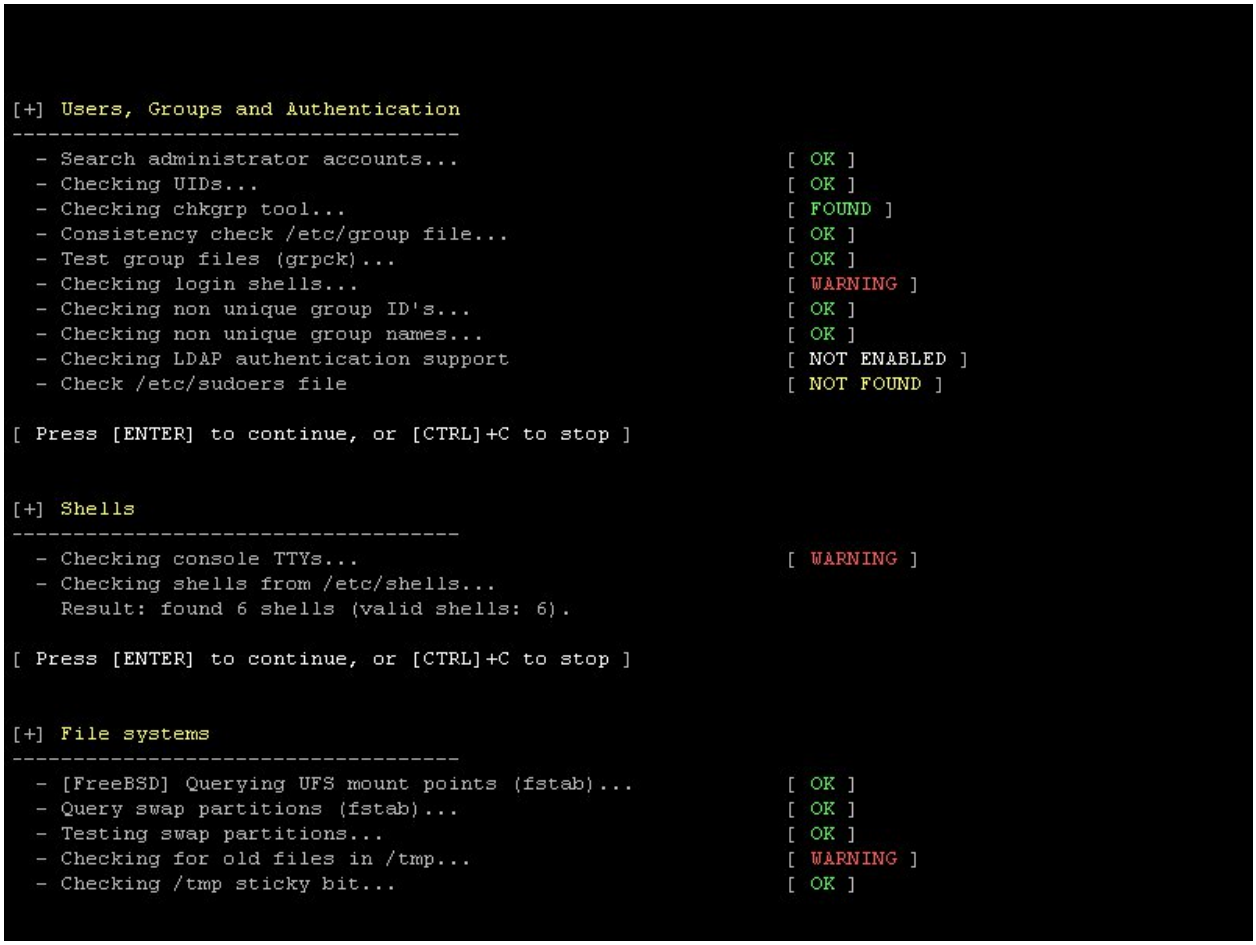
Lynis – Ferramenta para auditoria [By: Tr3nts]

GELOS

Grupo de Extensão em
Livre & Open Source

Contexto: Breve introdução

Lynis é uma ferramenta de auditoria em segurança, testada com finalidade em detecção ***IDS/IPS/Host IDS/Host IPS*** para sistemas rodando Linux, MacOS ou sistema operacional baseado em Unix.



O projeto é um software de código aberto com a **licença GPL** e disponível desde 2007. Foi escrito em Shell.

O Lynis também possui uma versão para empresas, chamada Lynis Enterprise com foco em plataforma *SaaS* e *Self-hosted*.

Para que serve?

Para quem gosta de verificar a confiabilidade, integridade e autenticidade e a disponibilidade do seu sistema padrão, essa é uma opção *Open Source* que valha a pena.

Objetivos do projeto -

- **Auditoria de segurança**
- **Teste de conformidade (por exemplo, PCI, HIPAA, SOx)**
- ***Pentesting***
- **Detecção de vulnerabilidades**
- **Mitigações do sistema**

Desenvolvedores: Testar imagens do Docker, e melhore as mitigações de sua aplicação web implantada;

Administradores de sistema: Escaneamentos diários de “saúde” para descobrir novos pontos fracos;

Auditores de TI: Mostrar aos usuários o que pode ser feito para melhorar a segurança.

Pentesters: Descubrir fraquezas de segurança nos sistemas dos usuários, podendo eventualmente resultar em comprometimentos do sistema.

Sistemas operacionais suportados

Lynis funciona em quase todos os sistemas e versões baseadas em UNIX, inclusive:

- **AIX**
- **FreeBSD**
- **HP-UX**
- **Linux**
- **MacOS**

- **NetBSD**
- **NixOS**
- **OpenBSD**
- **Solaris**

Funciona até mesmo em sistemas como o **Raspberry Pi**, dispositivos IoT, e dispositivos de armazenamento QNAP.