ESCUELA POLITÉCNICA NACIONAL
FACULTAD DE INGENIERÍA DE SISTEMAS
TECNOLOGÍAS DE SEGURIDAD

# Tarea Tecnologías de seguridad

**Tarea No. 1: Keylogger**
**Nombre:** Luis Enrique Pérez Señalin.

## Objetivos:

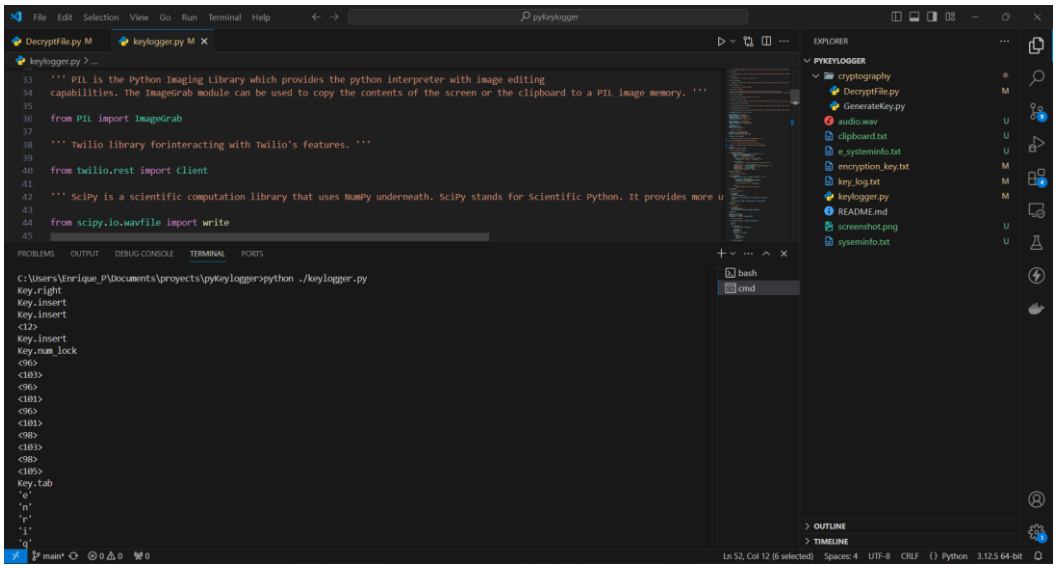
- Instalar un keylogger de tipo software y un keylogger de tipo addon de navegador web.
- Utilizar el computador con el software durante 3 días.
- Generar un pequeño informe del uso de los Keyloggers incluyendo su opinión personal.

## Proceso de instalación

Realizando la búsqueda permitente, se utilizará PyKeylogger y Ghostpress para probar los Keyloggers de tipo Software y de tipo Addon respectivamente, se reconocen estos Keyloggers por sus propósitos educativos o de prueba, ofreciendo transparencia al momento de utilizarlos, dando la seguridad de no ser maliciosos y robar información al usuario.

**PyKeylogger:**
Hecho en Python y de código libre es muy transparente con el usuario y permite muchas modificaciones.

1. Se clona el repositorio que está en github.
2. Se toma en cuenta una previa instalación de Python, y se instalan los paquetes extras.
3. Se genera la clave del programa con los pasos dados.
4. Se ejecuta el programa.




En esta captura podemos observar los archivos generados después de la ejecución, así como los mensajes en la terminal que emite, e incluso una grabación del micrófono como algo extra.

**Conclusión de PyKeylogger:**
Es una herramienta útil y versátil, con ciertas funcionalidades extras y muy transparente, mostrando el código completo junto con las tecnologías que utiliza, se puede apreciar correctamente los efectos de un Keylogger en un computador.

**Datos extra:** El keylogger solo puede estar activo al ejecutarlo directamente con comandos, por lo que el usuario fácilmente puede ver que está abierto, pero se puede esconder creando algún "servicio" utilizando esto, para que sea un Keylogger "malicioso" y también añadirle un "servidor" de destino para los datos capturados. Cabe añadir el fallo de ciertos momentos al utilizar teclas como "Tab" que automáticamente detienen la ejecución del Keylogger.

## Conclusión:

Los keylogger son sumamente peligrosos, aunque tienen bastantes faltas como los datos de las páginas o portales de entrada, ya que el navegador permite el "autocompletado", siendo este una forma de evitar escribir toda la página, y también los correos guardados que el navegador también recomienda para que el usuario no escriba todo, pero siempre o casi siempre debe escribir la contraseña. Todas estas "debilidades" pueden ser suplidas con capturadores de pantalla o de ratón, también con programas que guardan el historial de navegación.

## Links:

PyKeylogger: https://github.com/kartikmehta8/pyKeylogger