Herramientas de seguridad

Pueden utilizarse para revisar la **seguridad de un sistema** con buenas o con malas intenciones.

Analizadores de red

Búsqueda de equipos en la red.

Hacen barridos de puertos y descubrimiento de servicios.

Analizando los resultados para inferir información, como versión, tipo de sistema y/o servicios.

Exponer deficiencias de seguridad.

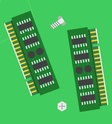
Algunos de los más utilizados son **nmap, SATAN y SAINT.**

Otro tipo de analizadores son los usados para **localizar todo tipo de posibles problemas** que permiten detectar y exponer aplicaciones conocidas por su fragilidad.

nessus® professional

- Aplicación gratuita para **uso no comercial.**
- Decenas de nuevos **análisis de vulnerabilidad a la semana.**
- Estos análisis **se publican para uso gratuito una semana después que los de pago.**
- **OpenVAS es un analizador libre** que nació como una ramificación del último Nessus libre.
- Los análisis de vulnerabilidades son llamados **NVT** (*Network Vulnerability Tests*).

Analizadores de paquetes



Captan todos los paquetes que llegan a la tarjeta de red (NIC) configurándose en modo promiscuo.

WIRESHARK

Luego permiten el análisis de dichos paquetes de red según los protocolos utilizados en los mismos.

En esta categoría figuran **WireShark**, dispone de interfaz gráfica, y tcpdump, disponible solo en modo comando, aunque existen frontispicios gráficos como WinDump.

Programas de descubrimiento

Analizan listados de claves cifradas o resumidas (mediante algoritmos como MD4) para intentar descubrirlas.

John the Ripper

La herramienta más utilizada es John The Ripper (JTR), que es libre y autodetecta el tipo de resumen de la clave y ataca claves de multitud de algoritmos como DES, MD5, Blowfish, Kerberos o LM Hash (Windows) tanto en ficheros de texto como en repositorios sobre LDAP o MySQL.

Puede trabajar con ataques de diccionario y alteraciones o mediante fuerza bruta **usando tablas de caracteres frecuentes para marcar el orden.**

Fuentes: Guimi.net (2009). Freepik. Recursos Educativos Digitales SENA (2021).