[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. Si se quieren realizar búsquedas parametrizadas por título, se usa el flag -t. Para realizar una búsqueda con un parámetro básico se usa -x. se puede guardar cualquier exploit identificado con el parámetro -m, se pueden usar tanto la ruta como el ID del exploit. Con el -j obtenemos toda la salida en formato json.

```
searchsploit -x --nmap
```

Metasploit

Proyecto Open Source que permite desarrollar y ejecutar exploits contra una máquina remota. Metasploti se compone de 5 módulos fundamentales:

- Payloads
- Exploits
- Encoders

- NOPS
- AUX

Módulos importantes de metasploit

- Auxiliary: Permite obtener información auxiliar de los explout
- Exploit: Contienen los porgramas que nos permiten entrar dentro de una máquina
- Payload: Programa que acompaña a un exploit para realizar funciones específicas a la vez que se compromete el sistema objetivo
    - Singles: Permiten realizar una conexión util desde dentro hasta fuera. Permiten crear un shell directo o inverso. En el inverso la víctima es la que realiza la conexión con el atacante.
    - Stagers: Son los que general la conexión, trabajan con los puertos.
    - Stages: Se descargan y son ejecutados por los Stagers. Realizan diversas tareas en el equipo de la víctima. Por ejemplo, un payload de escalado de privilegios.
- Encoders: Codigo cifrado para la evasión de antivirus, pueden ser ofuscadores de código.
- NOPS: Usados por los payloads para que se puedan ejecutar de manera satisfactoria en memoria. Aprovecha stack overflows
- Post: Se usan en la post-explotación

Escalado de Privilegios

- Getsystem en linux
- UAC en Windows: Es el controlador de cuentas de usuarios
- getsystem con Windows: se usa de forma serial

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

Permanent link:
https://www.knoppia.net/doku.php?id=master_cs:int:tm2&rev=1739375131

Last update: **2025/02/12 15:45**