

# Laboratório – Blindagem de um sistema Linux

## Objetivos

Demonstre o uso de uma ferramenta de auditoria de segurança para endurecer um sistema Linux.

## Histórico/Cenário

A auditoria de um sistema em busca de possíveis configurações erradas ou serviços não protegidos é um aspecto importante da blindagem de um sistema. Lynis é uma ferramenta de auditoria de segurança de código aberto com um conjunto automatizado de scripts desenvolvidos para testar um sistema Linux.

## Recursos necessários

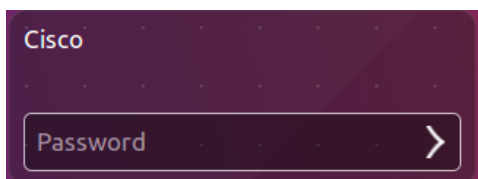
- PC com Ubuntu 16.04 Desktop LTS instalado em um VirtualBox ou em uma máquina virtual VMware.

### Passo 1: Abra uma janela de terminal no Ubuntu.

- Inicie uma sessão no Ubuntu usando as seguintes credenciais:

Usuário: **cisco**

Senha: **password**



- Clique no ícone do terminal para abrir uma janela de terminal.



### Passo 2: A ferramenta Lynis

- No command prompt (prompt de comando), digite o seguinte comando para mudar para o diretório lynis:

```
cisco@ubuntu:~$ cd Downloads/lynis/
```

```
cisco@ubuntu:~$ cd Downloads/lynis/
cisco@ubuntu:~/Downloads/lynis$
```

- b. No command prompt (prompt de comando), digite o seguinte comando e digite a senha **password** quando solicitado:

```
cisco@ubuntu:~/Downloads/lynis$ sudo ./lynis update info
```

```
cisco@ubuntu:~/Downloads/lynis$ sudo ./lynis update info

[ Lynis 2.2.0 ]

#####
 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.

 Copyright 2007-2016 - CISOfy, https://cisofy.com/lynis/
 Enterprise support and plugins available via CISOfy
#####

[+] Initializing program
-----
- Detecting OS... [ DONE ]
- Checking profile file (./default.prf)... [ NO UPDATE ]
- Program update status...

[+] Helper: update
-----
```

Esse comando verifica se essa é a versão mais recente e atualiza para a ferramenta utilizada no momento em que este laboratório estava sendo escrito.

### Passo 3: Executar a ferramenta

- a. Digite o seguinte comando no terminal e pressione **Enter**:

```
cisco@ubuntu:~/Downloads/lynis$ sudo ./lynis --auditor cisco
```

```
cisco@ubuntu:~/Downloads/lynis$ sudo ./lynis --auditor cisco

[ Lynis 2.2.0 ]

#####
 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.

 Copyright 2007-2016 - CISOfy, https://cisofy.com/lynis/
 Enterprise support and plugins available via CISOfy
#####

[+] Initializing program
-----
- Detecting OS... [ DONE ]

-----
Program version:      2.2.0
Operating system:     Linux
Operating system name: Ubuntu
Operating system version: 16.04
Kernel version:       4.4.0
Hardware platform:    x86_64
Hostname:             ubuntu
Auditor:              cisco
Profile:              ./default.prf
Log file:             /var/log/lynis.log
Report file:          /var/log/lynis-report.dat
```

Conforme exibido acima, a auditoria começará com o usuário **cisco** como o auditor.

Observação: Você receberá **avisos**.

- b. Para continuar com cada estágio do processo de auditoria, pressione **Enter**. Você receberá avisos, conforme mostrado a seguir.

```
[+] Boot and services
-----
- Service Manager [ systemd ]
- Checking UEFI boot [ DISABLED ]
- Checking presence GRUB2 [ FOUND ]
  - Checking for password protection [ WARNING ]
- Check running services (systemctl) [ DONE ]
  Result: found 23 running services
- Check enabled services at boot (systemctl) [ DONE ]
  Result: found 37 enabled services
- Check startup files (permissions) [ OK ]

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

- c. Você receberá sugestões, conforme mostrado a seguir.

```
[+] Users, Groups and Authentication
-----
- Search administrator accounts [ OK ]
- Checking for non-unique UIDs [ OK ]
- Checking consistency of group files (grpck) [ OK ]
- Checking non unique group ID's [ OK ]
- Checking non unique group names [ OK ]
- Checking password file consistency [ OK ]
- Query system users (non daemons) [ DONE ]
- Checking NIS+ authentication support [ NOT ENABLED ]
- Checking NIS authentication support [ NOT ENABLED ]
- Checking sudoers file [ FOUND ]
  - Check sudoers file permissions [ OK ]
- Checking PAM password strength tools [ SUGGESTION ]
- Checking PAM configuration files (pam.conf) [ FOUND ]
- Checking PAM configuration files (pam.d) [ FOUND ]
- Checking PAM modules [ FOUND ]
- Checking LDAP module in PAM [ NOT FOUND ]
- Checking accounts without expire date [ OK ]
- Checking accounts without password [ OK ]
- Checking user password aging (minimum) [ DISABLED ]
- Checking user password aging (maximum) [ DISABLED ]
- Checking expired passwords [ OK ]
```

- d. Você receberá uma notificação para qualquer configuração que esteja fraca, conforme mostrado abaixo:

```
[+] Banners and Identification
-----
- /etc/motd [ NOT FOUND ]
- /etc/issue [ FOUND ]
  - /etc/issue contents [ WEAK ]
- /etc/issue.net [ FOUND ]
  - /etc/issue.net contents [ WEAK ]

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

- e. Você receberá sugestões detalhadas de melhoria na segurança, além de um resumo final, que fornece o local onde você pode encontrar o arquivo de log.

```
Lynis security scan details:

Hardening index : 56 [##### ]
Tests performed : 188
Plugins enabled : 0

Quick overview:
- Firewall [X] - Malware scanner [X]

Lynis Modules:
- Compliance Status [NA]
- Security Audit [V]
- Vulnerability Scan [V]

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

**Passo 4: Analisar resultados**

- a. Role para cima, para a seção de resultados, depois que a ferramenta tiver concluído sua execução.

Quanto avisos você recebeu? \_\_\_\_\_

Quantas sugestões você recebeu? \_\_\_\_\_

- b. Role pelas sugestões e selecione uma. Você pesquisará uma sugestão que pode implementar para abordar o problema.

Qual sugestão você está abordando?

\_\_\_\_\_  
\_\_\_\_\_

Qual é sua solução sugerida?

\_\_\_\_\_  
\_\_\_\_\_

**Referências**

Lynis: <https://cisofy.com/lynis/>