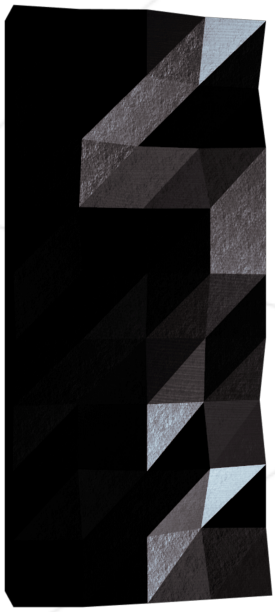

Bootcamp Ciberseguridad | 42

ft_otp

Resumen: Nada es para siempre, decían tus ojos tristes.

Versión: 1

Índice general

Capítulo I

Introducción

Las contraseñas son uno de los mayores `quebraderos de cabeza` de la seguridad informática. Los usuarios las olvidan, las comparten, las reutilizan y las escogen con un pésimo criterio. Además, las contraseñas tarde o temprano son filtradas en brechas de seguridad. Una forma de evitar esto es usar contraseñas de un solo uso, basadas en marcas de tiempo, que caducan tras unos minutos y luego dejan de ser válidas. Tanto si ya utilizas este sistema, como si nunca habías oído hablar de él, es bastante probable que alguna de tus contraseñas haya sido comprometida en algún momento de tu vida.

En este proyecto, el objetivo es `implementar un sistema de TOTP` (Time-based One-Time Password), que sea capaz de generar contraseñas efímeras a partir de una clave maestra.
Estará basado en el `RFC`: https://datatracker.ietf.org/doc/html/rfc6238, por lo que podrías utilizarlo en tu día a día.

Capítulo II

Prólogo

¿La contraseña?

Capítulo III

Parte Obligatoria

En el lenguaje de tu elección, debes implementar un programa que permita registrar una clave inicial, y sea capaz de generar una nueva contraseña cada vez que se solicite. Puedes utilizar cualquier librería que facilite la implementación del algoritmo, siempre que no hagan el trabajo sucio, es decir, queda terminantemente prohibido hacer uso de cualquier librería TOTP. Por supuesto, puedes y debes hacer uso de alguna librería o función que te permita acceder al tiempo del sistema.

Un ejemplo del uso del programa sería:

- El programa deberá llamarse `ft_otp`.
- Con la opción `-g` , el programa recibirá como argumento una clave hexadecimal de al menos 64 caracteres. El programa guardará a buen recaudo esta clave en un archivo llamado `ft_otp.key`, que estará cifrado en todo momento.
- Con la opción `-k`, el programa generará una nueva contraseña temporal y la mostrará en la salida estándar.

```
$ echo -n "NEVER GONNA  GIVE  YOU  UP" > key.txt
$ ./ft_otp -g key.txt
./ft_otp: error: key must be 64 hexadecimal characters.
$ xxd -p key.txt > key.hex
$ cat key.hex | wc -c
64
$ ./ft_otp -g key.hex
Key was successfully saved in ft_otp.key.
$ ./ft_otp -k ft_otp.key
836492
$ sleep 60
$ ./ft_otp -k ft_otp.key
123518
```

Puedes comprobar si tu programa funciona correctamente comparando las contraseñas generadas con `Oathtool` o cualquier herramienta de tu elección.

```
oathtool -totp $(cat key.hex)
```

Capítulo IV

Parte Bonus

La evaluación de los bonus se hará `SI Y SOLO SI` la parte obligatoria es `PERFECTA`. De lo contrario, los bonus serán totalmente `IGNORADOS`.

Puedes mejorar tu proyecto con las siguientes características:

- Permitir escoger la contraseña de cifrado de la clave maestra ft_otp.key y solicitarla cada vez que se genere una contraseña temporal nueva.
- Desarrollar un cliente que genere la contraseña maestra y valide los resultados con una interfaz gráfica.
- Cualquier otra característica que consideres útil. Tus compañeros juzgarán si lo es realmente.

Capítulo V

Evaluación por pares

Este proyecto será corregido por tus compañeros. Entrega los archivos en el repositorio Git y asegúrate de que todo funciona como se espera.