Security Manager Python Program

Welcome to the Security Manager Python program! This program is designed to implement specific security measures on a Windows 10 operating system. The primary goal of this program is to enhance system security by controlling various aspects such as USB ports, Bluetooth functionality, Command Prompt access, and website browsing.

Features Implemented

1. Blocking USB Ports and Disabling Bluetooth We use the Windows Management Instrumentation (WMI) to interact with USB devices and disable them. This helps prevent unauthorized devices from connecting to the system. The program also has a mechanism to disable Bluetooth functionality for security reasons.

2. Disabling Command Prompt We modify the Windows Registry to disable the Command Prompt. This prevents users from executing arbitrary commands, enhancing system security.

3. Blocking Website Access By modifying the Windows hosts file, we redirect specific website domains, like "facebook.com," to localhost (127.0.0.1). This effectively blocks access to these websites from any browser on the system.

Imported Libraries

This program utilizes various Python libraries to achieve its goals:

-os This library provides a way to interact with the operating system, allowing us to execute system commands and manage files and directories.

- subprocess The subprocess library enables us to run external processes and interact with their input and output streams.

- ctypes This library allows us to make calls to functions implemented in dynamic link libraries, enabling low-level interactions with the system.

- re The re library is used for regular expression matching, which can be useful for pattern-based tasks.

- time The time library provides functions to work with time-related operations, such as delays and measuring time intervals.