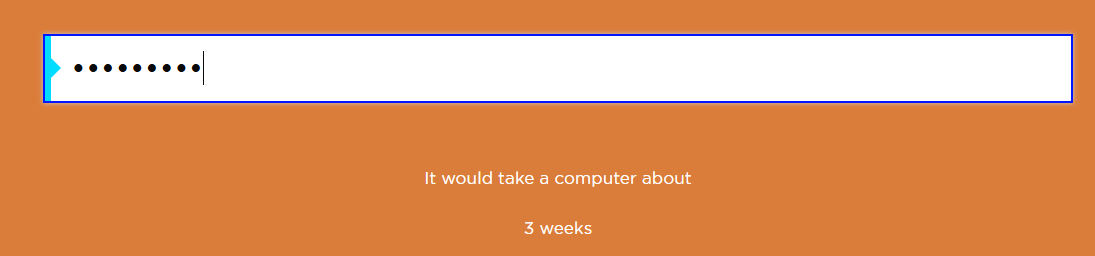
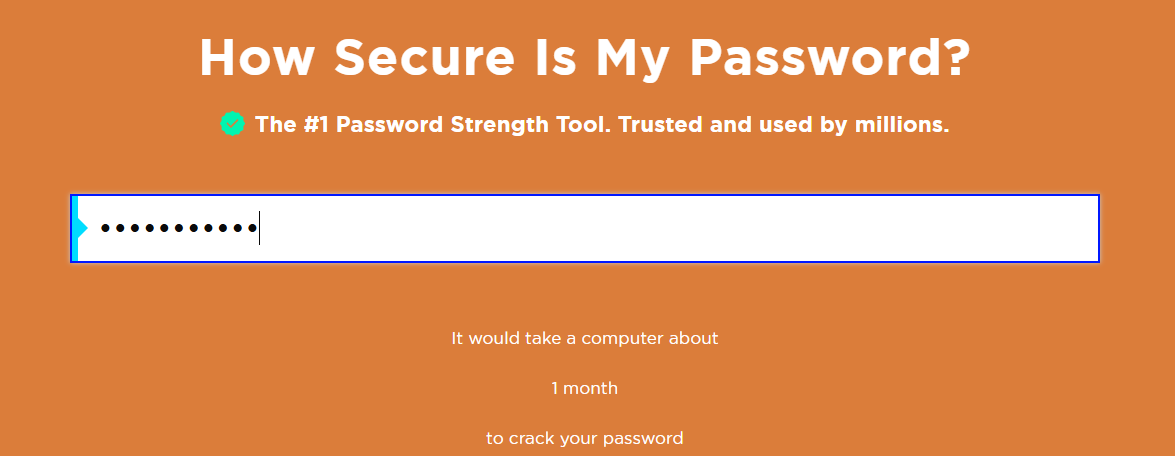
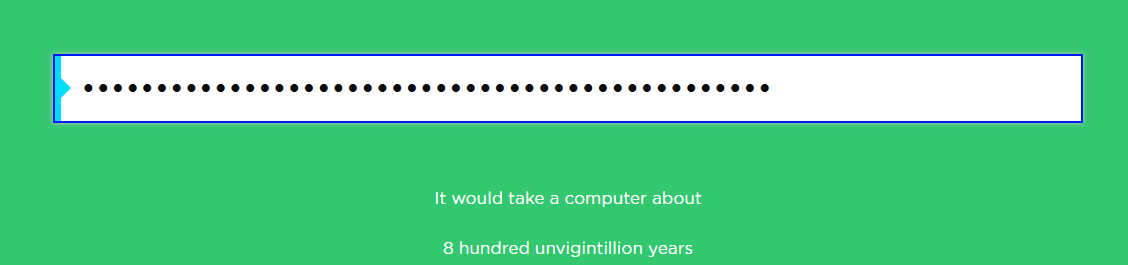
# Practicas contraseña

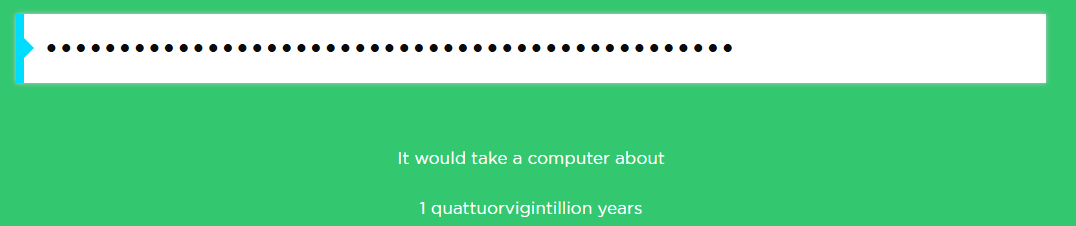
**1.- Frases de paso**

**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?**

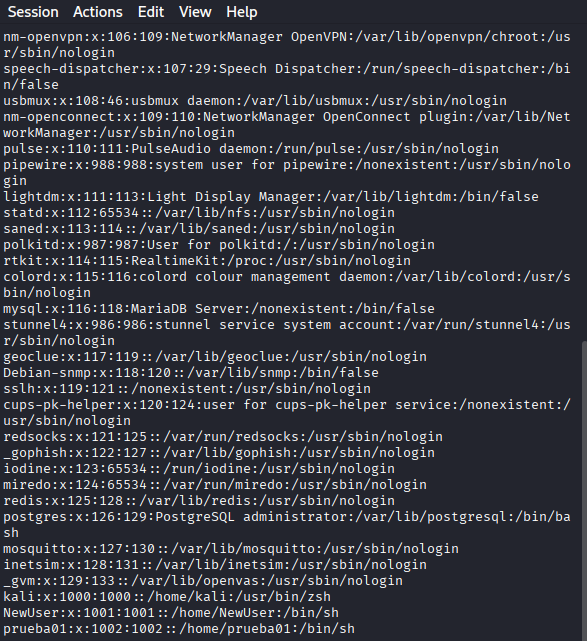
-La diferencia clara fue en la complejidad y en la longitud de la contraseña, porque proporciona más dificultad a la hora de romperlo.

**¿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?**

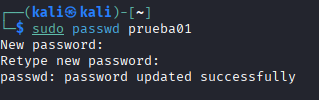
-Si

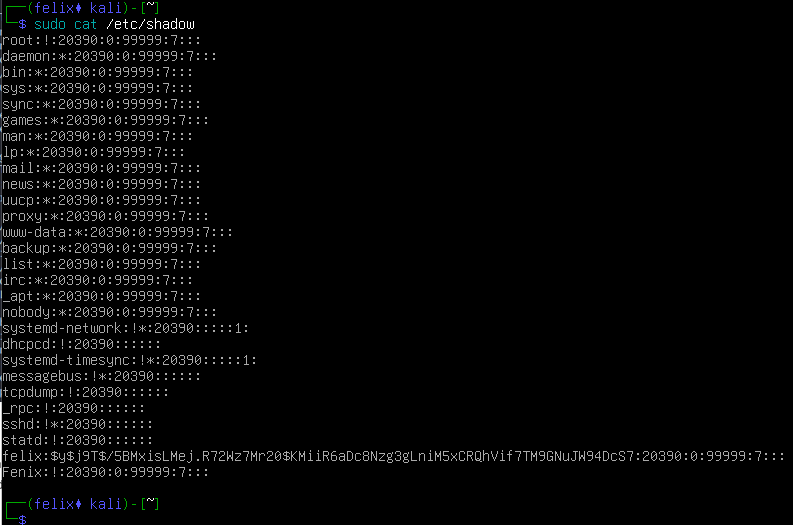
**Significado de los campos:**

* 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 **¡**



sudo cat /etc/shadow:

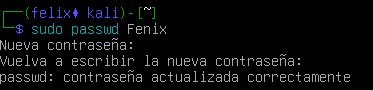
**¿Aparece el usuario que acabamos de crear?**

El formato es el siguiente:

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

|  |  |  |  |
| --- | --- | --- | --- |
| Nº | Campo | Ejemplo | Significado |
| 1 | **Usuario** | Felix | Nombre del usuario, debe coincidir con el de /etc/passwd. |
| 2 | **Contraseña (hasheada)** | $y$j9T$... o ! o \* | Contiene el **hash de la contraseña**  • ! o \* → cuenta bloqueada o sin contraseña.  • $id$salt$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. |

**Significado del formato:**

****

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.**

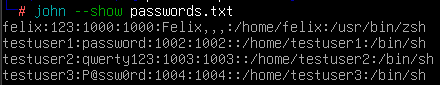
Se guarda en la base de datos del administrador de cuentas de seguridad (SAM)

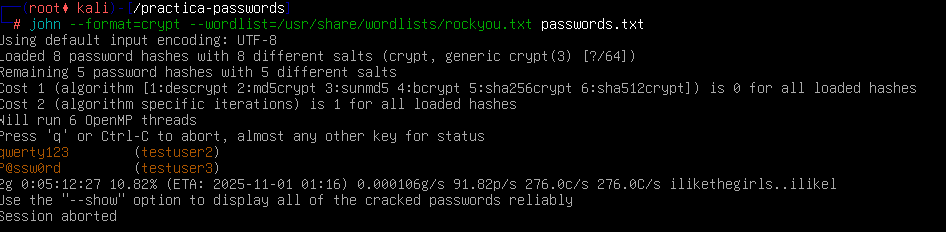
C:\Windows\System32\config\SAM

Formato: NTHash

Contraseñas crakeables:

Diccionario simple:

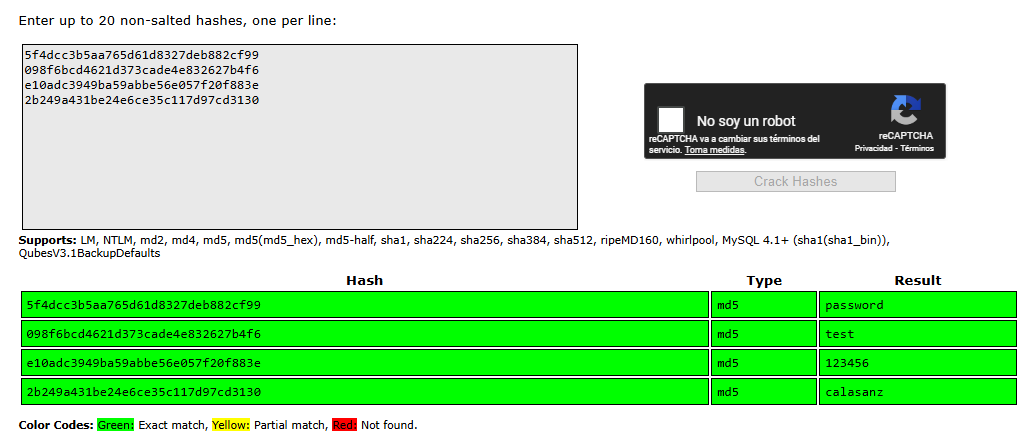


Diccionario ampliado:

Probando con reglas:



**Rainbow Tables**

****

Encontró todas las contraseñas y si, fue instantáneo

Creados:

