Bisoños Usuarios de GNU/Linux de Mallorca y Alrededores | Bergantells Usuaris de GNU/Linux de Mallorca i Afegitons

Contraseñas de un solo uso (20966 lectures)

Per **Carles Pina i Estany**, ***cpina*** (http://pinux.info)

Creado el 20/11/2002 00:13 modificado el 20/11/2002 00:13

En este mini-artículo veremos como tener un usuario duplicado, pero este con una contraseña nueva en cada login. Así, si alguien nos coge la contraseña, no le servirá de nada.

Mucha gente usa ssh, ssl, encriptación, cada vez más a menudo. Peroooo.... al final de todo, escribimos la contraseña en el teclado, cosa que irremediablemente tenemos que hacer y este paso es inseguro debido a que puede haber "keyloggers", es decir, programas que capturan todo lo que escribas. Y hasta hay keyloggers físicos(1) (es el primero que he encontrado buscando en Google, no lo he probado).O sniffers con ARP-Spoofing, etc.

Yo al menos cuando voy a la universidad, cibercafés, etc. no compruebo que no haya un keylogger físico (podria estar hasta dentro del PC). Y comprobar que no hay ninguno via software, puede ser difícil.

Por tanto, veremos una "solución" a este problema. La "solución" es tener un usuario duplicado, llamado en el ejemplo "carles2". Este usuario tendrá exactamente el mismo directorio home, UID, etc. solo que cada vez que entremos tendrá una contraseña diferente, y llevaremos un listado de las contraseñas futuras en un papel, tachando las ya usadas.

El ejemplo que hago es con Debian Woody. Y antes de ponerlo en máquinas delicadas (servidores) probadlo bien con alguna de pruebas. Y no hagais las pruebas con el usuario root.

Primero de todo tendremos que editar el */etc/passwd* y hacer un duplicado del usuario que usamos de esta forma:

```
carles:x:1000:1000:,,,:/home/carles:/bin/bash
carles2:x:1000:1000:,,,:/home/carles:/bin/bash
```

Pongamos el usuario falso después del verdadero.

Lo mismo hacemos en el */etc/shadow*

```
carles:blablablabla;-):12004:0:99999:7:::
carles2:blablablabla;-):12004:0:99999:7:::
```

En ~/bin ponemos un fichero llamado genera.sh que hace las contraseñas aleatorias:

```
#!/bin/bash

echo "Quantes en vols generar?"
read quantes

for i in $(seq 1 "$quantes")
do
        pwgen | cat >> ~/passwds
done

echo "Generat fitxer passwds"
```

Y le ponemos permisos de ejecución: *chmod 700 genera.sh*

Seguidamente imprimiremos las contraseñas, así las llevamos en la carpeta/cartera/agenda/Palm/etc.

Al final del fichero ~/.bashrc ponemos:

```
if [ "$USER" = "carles2" ]
then
        ~/bin/rota.sh > /dev/null
        echo "rotado"
fi
```

Así cuando entramos con *carles2* se ejecuta el fichero ~/bin/rota.sh. Este fichero es el siguiente (con permisos de ejecución, *chmod 700 rota.sh*):

```
#!/bin/bash

fitxer=~/bin/passwds
temp=~/bin/passwds.temp

vell=$(head -1 $fitxer)
nou=$(head -2 $fitxer | tail -1)
echo $vell $nou
bin/canviar.expect $USER $vell $nou

awk '{if(NR!=1)print $0}' $fitxer > $temp

mv $temp $fitxer
```

Lo qué hace el *rota.sh* es coger el fichero de contraseñas y llama a *canviar.expect* con 3 parámetros: el nombre del usuario, la contraseña vieja y la nueva. La vieja está en la línea 1 del passwds, la nueva está en la 2. El canviar.expect cambia la contraseña y por último quitamos la línea 1 del fichero.

El *canviar.expect* es el siguiente (con permisos de ejecución):

```
#!/usr/bin/expect

#copiat de google groups
#http://groups.google.com/groups?q=expect+%22Changing+password%22&hl=en&lr=&ie=U
TF-8&oe=UTF-8&selm=3hqb3v%24d2e%40gatekeeper.iis.ch.swissbank.com&rnum=2

set usuari [lindex $argv 0]
set old_password [lindex $argv 1]
set new_password [lindex $argv 2]
spawn passwd $usuari
expect "Changing password"
expect "(current) UNIX password:"
send "$old_password\r"
expect "Enter new UNIX"
send "$new_password\r"
expect "Retype new UNIX"
send "$new_password\r"
expect eof
```

Es altamente mejorable, ya que no comprueba qué pasa si hubiese errores. Las cadenas "Changing password" y otras son las de Debian, es posible que en otras distribuciones se tengan que cambiar.

Evaluación: te arriesgas con el papel, pero dejas los keyloggers de lado. Si pierdes el papel, alguien puede entrar. Eso sí, conservamos siempre el usuario legítimo.

A mejorar: tal como comentó Joan Miquel en Bulmailing, podriamos hacer una contraseña del tipo "_trozo_fijo_aleatorio". Y en el papel solo imprimir la parte aleatoria, así si perdemos el papel no sería tan grave. Eso cada uno lo puede hacer.
Tambien podemos hacer que cada mañana se generen las contraseñas (unas 10 o 20) nuevas para el dia, desde el cron por ejemplo. Nos levantamos, cogemos la hoja y a trabajar.

Paquetes: tuve que instalar el paquete *pwgen* y *expect*.

Lista de enlaces de este artículo:

1. http://www.spydevicecentral.com/comp_dev.htm

E-mail del autor: carles _ARROBA_ pinux.info
Podrás encontrar este artículo e información adicional en: http://bulma.net/body.phtml?nIdNoticia=1601