Hardening de Linux

Ing. Ernesto Pérez Estévez, Mg.

+593 9 9924 6504

eperez@ecualinux.com

Learning Academy

Agenda

- Introducción al hardening
- Seguridad durante la instalación
- Labores post instalación
- Endurecimiento de accesos remotos
- Herramientas de interés

Introducción al hardening

- **Pilares de la seguridad:**
  - Confidencialidad
  - Integridad
  - Disponibilidad
- **Hardening**: Es el proceso de hacer el sistema operativo más seguro ante ataques que puedan afectar la tríada CIA. Minimizando su superficie de ataque
  - NIST: Hardening: A process intended to eliminate a means of attack by patching vulnerabilities and turning off nonessential services.
- Es, al igual que todo en la seguridad, una labor continua, que comienza desde la instalación (o antes)
- En esta conferencia veremos algunos aspectos interesantes del hardening y aplicaremos varias técnicas para ayudar a comprender cómo realizar estas labores.

Learning Academy

Documentación

- Mastering Linux Security and hardening, 2nd ed 2020, Donald A. Tevault, Packt Publishing
- Guide to the Secure Configuration of Red Hat Enterprise Linux 5, Rev 4.2, 2011, NSA
- Red Hat Enterprise Linux 8 Security hardening, RedHat, 2022
- Red Hat Enterprise Linux 7 Security Guide, Robert Krátký, et al, RedHat 2016
- Hardening Linux, JAMES TURNBULL, Apress, 2005

Existen diversas guías, metodologías y hasta sistemas para realizar este proceso. Al finalizar les mencionaré uno que seguro les será de interés. Aquí vamos a ver temas generales que son cubiertos por la mayoría de las guías.

Learning Academy

¿Qué distribución escoger?

- Mayor tiempo de soporte con parches y actualizaciones
- Existen personas que conocen de ella en tu región o país

RHEL: ampliamente conocida, al menos 10 años de soporte (existe opción a un periodo extendido)

Clones de RHEL

- Rocky Linux
- AlmaLinux
- Oracle Linux (OL)

Seguridad durante la instalación

- La instalación debe ser:
  - Mínima
  - Contraseña segura (o mejor aún: usuario root deshabilitado, siguientes slides)
  - Correcta zona horaria
  - Adecuadamente particionada (más sobre esto en el siguiente slide)
- También debe considerar, si es factible, cifrar las particiones

Particionamiento adecuado del FS

- /
- /boot
- SWAP

Learning Academy

Particionamiento adecuado del FS

- /boot
- /
- /var
- /home
- /tmp
- SWAP

Learning Academy

Tareas post-instalación

- Actualizaciones
- Apagado de servicios innecesarios
- Opciones al sistema de archivos

Tareas post-instalación - Opciones al FS

- noatime
- nodev
- nosuid
- noexec

Tareas post-instalación - Opciones al FS

	noatime	nodev	nosuid	noexec
/boot	x	x	x	x
/	x			
/tmp	x	x	x	x
/home	x	x	x	x
/var	x	x	x	x

Hardening de accesos remotos

- Por qué evitar acceso directo como root
- Autenticación mediante clave pública/privada
- PermitRootLogin prohibit-password (antes: without-password)

Herramientas de interés

- telnet
- netstat
- nmap
- **OpenSCAP**

¿?

Hardening de Linux

Ing. Ernesto Pérez Estévez, Mg.

+593 9 9924 6504

eperez@ecualinux.com

Learning Academy