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

Como realizar un ataque a los archivos de contraseñas. (437625 lectures)

Per **Carlos Cortes Cortes**, ***carcoco*** (http://bulma.net/~carcoco/)

Creado el 24/01/2002 22:52 modificado el 24/01/2002 22:52

> Básicamente pretendo demostrar lo importante que es elegir buenos **passwords** en cualquier entorno informático. Para hacerlo os mostraré lo fácil que resulta un ataque al fichero de **passwords** para obtener las **contraseñas** débiles/inseguras ...

Cada vez las **contraseñas** son más y más habituales en nuestras vidas: claves del banco, código PIN del móvil, contraseñas ordenador, conexión a Internet, cuentas de correo, código radio-cassette del coche, y un largo etc...

Por este motivo es realmente importante el elegir **contraseñas seguras** y que nos ofrezcan unas mínimas garantias. Aquí os dejo algunos **consejos** relativos a las contraseñas:

- Se deben de cambiar cada cierto tiempo.
- Deben de contener, idealmente, una mezcla de letras, números y otros caracteres.
- Deben de tener cierto tamaño, puesto que cuando más cortas, más faciles serán de descubrir.
- No se deben de usar la misma contraseña para sitios distintos.
- No deben de contener información personal de ningún tipo.
- No debe de ser alguna palabra conocida o pertenecer a otro idioma.
- No deberia de ser mutaciones simples de palabras, sería contraseñas muy flojas: unouno, tr3s, casa23, amlub (bulma al revés).
- Aunque al mismo tiempo ha de ser facilmente recordable, porque no se debe escribir en ningún lugar.

Podemos controlar algunas de estas *sugerencias* a través del fichero **login.defs**, que se suele encontrar en el directorio **/etc**:

```
...
FAIL_DELAY              3
FAILLOG_ENAB            yes
LOG_UNKFAIL_ENAB        no
LASTLOG_ENAB            yes
PASS_MAX_DAYS           99999
PASS_MIN_DAYS           0
PASS_MIN_LEN            5
PASS_WARN_AGE           7
CRACKLIB_DICTPATH       /usr/lib/cracklib_dict
LOGIN_RETRIES           3
LOGIN_TIMEOUT           60
PASS_CHANGE_TRIES       3
PASS_ALWAYS_WARN        yes
PASS_MAX_LEN            8
...
```

Las contraseñas en Linux y otros Unix, se almacenan encriptadas, en ficheros de texto, *normalmente* en /etc/passwd, de forma que podemos lanzar ataques para intentar averiguar las contraseñas que se esconden en estos ficheros.

Hasta hace *"relativamente poco tiempo"*, las contraseñas de los sistemas linux/unix se almacenaban directamente en el fichero **/etc/passwd**, que era accesible en modo lectura por todo los usuarios del sistema, puesto que eran usado directamente para validar o no la entrada en el sistema a los usuarios. Esto era un grave problema de seguridad, por lo que actualmente todas las distribuciones linux suelen utilizar lo que se denomina **shadowing** de contraseñas, de forma que el fichero donde realmente se almacenan las contraseñas, es **/etc/shadow**:

```
$ l /etc/passwd
-rw-r--r--    1 root     root         2093 ene 22 20:01 /etc/passwd
$ l /etc/shadow
-rw-r-----    1 root     shadow        999 ene 22 20:01 /etc/shadow
```

Para averiguar si nuestros usuarios están usando contraseñas **debiles** y por lo tanto inseguras, tendremos que recurrir a programas que permiten realizar ataques por **fuerza bruta** (es decir ir realizando pruebas una tras otras, sin aplicar ningún algoritmo inteligente, utilizando una **lista de palabras**, que se suele denominar **diccionarios**, por lo que también se les conoce por ataques a diccionario), tales como Crack, SaltineCracker, slurpie, John the Ripper, Killer Cracker, Lard, PerlCrack, Xcrack, Nutcracker, ...

Veremos alguno de estos programas con los que es posible realizar un ataque por fuerza bruta (ataque usando diccionarios de palabras), por último para que practiqueís un poco os dejo un trozo de fichero de passwords, para que obtengaís las contraseñas de los mismos.

- **Crack**.
- **John the Ripper**

Crack
Crack, desarrollado por el galés **Alec Muffet**, fue uno de los primeros programas de este tipo que se desarrollaron, según el propio autor: *Está escrito para que sea flexible, configurable y rápido* y ciertamente podemos decir que lo ha logrado.
Para usarlo tendremos que ejecutar:

```
Crack passwords.txt
```

Lo podeís obtener de: http://www.users.dircon.co.uk/~crypto/(1)
ftp://ftp.cert.dfn.de/pub/tools/password/Crack/Crack_5.0a.tar.gz(2)

John the Ripper
Un crackeador de contraseñas para detectar contraseñas débiles en Unix
Uso:

```
# john passwords.txt
```

```
john passwords.txt
Loaded 2 passwords with 2 different salts (Standard DES [24/32 4K])
guesses: 0  time: 0:00:00:00 10% (2)  c/s: 23462  trying: Nascar1 - Cesar1
guesses: 0  time: 0:00:00:01 21% (2)  c/s: 48806  trying: brandon3 - terry3
guesses: 0  time: 0:00:00:02 33% (2)  c/s: 37075  trying: million6 - vermont6
guesses: 0  time: 0:00:00:03 48% (2)  c/s: 32994  trying: Oodoov - Dnomyar
guesses: 0  time: 0:00:00:04 60% (2)  c/s: 31017  trying: Melissa3 - Biteme3
guesses: 0  time: 0:00:00:05 71% (2)  c/s: 29882  trying: Special8 - Dollars8
```

Cada vez que presionamos cualquier tecla, el programa nos muestra una línea indicando por las combinaciones de caracteres que esta testeando en ese momento, tal y como podemos ver, en el ejemplo anterior.

Por otra parte, para ver los password que ya hemos encontrado, bastará con invocar al programa de esta forma:

```
john -show passwords.txt
```

Para obtener **John the Ripper**, tendremos que la sección dedicada al mismo del proyecto **OpenWall**, http://www.openwall.com/john/(3), que incluyen otros programas relacionados con la seguridad, como **owl**, **scanlogd**, **popa3d**, ... http://www.openwall.com/(4).

Para que podaís practicar con ambos y ver por vosotros mismos los problemas que se comentan en este articulo, os dejo este trozo de archivo de passwords, para que obtengaís las contraseñas contenidas en el mismo:

```
uno:PdPPzjKWABro6:11708:0:99999:7:::
dos:JeG2YPCO65zio:11708:0:99999:7:::
tres:Ifp4Wl.Bzwebc:11708:0:99999:7:::
quatre:BidfFQXn3Wr6c:11708:0:99999:7:::
cinc:Ojmk0VSOfQIX6:11708:0:99999:7:::
sis:JnLdKWzuyW4Bk:11708:0:99999:7:::
```

Cualquiera de estos 2 programas (**crack** y **john**) tienen una excelente documentación que además de explicar el funcionamiento de los mismo, detallan ampliamente las nociones relativas con las contraseñas, como por ejemplo, este trozo de la documentación del Crack:

```
For instance, NEVER use passwords like:
alec7       - it's based on the users name (& it's too short anyway)
tteffum     - based on the users name again
gillian     - girlfiends name (in a dictionary)
naillig     - ditto, backwards
PORSCHE911  - it's in a dictionary
12345678    - it's in a dictionary (& people can watch you type it easily)
qwertyui    - ...ditto...
abcxyz      - ...ditto...
0ooooooo    - ...ditto...
Computer    - just because it's capitalised doesn't make it safe
wombat6     - ditto for appending some random character
6wombat     - ditto for prepending some random character
merde3      - even for french words...
mr.spock    - it's in a sci-fi dictionary
zeolite     - it's in a geological dictionary
ze0lite     - corrupted version of a word in a geological dictionary
ze0l1te     - ...ditto...
Z30L1T3     - ...ditto...
```

Comentar también la existencia de **comprobadores proactivos de contraseñas**, que son unos programas que se instalan de forma que evitan el que se introduzan contraseñas débiles en la base de datos de contraseñas. El funcionamiento es muy sencillo, se realiza una especie de mini ataque a diccionario y unas ciertas reglas, de forma que si se averigua el password, se imposibilita el uso del mismo. Encontramos entre otros: **anlpasswd**, **npasswd**, **passwd+**, ...

FAQ del **PAM** (Pluggable Authentication Modules):
http://www.kernel.org/pub/linux/libs/pam/FAQ[5]

The Linux-PAM System Administrators' Guide:
http://www.kernel.org/pub/linux/libs/pam/Linux-PAM-html/pam.html [6]

Interesante articulo e inglés sobre el tema:
The Simplest Security: **A Guide To Better Password Practices**.
http://www.securityfocus.com/infocus/1537[7]

--
Carlos Cortes(aka carcoco)
http://bulma.net/todos.phtml?id_autor=132 [8]

Lista de enlaces de este artículo:

1. http://www.users.dircon.co.uk/~crypto/
2. ftp://ftp.cert.dfn.de/pub/tools/password/Crack/Crack_5.0a.tar.gz
3. http://www.openwall.com/john/
4. http://www.openwall.com/
5. http://www.kernel.org/pub/linux/libs/pam/FAQ
6. http://www.kernel.org/pub/linux/libs/pam/Linux-PAM-html/pam.html
7. http://www.securityfocus.com/infocus/1537
8. http://bulma.net/todos.phtml?id_autor=132

E-mail del autor: carcoco _ARROBA_ gmail.com
Podrás encontrar este artículo e información adicional en: http://bulma.net/body.phtml?nIdNoticia=1152