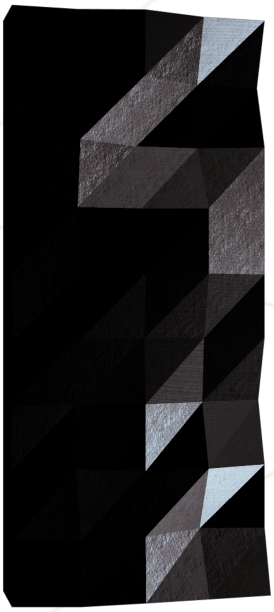

Tinky Winkey

Windows? What's that?

Summary: This project introduces you to the windows operating system, you know the most used one...

Version:

Contents

Chapter I

Preamble

Teletubbyland is the place of the Teletubbies. It is the away in the hills. Let me introduce you the main characters.

- `Tinky Winky` is the first Teletubby, as well as the largest and oldest of the group. He is covered in purple terrycloth and has a triangular antenna on his head. He often carries a red bag.
- `Dipsy` is the second Teletubby. He is green and named after his antenna, which resembles a dipstick. Dipsy is the most stubborn of the Teletubbies, and will occasionally refuse to go along with the group opinion.
- `Laa-Laa` is the third Teletubby. She is yellow and has a curly antenna. Laa-Laa is very sweet, likes to sing and dance, and is often shown looking out for the other Teletubbies.
- `Po` is the fourth Teletubby, as well as the shortest and youngest. She is red and has an antenna shaped like a stick used for blowing soap bubbles. Her favourite toy is a pink and blue scooter.

Chapter II

Introduction

This project invites you to broaden your knowledge by making a first step into the Windows operating system.
You will write two programs, a Service and a Keylogger.

- Windows services are program that operate in background. They are often managed by the `Service Control Manager`. Services interact with the SCM through the Windows API or Windows service management tools such as `sc.exe`.
  note: terminating `sc.exe` is used as a method of causing the Blue Screen of Death.

- Keyloggers are programs that track the activities of a keyboard. Keyloggers are a form of spyware where users are unaware their actions are being tracked. Keyloggers can be used for a variety of purposes; hackers may use them to maliciously gain access to your private information, while employers might use them to monitor employee activities.

Chapter III

General guidelines

- This project needs to be done on a Virtual Machine.
- Only `C` or `C++` is allowed.
- Your Makefile will need to be evaluated with `NMAKE`.
- You must use `CL` as compiler.
- You must compile with the flags `/Wall` and `/WX`
- Within the mandatory part, you must use the following functions:
    - OpenSCManager
    - CreateService
    - OpenService
    - StartService
    - ControlService
    - CloseServiceHandle
    - DuplicateTokenEx
- Disable Windows defender if needed.

Please read the the official MSDN documentation.

`You can use any tools you want to set up your host` **`virtual machine`**`.`

Chapter IV

Mandatory part

IV.1 Service

- The program must be named `svc`.
- The service must be named `tinky`.
- The following options are available to handle the service:
    - install
    - start
    - stop
    - delete
- Once the service starts running it must:
    - Impersonate a SYSTEM token.
    - Launch the Keylogger with it in the background.
- Only one instance of the Keylogger can run.
- On removal of the service, the Keylogger must be killed.

`winlogon.exe`

IV.2 Keylogger

- The program must be named `winkey`.
- This must detect foreground processes.
- This must save every keystroke related to the current foreground process.
- Keyboard input must be handled in a low-level hook.
- Timestamp, foreground process information and their related key stroke must be saved in a log file.
- Keystroke input must be saved in a human readable format.
- Keystroke input must be saved accordingly to the current locale identifier.

Please read the the official MSDN documentation.

Chapter V

Exemple

```
coconut\ svc.exe install
Service {tinky} installed successfully.
coconut\ sc.exe queryex type=service state=all | Select-String "SERVICE_NAME: tinky" -Context 0,3
SERVICE_NAME: tinky
DISPLAY_NAME: tinky
           TYPE                 : 10   WIN32_OWN_PROCESS
           STATE                : 1    STOPPED
coconut\ tasklist | Select-String "winkey"
coconut\
coconut\ svc.exe start
Service {tinky} started successfully.
coconut\ sc.exe queryex type=service state=all | Select-String "SERVICE_NAME: tinky" -Context 0,3
SERVICE_NAME: tinky
DISPLAY_NAME: tinky
           TYPE                 : 10   WIN32_OWN_PROCESS
           STATE                : 4    RUNNING
coconut\ tasklist | Select-String "winkey"
winkey.exe               2052 Console                     1      4028 Ko
coconut\ svc.exe stop
Service {tinky} stopped successfully.
coconut\ sc.exe queryex type=service state=all | Select-String "SERVICE_NAME: tinky" -Context 0,3
coconut\ svc.exe delete
Service {tinky} deleted successfully.
coconut\ sc.exe queryex type=service state=all | Select-String "SERVICE_NAME: tinky" -Context 0,3
coconut\
coconut\ tasklist | Select-String "winkey"
coconut\
coconut\ type winkey.log
[01.11.2021 06:58:46] - 'New tab - Google Chrome'
ShiftHey i'm currently on tab 1 of my ShiftGoogle ShiftChrome.
[01.11.2021 06:58:56] - 'Intra Profile Home - Google Chrome'
tinky-winkey\n
[01.11.2021 07:01:23] - 'coconut@DESKTOP-C6PDFQLM: ~'
ShiftWelcome_to kali-linux
[01.11.2021 07:10:23] - '? Keylogger.c - Keylogger - Visual Studio Code'
CtrlS
```

Chapter VI

Bonus part

You are free to add bonuses of your choice, but here are some interesting ideas:

- Hide service and keylogger from their respective listing tools.
- Be able to update the service during his runtime.
- Clipboard, screen and/or microphone logging.
- Applications, Users filtering.
- Control text capture (capture password behind a password mask).
- remote shell.

`The bonus part will only be accessed if the mandatory part is PERFECT. Perfect means the mandatory part has been integrally done and works without malfunctioning.  If you have not passed ALL the mandatory requirements, your bonus part will be evaluated at all.`

Chapter VII

Turn-in and peer-evualation

- As usual, turn in your work on your repo GiT. Only the work included on your repo will be reviewed during the evaluation.
- Windows 10 or superior must be used, the grading scale was built with a stable windows 10.
- Microsoft provide free official Virtual Machine ready to launch, pick it there.

Good luck.