THE BRIDGE

Hardening

Hardening

- El **hardening** o **endurecimiento de sistemas**, es el proceso de asegurar y reforzar la configuración.
-
- Eliminar configuraciones débiles o innecesarias y aplicar configuraciones de seguridad más estrictas.
- El Objetivo del **Hardening** es reducir la superficie de ataque del sistema
- El **hardening** es esencial porque:
  - **Reduce las oportunidades para los atacantes.**
  - **Refuerza la seguridad en cada capa**.
  - **Minimiza errores de configuración**.

https://internetpasoapaso.com/hardening/

Ejemplo de hardening

- En el sistema Operativo
- En redes
- En Aplicaciones
- Dispositivos IoT y Móviles
- Bases de Datos

Guias de Hardening

- Existen guías específicas que facilitan el hardening, como:
  - **Guías**
    - CIS Benchmarks
    - NIST SP 800-XX
    - ISO/IEC 27001 y 27002
    - DISA STIGs (Security Technical Implementation Guides)
    - OWASP (Open Web Application Security Project)
    - Microsoft Security Baselines
    - PCI DSS (Payment Card Industry Data Security Standard)
    - SANS Institute Security Configuration Guides
    - CCN (centro Criptológico Nacional)
      - Guías CCN-STIC 800
      - Guía CCN-STIC 400
      - Guías CCN-STIC 500
      - Guías CCN-STIC 600

Herramientas de Hardening

- Existen herramientas para aplicar hardening como lo son:
- **Herramientas**
  - Microsoft Security Compliance Toolkit 1.0
  - CIS-CAT
  - Lynis
  - Open scap
  - Jshielder
  - Ansible
  - Puppet
  - Etc.


THE
BRIDGE

Hardening o Bastionado de activos

- **CIS Benchmarks**
  - Desarrollados por el “Center for Internet Security”.
  - Son un conjunto prescriptivo y prioritario de mejores prácticas en seguridad cibernética y acciones defensivas.
  - Estas mejores prácticas procesables para la defensa cibernética son formuladas por un grupo de expertos
  - Abordan una amplia variedad de sistemas y aplicaciones.
  - Están divididos en niveles de seguridad.
  - Función:
    - **Asegurar la conformidad.**
    - **Mejorar la postura de seguridad.**
    - **Estandarizar la seguridad.**
  - https://www.cisecurity.org/cis-benchmarks/

Hardening o Bastionado de activos

- **Automático:**
  - **Windows tools**
    - **Microsoft Security Compliance Toolkit 1.0**
      - Conjunto de herramientas que permite a los administradores de la seguridad empresarial descargar, analizar, probar, editar y almacenar líneas base de configuración de seguridad recomendadas por Microsoft para Windows y otros productos de Microsoft.
        - https://learn.microsoft.com/es-es/windows/security/threat-protection/windows-security-configuration-framework/security-compliance-toolkit-10

      - Descarga de la Herramienta
        - https://www.microsoft.com/en-us/download/details.aspx?id=55319

Hardening o Bastionado de activos

- **Linux tools**
  - **Lynis**

  - **Open scap**
    - Esta diseñada para realizar escaneos de configuración y vulnerabilidad en un sistema local, para validar el contenido de cumplimiento de la configuración y para generar informes y guías basados en estos escaneos y evaluaciones.
    - https://www.open-scap.org/

  - **Jshielder**
    - Es un script Bash de código abierto desarrollado para ayudar a SysAdmin y a los desarrolladores a proteger los servidores Linux en los que implementarán cualquier aplicación o servicio web.
    - Esta herramienta automatiza el proceso de instalación de todos los paquetes necesarios para alojar una aplicación web y fortalecer un servidor Linux con poca interacción por parte del usuario.
    - La secuencia de comandos recién agregada sigue la Orientación comparativa de CIS para establecer una postura de configuración segura para los sistemas Linux.
    - https://github.com/Jsitech/JShielder