Has perdido las password de root??? no te preocupes he aquí la solución!!!!

fuente: www.open-sec.com

Puesto que la acción natural debería ser ingresar como root al sistema y utilizar el comando passwd para cambiar el password de este usuario y para ello se requiere el password actual que no se tiene, se tendrá que reiniciar cada unos de los servidores Linux y ejecutar una de las **tres**
siguientes acciones :

1) En la pantalla inicial donde aparece un menu de texto con opciones (primera pantalla, GRUB), presionar e y aparecerá un nuevo menu donde se deberá presionar nuevamente e y se presentará una línea de edición. Ir hasta el final y adicionar la palabra single, presionar Enter y luego la letra b. Esto hará que el sistema inicie en modo de usuario único, como root y sin solicitar password. Una vez ubicado en el prompt del sistema (XXXX#), ejecutar el comando passwd e ingresar el nuevo password 2 veces.

2) Si al ingresar en el modo de usuario único de todas formas se solicita el password actual (lo más común en distros hace un par de años), entonces proceder de una de las siguientes formas :

3) Usar el Modo e Rescate o Emergency Disk o Rescue Mode o Emergency Mode donde se obtendrá un fake root filesystem y se debe proceder a montar el filesystem real y luego, proceder de forma similar a la siguiente opción.
* Reiniciar el equipo con el CD número 1 de su distro
- Aceptar las opciones default presentadas.
- Al llegar a la selección de idioma, presionar simultáneamente CTRL y ALT y F2
- En este prompt del sistema (#) se pueden ejecutar tareas a nivel de administrador
- Montar el sistema raíz actual de Linux con los comandos :
mkdir /tempo

mount /dev/hda2 /tempo
vi /tempo/etc/shadow (abrirá el archivo de passwords con el editor vi)
Buscar la línea que empieza con la palabra root, ejemplo :
root:$1$3Z3ZLRxz$WPVAiNbpYn5xKrZSMKAZc/:12824:0:10000::::
Posicionar el cursor sobre el primer caracter después de root: ($ según el ejemplo) Presionar x hasta que desaparezca el password y antes de llegar a los dos puntos siguientes (:12811... según el ejemplo)
Grabar el archivo presionando : wq!
umount /tempo
Reiniciar el equipo con el comando reboot o init 6
Retirar el CD del equipo
El sistema reiniciará y permitirá el acceso como usuario root sin password, por lo cual, lo primero que debe hacerse es ingresar por una pantalla de consola (CTRL, ALT y F1), ingresar como root y apenas aparezca el prompt (XXXX#) ejecutar el comando passwd.

NOTA: Si al ejecutar el comando mount /dev/hda2 /tempo se obtiene un error, probar reemplazando /dev/hda2 por /dev/hda1 o /dev/sda1 o /dev/sda2. Una persona conocedora de Linux y/o Unix no probará sino sabrá como deducir donde se encuentra el root filesystem utilizando el comando fdisk -l o similar o reconociendo el hardware que dispone.

Otras acciones posteriores incluyen :
*Eliminar los usuarios que no corresponden a empleados de la organización o usuarios aprobados.
*Pueden existir usuarios del sistema con los siguientes nombres que NO deben ser eliminados : bin, daemon, lp, mail, games, at, wwwrun, squid, irc, ftp, named, gdm, postfix, mysql, pop, sshd, mailman, ntp, ldap, radiusd, privoxy, nobody, dhcpd, man, bews, uucp. Los usuarios no adecuados se eliminan con el comando userdel nombre_de_usuario.
* Muchos de estos usuarios válidos del sistema no requieren un shell, por lo cual, su shell debería ser /bin/false (en el /etc/passwd).
*Otras labores implican acciones como reconocimiento de puertos abiertos e innecesarios (netstat -pan), revisión de derechos sobre el sistema de archivos (ls -al), revisión de atributos de los archivos del sistema (lsattr) que pueden requerir la intervención de alguna persona con experiencia en aseguramiento de servidores Linux.