Black System

Seguridad Informática

Seguridad Informática

FPTD/2021/019/2080

http://www.free-powerpoint-templates-design.com

Pipe: creamos tuberías entre varios comandos. Lo que hace es redirigir la salida del primer comando a la entrada del segundo: ls –l | grep Documents
Nos sacaría los permisos de la carpeta Documents

cat lista.txt | grep ordenadores (no sería muy eficiente, seria mejor directamente el grep)

Añadir: para añadir texto a un archivo usamos >>

echo hola > archivo
echo adiós >> archivo

Alias: Usamos los alias para poder poner atajos en las Shell de cada usuario. Por ejemplo, podemos crear un alias llamado alias cd..= ‘cd ..’ - alias ls=‘sl’

SUID: Cuando se activa el bit SUID sobre un fichero significa que el que lo ejecute va a tener los mismos permisos que el que creó el archivo. Esto es útil en algunas ocasiones, aunque hay que utilizarlo con cuidado, ya que puede acarrear problemas de seguridad

chmod 4755 /usr/bin/find
Vemos que la x se ha convertido en una s

La página que tenemos para explotar muchas vulnerabilidades es:
https://gtfobins.github.io/
En esta página buscamos el comando find y presionamos en suid, copiamos find . -exec /bin/sh -p \; -quit y lo pegamos en la terminal.

Romper contraseña Linux por fuerza bruta: Para poder decodificar una contraseña por fuerza bruta podemos usar diccionarios para encontrar dicha pass. Uno de los más conocidos es el Rockyou que ya viene descargado en Kali Linux.
Se encuentra comprimido en la carpeta: /usr/sahre/wordlists
Para descomprimir el archivo usamo: gunzip rockyou.txt.gz
Creamos el archivo con el hash de la contraseña del usuario: cat /etc/shadow | grep alumno > hash
Despues con la utilidad John usamos ese diccionario para romper la contraseña:
John - -wordlist=rockyou.txt hash
`

Si podemos escribir en /etc/passwd: Es muy importante tener bien seguros los permisos de este archivo, ya que si este archivo tuviera permiso de escritura para otros podríamos cambiar la contraseña de root

Lo primero seria sacar el hash de la nueva contraseña que le vamos a poner a root. Para ello utilizamos una utilidad de kali que se llama openssl passwd
Despues introducimos la clave que queremos 2 veces
Copiamos el resultado que es la palabra hasheada.
Con nano abrimos el /etc/passwd
Y cambiamos la primera x (que es donde mira en el archivo shadow) por el hash que hemos calculado
Grabamos y probamos la nueva contraseña de root (o de cualquier usuario)