Análisis de vulnerabilidades

Consiste en identificar y analizar las vulnerabilidades en los sistemas de la red objetivo, tras completar el descibrimiento y la enumeración se identifican las vulnerabilidades locales y remotas.

- Vulnerabilidad local: Se requiere acceso local para explotar la vulnerabilidad.
- Vulnerabilidad remota: El atacante no tiene acceso a la red local, pero la vulnerabilidad se puede explotar a través de la red.

Mapeadores de vulnerabilidades

- OpenVAS (Open Vulnerability Assesment System): Suite de software para integrar servicios y herramientas especializadas en el escaneo y gestión de vulnerabilidades de seguridad.
    - Se compone de varios servicios y herramientas, siendo su núcleo el escaner de vulnerabilidades.
    - Niveles de alerta
        - Riesgo de amenaza alto: Nombre y nivel de amenaza, resumen de susceptibilidad, solución propuesta, método de detección, información detallada...
        - Riesgo de Amenaza medio: Mismo informe que el anterior
        - Riesgo de amenaza bajo: Incluye un conjunto de recomendaciones para mejorar la seguridad del sistema.
- NESSUS: Plataforma de escaneo de vulnerabilidades. Permite programar escaneos a través de diversos escaners, utiliza un asistente para crear políticas y programas de escaneo. Envia los resultados mediante email.
- NIKTO: Permite detectar vulnerabilidades en servidores web y comprende un abanico enorme de opciones a la hora de realizar tests de intrusión. Destaca el Scan Tuning, que permite especificar los tipos de test que se realizan contra el objetivo, reduciendo el ruido generado.