



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.

```
[+] Users, Groups and Authentication
-----
- Search administrator accounts... [ OK ]
- Checking UIDs... [ OK ]
- Checking chkgrp tool... [ FOUND ]
- Consistency check /etc/group file... [ OK ]
- Test group files (grpck)... [ OK ]
- Checking login shells... [ WARNING ]
- Checking non unique group ID's... [ OK ]
- Checking non unique group names... [ OK ]
- Checking LDAP authentication support [ NOT ENABLED ]
- Check /etc/sudoers file [ NOT FOUND ]

[ Press [ENTER] to continue, or [CTRL]+C to stop ]

[+] Shells
-----
- Checking console TTYs... [ WARNING ]
- Checking shells from /etc/shells...
  Result: found 6 shells (valid shells: 6).

[ Press [ENTER] to continue, or [CTRL]+C to stop ]

[+] File systems
-----
- [FreeBSD] Querying UFS mount points (fstab)... [ OK ]
- Query swap partitions (fstab)... [ OK ]
- Testing swap partitions... [ OK ]
- Checking for old files in /tmp... [ WARNING ]
- Checking /tmp sticky bit... [ OK ]
```

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;

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

Pentesters: Descobrir 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.