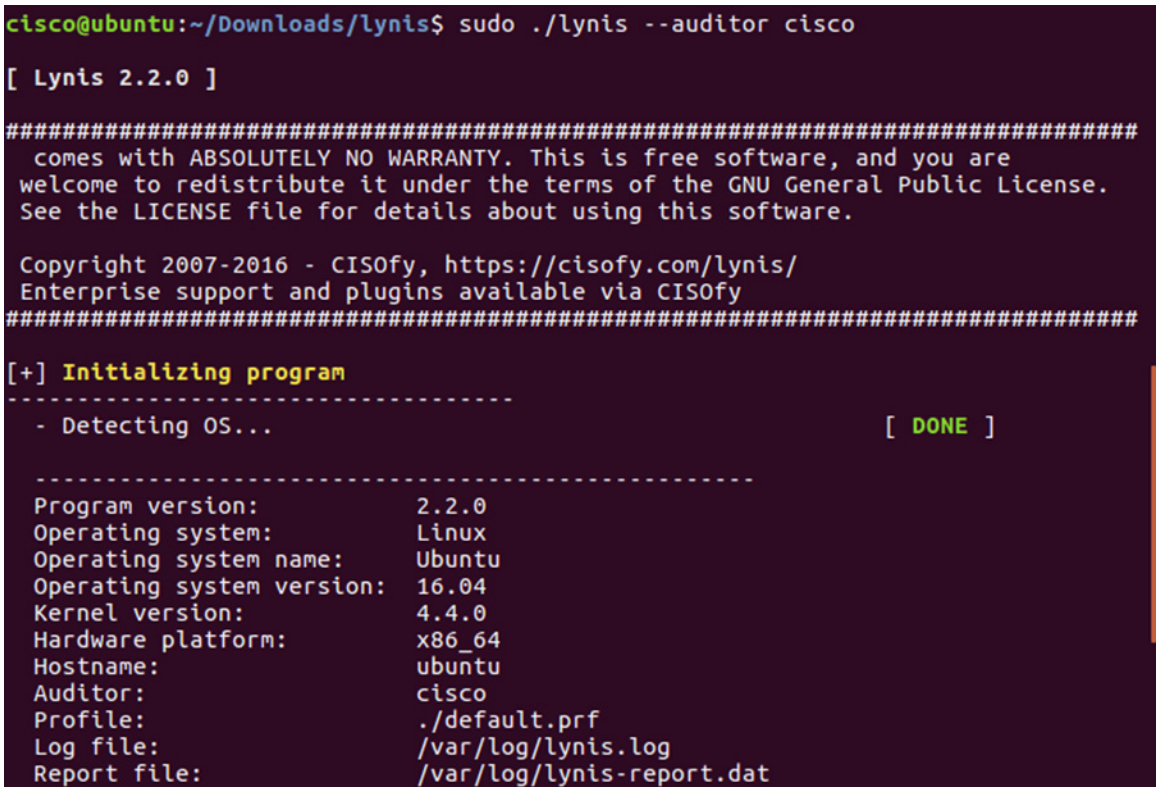


Esse comando verifica se essa é a versão mais recente e atualiza para a ferramenta utilizada no momento em que este laboratório estava sendo escrito.

Passo 3: Executar a ferramenta

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

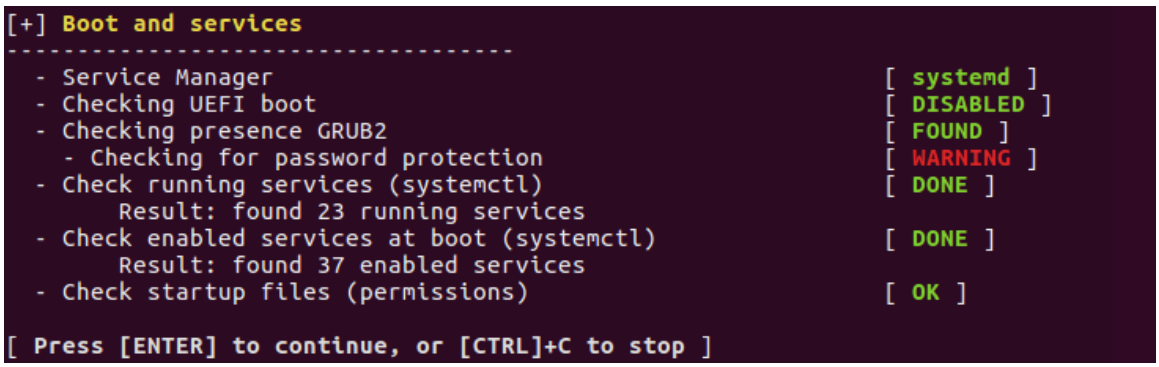
```
cisco@ubuntu:~/Downloads/lynis$ sudo ./lynis --auditor cisco
```



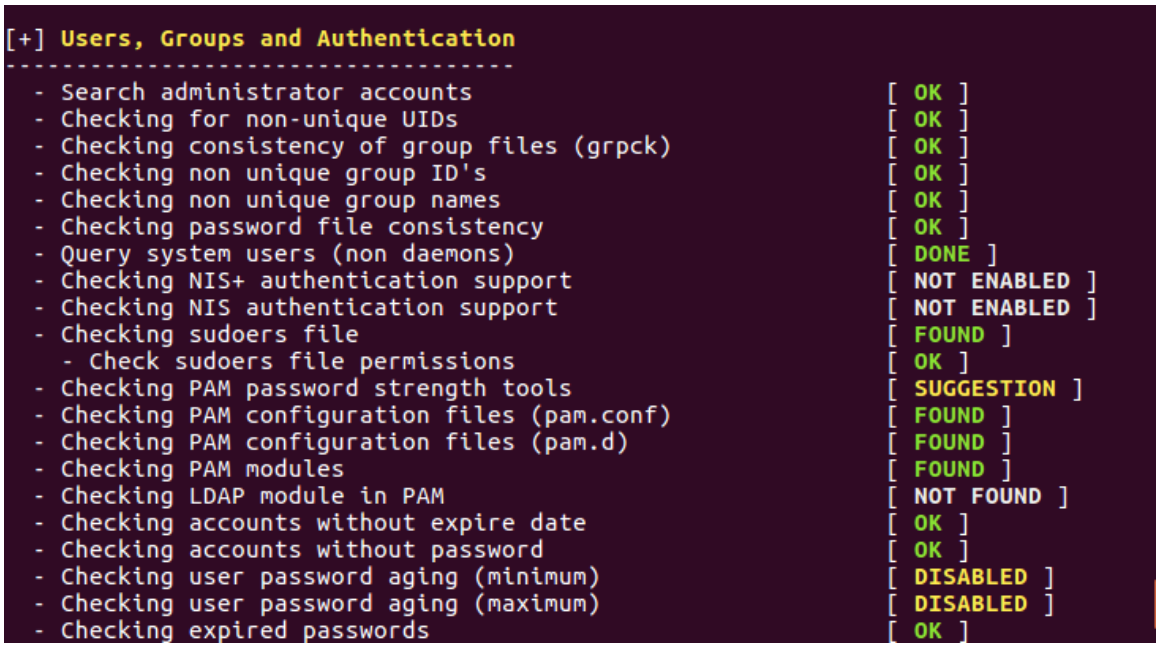
Conforme exibido acima, a auditoria começará com o usuário **cisco** como o auditor.

Observação: Você receberá **avisos**.

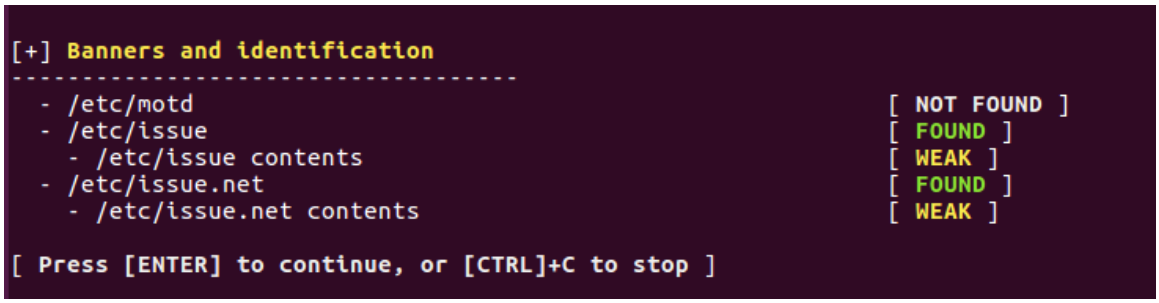
b. Para continuar com cada estágio do processo de auditoria, pressione **Enter**. Você receberá avisos, conforme mostrado a seguir.



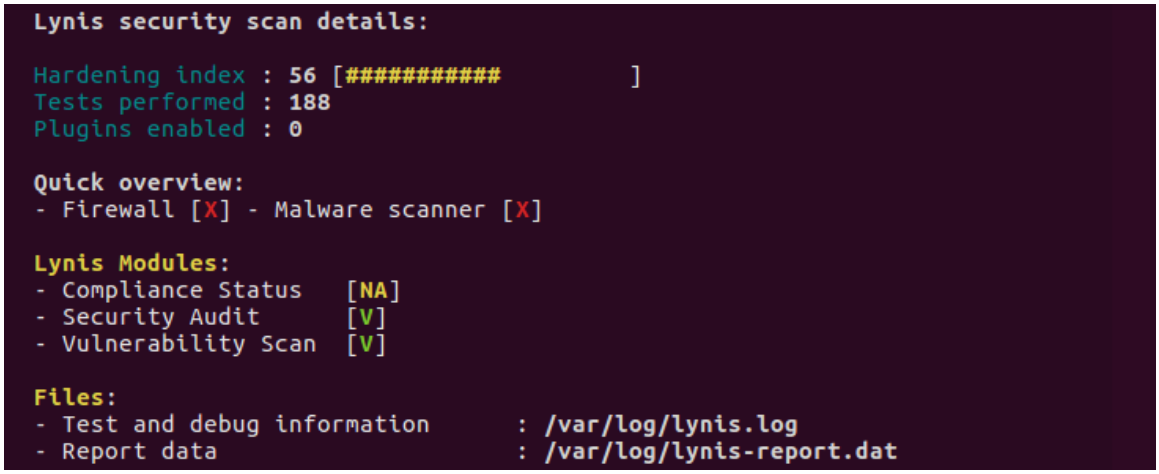
c. Você receberá sugestões, conforme mostrado a seguir.



d. Você receberá uma notificação para qualquer configuração que esteja fraca, conforme mostrado abaixo:



e. Você receberá sugestões detalhadas de melhoria na segurança, além de um resumo final, que fornece o local onde você pode encontrar o arquivo de log.



Passo 4: Analisar resultados

a. Role para cima, para a seção de resultados, depois que a ferramenta tiver concluído sua execução.

   Quantos avisos você recebeu? _____

   Quantas sugestões você recebeu?

b. Role pelas sugestões e selecione uma. Você pesquisará uma sugestão que pode implementar para abordar o problema.

   Qual sugestão você está abordando?

   Qual é sua solução sugerida?

Referências

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

