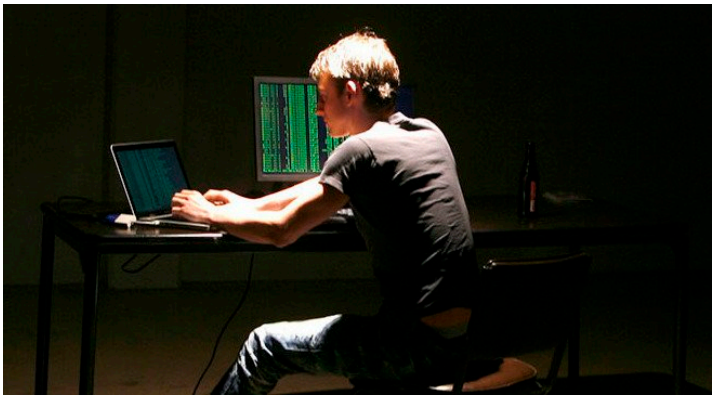
Mejorar La Seguridad De Contraseñas En Linux



La administración de ***cuentas de usuario en Linux***, es uno de los trabajos más críticos para los ***administradores de sistemas Linux***. En particular, la seguridad de contraseña debe ser considerada la principal preocupación para cualquier sistema seguro en Linux. En este tutorial, te mostraremos cómo configurar y **mejorar las políticas de contraseñas en Linux**. Para esto haremos uso de PAM (Pluggable Authentication Modules) en el sistema.

Preparación

Si por alguna razón en tu SO Linux no esta instalada la librería, el primero paso es **instalar el módulo PAM** para habilitar el soporte de cracklib, el cual proporciona capacidades adicionales para la comprobación de contraseñas.

En Debian, Ubuntu o Linux Mint:

[bash]$ sudo apt-get install libpam-cracklib[/bash]

El módulo PAM cracklib se instala por defecto en CentOS, Fedora o Red Hat Enterprise. Así que simplifica la instalación necesaria en estos sistemas. Para hacer cumplir la política de contraseñas, se debe modificar un ***archivo de configuración PAM*** relacionado con la autenticación ubicado en /etc/pam.d. El cambio de política se llevará a efecto inmediatamente después del cambio.

Prevenir Usar Contraseñas Antiguas En Linux

Busque una línea que contiene tanto «password» y «pam_unix.so» y añadir «remember=5» a esa línea. Con esto se evitará cinco contraseñas usadas recientemente (almacenándolos en /etc/security/opasswd).

En Debian, Ubuntu o Linux Mint:

[bash]$ sudo vi /etc/pam.d/common-password[/bash]

Se ha usado el editor vi para modificar el archivo correspondiente, pero puedes usar otro editor como nano para realizar la modificación.

En Fedora, CentOS o RHEL:

[bash]$ sudo vi /etc/pam.d/system-auth[/bash]

Configurar Longitud Mínima De La Contraseñas En Linux

Busque una línea que contenga tanto «password» y «pam_cracklib.so» y añada «minlen = 10» a esa línea. Esto hará que la longitud de la contraseña sea de 10, si deseas otro valor, puedes modificarlo. Existen cuatro tipos de validación para caracteres (mayúsculas, minúsculas, numéricos y símbolos). Si usas la mezcla con este tipo de validación, solo

podrás usar un mínimo de 6 caracteres.

En Debian, Ubuntu o Linux Mint:

[bash]$ sudo vi /etc/pam.d/common-password[/bash]

En Fedora, CentOS o RHEL:

[bash]$ sudo vi /etc/pam.d/system-auth[/bash]

Definir Complejidad De La Contraseña En Linux

Busque en la línea que contiene «password» y «pam_cracklib.so» y añada «ucredit=-1 lcredit=-2 dcredit=-1 ocredit=-1» a esa línea. Esto obligará a incluir al menos una letra mayúscula (ucredit), dos letras minúsculas (lcredit), un dígito (dcredit) y un símbolo (ocredit).

En Debian, Ubuntu o Linux Mint:

[bash]$ sudo vi /etc/pam.d/common-password[/bash]

En Fedora, CentOS o RHEL:

[bash]$ sudo vi /etc/pam.d/system-auth[/bash]

Definir El Período En Expirar La Contraseña

Para establecer un período máximo para la contraseña, se debe editar las siguientes variables en /etc/login.defs.

[bash]

$ sudo vi /etc/login.defs

PASS_MAX_DAYS 150
PASS_MIN_DAYS 0
PASS_WARN_AGE 7

[/bash]

Esto obligará a todos los usuarios a cambiar su contraseña una vez cada seis meses, y enviar un mensaje de advertencia siete días antes de caducidad de la contraseña. Si desea establecer la caducidad de contraseñas en función de cada usuario, utilice el comando **instead**. Para ver la directiva de caducidad de la contraseña para un usuario específico:

[bash]

$ sudo chage -l xmodulo
Last password change : Dec 30, 2013
Password expires : never
Password inactive : never
Account expires : never
Minimum number of days between password change : 0
Maximum number of days between password change : 99999
Number of days of warning before password expires : 7

[/bash]

De forma predeterminada, la contraseña de un usuario se establece para que no caduque nunca. Para cambiar el período de caducidad de contraseña para determinado usuario, es bastante útil usar xmodulo:

[bash]$ sudo chage -E 1/30/2015 -m 5 -M 90 -I 30 -W 14 xmodulo[/bash]

El comando anterior establecer la contraseña expira el 01/30/2015. Además, el número máximo/mínimo de días entre cambios de contraseña se establece en 5 y 90, respectivamente. La cuenta será bloqueada 30 días después de que expire una contraseña y un mensaje de advertencia será enviado 14 días

antes de la expiración de contraseña.