Pauta Laboratorio 1

Seguridad en TI – 2023/2

Se entregaba un archivo PDF cifrado con contraseña. Para abrirlo, se indicaba que debía utilizarse la herramienta “John The Ripper”, incluida en Kali Linux, utilizando fuerza bruta.

Así, se debía transformar el archivo PDF a un Hash que permitiera ser utilizado con John. Para esto, se debía descargar el PDF, y mediante una Terminal, ingresar el siguiente comando, sin comillas:

```
$pdf2john “ruta a PDF” > “ruta a HASH”
```

Esto creaba un archivo .hash en la ruta seleccionada, el cual se podía utilizar con John utilizando el siguiente comando, sin comillas:

```
$john “ruta a HASH”
```

Luego de un momento, la herramienta entregaba el número con el que se desbloqueaba el archivo PDF, correspondiendo a “185020”.

El archivo contenía pistas para lograr descifrar el mensaje que se buscaba en la Parte 2, siendo éste “87652b6fc0d718f54cc82637453cab2”. Se mencionaba que el cifrado utilizado era AES-128, el cual se puede descifrar utilizando CyberChef.

AES utiliza una llave (“key”) y el campo “IV” para cifrar y descifrar. En el caso de AES-128, cada campo tiene una longitud de 16 bytes (32 caracteres). Utilizando las pistas del PDF, se puede notar que la llave son 32 letras “F” y el campo IV son 32 letras “A”. Así, se descifra el mensaje final, teniendo “LAB1 – logrado”.