Contraseñas shadow

Antonia Estero Botaro y Antonio García Domínguez

Seguridad y Competencias Profesionales
Curso 2009-2010
29 octubre 2009

El método clásico que utilizaban los sistemas UNIX para almacenar las contraseñas de los usuarios, daba lugar a una serie de problemas. Al ser el fichero `/etc/passwd` de lectura pública, cualquier usuario del sistema podía emplear mecanismos de fuerza bruta para encontrar contraseñas de los usuarios. Por otro lado, un intruso que tuviera acceso al sistema también podía hacerse con este fichero y emplear la misma técnica anterior, asegurándose el conocimiento de algunas contraseñas, para así poder acceder al sistema posteriormente. Todo esto condujo a la implantación de un método más seguro para almacenar las contraseñas, que se conoce como *shadow passwords*.

Cuando se utiliza el oscurecimiento de contraseñas, el formato del fichero `/etc/passwd` queda como se muestra a continuación; es decir, en el segundo campo aparece una `x` en vez de la contraseña codificada.

```
antonia:x:501:100:Antonia Estero Botaro:/home/antonia:/bin/bash
```

Además de éste tendremos el fichero `/etc/shadow` que es el que almacena la contraseña codificada, utilizando el siguiente formato:

```
antonia:3s5RxKpTg7b0Q:12078:2:180:7:7:12265:
```

Los dos primeros campos se corresponden con el nombre de usuario y su contraseña codificada, respectivamente. El resto de campos de este fichero corresponden a información que permite implementar otro mecanismo para proteger las contraseñas de los usuarios, el «envejecimiento de contraseñas».

La idea básica de este mecanismo es proteger las contraseñas de los usuarios dándoles un período de vida máximo, es decir, las contraseñas de los usuarios sólo son válidas durante un cierto tiempo, pasado el cual expirarán y deberán ser cambiadas.

¿De qué nos protege este mecanismo? La idea es la siguiente si un intruso ha conseguido nuestra contraseña por la razón que sea, y ésta es siempre es la misma (no expira), tiene asegurado el acceso al sistema durante tiempo indefinido. Sin embargo, si la contraseña expira, cuando la cambiemos dejará de tener acceso al sistema.

Los campos que almacena `/etc/shadow` relacionados con el envejecimiento son los siguientes:

- Cuándo se cambió la contraseña por última vez, en forma de los días transcurridos desde el 1 de enero de 1970 hasta ese momento.
- Días que han de transcurrir antes de que el usuario pueda volver a cambiar su contraseña.
- Días tras los cuales se ha de cambiar la contraseña.
- Días durante los que el usuario será avisado de que su contraseña va a expirar antes de que ésta lo haga.
- Días que la cuenta estará habilitada tras la expiración de la contraseña.
- Días desde el 1 de enero de 1970 hasta que la cuenta se deshabilite.
- Campo reservado.

Cuando un usuario cambia su contraseña, se le puede impedir cambiarla durante un cierto tiempo; esto tiene como objetivo que el usuario no restaure inmediatamente la contraseña antigua después de haberla cambiado. Pasado este período el usuario podrá volver a cambiar su contraseña de forma voluntaria. Si el número máximo de días en los que el usuario no puede cambiar su contraseña es mayor que el número de días tras los cuales es obligatorio el cambio, el usuario no podrá cambiarla nunca, y la cuenta quedará bloqueada después del período de gracia que se da una vez expirada la contraseña.

Aunque **root** tiene acceso para modificar los ficheros `/etc/passwd` y `/etc/shadow`, no debería editarlos utilizando un editor de texto. La razón de ésto es la seguridad del sistema, ya que en la edición de estos ficheros se podría cometer un error que la comprometiera.

Aún así, si se necesita editar estos ficheros porque están corruptos, se debería utilizar la orden *vipw*, ya que ésta bloquea el fichero `/etc/passwd` antes de lanzar el editor *vi* o aquel que tengamos establecido en la variable del *shell* EDITOR. Esto previene los conflictos que pudieran aparecer si varios administradores decidieran editar el fichero. La orden *vigr* es similar a la anterior y sirve para editar el fichero `/etc/group`. Una vez editado el fichero de grupos con `vigr` podemos utilizar la orden *grpck* para verificar que todas las líneas tienen el número correcto de campos, un nombre de grupo único, y una lista válida de miembros.

Si lo que se desea es editar los ficheros `/etc/shadow` o `/etc/gshadow` podemos utilizar las órdenes anteriores pero con la opción `-s`.

Todas las opciones que se contemplan en el fichero `/etc/shadow` pueden ser controladas cuando creamos una cuenta de usuario con *useradd* o cuando cambiamos su contraseña con *passwd*.

La orden *passwd* proporciona una serie de opciones que permiten controlar los aspectos comentados anteriormente.

Opción	Significado
`-l`	Bloquea la cuenta de un usuario.
`-u`	Desbloquea una cuenta que ha sido bloqueada anteriormente con la opción `-l`. La contraseña de la cuenta no varía.
`-n`	Establece el número mínimo de días que el usuario debe esperar antes de cambiar su contraseña.
`-x`	Establece el número máximo de días durante los que va a ser válida la contraseña actual.
`-w`	Establece el número de días durante los cuales el usuario va a ser avisado (al entrar en su cuenta) de que debe cambiar la contraseña para evitar que la cuenta se bloquee.
`-i`	Establece el número de días en que la cuenta estará habilitada después de que la contraseña haya expirado. Pasado este tiempo la cuenta se bloqueará.