

Laboratório — Blindagem de um sistema Linux

Objetivos

Demonstrar a utilização de uma ferramenta de auditoria de segurança para blindar um sistema Linux.

Contexto/cenário

A auditoria de um sistema para possíveis configurações incorretas ou serviços desprotegidos é um aspecto importante da blindagem do sistema. O 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

- Um PC com o Ubuntu 16.04 Desktop LTS instalado no VirtualBox ou numa máquina virtual VMware.

Passo 1: Abrir uma janela de terminal no Ubuntu.

- Inicie uma sessão no Ubuntu utilizando as seguintes credenciais:

Utilizador: **cisco**

Palavra-passe: **password**



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



Passo 2: A ferramenta Lynis

- No prompt de comandos, introduza o seguinte comando para mudar para o diretório do lynis:

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

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

- b. No prompt de comandos, introduza o seguinte comando e introduza a palavra-passe **password** quando lhe for pedida:

```
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
-----
```

Este comando verifica se esta é a versão mais recente da ferramenta e as atualizações para a ferramenta à data de escrita deste laboratório.

Passo 3: Executar a ferramenta

- a. Introduza 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 mostrado em cima, a ferramenta começará a auditar usando o utilizador **cisco** como o auditor.

Nota: Irá receber **alertas** (warnings).

- b. Para continuar com cada passo da auditoria pressione **Enter**. Irá receber alertas conforme mostrado em baixo.

```
[+] 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. Irá receber sugestões, conforme mostrado em baixo.

```
[+] 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. Irá receber uma notificação sobre uma qualquer configuração que seja fraca conforme mostrado em baixo.

```
[+] 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. Irá receber sugestões detalhadas de melhorias de segurança, bem como um resumo final que fornece a localização onde pode encontrar o ficheiro 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 os Resultados

- a. Faça Scroll para cima até à seção de resultados depois da ferramenta ter concluído a sua execução.
Quantos Alertas (Warnings) recebeu? _____
Quantas sugestões recebeu? _____
- b. Percorra as sugestões e selecione uma. Pesquise uma sugestão que possa implementar para resolver o problema.
Qual é a sugestão que optou por seguir?

Qual é a sua solução sugerida?

SKUs

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