

Relatório para Hardening de Linux com Lynis.

Lynis é uma ferramenta de código aberto desenvolvida por Michael Boelen para realizar auditoria de segurança em sistemas da família Unix/Linux, com o Lynis os administradores de sistema podem verificar as configurações de segurança através de um extensivo escâner de vulnerabilidades e posteriormente aplicar as devidas correções a fim de obter um ambiente seguro.

Segundo o próprio site do desenvolvedor o Lynis executa centenas de testes individuais para determinar a segurança de um sistema e armazena o resultado em um arquivo de “log” com as informações de obtidas durante o escaneamento com avisos e sugestões para solucionar a possível vulnerabilidade.

Sequência de procedimentos durante o “scan” do Lynis.

1. Determina o sistema operacional.
2. Procura por utilitários e ferramentas disponíveis.
3. Checa por atualizações de Lynis.
4. Executa testes através dos “plugins” ativados.
5. Executa testes de segurança por categoria.
6. Exibe um relatório do “scan” de segurança com o atual status do sistema.

A principal vantagem do Lynis sobre outras ferramentas similares é sua vasta quantidade de testes de segurança baseados em recomendações do CIS, NIST, NSA, OpenSCAP e dos próprios fornecedores como Red Hat e Debian.

O Lynis possui quatro opções de instalação:

1. Via gerenciador de pacotes dos sistemas operacionais Red Hat (**#yum install lynis**), Debian/Ubuntu (**#apt-get install lynis**).
2. Via clone do projeto Git (**\$ git clone <https://github.com/CISOfy/lynis>**), para executar abra o diretório (**\$cd lynis**) e digite o comando (**\$lynis audit system**).
3. Via download do arquivo comprimido em “tarball” direto do site do desenvolvedor utilizando (**\$wget <https://cisofy.com/files/lynis><versão>.tar.gz**).
4. Via Homebrew para macOS (**\$brew install lynis**).

Para realizar a instalação deste tutorial utilizaremos o modo via gerenciador de pacotes do sistema operacional Ubuntu 16.04.3 Xenial Xerus, antes de instalar a ferramenta Lynis é necessário alguns procedimentos preliminares. Este modo garante a segurança através da verificação da chave GPG publica do desenvolvedor pelo “APT” validando a autenticidade do software.

1. Importar a chave publica localizada no repositório do site da CISOfy.



```
root@Aspire-4720Z: /home/sergio
root@Aspire-4720Z:/home/sergio# wget -O - https://packages.cisofy.com/keys/cisofy-software-public.key | apt-key add -
--2017-11-30 18:07:27-- https://packages.cisofy.com/keys/cisofy-software-public.key
Resolvendo packages.cisofy.com (packages.cisofy.com)... 37.97.194.171, 2a01:7c8:aac2:37b::1
Conectando-se a packages.cisofy.com (packages.cisofy.com)[37.97.194.171]:443... conectado.
A requisição HTTP foi enviada, aguardando resposta... 200 OK
Tamanho: 5342 (5,2K) [application/octet-stream]
Salvando em: "STDOUT"

100%[=====] 5,22K --KB/s in 0s

2017-11-30 18:07:28 (240 MB/s) - escrito para a saída padrão [5342/5342]
OK
```

2. Adicionar o caminho do repositório de pacotes do Lynis ao arquivo source.list do “APT”. (**#echo "deb <https://packages.cisofy.com/community/lynis/deb/xenial/main>" > /etc/apt/sources.list.d/cisofy-lynis.list**).
3. instalar o Lynis (**#apt-get update && apt-get install lynis**).

Para executar o “Lynis” e realizar o primeiro “scan” básico no sistema digite o comando no terminal “shell” do Ubuntu (**#lynis audit system**) e aguarde o fim do processo.

```
root@Aspire-4720Z:/home/sergic# lynis audit system

[ Lynis 2.5.7 ]

#####
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.

2007-2017, CISOfy - https://cisofy.com/lynis/
Enterprise support available (compliance, plugins, interface and tools)
#####

[+] Initializing program
-----
- Detecting OS... [ DONE ]
- Checking profiles... [ DONE ]
- Detecting language and localization [ pt ]

-----
Program version: 2.5.7
Operating system: Linux
Operating system name: Ubuntu Linux
Operating system version: 16.04
Kernel version: 4.10.0
Hardware platform: i686
Hostname: Aspire-4720Z
-----
Profiles: /etc/lynis/default.prf
Log file: /var/log/lynis.log
Report file: /var/log/lynis-report.dat
Report version: 1.0
Plugin directory: /usr/share/lynis/plugins
-----
Auditor: [Not Specified]
Language: pt
Test category: all
Test group: all
-----
- Program update status... [ NO UPDATE ]
```

Para visualizar os resultados do scan o Lynis fornece três meios: em tempo real através de visualização da tela do “host”, via arquivo de “log” através do diretório “/var/log/lynis.log” e via arquivo de relatório “/var/log/lynis-report.dat”.

```
Lynis security scan details:

Hardening index : 57 [#####]
Tests performed : 201
Plugins enabled : 0

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

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
```

Relatórios

<https://github.com/d4t4king/lynis-report-converter>

Comandos:

Comando	Descrição
#lynis update	Atualização da ferramenta.
#lynis update info	Verifica a atualização da ferramenta.
#lynis audit system	Executa auditoria básica do sistema.
#lynis show commands	Mostra os comandos disponíveis.
#lynis show help	Ajuda da ferramenta.
#lynis show profiles	Visualiza os perfis descobertos.
#lynis settings	Lista todas as configurações dos perfis ativos.
#lynis show version	Mostra a versão do Lynis.

Opções:

Opção	Descrição
- -auditor	Atribui um nome de auditor no relatório.
- -cronjob	Executa o Lynis através do Cronjob.
- -debug	Visualiza informações de Debug da ferramenta.
- -help ou -h	Mostra ajuda da ferramenta.
- -man-page	Visualiza o manual da ferramenta.
- -no-colors	Não usa cores para o relatório.
- -pentest	Scan para pentest.
- -quick ou -Q	Não espera interação do usuário.
- -quiet ou -q	Mostra somente avisos de alerta.
- -reverse-colors	Reverte as cores para o relatório.
- -verbose	Mostra mais saídas na tela de execução.