WinPEAS (Windows Privilege Escalation Awesome Scripts) es una herramienta diseñada para la auditoría de seguridad en sistemas operativos Windows. Ayuda a los profesionales de seguridad y pentesters a identificar posibles vectores de escalada de privilegios en sistemas Windows al enumerar información detallada sobre la configuración del sistema, permisos de archivos, configuraciones de red y más.

**Características de WinPEAS**

* **Enumeración de Información del Sistema**: Recopila datos sobre el sistema operativo, versiones instaladas, parches, y configuraciones.
* **Enumeración de Servicios y Permisos**: Muestra servicios y procesos que podrían ser aprovechados para la escalada de privilegios.
* **Enumeración de Usuarios y Grupos**: Lista los usuarios y grupos en el sistema, destacando posibles configuraciones erróneas.
* **Enumeración de Programas Instalados**: Identifica programas instalados que podrían ser vulnerables.
* **Configuraciones de Red**: Muestra detalles sobre la configuración de la red y adaptadores de red.
* **Permisos de Archivos y Carpetas**: Examina los permisos de archivos y carpetas en busca de configuraciones inseguras.
* **Políticas de Seguridad**: Revisa las políticas de seguridad configuradas en el sistema.
* **Credenciales y Contraseñas Guardadas**: Intenta identificar contraseñas guardadas y credenciales.

**Instalación y Uso**

Puedes obtener WinPEAS desde el repositorio oficial en GitHub. Aquí tienes los pasos para descargar y ejecutar WinPEAS:

**Descarga de WinPEAS**

1. **Clona el repositorio de GitHub**:

bash

Copy code

git clone https://github.com/carlospolop/PEASS-ng.git

1. **Navega al directorio de WinPEAS**:

bash

Copy code

cd PEASS-ng/winPEAS

**Ejecución de WinPEAS**

WinPEAS se puede ejecutar directamente en el sistema objetivo. Existen varias versiones (binaria, script por lotes, y más), pero la forma más sencilla de ejecutarlo es usar la versión binaria. Puedes transferir el binario a la máquina objetivo y ejecutarlo desde allí.

1. **Transferir el binario a la máquina objetivo**:

Puedes usar métodos como scp, ftp, smb, etc., para transferir el archivo winPEAS.exe al sistema objetivo.

1. **Ejecutar WinPEAS**:

Abre una consola de comandos en la máquina objetivo y navega al directorio donde has transferido winPEAS.exe. Luego, ejecuta:

bash

Copy code

winPEAS.exe

WinPEAS comenzará a enumerar y recopilar información del sistema, mostrando resultados en la consola.

**Ejemplo de Ejecución**

1. **Ejecución Básica**:

bash

Copy code

winPEAS.exe

1. **Ejecución con Opciones Adicionales**:

WinPEAS tiene varias opciones y parámetros que puedes utilizar para personalizar su ejecución. Puedes ver todas las opciones disponibles ejecutando:

bash

Copy code

winPEAS.exe -h

**Análisis de Resultados**

Los resultados de WinPEAS pueden ser extensos y detallados. Algunos puntos clave a buscar incluyen:

* **Archivos y Carpetas con Permisos Inseguros**: Archivos que permiten escritura a usuarios no privilegiados.
* **Servicios y Tareas Programadas**: Servicios que ejecutan con permisos elevados y pueden ser manipulados.
* **Credenciales Guardadas**: Contraseñas y credenciales almacenadas en archivos de configuración.
* **Usuarios y Grupos con Permisos Elevados**: Usuarios que tienen permisos elevados pero no deberían tenerlos.

**Conclusión**

WinPEAS es una herramienta poderosa para la enumeración y detección de posibles vectores de escalada de privilegios en sistemas Windows. Su uso es crucial en auditorías de seguridad y pruebas de penetración para identificar y mitigar configuraciones inseguras.

Si necesitas más información o ejemplos específicos sobre cómo utilizar WinPEAS, estaré encantado de ayudarte.