SPRING 15

EJERCICIO 2 – UNIDAD 2

ELEVACION DE PRIVILEGIOS EN LINUX II

SUID

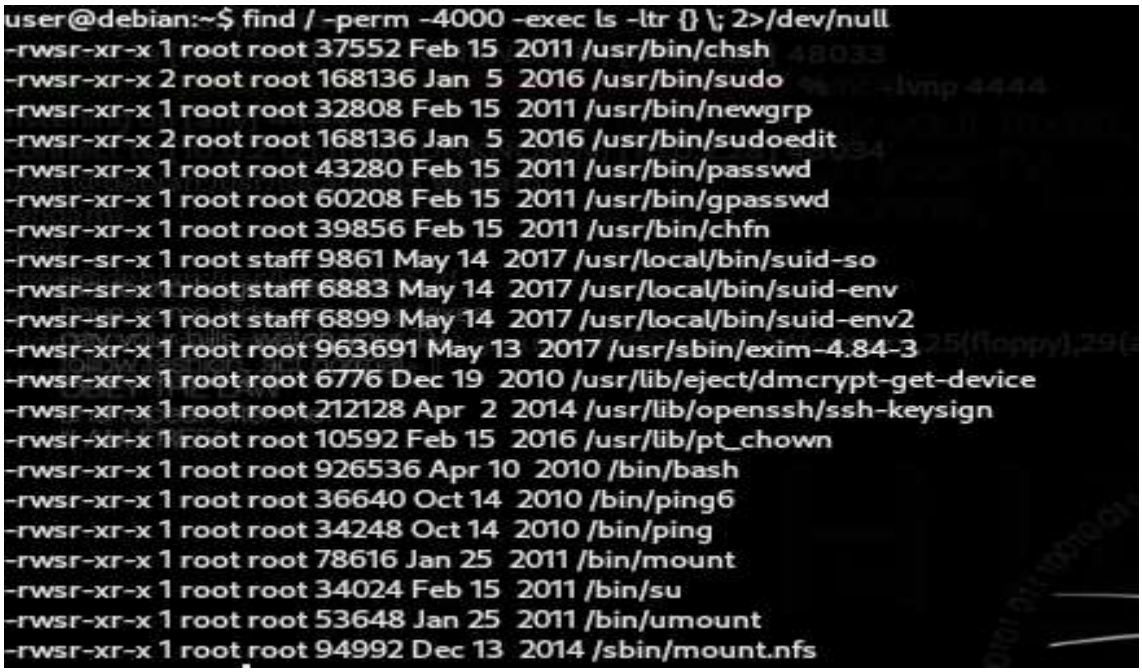
SHARED OBJECT INJECTION Y VARIABLES DE AMBIENTE

En este ejercicio se trabajará la escalada de privilegios de las siguientes formas, debiendo explicar con capturas y texto el procedimiento seguido para cada una de ellas:

- En ambos ejercicios nos conectamos a la Maquina Debian 6 con IP 10.0.2.28, la cual, ya ha sido comprometida anteriormente y ahora vamos a escalar privilegios a través de SSH en el sistema:

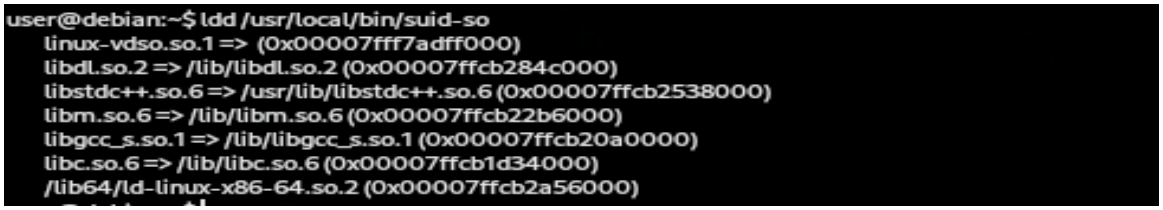
1. Escala de privilegios mediante SUID (Shared Object Injection):

- Buscamos en el sistema los archivos Bits SUID:

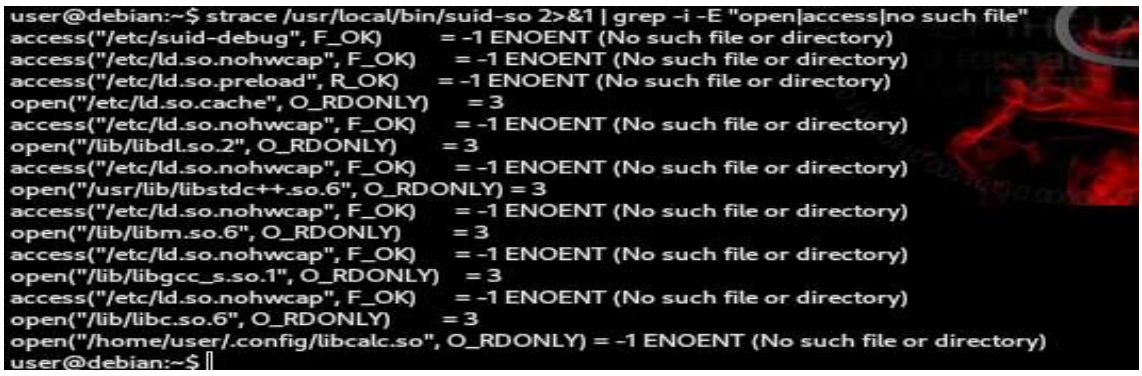


- Ahora dentro de estos archivos SUID se procede a buscar alguno que use y cargue bibliotecas compartidas (Shared Objects) de manera insegura, que nos permita cargar una biblioteca compartida maliciosa.

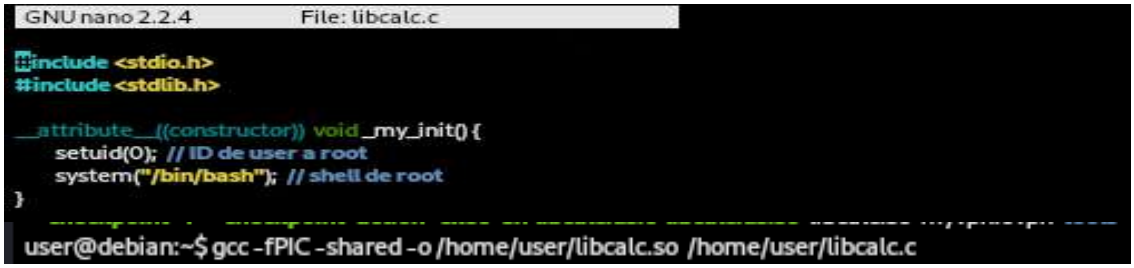
- Para ello usaremos en primer lugar, el comando *"ldd"* , el cual muestra las bibliotecas compartidas que un archivo necesita para ejecutarse:



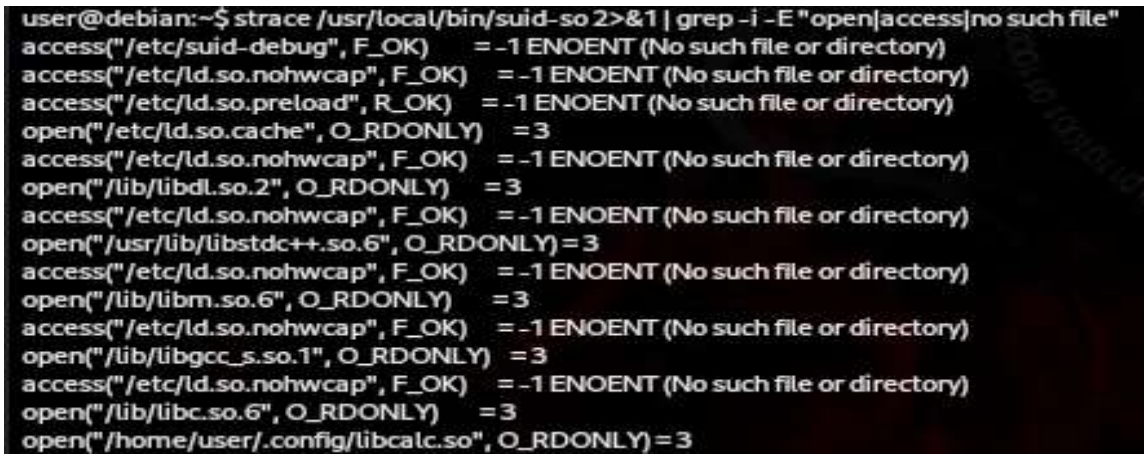
- Ahora con *"strace"* y haciendo un filtrado, comprobaremos los archivos y bibliotecas compartidas que realmente intenta abrir:



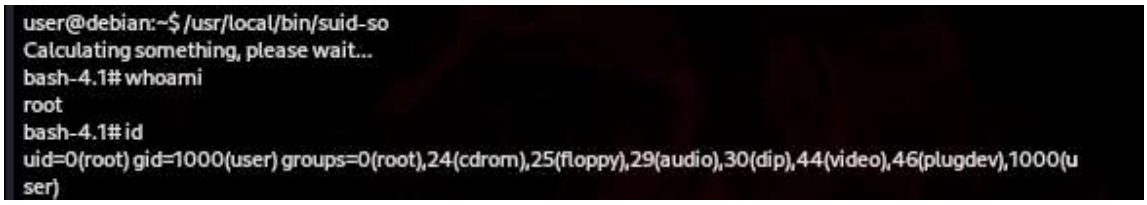
- Como podemos ver comparando, que existe una biblioteca irregular que se esta ejecutando desde home/user que no debía tener, además esta intentando abrir el archivo libcal.so con resultado negativo (ENOENT / not such file or directory), asi que aprovecharemos esto para hacer un script malicioso y poder elevar privilegios.
- Se crea y se compila un script malicioso en lenguaje C llamado *"libcalc.so",* incluyendo el atributo constructor, que hará que el código malicioso se cargue tan pronto como el programa suid-so la cargue en el sistema. Además, Se va a incluir en el Path LD_PRELOAD, siendo una variable de entorno que prioriza sus archivos y bibliotecas sobre otras bibliotecas del sistema.



- Comprobamos que ya no dice el mensaje que no encuentra el archivo, por lo que nuestra biblioteca maliciosa está ejecutándose:



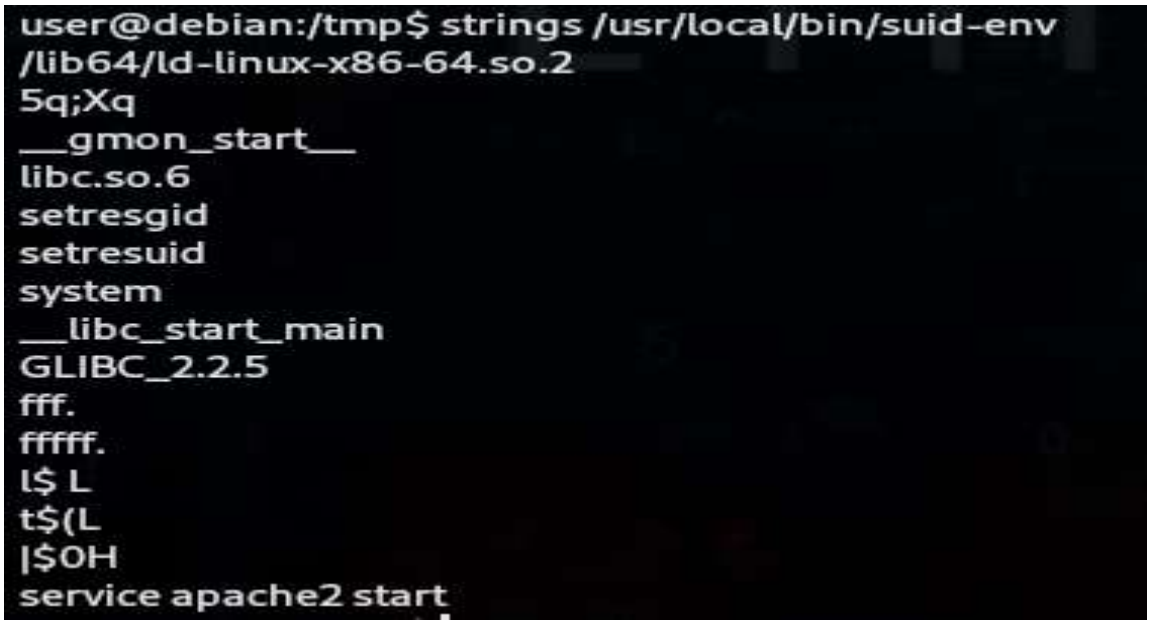
- Ejecutamos el archivo suid-so para comprobar que hemos conseguido elevar privilegios a root, siendo positivo:



2. Escala de privilegios mediante SUID (Variables de ambiente):

- El primer paso coincide con lo realizado anteriormente buscando los archivos SUID:

- Las variables de ambiente son valores o cadenas de texto, que los programas utilizan para configurar su entorno de ejecución, como pueden ser LD_PRELOAD (prioriza el uso de bibliotecas), LD_LIBRARY_PATH (prioriza los directorios donde buscar bibliotecas compartidas antes de usar las rutas predeterminadas del sistema) o el PATH (establece directorios donde se buscan ejecutables), entre otras.
- Para explotar este método nos centraremos en buscar en eso valores o cadenas de texto llamados *“strings”* , los cuales, contienen rutas, comandos e instrucciones que después pasan a programas en ejecución.



Si observamos, este binario ejecuta un comando externo que inicia apache2, por lo que, si creamos un servicio malicioso que se ejecute en vez del servicio de apache, cambiándole el PATH, podríamos conseguir elevar privilegios:

- Se crea un archivo malicioso en la ruta *“/temp/Service*” y con chmod se le da permisos de ejecucion:

EL archivo malicioso realiza una copia del Bash, le da permisos Bit SUID, por lo que hereda los permisos del propietario del archivo y ejecuta una shell.

- Cambiamos temporalmente el PATH, para que el sistema busque en primer lugar nuestro archivo en *"/tmp"* y ejecutamos el binario que estamos explotando, consiguiendo elevación de privilegios a root: