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.

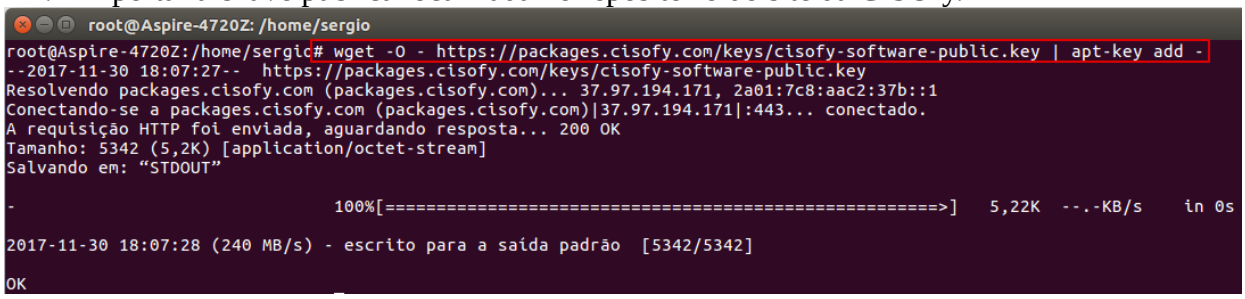
A principal vantagem do Lynis sobre outras ferramentas similares é sua vasta quantidade de testes de segurança baseados em recomendações do CIS, NIST, NSA, OpenSCAP e dos próprios fornecedores como Red Hat e Debian.

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***).

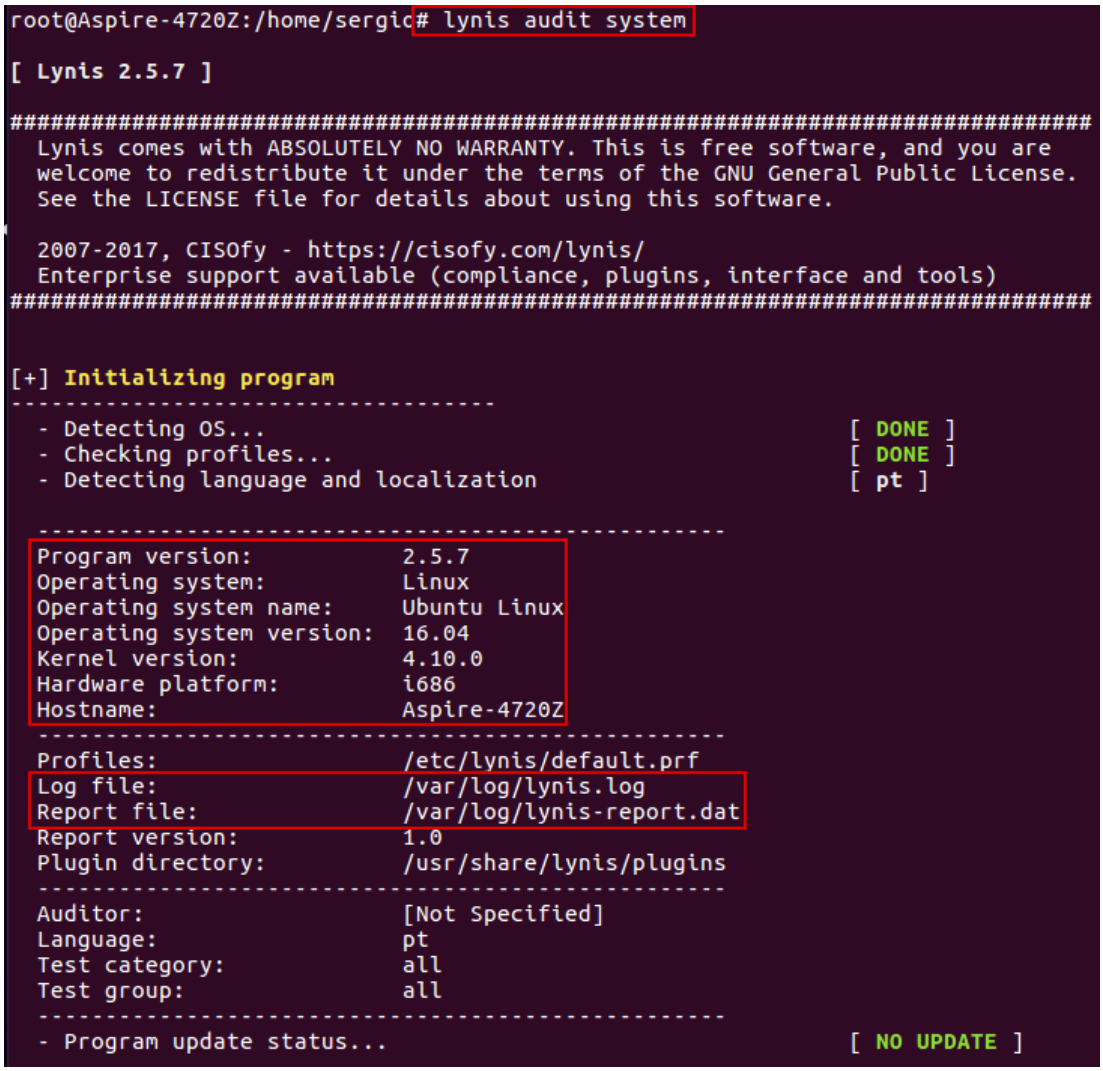
Para realizar a instalação deste tutorial utilizaremos o modo via gerenciador de pacotes do sistema operacional Ubuntu 16.04.3 Xenial Xerus, antes de instalar a ferramenta Lynis é necessário alguns procedimentos preliminares. Este modo garante a segurança através da verificação da chave GPG publica do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

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

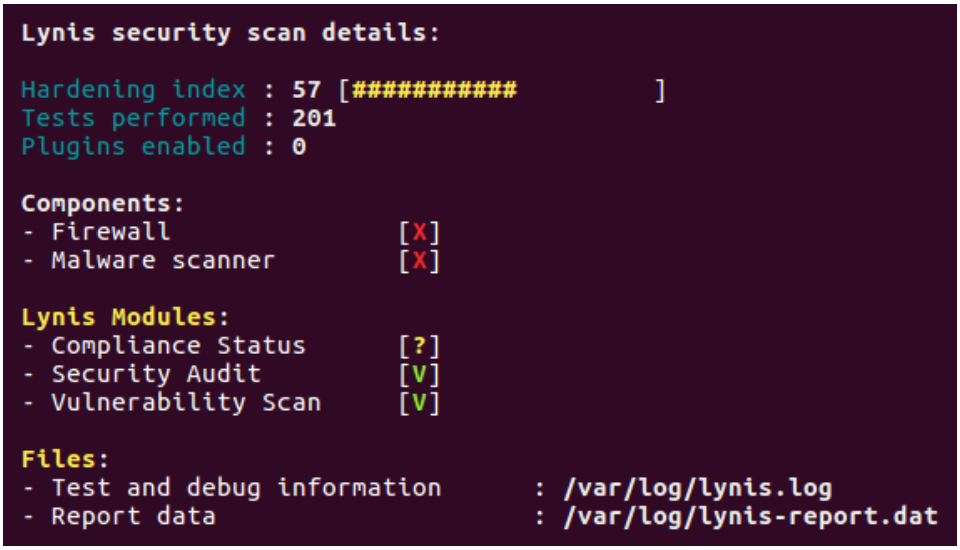


2. Adicionar o caminho do repositório de pacotes do Lynis ao arquivo source.list do "APT". (***#echo "deb https://packages.cisofy.com/community/lynis/deb/ xenial main" > /etc/apt/sources.list.d/cisofy-lynis.list***).
3. instalar o Lynis (***#apt-get update && apt-get install lynis***).

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.



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”**.



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.