



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
```

```
(kali@kali):~$ sudo apt-get update
[sudo] password for kali:
Get:1 http://kali.download/kali kali-rolling InRelease [41.5 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 Packages [19.9 MB]
Get:3 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [47.3 MB]
Get:4 http://kali.download/kali kali-rolling/contrib amd64 Packages [115 kB]
Get:5 http://kali.download/kali kali-rolling/contrib amd64 Contents (deb) [271 kB]
Get:6 http://kali.download/kali kali-rolling/non-free amd64 Packages [192 kB]
Get:7 http://kali.download/kali kali-rolling/non-free amd64 Contents (deb) [862 kB]
Get:8 http://kali.download/kali kali-rolling/non-free-firmware amd64 Packages [33.1 kB]
Get:9 http://kali.download/kali kali-rolling/non-free-firmware amd64 Contents (deb) [16.9 kB]
Fetched 68.8 MB in 22s (3,159 kB/s)
Reading package lists... Done
```

```
(kali@kali):~$ sudo apt-get install lynis
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  menu
Suggested packages:
  apt-listbugs debsecan debsums tripwire samhain aide fail2ban menu-l10n gksu | kde-cli-tools | ktsuss
The following NEW packages will be installed:
  lynis menu
0 upgraded, 2 newly installed, 0 to remove and 339 not upgraded.
Need to get 612 kB of archives.
After this operation, 3,225 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://kali.download/kali kali-rolling/main amd64 lynis all 3.1.1-1 [266 kB]
Get:2 http://mirror.ufpa.br/kali kali-rolling/main amd64 menu amd64 2.1.50 [346 kB]
Fetched 612 kB in 2s (248 kB/s)
```

Auditoria Completa

```
sudo lynis audit system
```

```
(kali@kali)-[~]
└─$ sudo lynis audit system

[ Lynis 3.1.1 ]

#####
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 ]

Program version: 3.1.1
Operating system: Linux
Operating system name: Kali Linux
Operating system version: Rolling release
Kernel version: 6.6.15
Hardware platform: x86_64
Hostname: kali

Profiles: /etc/lynis/default.prf
Log file: /var/log/lynis.log
Report file: /var/log/lynis-report.dat
Report version: 1.0
Plugin directory: /etc/lynis/plugins

Auditor: [Not Specified]
Language: en
Test category: all
Test group: all

- Program update status ... [ NO UPDATE ]
```

```
[+] System tools
- Scanning available tools ...
- Checking system binaries ...

[+] Plugins (phase 1)
Note: plugins have more extensive tests and may take several minutes to complete

- Plugin: debian
[
[+] Debian Tests
- Checking for system binaries that are required by Debian Tests ...
- Checking /bin ... [ FOUND ]
- Checking /sbin ... [ FOUND ]
- Checking /usr/bin ... [ FOUND ]
- Checking /usr/sbin ... [ FOUND ]
- Checking /usr/local/bin ... [ FOUND ]
- Checking /usr/local/sbin ... [ FOUND ]
- Authentication:
- PAM (Pluggable Authentication Modules):
[WARNING]: Test DEB-0001 had a long execution: 76.258800 seconds
- libpam-tmpdir [ Not Installed ]
- File System Checks:
- DM-Crypt, Cryptsetup & Cryptmount:
[WARNING]: Test DEB-0280 had a long execution: 18.864268 seconds
- Software:
- apt-listbugs [ Not Installed ]
- apt-listchanges [ Not Installed ]
- needrestart [ Not Installed ]
- fail2ban [ Not Installed ]
]
```

... (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
```

```

(kali@kali)~$ sudo lynis audit system --tests-from-group logs
[ Lynis 3.1.1 ]

#####
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 ]

Program version: 3.1.1
Operating system: Linux
Operating system name: Kali Linux
Operating system version: Rolling release
Kernel version: 6.6.15
Hardware platform: x86_64
Hostname: kali

Profiles: /etc/lynis/default.prf
Log file: /var/log/lynis.log
Report file: /var/log/lynis-report.dat
Report version: 1.0

```

```

Suggestions (5):
- Install libpam-tmpdir to set TMP and TMPDIR for PAM sessions [DEB-0208]
  https://cisofy.com/lynis/controls/DEB-0208/
- Install apt-listbugs to display a list of critical bugs prior to each APT installation. [DEB-0310]
  https://cisofy.com/lynis/controls/DEB-0310/
- Install apt-listchanges to display any significant changes prior to an upgrade via APT. [DEB-0611]
  https://cisofy.com/lynis/controls/DEB-0611/
- Install mdestart, alternatively to debian-goodies, so that you can run mdestart after upgrades to determine which daemons are using old versions of libraries and need restarting. [DEB-0613]
  https://cisofy.com/lynis/controls/DEB-0613/
- Install fail2ban to automatically ban hosts that commit multiple authentication errors. [DEB-0800]
  https://cisofy.com/lynis/controls/DEB-0800/

Follow-up:
- Show details of a test (lynis show details TEST-ID)
- Check the logfile for all details (less /var/log/lynis.log)
- Read security controls texts (https://cisofy.com)
- Use --upload to upload data to control system (lynis enterprise users)

```

Verificação de Configuração de SSH

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

```

(kali@kali)~$ sudo lynis audit system --tests-from-group logs
[ Lynis 3.1.1 ]

#####
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 ]

Program version: 3.1.1
Operating system: Linux
Operating system name: Kali Linux
Operating system version: Rolling release
Kernel version: 6.6.15
Hardware platform: x86_64
Hostname: kali

Profiles: /etc/lynis/default.prf
Log file: /var/log/lynis.log
Report file: /var/log/lynis-report.dat
Report version: 1.0

```

```

[+] System tools
- Scanning available tools...
- Checking system binaries...

[+] Plugins (phase 1)
Note: plugins have more extensive tests and may take several minutes to complete

- Plugin: debian
[
[+] Debian Tests
- Checking for system binaries that are required by Debian Tests...
- Checking /bin... [ FOUND ]
- Checking /sbin... [ FOUND ]
- Checking /usr/bin... [ FOUND ]
- Checking /usr/sbin... [ FOUND ]
- Checking /usr/local/bin... [ FOUND ]
- Checking /usr/local/sbin... [ FOUND ]
- Authentication:
- PAM (Pluggable Authentication Modules):

[WARNING]: Test DEB-0001 had a long execution: 71.756326 seconds

- libpam-tmpdir [ Not Installed ]
- File System Checks:
- DM-Crypt, Cryptsetup & Cryptmount:
- Software:
- apt-listbugs [ Not Installed ]

```

Verificação de Hardening

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

```

(kali@kali)~$ sudo lynis audit system --profile Hardening
[ Lynis 3.1.1 ]

#####
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

Fatal error: Could not find or read profile (Hardening)

```

?

Vulnerabilidades em Pacote

```
sudo lynis audit system --tests package
```

```
(kali@kali)-[~]
└─$ sudo lynis audit system --tests package

[ Lynis 3.1.1 ]

#####
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 ]

Program version:      3.1.1
Operating system:     Linux
Operating system name: Kali Linux
Operating system version: Rolling release
Kernel version:       6.6.15
Hardware platform:    x86_64
Hostname:              kali
```

```
-[ 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 [ X ]
- Malware scanner [ X ]

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

Integridade de Arquivos

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

```
(kali@kali)-[~]
└─$ sudo lynis audit system --tests file-integrity

[ Lynis 3.1.1 ]

#####
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 ]

Program version:      3.1.1
Operating system:     Linux
Operating system name: Kali Linux
```

```
-[ 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 [ X ]
- Malware scanner [ X ]

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

Lynis modules:
- Compliance status [ ? ]
- Security audit [ V ]
- Vulnerability scan [ V ]

Files:
- Test and debug information : /var/log/lynis.log
- Report data : /var/log/lynis-report.dat
```

Geração de Relatório Personalizado

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

```
(kali@kali) ~$ sudo lynis audit system --report-file /tmp/lynis-report.txt
[ Lynis 3.1.1 ]

=====
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 ]

Program version: 3.1.1
Operating system: Linux
Operating system name: Kali Linux
Operating system version: Rolling release
Kernel version: 6.6.15
Hardware platform: x86_64
Hostname: kali

Profiles: /etc/lynis/default.prf
Log file: /var/log/lynis.log
Report file: /tmp/lynis-report.txt
Report version: 1.0
```

```
-[ Lynis 3.1.1 Results ]-

Warnings (2):
1 Couldn't find 2 responsive nameservers [NETW-2705]
https://cisofy.com/lynis/controls/NETW-2705/
1 iptables module(s) loaded, but no rules active [FIRE-4512]
https://cisofy.com/lynis/controls/FIRE-4512/

Suggestions (49):
1]
* Install libpam-tmpdir to set $TMP and $TMPDIR for PAM sessions [DEB-0280]
https://cisofy.com/lynis/controls/DEB-0280/
* Install apt-listbugs to display a list of critical bugs prior to each APT installation. [DEB-0810]
https://cisofy.com/lynis/controls/DEB-0810/
* Install apt-listchanges to display any significant changes prior to any upgrade via APT. [DEB-0811]
https://cisofy.com/lynis/controls/DEB-0811/
* Install needrestart, alternatively to debian-goodies, so that you can run needrestart after upgrades to determin
https://cisofy.com/lynis/controls/DEB-0831/
* Install fail2ban to automatically ban hosts that commit multiple authentication errors. [DEB-0880]
https://cisofy.com/lynis/controls/DEB-0880/
* Set a password on GRUB boot loader to prevent altering boot configuration (e.g. boot in single user mode without
https://cisofy.com/lynis/controls/BOOT-5122/
* Consider hardening system services [BOOT-5264]
- Details : Run '/usr/bin/systemd-analyze security SERVICE' for each service
https://cisofy.com/lynis/controls/BOOT-5264/
* If not required, consider explicit disabling of core dump in /etc/security/limits.conf file [KRNL-5820]
```

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.