

# Práctica 10. Gestión de contraseñas

Seguridad de Sistemas Informáticos

Cheuk Kelly Ng Pante (alu0101364544@ull.edu.es)

6 de diciembre de 2023

# Índice general

1. Instalación de paquetes	1
2. Generar un fichero de contraseñas con hashes MD5	2
3. Creacion de usuarios con contraseñas generadas por <i>pwgen</i>	3
3.1. Contraseñas de menor a mayor fortaleza . . . . .	4
4. Crackear las contraseñas con la herramienta <i>John the Ripper</i>	5
5. Bibliografía	6

## 1. Instalación de paquetes

- **pwgen**. Generador de contraseñas fuertes: `sudo apt-get install pwgen`

```
usuario@MV-p10:~$ sudo apt install pwgen
[sudo] contraseña para usuario:
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes NUEVOS:
  pwgen
0 actualizados, 1 nuevos se instalarán, 0 para eliminar y 0 no actualizados.
Se necesita descargar 19,6 kB de archivos.
Se utilizarán 52,2 kB de espacio de disco adicional después de esta operación.
Des:1 http://deb.debian.org/debian bookworm/main amd64 pwgen amd64 2.08-2 [19,6 kB]
Descargados 19,6 kB en 0s (122 kB/s)
Seleccionando el paquete pwgen previamente no seleccionado.
(Leyendo la base de datos ... 43557 ficheros o directorios instalados actualmente.)
Preparando para desempaquetar .../pwgen_2.08-2_amd64.deb ...
Desempaquetando pwgen (2.08-2) ...
Configurando pwgen (2.08-2) ...
Procesando disparadores para man-db (2.11.2-2) ...
usuario@MV-p10:~$
```

Figura 1.1: Instalación de pwgen

- **makepasswd**. Generador de contraseñas aleatorias seguras y fiables: `sudo apt-get install makepasswd`

```
usuario@MV-p10:~$ sudo apt install makepasswd
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
  libbytes-random-secure-perl libcrypt-passwdmd5-perl libcrypt-random-seed-perl libmath-random-isaac-perl
  libmath-random-isaac-xs-perl
Se instalarán los siguientes paquetes NUEVOS:
  libbytes-random-secure-perl libcrypt-passwdmd5-perl libcrypt-random-seed-perl libmath-random-isaac-perl
  libmath-random-isaac-xs-perl makepasswd
0 actualizados, 6 nuevos se instalarán, 0 para eliminar y 0 no actualizados.
Se necesita descargar 106 kB de archivos.
Se utilizarán 301 kB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n] s
```

Figura 1.2: Instalación de makepasswd

- **apg**. Generador automático de contraseñas: `sudo apt-get install apg`

```
usuario@MV-p10:~$ sudo apt install apg
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes NUEVOS:
  apg
0 actualizados, 1 nuevos se instalarán, 0 para eliminar y 0 no actualizados.
Se necesita descargar 52,7 kB de archivos.
Se utilizarán 145 kB de espacio de disco adicional después de esta operación.
Des:1 http://deb.debian.org/debian bookworm/main amd64 apg amd64 2.2.3.dfsg.1-5+b2 [52,7 kB]
Descargados 52,7 kB en 0s (363 kB/s)
Seleccionando el paquete apg previamente no seleccionado.
(Leyendo la base de datos ... 43632 ficheros o directorios instalados actualmente.)
Preparando para desempaquetar .../apg_2.2.3.dfsg.1-5+b2_amd64.deb ...
Desempaquetando apg (2.2.3.dfsg.1-5+b2) ...
Configurando apg (2.2.3.dfsg.1-5+b2) ...
Procesando disparadores para man-db (2.11.2-2) ...
```

Figura 1.3: Instalación de apg

- **john (John The Ripper)**. Crackeador de contraseñas: `sudo apt-get install john`

```
usuario@MV-p10:~$ sudo apt install john
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
  john-data
Se instalarán los siguientes paquetes NUEVOS:
  john john-data
0 actualizados, 2 nuevos se instalarán, 0 para eliminar y 0 no actualizados.
Se necesita descargar 8.964 kB de archivos.
Se utilizarán 20,7 MB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n] s
```

Figura 1.4: Instalación de john

## 2. Generar un fichero de contraseñas con hashes MD5

Para generar un fichero de contraseñas con hashes MD5, se utilizará la herramienta *makepasswd* pero como se está usando una máquina virtual del IAAS de la ULL y estas máquinas tienen baja entropía en el generador de números aleatorios, hay que instalar y configurar *haveged* para resolverlo. Para ello, se ejecuta el siguiente comando: `sudo apt-get install haveged` y configuramos el fichero `/etc/default/haveged` asegurando que la variable `DAEMON_ARGS` contenga lo siguiente: `DAEMON_ARGS="-w 1024"`. Una vez hecho esto, hay que estar seguro de que el servicio *haveged* se está ejecutando: `update-rc.d haveged defaults`

Ahora, se puede generar el fichero de contraseñas con hashes MD5 con el siguiente comando:

```
1 echo "mypassword" | makepasswd --clearfrom=- --crypt-md5 | awk '{ print $2 }'
```

```
usuario@MV-p10:~$ echo "mypassword" | makepasswd --clearfrom=- --crypt-md5 | awk '{ print $2 }'  
$1$CWB5g.e8$ErLD5H/MR0dThDZ7ebWAZ.  
usuario@MV-p10:~$
```

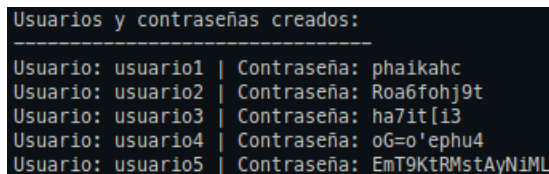
Figura 2.1: Generación de un fichero de contraseñas con hashes MD5

### 3. Creacion de usuarios con contraseñas generadas por *pwgen*

Para crear usuarios con contraseñas generadas por *pwgen*, se ha creado un script que genera cinco usuarios con contraseñas de menor a mayor fortaleza. El script es el siguiente:

```
1  #!/bin/bash
2
3  USERS=("usuario1" "usuario2" "usuario3" "usuario4" "usuario5")
4
5  PASSWORDS=()
6
7  sudo adduser usuario1
8  password1=$(pwgen -0 8 -A -1)
9  echo "usuario1:$password1" | sudo chpasswd
10 PASSWORDS+=("$password1")
11
12 sudo adduser usuario2
13 password2=$(pwgen -n -1 10)
14 echo "usuario2:$password2" | sudo chpasswd
15 PASSWORDS+=("$password2")
16
17 sudo adduser usuario3
18 password3=$(pwgen -y -A 8 -1)
19 echo "usuario3:$password3" | sudo chpasswd
20 PASSWORDS+=("$password3")
21
22 sudo adduser usuario4
23 password4=$(pwgen -c -n -y 10 -1)
24 echo "usuario4:$password4" | sudo chpasswd
25 PASSWORDS+=("$password4")
26
27 sudo adduser usuario5
28 password5=$(pwgen -c -n -s -B -1 16)
29 echo "usuario5:$password5" | sudo chpasswd
30 PASSWORDS+=("$password5")
31
32 echo "Usuarios y contraseñas creados:"
33 echo "-----"
34 for ((i=0; i<${#USERS[@]}; i++)); do
35     echo "Usuario: ${USERS[i]} | Contraseña: ${PASSWORDS[i]}"
36 done
```

Al ejecutar el script, se crean los usuarios con las contraseñas generadas por *pwgen*:



```
Usuarios y contraseñas creados:
-----
Usuario: usuario1 | Contraseña: pha1kahc
Usuario: usuario2 | Contraseña: Roa6fohj9t
Usuario: usuario3 | Contraseña: ha7it[i3
Usuario: usuario4 | Contraseña: oG=o'ephu4
Usuario: usuario5 | Contraseña: EmT9KtRMstAyN1ML
```

Figura 3.1: Creación de usuarios con contraseñas generadas por *pwgen*

Una vez creado los usuarios, copiamos el fichero */etc/passwd* a un directorio de trabajo como se muestra en la figura 3.2:

```

usuario@MV-p10:~$ mkdir p10 && cd p10
usuario@MV-p10:~/p10$ sudo cp /etc/passwd passwd
[sudo] contraseña para usuario:
usuario@MV-p10:~/p10$ cat passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
_apt:x:42:65534:./nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:998:998:systemd Network Management:./usr/sbin/nologin
systemd-timesync:x:997:997:systemd Time Synchronization:./usr/sbin/nologin
messagebus:x:100:107:./nonexistent:/usr/sbin/nologin
sshd:x:101:65534:./run/sshd:/usr/sbin/nologin
usuario:x:1000:1000:usuario,,,:/home/usuario:/bin/bash
adminstic:x:1001:1001:./home/adminstic:/bin/bash
soporteiaas:x:1002:1002:./home/soporteiaas:/bin/bash
usuario1:x:1003:1003:./home/usuario1:/bin/bash
usuario2:x:1004:1004:./home/usuario2:/bin/bash
usuario3:x:1005:1005:./home/usuario3:/bin/bash
usuario4:x:1006:1006:./home/usuario4:/bin/bash
usuario5:x:1007:1007:./home/usuario5:/bin/bash
usuario@MV-p10:~/p10$

```

Figura 3.2: Copia del fichero */etc/passwd*

### 3.1. Contraseñas de menor a mayor fortaleza

- ***pwgen -o -A 8 -1***: Contraseña donde no incluye numeros, solo letras minúsculas y de longitud 8.
- ***pwgen -n -1 10***: Contraseña que al menos una letra mayúscula, sin numeros y de longitud 12.
- ***pwgen -y -A 8 -1***: Contraseña que incluye al menos un símbolo especial con todas las letras minúsculas y de longitud 8.
- ***pwgen -c -n -y 10 -1***: Contraseña que incluye al menos una mayúscula, al menos algún número y algún símbolo especial con longitud 10.
- ***pwgen -c -n -s -B -1 16***: Contraseña que incluye al menos una mayúscula, al menos algún número, donde no incluye caracteres ambiguos y generando contraseñas completamente aleatorias de longitud 16.

#### 4. Crackear las contraseñas con la herramienta *John the Ripper*

## 5. Bibliografía

1. LaMendola, S. (2013). How to Setup Additional Entropy for Cloud Servers Using Haveged. DigitalOcean. Recuperado de <https://www.digitalocean.com/community/tutorials/how-to-setup-additional-entropy-for-cloud-servers-using-haveged>