Activitat 09

Tipo de contraseña rota	Promedio de contraseñas por segundo	Contraseña encontrada	Tiempo total del intento	Mensaje dentro del archivo cifrado
Archive 7z (10-secret.7z)	82.76 p/s	secret	1 seconde	Punt 1 complert
Archive 7z (10-dificil.7z)	84.96 p/s	dificil01	36 secondes	Pas 2 aconseguit
Archive LibreOffice (.odt)	442.3p/S	difícil01	11 secondes	Aquesta és més difícil
10-vbox.txt.	306650p/s	changeme	8 secondes	

1. Com has fet per obtenir els hash dels *.7z?

   Utilicé el script `7z2john.pl` incluido en John the Ripper, que extrae el hash del archivo 7z para luego atacarlo con fuerza bruta.

2. Com has fet per obtenir els hash dels *.odt?

   Utilicé el script `libreoffice2john.py`, que extrae los hashes de documentos LibreOffice (.odt) para ser analizados con John the Ripper.

3. **Com creus que es fa per obtenir els hash de un ordinador amb Windows?**

   En un ordenador con Windows, los hashes de las contraseñas se sacan normalmente de unos archivos especiales del sistema, como el archivo SAM (Security Account Manager) y a veces también el archivo SYSTEM. Estos archivos están protegidos y no se pueden abrir directamente cuando el sistema está funcionando.

   Para conseguir esos hashes, se usan herramientas específicas como **samdump2**, que extrae los hashes del archivo SAM, o programas más avanzados como **creddump** o **mimikatz**, que pueden obtener los hashes o incluso las contraseñas en texto claro si se tienen los permisos necesarios.

   Estas herramientas acceden a esos archivos protegidos o usan métodos para sacar la información de la memoria. Después, con esos hashes, se puede usar un programa como John the Ripper para intentar descubrir las contraseñas

4. **Creus que eines com JTRipper són útils només per a pirates i hackers o també per als administradors de sistemes?. Per què?**

   Estas herramientas son también muy útiles para administradores de sistemas, ya que les permiten comprobar la seguridad de las contraseñas en su red y detectar contraseñas débiles para mejorar la seguridad. No son solo para hackers, sino también para defensa.

Conclusiones

- Las contraseñas elegidas en estos ejercicios son cortas y sencillas porque así es más fácil para John the Ripper encontrarlas rápidamente, lo que facilita el aprendizaje y la demostración de las técnicas de cracking. Contraseñas más largas, de 10 caracteres o más, serían mucho más difíciles de romper y tomarían mucho más tiempo, lo cual no es práctico para una práctica introductoria.

- El cifrado más seguro que hemos probado es el del archivo de Windows (10-vbox.txt), porque se pudo atacar rápidamente debido a que John the Ripper mostró una velocidad muy alta de intentos por segundo, pero aún así, la contraseña "changeme" es muy común y sencilla, lo que indica que el cifrado usado es fuerte pero la contraseña débil facilita el acceso.

- El método de cifrado más débil fue el del archivo 7z (10-secret.7z), porque la velocidad de ataque fue muy baja (82 contraseñas por segundo) y se rompió casi instantáneamente, lo que indica que su cifrado o la configuración de la contraseña es más vulnerable frente a ataques rápidos.