LinPEAS (Linux Privilege Escalation Awesome Script) es una herramienta que ayuda a identificar vectores de escalada de privilegios en sistemas Linux. Es especialmente útil para pentesters y administradores de sistemas que buscan posibles fallos de seguridad en configuraciones de sistemas operativos Linux.

**Características de LinPEAS**

* **Enumeración de Información del Sistema**: Recopila detalles sobre el sistema operativo, kernel, parches y configuraciones.
* **Servicios y Procesos**: Lista servicios y procesos que podrían ser vulnerables.
* **Usuarios y Grupos**: Muestra información sobre los usuarios y grupos en el sistema.
* **Permisos de Archivos y Directorios**: Identifica archivos y directorios con permisos incorrectos.
* **Configuración de Red**: Muestra detalles de la configuración de red y adaptadores de red.
* **Credenciales Guardadas**: Intenta identificar contraseñas y credenciales almacenadas.
* **Políticas de Seguridad**: Revisa las políticas de seguridad configuradas en el sistema.
* **SUID y SGID**: Identifica archivos con bits SUID y SGID establecidos.
* **Configuraciones de SSH**: Revisa configuraciones y claves SSH en el sistema.

**Instalación y Uso**

LinPEAS se puede obtener del repositorio oficial en GitHub. Aquí tienes los pasos para descargar y ejecutar LinPEAS:

**Descarga de LinPEAS**

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

bash

Copy code

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

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

bash

Copy code

cd PEASS-ng/linPEAS

**Ejecución de LinPEAS**

LinPEAS se puede ejecutar directamente en la máquina objetivo. Puedes transferir el script a la máquina objetivo y ejecutarlo desde allí.

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

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

1. **Dar permisos de ejecución al script**:

bash

Copy code

chmod +x linpeas.sh

1. **Ejecutar LinPEAS**:

Abre una terminal en la máquina objetivo y navega al directorio donde has transferido linpeas.sh. Luego, ejecuta:

bash

Copy code

./linpeas.sh

LinPEAS comenzará a enumerar y recopilar información del sistema, mostrando resultados en la terminal.

**Ejemplo de Ejecución**

1. **Ejecución Básica**:

bash

Copy code

./linpeas.sh

1. **Ejecución con Opciones Adicionales**:

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

bash

Copy code

./linpeas.sh -h

**Análisis de Resultados**

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

* **Archivos y Directorios con Permisos Incorrectos**: Archivos que permiten escritura a usuarios no privilegiados.
* **SUID y SGID**: Archivos con bits SUID y SGID que pueden ser explotados.
* **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.
* **Vulnerabilidades de Kernel**: Versiones del kernel con vulnerabilidades conocidas.

**Conclusión**

LinPEAS es una herramienta poderosa para la enumeración y detección de posibles vectores de escalada de privilegios en sistemas Linux. 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 LinPEAS, estaré encantado de ayudarte.