

Práctica de laboratorio: fortalecimiento de un sistema Linux

Objetivos

Demostrar el uso de la herramienta de auditoría seguridad para reforzar un sistema Linux.

Aspectos básicos/situación

La auditoría de un sistema para detectar posibles configuraciones incorrectas o servicios sin protección es un aspecto importante del fortalecimiento del sistema. Lynis es una herramienta de auditoría de seguridad de código abierto con un conjunto automatizado de scripts desarrollados para probar un sistema Linux.

Recursos necesarios

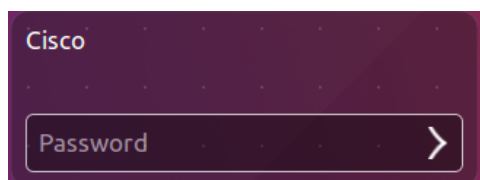
- Computadora con sistema Ubuntu 16.04.4 Desktop LTS instalado en una máquina virtual de VirtualBox o VMware.

Paso 1: Abra una ventana del terminal en Ubuntu.

- a. Inicie sesión en Ubuntu con las siguientes credenciales:

Usuario: **cisco**

Contraseña: **password**



- b. Haga clic en el icono de terminal para abrir una ventana de terminal.



Paso 2: La herramienta Lynis

- a. En la petición de ingreso de comando, ingrese el siguiente comando para cambiar el directorio de lynis:

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

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

- b. En la petición de ingreso de comandos, introduzca el siguiente comando y la contraseña **password** cuando se le solicite:

```
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)...
- Program update status... [ NO UPDATE ]

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

Este comando verifica que esta es la versión más recientes y actualiza la herramienta al momento de la redacción de esta práctica de laboratorio.

Paso 3: Ejecute la herramienta

- a. Escriba el siguiente comando en el terminal y presione **Intro**:

```
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
```

Como se muestra arriba, la herramienta comenzará a auditar mediante el usuario **cisco** como el auditor. Aviso: recibirá **advertencias**.

- b. Para continuar con cada etapa de la auditoría presione **Intro**. Recibirá advertencias como se muestra a continuación.

```
[+] 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. Recibirá advertencias como se muestra a continuación.

```
[+] 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. Recibirá una notificación para cada configuración que es débil como se muestra a continuación:

```
[+] 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. Recibirá sugerencias detalladas de mejora de la seguridad y también un resumen final que proporciona la ubicación donde puede encontrar el archivo de registro.

```
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
```

Paso 4: Revise los resultados

- a. Desplácese hasta la sección de resultados después de que la herramienta haya terminado de ejecutarse.

¿Cuántas advertencias recibió? _____

¿Cuántas sugerencias recibió? _____

- b. Desplácese hasta las sugerencias y seleccione uno. Investigará una sugerencia que pueda implementar para resolver el problema.

¿Qué sugerencia considerará?

¿Cuál es la solución sugerida?

Referencias

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