# Tinky Winkey

## ¿Windows? ¿Qué es eso?

Resumen: Este proyecto te introduce al sistema operativo windows, ya sabes el más utilizado...

Versión: 2

# Contenido

# Capítulo I

# Preámbulo

Teletubbyland es el lugar de los Teletubbies. Es un lugar apartado en las colinas. Permítanme presentarles a los personajes principales.

- Tinky Winky es el primer Teletubby, además del más grande y antiguo del grupo. Está cubierto con una tela de rizo violeta y tiene una antena triangular en la cabeza. Suele llevar una bolsa roja.
- Dipsy es el segundo Teletubbie. Es verde y recibe su nombre por su antena, que se parece a una varilla de medición. Dipsy es el más testarudo de los Teletubbies y, en ocasiones, se niega a aceptar la opinión del grupo.
- Laa-Laa es la tercera Teletubbie. Es amarilla y tiene una antena rizada. Laa-Laa es muy dulce, le gusta cantar y bailar y a menudo se la muestra cuidando a los otros Teletubbies.
- Po es el cuarto Teletubby, además del más pequeño y joven. Es de color rojo y tiene una antena con forma de palo que se usa para hacer pompas de jabón. Su juguete favorito es un patinete rosa y azul.

# Capítulo II

# Introducción

Este proyecto te invita a ampliar tus conocimientos dando un primer paso en el sistema operativo Windows.

Escribirás dos programas, un Servicio y un Keylogger.

- Los servicios de Windows son programas que funcionan en segundo plano. Suelen ser administrados por el Administrador de control de servicios. Los servicios interactúan con el SCM a través de la API de Windows o herramientas de administración de servicios de Windows como sc.exe. Nota: la terminación de sc.exe se utiliza como método para provocar la pantalla azul de la muerte.

- Los keyloggers son programas que rastrean las actividades de un teclado. Los keyloggers son una forma de software espía en el que los usuarios no son conscientes de que se están rastreando sus acciones. Los keyloggers se pueden utilizar para diversos fines: los piratas informáticos pueden utilizarlos para obtener acceso malicioso a su información privada, mientras que los empleadores pueden utilizarlos para supervisar las actividades de los empleados.

# Capítulo III

# Pautas generales

- Este proyecto debe realizarse en una máquina virtual.
- Sólo se permite C o C++.
- Su Makefile deberá evaluarse con NMAKE.
- Debes utilizar CL como compilador.
- Debes compilar con los indicadores /Wall y /WX
- Dentro de la parte obligatoria deberás utilizar las siguientes funciones:
    - Administrador de OpenSC
    - Crear servicio
    - Servicio abierto
    - Iniciar servicio
    - Servicio de Control
    - CerrarServiceHandle
    - TokenEx Duplicado
- Deshabilite Windows Defender si es necesario.

Lea la documentación oficial de MSDN.

Puede utilizar cualquier herramienta que desee para configurar su máquina virtual host.

# Capítulo IV

# Parte obligatoria

## IV.1 Servicio

- El programa debe llamarse svc.
- El servicio debe llamarse tinky.
- Para gestionar el servicio están disponibles las siguientes opciones:
  - instalar
  - inicio
  - parada
  - eliminar
- Una vez que el servicio comienza a funcionar debe:
  - Suplantar un token del SISTEMA.
  - Ejecute el Keylogger con él en segundo plano.
- Sólo se puede ejecutar una instancia del Keylogger.
- Al eliminar el servicio, se debe eliminar el Keylogger.

winlogon.exe

## IV.2 Registrador de teclas

- El programa debe llamarse winkey.
- Esto debe detectar procesos en primer plano.
- Esto debe guardar cada pulsación de tecla relacionada con el proceso en primer plano actual.
- La entrada del teclado debe manejarse en un gancho de bajo nivel.
- La marca de tiempo, la información del proceso en primer plano y las pulsaciones de teclas relacionadas deben guardarse en un archivo de registro.
- La entrada de teclas debe guardarse en un formato legible para humanos.
- La entrada de teclas debe guardarse de acuerdo con el identificador de configuración regional actual.

Lea la documentación oficial de MSDN.

# Capítulo V

# Ejemplo

# Capítulo VI

# Parte extra

Eres libre de agregar bonos de tu elección, pero aquí hay algunas ideas interesantes:

- Ocultar el servicio y el keylogger de sus respectivas herramientas de listado.
- Poder actualizar el servicio durante su tiempo de ejecución.
- Registro de portapapeles, pantalla y/o micrófono.
- Aplicaciones, filtrado de usuarios.
- Control de captura de texto (capturar contraseña detrás de una máscara de contraseña).
- shell remoto.

Solo se podrá acceder a la parte adicional si la parte obligatoria es PERFECTA. Perfecto significa que la parte obligatoria se ha realizado íntegramente y funciona sin fallas. Si no ha aprobado TODOS los requisitos obligatorios, no se evaluará la parte adicional.

# Capítulo VII

# Entrega y evaluación por pares

- Como siempre, entrega tu trabajo en tu repositorio GiT. Solo el trabajo incluido en tu El repositorio será revisado durante la evaluación.
- Se debe utilizar Windows 10 o superior, la escala de calificación fue construida con un sistema estable ventanas 10.
- Microsoft proporciona una máquina virtual oficial gratuita lista para ejecutarse, selecciónela allí.

Buena suerte.