

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.
- Pesquisar sobre as vulnerabilidades e falhas encontradas e tentar resolvêlas, 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

```
| Calignois | Cali
```

```
["(kali@kali)-[")

| dud pat-get install lymis
| Reading package lists ... Done
| Bullding dependency tree ... Done
| Bullding dependency tree ... Done
| Reading state information ... Done
| The following additional packages will be installed:
| Suggested packages:
| apt-listbugs debsecan debsums tripwire sambain aide failZban menu-li0n gksu | kde-cli-tools | ktsuss |
| the following MKW packages will be installed:
| Lymis menu | Size of states |
| tymis menu | tymis menu | tymis menu | tymis menu |
| tymis menu | tymis menu | tymis men
```

Auditoria Completa

sudo lynis audit system

```
[ Lymis 3.1.1 ]

***HINDENTHERM PROPROSED STATES OF THE PROPRESEDENT P
```

... (muitos e muitos prints)

Verificação de Atualização do Sistema

sudo lynis update info

```
(kali® kali)-[~]
$ sudo lynis update info

= Lynis =

Version : 3.1.1
Status : Up-to-date
Release date : 2024-03-17
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/
```

Auditoria de Logs

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

```
| Carticle Statistics | Carticle Statistics
```

```
Install Liginar-report to set 100 and Stemper for PAM Sessions (COL-0280)

**Install Liginar-report to set 100 and Stemper for PAM Sessions (COL-0280)

**Install Liginar-report to set 100 and Stemper for PAM Sessions (COL-0280)

**Install Light-Liginar Sessions are simpley a little of control bugs prior to each APT installation. (COL-0280)

**Install Light-Liginary are specificated thanges prior to any suggrade via APT. (COL-0211)

**Install Liginary Anni Liginary and Sessions (Color Liginary APT. (COL-0211)

**Install Liginary Anni Liginary APT.

**Install Liginary Anni Liginary APT.

**Install Liginary APT.

**Install Liginary Confusions (Color Liginary APT.)

**Install Liginary Color Lig
```

Verificação de Configuração de SSH

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

```
[*] Initializing program

Detecting OS ...

Checking profiles ...

[*] Program version:

Operating system:

Linux

Operating system:

Linux

Operating system:

Linux

Operating system ension:

6.0.15

Hardware platform:

8.60

Audit system of the GNU General Public License.

[*] DONE ]

DONE ]

**Profiles:

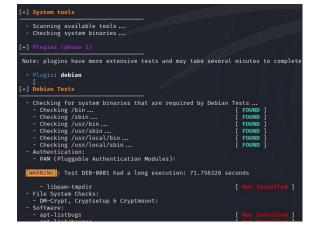
/*etc/lynis/default.prf

/*etc/lynis/default.prf

/*etc/lynis/default.prf

/*etc/lynis/default.prf

/*etc/lynis/default.prf
```



Verificação de Hardening

sudo lynis audit system --profile Hardening

?

Vulnerabilidades em Pacote

sudo lynis audit system --tests package

```
| Carlo | Carl
```

```
-[ Lynis 3.1.1 Results ]-
Great, no warnings
No suggestions

Lynis security scan details:
Hardening index : 1 [# ]
Tests performed: 0
Plugins enabled: 1

Components:
- Firewall [M]
- Malware scanner [M]

Scan mode:
Normal [V] Forensics [ ] Integration [ ] Pentest [ ]
```

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.