[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.

SearchSploit

Es una herramienta de búsqueda en línea de comandos para exploit DB que permite llevar una copia de exploit Database, una base de datos de exploits, que puede ser útil si no se tiene internet. Permite realizar búsquedas por distintos campos, devolviendo un título autoexplicativo y la ruta local o remota del exploit. La búsqueda es muy precisa, usando AND exclusivo (No como google, que usa el OR), de forma que muestra solo lo que contenga las palabras buscadas.

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

Permanent link:
https://knoppia.net/doku.php?id=master_cs:int:tm2&rev=1739369528

Last update: **2025/02/12 14:12**