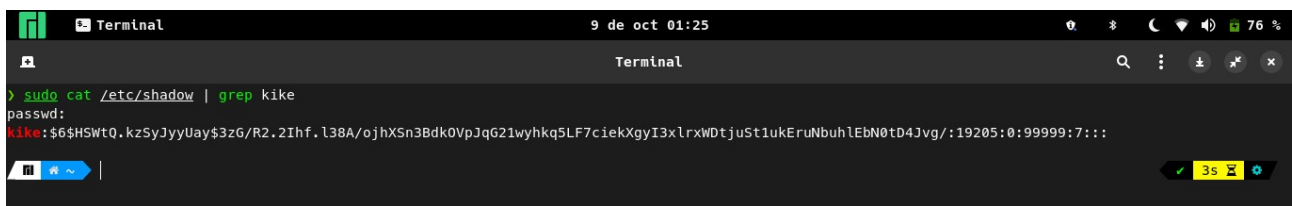


- **NOMBRE:** Enrique Martínez Añón
- **FECHA INICIO:** 9 de octubre 2023
- **FECHA FINAL:** 9 de octubre 2023
- **UNIDAD:** Seguridad Informática
- **CASO PRÁCTICO:** R3T0 - R3PT3 23
- **ENUNCIADO:** Conocer los hash passwords en Ubuntu
- **VERSIÓN ACTIVIDAD:** A
- **DIFICULTAD:** BAJO
- **TIEMPO ESTIMADO:** 1 hora
- **TIEMPO REAL:** 40 minutos
- **CONCLUSIÓN:** Hay muchos tipos de hash y es bastante difícil descriptarlos.

INDICE

En este caso voy a hacer el mismo caso que en Ubuntu pero con mi portátil que usa una versión basada en ARCH LINUX.

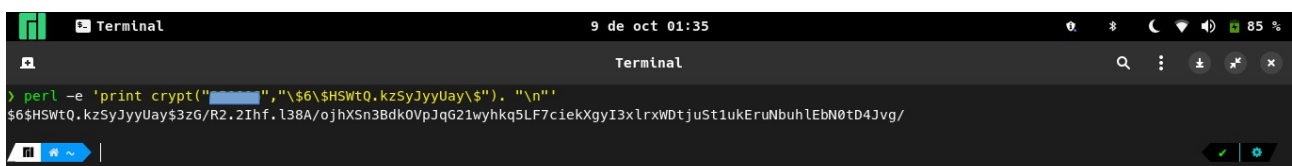
Lo primero que hago es un cat al fichero /etc/shadow para saber mi hash de usuario.



```

Terminal
9 de oct 01:25
Terminal
> sudo cat /etc/shadow | grep kike
passwd:
kike:$6$HSwtQ,kzSyJyyUay$3zG/R2.2Ihf.l38A/ojhXSn3Bdk0VpJqG21wyhkq5LF7ciekXgyI3xlrXWdtjuSt1uEruNbuhlEbN0tD4Jvg/:19205:0:99999:7:::
  
```

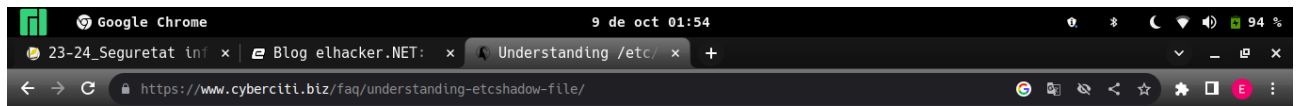
Una vez obtenido el hash podemos ver que usa también el sha512sum (\$6\$) como en el de Ubuntu. Con eso voy a aplicarle el código que puso en perl para ver que esta todo correcto igual que en el video.



```

Terminal
9 de oct 01:35
Terminal
> perl -e 'print crypt(" ", "\$6$HSwtQ,kzSyJyyUay\$"). "\n"'
$6$HSwtQ,kzSyJyyUay$3zG/R2.2Ihf.l38A/ojhXSn3Bdk0VpJqG21wyhkq5LF7ciekXgyI3xlrXWdtjuSt1uEruNbuhlEbN0tD4Jvg/
  
```

Con esta línea de código escrita en perl hemos podido sacar el hash con nuestra contraseña y el salt del usuario.



```
sai : $6 $YTJ7JKnfsB4esnb$ $5XvmYk2.GXVWhDo2TYGN2hCitD/wU9Kov.uZD
```

- **sai** – ID de usuario
- **\$6** : el prefijo del algoritmo hash utilizado para esta contraseña. En este caso se trata de un hash SHA-512 (512 bits). Fue desarrollado originalmente por Ulrich Drepper para GNU libc. Compatible con Linux pero no común en otros lugares. Aceptable para nuevos hashes. El parámetro predeterminado de costo de tiempo de CPU es 5000, que es demasiado bajo para el hardware moderno.
- **\$YTJ7JKnfsB4esnb\$** – El salt utilizado para cifrar la contraseña y se elige al azar (6 a 96 bits).
- **\$5XvmYk2.GXVWhDo2TYGN2hCitD/wU9Kov.uZD8xsnleuf1r0ARX3qodlKiDsdQA444b8IMPMOnUWDmVJVkeg1** : el hash cifrado de la contraseña del usuario se denomina 'sai'. Luego, el salt y la contraseña no cifrada se combinan y cifran para generar el hash cifrado de la contraseña. ¿Por qué usar sal? Evita que dos usuarios con la misma contraseña tengan entradas duplicadas en el archivo /etc/shadow. Digamos que si los usuarios llamados 'sai' y 'ram' usan 'abracadabra' como contraseña, sus contraseñas cifradas en /etc/shadow serán diferentes si sus sales son diferentes.

BIBLIOGRAFIA

[Video explicativo del funcionamiento del hash de Ubuntu.](#)

[Pdf explicativo del hash password de Ubuntu.](#)