

## Parte 1: Frases de paso

Number of Dice Rolls:

2 3 4 5 6 7 8

► Roll Dice!

"Exposable"

Number of Dice Rolls:

2 3 4 5 6 7 8

► Roll Dice!

"Fried"

Number of Dice Rolls:

2 3 4 5 6 7 8

► Roll Dice!

"Cringe"

Number of Dice Rolls:

2 3 4 5 6 7 8

► Roll Dice!

"Probation"

Number of Dice Rolls:

2 3 4 5 6 7 8

► Roll Dice!

"Breeches"

Number of Dice Rolls:

2 3 4 5 6 7 8

► Roll Dice!

"Kleenex"

Your words are:

Exposable Fried Cringe Probation Breeches Kleenex

Your passphrase is:

ExposableFriedCringeProbationBreechesKleenex

## Parte 2: Comparar fortaleza de contraseñas

password123

### How Secure Is My Password?

The #1 Password Strength Tool. Trusted and used by millions.



It would take a computer about  
6 hundred years  
to crack your password

P@ssw0rd!

### How Secure Is My Password?

The #1 Password Strength Tool. Trusted and used by millions.



It would take a computer about  
3 weeks  
to crack your password

**ExposableFriedCringeProbationBreechesKleenex**

## How Secure Is My Password?

The #1 Password Strength Tool. Trusted and used by millions.

.....

it would take a computer about:

2 octodecillion years

to crack your password

**ExposableFriedCringeProbationBreechesKleenex@**

## How Secure Is My Password?

The #1 Password Strength Tool. Trusted and used by millions.

.....

it would take a computer about:

11 vigintillion years

to crack your password

*Las contraseñas largas suponen un problema mayor para el atacante ya que son más caracteres que tiene que descifrar.*

*Las contraseñas cortas son más fáciles de recordar.*

# Parte 3: Almacenamiento de contraseñas en Linux y Windows

```
kali㉿kali: ~
Session Actions Edit View Help
(kali㉿kali)-[~]
$ sudo useradd -m user
```

```
user:x:1001:1001::/home/user:/bin/sh
```

```
Session Actions Edit View Help
(kali㉿kali: ~
statd:x:112:65534::/var/lib/nfs:/usr/sbin/nologin
saned:x:113:114::/var/lib/saned:/usr/sbin/nologin
polkitd:x:987:987:User for polkitd:/usr/sbin/nologin
rtkit:x:114:115:RealtimeKit:/proc:/usr/sbin/nologin
colord:x:115:116:colord colour management daemon:/var/lib/colord:/usr/sbin/no
login
mysql:x:110:118:MariaDB Server:/nonexistent:/bin/false
stunnel4:x:986:986:stunnel service system account:/var/run/stunnel4:/usr/sbin/
/nologin
geoipclue:x:117:119::/var/lib/geoipclue:/usr/sbin/nologin
Debian-snmp:x:118:120::/var/lib/snmp:/bin/false
sshh:x:119:121::/nonexistent:/usr/sbin/nologin
cups-pk-helper:x:128:124:user for cups-pk-helper service:/nonexistent:/usr/sb
in/nologin
redsocks:x:121:125::/var/run/redsocks:/usr/sbin/nologin
_gopherish:x:127:127::/var/lib/gopherish:/usr/sbin/nologin
iodine:x:123:65534::/run/iodine:/usr/sbin/nologin
miredo:x:124:65534::/var/run/miredo:/usr/sbin/nologin
redis:x:125:128::/var/lib/redis:/usr/sbin/nologin
postgres:x:126:129:PostgreSQL administrator:/var/lib/postgresql:/bin/bash
mosquitto:x:127:130::/var/lib/mosquitto:/usr/sbin/nologin
inetutils:x:128:131::/var/lib/inetutils:/usr/sbin/nologin
guru:x:130:132::/var/run/ttcb/guru:/usr/sbin/nologin
kali:x:1000:1000::/home/kali:/usr/bin/zsh
user:x:1001:1001::/home/user:/bin/sh
```

```
(kali㉿kali)-[~/etc]
```

user:x:1001:1001::/home/user:/bin/sh

Significa:

- Nombre de usuario: user
- Contraseña: almacenada en /etc/shadow
- UID: 1001
- GID: 1001
- Comentario: vacío
- Directorio personal: /home/user
- Shell: /bin/sh

ukali:x:1000:1000::/home/kali:/usr/bin/zsh

**1. kali Nombre de usuario** Es el nombre con el que el usuario inicia sesión en el sistema.

**2. x Contraseña** *Antes contenía la contraseña cifrada, pero ahora solo aparece una "x" porque las contraseñas están guardadas en otro archivo más seguro: /etc/shadow.*

**3. 1000 UID (User ID)** Es el número identificador único del usuario. En la mayoría de sistemas, los usuarios normales comienzan desde el 1000.

**4. 1000 GID (Group ID)** Es el identificador del grupo principal al que pertenece el usuario. Los grupos se definen en /etc/group.

**5. (vacío) Campo de información o comentario (GECOS)** Se usa para información adicional como el nombre completo, teléfono, etc. Puede estar vacío.

**6. /home/kali Directorio home** Es la carpeta personal del usuario, donde guarda sus archivos y configuraciones.

**7. /usr/bin/zsh Intérprete de comandos (shell)** Es el programa que se ejecuta al iniciar sesión (por ejemplo /bin/bash, /bin/sh, /usr/bin/zsh).

```
inet$sim:::20340:::::  
_gvim:::20340.....  
kali:$y$j9T$ZjVER7AuUFBpA18/s0KpK1$zgO3ZvxVSDjjC.M6ltxfP22.SbNSM5SvZ9NW.M0rzS  
0:20340:0:99999:7:::  
user:::20384:0:99999:7:::  
  
[kali㉿kali)-[/etc]  
$
```

kali:\$y\$j9T\$jeVER7AAUFbPa18/s0KpK1\$zgO3ZvxVSDjjC.M6ltxfP22.SbNSM5SvZ9NW.M0rzS0:20340:0:9999  
9:7:::

Campo	Valor	Significado
1	kali	Nombre del usuario
2	\$y\$j9T\$jeVER7AAUFbPa 18/s0KpK1\$zgO3ZvxVS DjjC.M6ltxfP22.SbNSM 5SvZ9NW.M0rzS0	Contraseña cifrada usando el algoritmo yescrypt.
3	20340	Fecha del último cambio de contraseña (en días desde 1/1/1970).
4	0	No hay tiempo mínimo antes de volver a cambiar la contraseña.
5	99999	La contraseña expira después de 99 999 días.
6	7	El sistema avisa 7 días antes de que la contraseña caduque.
7, 8, 9	vacíos	No hay inactividad ni fecha de expiración establecida.

user:::20384:0:99999:7:::

Campo	Valor	Significado
1	user	Usuario del sistema
2	(vacío)	No tiene contraseña configurada → puede significar que la cuenta está deshabilitada o sin protección.
3	20384	Último cambio de contraseña.
4	0	Sin restricción mínima para cambio de contraseña.
5	99999	No caduca prácticamente nunca.
6	7	Aviso 7 días antes de expirar.
7-9	vacíos	Sin límites de inactividad ni expiración de cuenta.

```
kali:$y$j9T$ZjVER7AuUFBpA18/s0KpK1$zg03ZVxVSDjjC.M6ltxfP22.SbNSM5SvZ9NW.M0rzS0:20340:0:9999  
9:7 :::  
user:$y$j9T$ke2yPnk9posaCRT71q9d81$j2vquz936UYUeF1hxR1GXcAzWhprrrPVecD09uA7f2h2:20384:0:9999  
9:7 :::
```

Se ha actualizado la contraseña.

¿Dónde se guardan los hashes en un equipo Windows?

Máquinas clientes

C:\Windows\System32\config\SAM

(es el fichero del SAM hive del registro).

¿En qué formato están los hashes?

- Hash NT (NTLM hash)
  - Técnica: MD4 aplicado a la contraseña codificada en UTF-16LE. Resultado: 16 bytes (habitualmente mostrado en hexadecimal, 32 caracteres).

# Parte 4: Crækkeando contraseñas con John The Ripper

```
(kali㉿kali)-[~]
$ sudo passwd testuser1
New password:
Retype new password:
passwd: password updated successfully

(kali㉿kali)-[~]
$ sudo useradd testuser2

(kali㉿kali)-[~]
$ sudo passwd testuser2
New password:
Retype new password:
passwd: password updated successfully

(kali㉿kali)-[~]
$ sudo useradd testuser3

(kali㉿kali)-[~]
$ sudo passwd testuser3
New password:
Retype new password:
Sorry, passwords do not match.
passwd: Authentication token manipulation error
passwd: password unchanged

(kali㉿kali)-[~]
$ sudo passwd testuser3
New password:
Retype new password:
passwd: password updated successfully

(kali㉿kali)-[~]
$
```

```
Session Actions Edit View Help
sudo: the -s option may be used to run a privileged shell.
sudo: the -D option may be used to run a command in a specific directory.

(kali㉿kali)-[~/Documents/practica-passwords]
$ ls
practica-passwords

(kali㉿kali)-[~/Documents/practica-passwords]
$ cd practica-passwords

(kali㉿kali)-[~/Documents/practica-passwords]
$ unshadow passwd-test shadow-test > passwords.txt
Fopen: shadow-test: Permission denied

(kali㉿kali)-[~/Documents/practica-passwords]
$ sudo unshadow passwd-test shadow-test > passwords.txt

(kali㉿kali)-[~/Documents/practica-passwords]
$ cat passwords.txt
1000:1002::/home/testuser1:/bin/sh
1001:1003::/home/testuser2:/bin/sh
1004:1004::/home/testuser3:/bin/sh
1005:1005::/home/testuser4:/bin/sh
1006:1006::/home/testuser5:/bin/sh
1007:1007::/home/testuser6:/bin/sh

(kali㉿kali)-[~/Documents/practica-passwords]
```

```
(kali㉿kali)-[~/Documents/practica-passwords]
$ sudo john --format=crypt --wordlist=/usr/share/wordLists/rockyou.txt password.txt
Using default input encoding: UTF-8
Loaded 5 password hashes with 5 different salts (crypt, generic_crypt(3) [?/84])
Cost 1 (algorithm [1:descrypt 2:md5crypt 3:sunmd5 4:bcrypt 5:sha256crypt 6:sha512crypt]) is 0 for all loaded hashes
Cost 2 (algorithm specific iterations) is 1 for all loaded hashes
Will run 5 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
password      (testuser1)
qwertv123     (testuser2)
1g 0:00:01:48 0.03% (ETA: 2025-10-27 22:45) 0.81849g/s 54.82p/s 185.8C/s 185.8C/s
tractor..prettyinpink
2g 0:00:02:02 0.04% (ETA: 2025-10-27 23:54) 0.82628g/s 53.15p/s 179.8C/s 179.8C/s
oblivion..alejo
Use the "--show" option to display all of the cracked passwords reliably
Session aborted

(kali㉿kali)-[~/Documents/practica-passwords]
```

Se crackearon las contraseñas simples y predecibles, las contraseñas largas y con caracteres especiales cuestan más de descifrar.

```
(kali㉿kali)-[~/Documents/practica-passwords]
$ sudo john --wordlist=/usr/share/john/password.lst --rules passwords.txt
Using default input encoding: UTF-8
Loaded 1 password hash (HMAC-SHA256 [password is key, SHA256 256/256 AVX2 8x])
No password hashes left to crack (see FAQ)

(kali㉿kali)-[~/Documents/practica-passwords]
$ sudo john --show passwords.txt
testuser1:password:1002:1002::/home/testuser1:/bin/sh

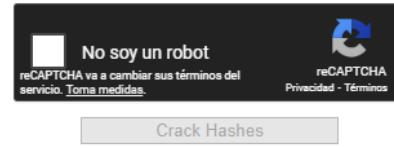
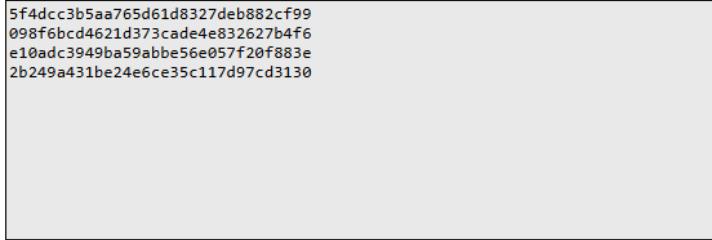
1 password hash cracked, 1 left

(kali㉿kali)-[~/Documents/practica-passwords]
```

En mi caso no sacó ninguna adicional.

# Parte 5: Explorando Rainbow Tables

Se encontraron todas las contraseñas y fue instantáneo.



**Supports:** LM, NTLM, md2, md4, md5, md5(md5\_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sh1\_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
5f4dcc3b5aa765d61d8327deb882cf99	md5	password
098f6bcd4621d373cade4e832627b4f6	md5	test
e10adc3949ba59abbe56e057f20f883e	md5	123456
2b249a431be24e6ce35c117d97cd3130	md5	calasanz

```
(halil@halil)-[~] $ echo -n "admin" | md5sum  
21332f297a57a5a7e3894a0e4a801fc3 -  
(halil@halil)-[~] $ echo -n "123456" | md5sum  
7c48005fac17b3f82daf3015b9aae86db5adc8275ebfbf05ec03885a4a8ba3e -  
(halil@halil)-[~] $ echo -n "David10" | md5sum  
07046d5fac12b3f82daf3015b9aae86db5adc8275ebfbf05ec03885a4a8ba3e -  
(halil@halil)-[~] $ echo -n "davidXP10" | md5sum  
8e0ed9b865874cff99d31a179c0fe31574466083227cc6f684d173a9d52eb -  
(halil@halil)-[~] $
```

Supports: LM, NTLM, md2, md4, md5(md5\_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sh1\_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
21332f297a57a5a7e3894a0e4a801fc3	md5	password
7c48005fac17b3f82daf3015b9aae86db5adc8275ebfbf05ec03885a4a8ba3e	md5	123456
07046d5fac12b3f82daf3015b9aae86db5adc8275ebfbf05ec03885a4a8ba3e	md5	David.
8e0ed9b865874cff99d31a179c0fe31574466083227cc6f684d173a9d52eb	md5	David - David_

Solo se encontraron las contraseñas comunes. Solo encuentra este tipo de contraseñas ya que son las más usadas.

El uso de sal invalida completamente las tablas. Requieren mucho almacenamiento. Ineficientes con bcrypt, scrypt, etc. Solo sirven para contraseñas dentro de un rango precomputado.

# Parte 6: Política de contraseñas

## Alcance

Esta política aplica a:

- Todos los empleados y colaboradores que tengan acceso a los sistemas internos o externos de la empresa (correo corporativo, panel de administración, servidores, repositorios, etc.).
- Todas las cuentas de usuario creadas en servicios críticos (intranet, bases de datos, hosting, etc.).

## Longitud y complejidad

- Longitud mínima: 12 caracteres.
- Longitud recomendada: 14 o más caracteres.
- Debe contener al menos 3 de los siguientes 4 tipos de caracteres:
  - Mayúsculas (A–Z)
  - Minúsculas (a–z)
  - Números (0–9)
  - Símbolos (! @ # \$ % ^ & \* \_ - + = ? etc.)
- No debe incluir:
  - El nombre del usuario, la empresa ni palabras comunes (ej. “password”, “empresa123”).
  - Contraseñas previamente usadas (mínimo recordar las últimas 5).

## Expiración

- Expiración cada 180 días (6 meses) como medida general.
- No forzar cambio frecuente si no hay indicios de compromiso
- El cambio obligatorio solo se requerirá:
  - Tras una brecha o sospecha de seguridad.
  - Al incorporarse o salir un empleado.

## Cambio y recuperación

- El cambio de contraseña debe realizarse desde un canal autenticado.
- En caso de olvido, el restablecimiento debe enviarse al **correo corporativo** del empleado y requerir un segundo factor.
- Se prohíbe compartir contraseñas entre compañeros.

## Supervisión y concienciación

- Se realizará una revisión anual de esta política.
- Se ofrecerá formación básica sobre creación de contraseñas seguras y detección de phishing.
- Se fomentará el uso de frases largas y únicas en lugar de contraseñas cortas con símbolos aleatorios.

## Gestión y almacenamiento

- Las contraseñas no deben almacenarse en texto plano en ningún sistema o documento.
- Los servidores deben guardar las contraseñas hasheadas con algoritmos robustos como bcrypt, scrypt o Argon2.
- Los empleados deben usar un gestor de contraseñas corporativo (como Bitwarden, 1Password o KeePassXC).
- Se recomienda autenticación multifactor (MFA) para acceder a:
  - Paneles administrativos.
  - Servicios en la nube (GitHub, correo, hosting).
  - VPN o servidores SSH.