

El Día a Día del Administrador de Sistemas

# CONTRASEÑAS

Fácil de recordar pero segura, éste es el problema típico a la hora de elegir una contraseña. La herramienta PWGen ofrece una solución práctica.

## POR CHARLY KÜHNAST

Si tiene buena memoria recordará que en números anteriores me quejaba de la debilidad de las contraseñas. La herramienta Fail2ban [1] de la que hablaba en ese artículo impide los desastres, pero en realidad sólo trata los síntomas. Si se escoge el parámetro de tiempo adecuado, Fail2ban repelerá los ataques de fuerza bruta, pero no tiene nada que hacer frente a las contraseñas introducidas por el teclado o las que son fáciles de adivinar (Figura 1). Como siempre sucede cuando se trata de tecnologías de seguridad, el grado deseado de protección determinado por el administrador y la conveniencia, preferida por los usuarios, siempre están en conflicto.

Rotar las contraseñas cada cuatro semanas es tan sólo una medida más de seguridad que acaba con la paciencia de los usuarios; además, no puede esperarse que recuerden este tipo de asuntos. De este modo, los usuarios anotan sus contraseñas, y las Leyes de Murphy dictan que dejarán el papelito en el peor de los sitios posibles. El reverso de la moneda consiste en un entorno en el que los administradores permiten que los usuarios tengan sus propias contraseñas, que acabarán

siendo del tipo *tux* o *alto\_secreto*. ¿Y ahora qué?

### Repartidor de Contraseñas

PWGen [2] ofrece un compromiso: la herramienta genera contraseñas con propiedades configurables. Si se llama a PWGen sin ningún parámetro desde la línea de comandos engendra una lista de contraseñas con letras, minúsculas y mayúsculas, y números. *pwgen -s -y* genera contraseñas realmente robustas que podrían parecerse a las siguientes:

```
+3HEg,_5
1P.A@=2U
@|{|}9Cy
```

Pero PWGen puede gestar contraseñas más sencillas sin llegar a rebajar el nivel de seguridad al extremo de poner como contraseña el nombre del perro de su vecino. Esta herramienta no usará el juego de caracteres estándar por defecto, mientras que el parámetro *-B* suprime los caracteres que los usuarios tienden a confundir, como *l* y *l* o *O* y *0*. Si se hace una concesión y se suprimen



Figura 2: PWGen genera listas completas de contraseñas, algunas de las cuales son bastante sencillas de memorizar por los usuarios.

los números, se pueden generar contraseñas que la gente puede pronunciar con algo de imaginación, estableciendo un compromiso entre conveniencia y seguridad, siempre que se use para proteger a los usuarios con cuentas sin privilegios y no a las joyas de la corona.

En teoría, se podría hacer más simple indicándole a PWGen que no utilice letras en mayúsculas, pero no es algo que yo recomendaría. No quiero ponerlo tan fácil a mis usuarios, después de todo, el ejercicio mental es algo que nos viene bien a todos.

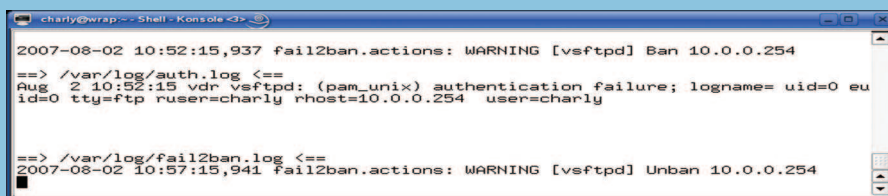


Figura 1: El bloqueo de IPtables al equipo 10.0.0.254 comenzó a las 10:52 y finalizó a las 10:57.

### RECURSOS

[1] "Fail2ban" por Charly Kühnast, Linux Magazine – Edición en Castellano, número 40.

[2] PWGen: <http://sourceforge.net/projects/pwgen/>

### SYSADMIN

**Kosmos** .....54  
Presentamos Kosmos, un sistema de ficheros distribuido de altas prestaciones.

**DNSSEC** .....58  
Vemos cómo utilizar la criptografía para la protección del servicio de resolución de nombres.