[INT] Test de Intrusión

Tenemos dos principales mapeadores de vulnerabilidades:

- OpenVAS: Open Vulnerability Assesment System: Es una suite de software que integra servicios y herramientas especializadas en el escaneo y gestión de vulnerabilidades de seguridad en sistemas informáticos
  - El núcleo de OpenVAS es un escáner de vulnerabilidades
  - EN el momento que detecta una vulnerabilidad, reporta el CWE y CVE de esta y si es posible dice como puede ser parcheada y como se puede explotar.
- Nessus: De pago (1500$ al año por licencia). Permite escanear más dispositivos que OpenVAS, incluidos smartphone.
  - Es la plataforma más confibale para el escaneo de vulnerabilidades para auditores y especialistas en seguridad.
  - Los usuarios pueden programar escaneos a través de diversos scaners, utilizar asistentes para crear políticas y programas de escaneo y enviar los resultados por correo electrónico.
  - Tras finalizar la instalación de Nessus y la ejecución de servidor, se debe abrir la ip 127.0.0.1:8834 en el navegador.
  - Políticas y escaneos
    - Políticas: Está compuestas por opciones de configuración que se relacionan con la realización de análisis de vulnerabilidades
    - Escaneos: Despues de crear una directiva se puede crear un nuevo análisis o escaneo.
  - Nikto:

From:
https://www.knoppia.net/ - **Knoppia**

Permanent link:
https://www.knoppia.net/doku.php?id=master_cs:int:tm2&rev=1738855939

Last update: **2025/02/06 15:32**