httpsgithub.compeass-ngPEASS-ngtreemasterlinPEAS  
  
Linpeas

Enumera automáticamente la información de un sistema linux para que puedas elegir qué hacer con ella.

1. Vamos a: <https://github.com/carlospolop/PEASS-ng/releases/tag/20230917-ec588706>
2. Descargamos específicamente el archivo: linpeas[.]sh en nuestra máquina host. (primero desactiva el antivirus).
3. Copia el archivo en tu Kali.
4. Ahora haremos uso de la herramienta scp, que nos permite enviar archivos por medio de SSH.

scp linpeas.sh nombre\_usuario@192.168.10.1:/tmp/linpeas.sh

I**mportante:** usamos la carpeta /tmp porque, usualmente, es aquella que suele tener todos los permisos.

1. Verificamos permisos de ejecución, y si no los posee, los añadimos con:

chmon +x linpeas.sh

1. Ejecutamos con:

./linpeas.sh

1. Analizamos los hallazgos.

LINPEAS es una herramienta de escaneo diseñada específicamente para sistemas Linux que ayuda en la recopilación de información detallada y relevante para la auditoría de seguridad. Aquí tienes más información sobre algunas de las características y funcionalidades principales de LINPEAS:

1. **Recopilación de Información del Sistema**:
   * Identificación de la distribución de Linux y su versión.
   * Detalles del kernel y arquitectura del sistema.
   * Listado de usuarios y grupos del sistema, incluyendo privilegios especiales (SUID/SGID).
2. **Análisis de Configuraciones Sensibles**:
   * Búsqueda de archivos de configuración críticos y sus permisos.
   * Análisis de cron jobs y otros scripts programados.
   * Revisión de configuraciones de red y servicios en ejecución.
3. **Detección de Potenciales Vectores de Ataque**:
   * Identificación de puertos abiertos y conexiones de red activas.
   * Análisis de procesos en ejecución y servicios asociados.
4. **Exploración de Vulnerabilidades**:
   * Búsqueda de vulnerabilidades conocidas o configuraciones inseguras.
   * Identificación de archivos sensibles con permisos inadecuados.

LINPEAS es útil para realizar auditorías de seguridad, diagnósticos de sistemas y evaluaciones de vulnerabilidades en entornos Linux. Se distribuye generalmente como un script que se ejecuta localmente en el sistema objetivo, proporcionando resultados detallados y estructurados para su análisis posterior.

Es importante destacar que LINPEAS y herramientas similares deben ser utilizadas con permiso y bajo las políticas de seguridad adecuadas para evitar problemas legales y éticos. Si estás interesado en utilizar LINPEAS, te recomendaría investigar más sobre su uso seguro y responsable en entornos de seguridad informática.