Lynis

Ary Felipe Farah e Silva

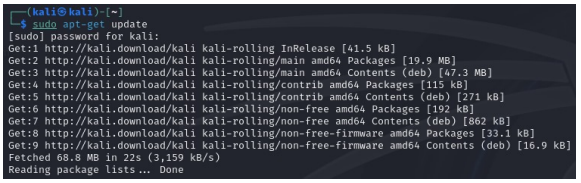
1. Criar e configurar o ambiente com a VM Linux com o VMWare, como feito nas últimas práticas.
2. Executar os exercícios do texto "Auditoria de SO Linux com Lynis", registrando no relatório os resultados obtidos.
3. Pesquisar sobre as vulnerabilidades e falhas encontradas e tentar resolvê-las, registrando no relatório os resultados obtidos.
4. Finalizar o relatório com seus comentários sobre os resultados obtidos, o que aprendeu, as dúvidas, críticas e sugestões sobre a atividade.
5. Fazer a entrega do relatório em formato PDF ou TXT.

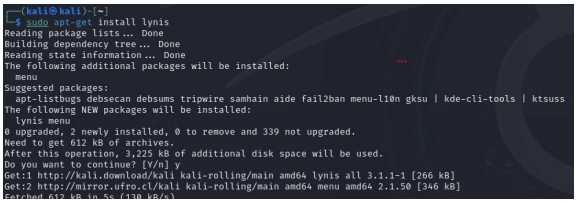
Praticando

Instalação

`sudo apt-get update`

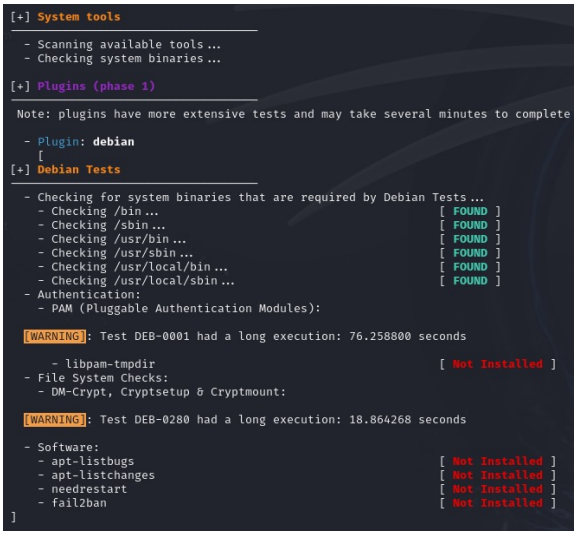
`sudo apt-get install lynis`





Auditoria Completa

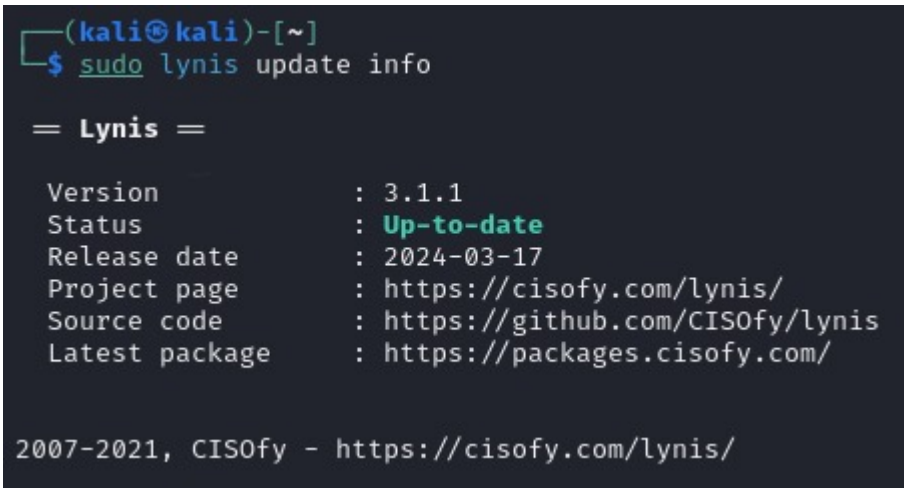
`sudo lynis audit system`



... (muitos e muitos prints)

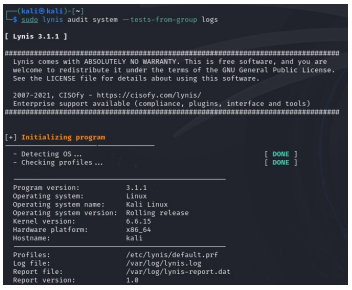
Verificação de Atualização do Sistema

`sudo lynis update info`



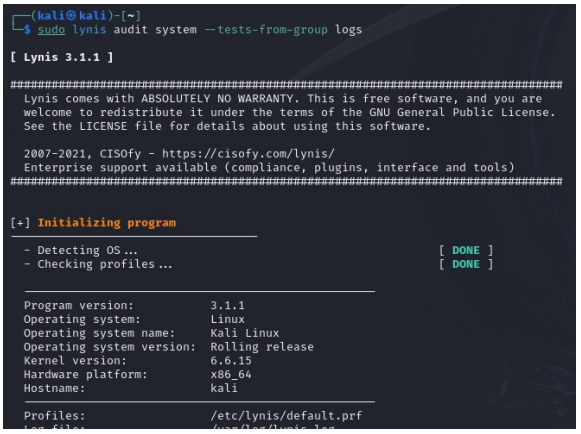
Auditoria de Logs

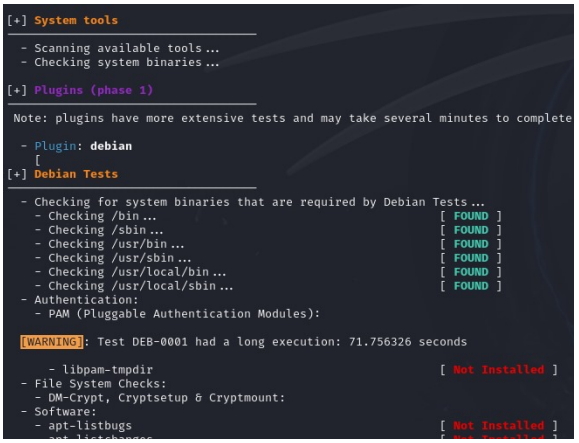
`sudo lynis audit system --tests-from-group logs`



Verificação de Configuração de SSH

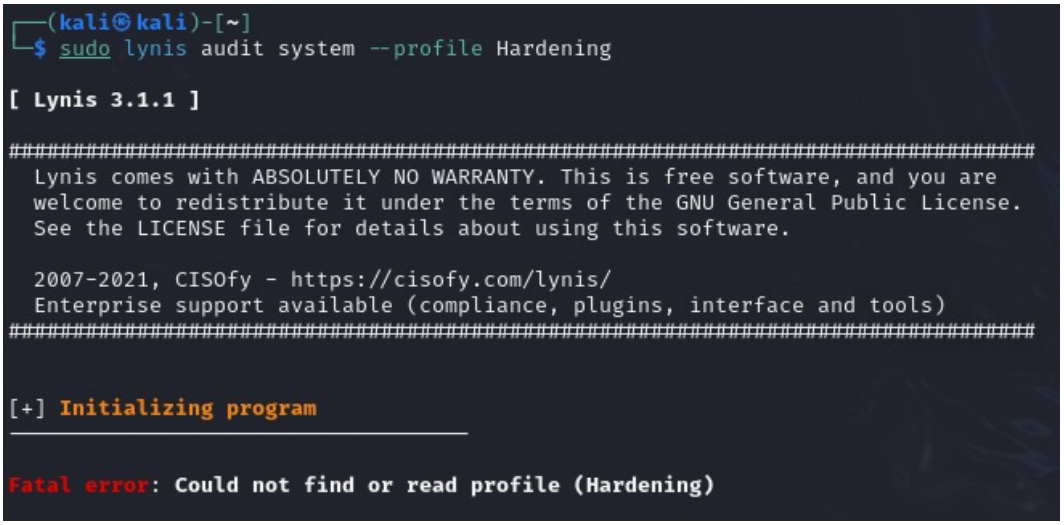
```
sudo lynis audit system --tests-from-group ssh
```





Verificação de Hardening

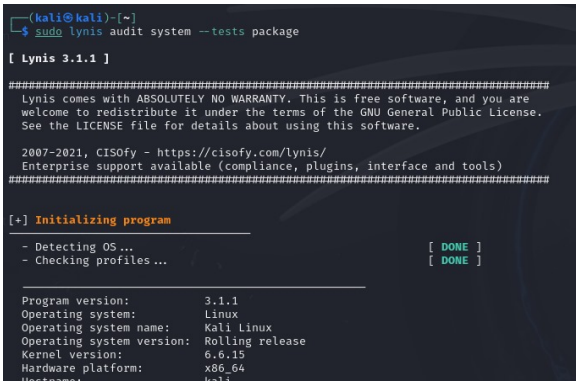
```
sudo lynis audit system --profile Hardening
```

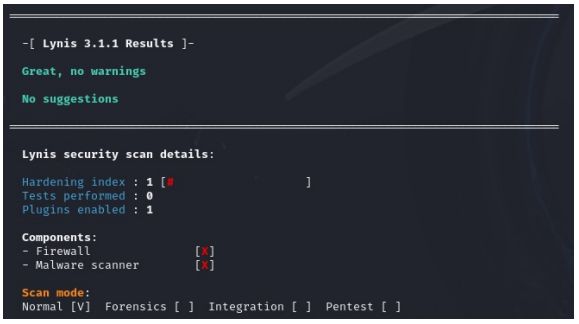


?

Vulnerabilidades em Pacote

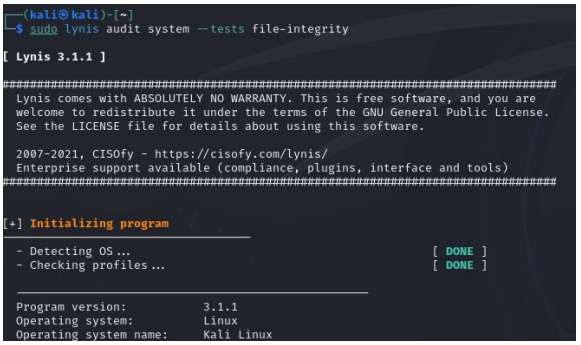
`sudo lynis audit system --tests package`





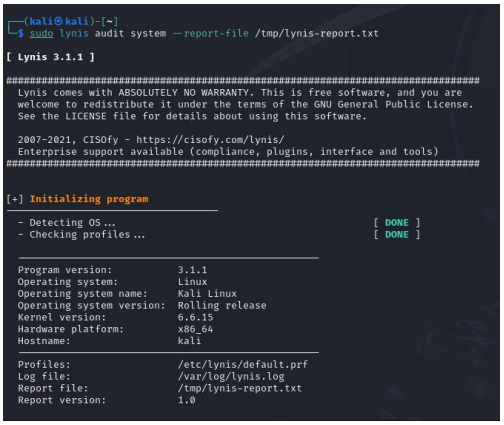
Integridade de Arquivos

`sudo lynis audit system --tests file-integrity`



Geração de Relatório Personalizado

`sudo lynis audit system --report-file /tmp/lynis-report.txt`



Conclusões

Acredito que com essa atividade prática eu consegui entendner bem o propósito do Lynis, testando (quase) todas as funcionalidades presentes no documento ***Auditoria de SO Linux com Lynis*** com sucesso. consegui distinguir os tópicos, plugins, etc. Os prints acima são todos demosntrativos, sem conter todo o conteúdo de cada comando, só pra mostrar que foi realizado no meu computador.