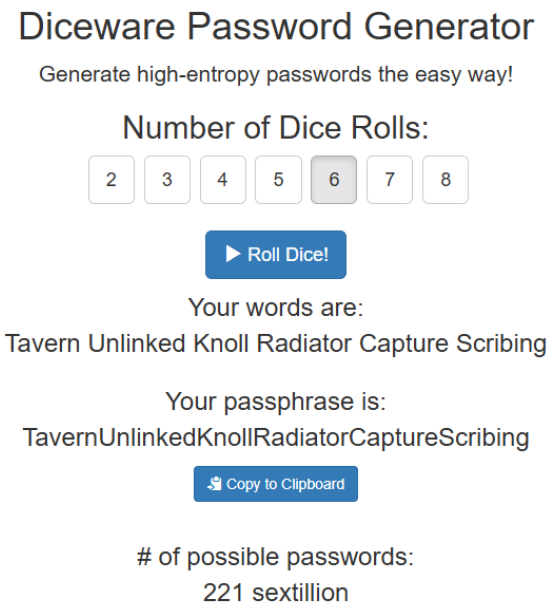
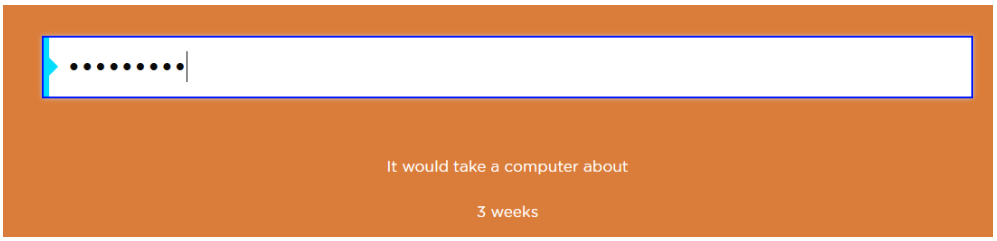
Practicas contraseña

1.- Frases de paso

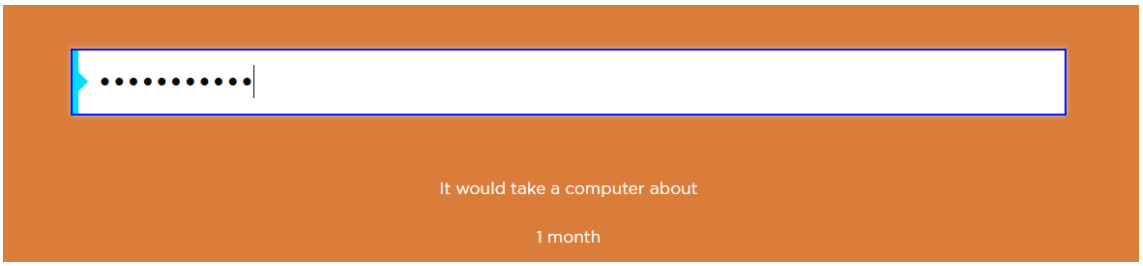


2.- Comparar fortaleza de contraseñas

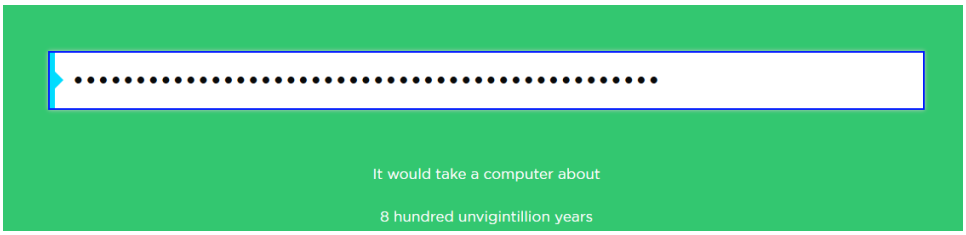
password123 ->



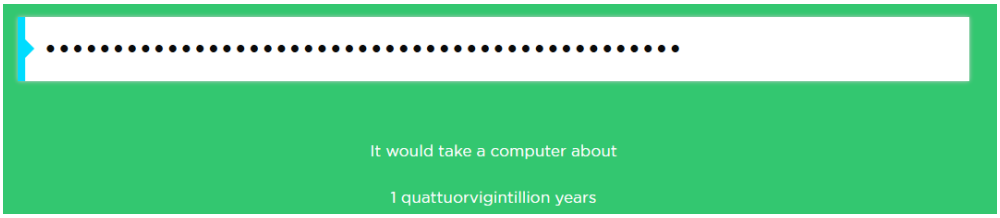
P@ssw0rd! ->



Tavern Unlinked Knoll Radiator Capture Scribing ->



T4vern-UnlinK3d_Kn0lL/r4dIat0r-Ca9tUre*5CribInG ->



¿Qué diferencias notas entre una contraseña corta y compleja vs. una frase de paso larga?

-La diferencia clara fue en la complejidad y en la longitud de la contraseña, porque proporciona más dificultad a la hora de romperlo.

¿Cuál es más fácil de recordar para ti?

-Claramente la corta

3.- Almacenamiento de contraseñas en Linux y Windows

¿Aparece el usuario que acabamos de crear?

-Si

```
usbmux:x:108:46:usbmux daemon:/var/lib/usbmux:/usr/sbin/nologin
nm-openconnect:x:109:110:NetworkManager OpenConnect plugin:/var/lib/Net
workManager:/usr/sbin/nologin
pulse:x:110:111:PulseAudio daemon:/run/pulse:/usr/sbin/nologin
pipewire:x:988:988:system user for pipewire:/nonexistent:/usr/sbin/nolo
gin
lightdm:x:111:113:Light Display Manager:/var/lib/lightdm:/bin/false
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/s
bin/nologin
mysql:x:116:118:MariaDB Server:/nonexistent:/bin/false
stunnel4:x:986:986:stunnel service system account:/var/run/stunnel4:/us
r/sbin/nologin
geoclue:x:117:119::/var/lib/geoclue:/usr/sbin/nologin
Debian-snmp:x:118:120::/var/lib/snmp:/bin/false
sslh:x:119:121::/nonexistent:/usr/sbin/nologin
cups-pk-helper:x:120:124:user for cups-pk-helper service:/nonexistent:/
usr/sbin/nologin
redsocks:x:121:125::/var/run/redsocks:/usr/sbin/nologin
_gophish:x:122:127::/var/lib/gophish:/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/ba
sh
mosquitto:x:127:130::/var/lib/mosquitto:/usr/sbin/nologin
inetsim:x:128:131::/var/lib/inetsim:/usr/sbin/nologin
_gvm:x:129:133::/var/lib/openvas:/usr/sbin/nologin
kali:x:1000:1000::/home/kali:/usr/bin/zsh
NewUser:x:1001:1001::/home/NewUser:/bin/sh
prueba01:x:1002:1002::/home/prueba01:/bin/sh
```

Significado de los campos:

- Usuario -> prueba01
- X -> Contraseña almacenada en /etc/shadow
- Identificador de usuario dentro del sistema->1002
- Grupo ID(GID) -> 1002
- Comentario(Puede contener el nombre del usuario u otra información)-> :-:
- Directorio -> /home
- Shell Programa que se ejecuta al iniciar sesión ->/bin/sh

¿Por qué el segundo campo solo tiene una “x”?

- Se almacenaba el hash de la contraseña. Puede ser una **x** o a veces ***** o **¡**

```
┌──(kali㉿kali)-[~]
└─$ sudo passwd prueba01
New password:
Retype new password:
passwd: password updated successfully
```

sudo cat /etc/shadow:

```
┌──(felix♦ kali)-[~]
└─$ sudo cat /etc/shadow
root:!:20390:0:99999:7:::
daemon:*:20390:0:99999:7:::
bin:*:20390:0:99999:7:::
sys:*:20390:0:99999:7:::
sync:*:20390:0:99999:7:::
games:*:20390:0:99999:7:::
man:*:20390:0:99999:7:::
lp:*:20390:0:99999:7:::
mail:*:20390:0:99999:7:::
news:*:20390:0:99999:7:::
uucp:*:20390:0:99999:7:::
proxy:*:20390:0:99999:7:::
www-data:*:20390:0:99999:7:::
backup:*:20390:0:99999:7:::
list:*:20390:0:99999:7:::
irc:*:20390:0:99999:7:::
_apt:*:20390:0:99999:7:::
nobody:*:20390:0:99999:7:::
systemd-network:!*:20390:::::1:
dhcpcd:!:20390::::::
systemd-timesync:!*:20390:::::1:
messagebus:!*:20390::::::
tcpdump:!:20390::::::
_rpc:!:20390::::::
sshd:!*:20390::::::
statd:!:20390::::::
felix:$y$j9T$/5BMxisLMej.R72Wz7Mr20$KMiiR6aDc8Nzg3gLniM5xCRQhVif7TM9GNuJW94DcS7:20390:0:99999:7:::
Fenix:!:20390:0:99999:7:::

┌──(felix♦ kali)-[~]
└─$
```

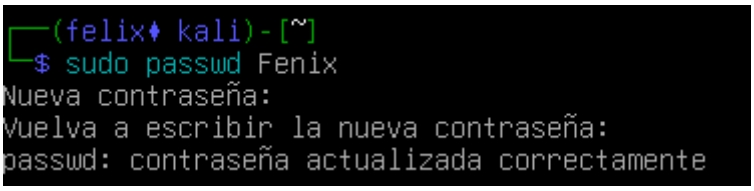
¿Aparece el usuario que acabamos de crear?

El formato es el siguiente:

usuario:contraseña:lastchg:min:max:warn:inactive:expire:reserved

Significado del formato:

Nº	Campo	Ejemplo	Significado
1	**Usuario**	Felix	Nombre del usuario, debe coincidir con el de /etc/passwd.
2	**Contraseña (hasheada)**	yj9T$... o ! o *	Contiene el **hash de la contraseña** • ! o * → cuenta bloqueada o sin contraseña. • idsalt$hash → hash con identificador del algoritmo (6=SHA-512, y=yescrypt, etc.).
3	**Último cambio de contraseña (lastchg)**	20390	Número de días desde el **1 de enero de 1970** en que se cambió por última vez la contraseña.
4	**Mínimo (min)**	0	Número mínimo de días que deben pasar antes de poder cambiar la contraseña de nuevo.
5	**Máximo (max)**	99999	Número máximo de días antes de que la contraseña caduque (99999 ≈ nunca expira).
6	**Aviso (warn)**	7	Días antes de que expire la contraseña para empezar a avisar al usuario.
7	**Inactivo (inactive)**	(vacío o 7)	Días después de expirar la contraseña en los que la cuenta aún puede ser usada. Luego queda bloqueada.
8	**Expira (expire)**	(vacío)	Día (en formato días desde 1970) en el que **expira la cuenta** completa, no solo la contraseña.
9	**Reservado**	(vacío)	Campo reservado para uso futuro; generalmente está vacío.



Se ha actualizado la contraseña

¿Se ha actualizado el fichero /etc/shadow con la contraseña?

Localizar en qué fichero(s) y con qué formato se almacenan los resúmenes de las contraseñas en sistemas Windows.

Se guarda en la base de datos del administrador de cuentas de seguridad (SAM)

C:\Windows\System32\config\SAM

Formato: NTHash

Contraseñas crakeables:

Diccionario simple:

```
└─# john --show passwords.txt
felix:123:1000:1000:Felix,,,:/home/felix:/usr/bin/zsh
testuser1:password:1002:1002::/home/testuser1:/bin/sh
testuser2:qwerty123:1003:1003::/home/testuser2:/bin/sh
testuser3:P@ssw0rd:1004:1004::/home/testuser3:/bin/sh
```

Diccionario ampliado:

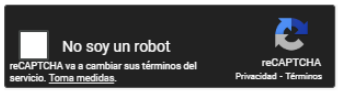
```
┌──(root㉿kali)-[/practica-passwords]
└─# john --format=crypt --wordlist=/usr/share/wordlists/rockyou.txt passwords.txt
Using default input encoding: UTF-8
Loaded 8 password hashes with 8 different salts (crypt, generic crypt(3) [?/64])
Remaining 5 password hashes with 5 different salts
Cost 1 (algorithm [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 6 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
qwerty123        (testuser2)
P@ssw0rd         (testuser3)
2g 0:05:12:27 10.82% (ETA: 2025-11-01 01:16) 0.000106g/s 91.82p/s 276.0c/s 276.0C/s ilikethegirls..ilikel
Use the "--show" option to display all of the cracked passwords reliably
Session aborted
```

Probando con reglas:

```
┌──(root㉿kali)-[/practica-passwords]
└─# 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 128/128 SSE2 4x])
No password hashes left to crack (see FAQ)
```

Rainbow Tables

```
5f4dcc3b5aa765d61d8327deb882cf99
098f6bcd4621d373cade4e832627b4f6
e10adc3949ba59abbe56e057f20f883e
2b249a431be24e6ce35c117d97cd3130
```



Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

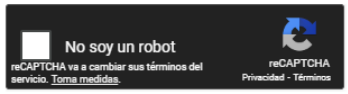
Hash	Type	Result
5f4dcc3b5aa765d61d8327deb882cf99	md5	password
098f6bcd4621d373cade4e832627b4f6	md5	test
e10adc3949ba59abbe56e057f20f883e	md5	123456
2b249a431be24e6ce35c117d97cd3130	md5	calasanz

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

Encontró todas las contraseñas y si, fue instantáneo

Creados:

```
542af68d152e398e5cbd0014fbd24ce7
15a9dbc58429fe5ab25decff36ba84ff0cd131f1
```



Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
542af68d152e398e5cbd0014fbd24ce7	Unknown	Not found.
15a9dbc58429fe5ab25decff36ba84ff0cd131f1	Unknown	Not found.

¿Pudo CrackStation encontrar tus contraseñas personalizadas?

Pudo

¿Por qué las contraseñas comunes se encuentran inmediatamente?

Por que al ser comunes ya lo tienen previsto

¿Qué limitación tienen las rainbow tables?

Las contraseñas con modificaciones y no muy comunes habitualmente

Política de contraseñas:

Deben de contener al menos mayúsculas, minúsculas, números, símbolos especiales.

Tener un sistema de recordar y prohibir la reutilización de las últimas de 5 contraseñas.

Bloquear temporalmente la cuenta después de 5 intentos fallidos y se bloquear por 15min.

Antes de una contraseña con más de 10 letras, con algunas variaciones, con símbolos, mayúsculas, minúsculas, etc. Lo más correcto seria una contraseña temporal que se vaya generando cada cierto tiempo o que se necesite de un dispositivo externo.