Министерство науки и высшего образования Российской Федерации

Санкт-Петербургский Политехнический Университет Петра Великого

—

Институт компьютерных наук и кибербезопасности

ЛАБОРАТОРНАЯ РАБОТА № 3

«Планировщик задач Windows»

1. по дисциплине «Безопасность современных информационных технологий»
2. Выполнил
3. студент гр. 5151004/10101 Веремейчук Я.Ю.

<подпись>

1. Преподаватель Соловей Р.С.

<подпись>

1. Санкт-Петербург
2. 2024
3. Цель работы

Изучить возможности встроенного в ОС Windows планировщика задач.

1. Задача

Реализовать программу для управления планировщиком задач в ОС Windows, использующую возможности Windows API.

1. Требования

* язык программирования: C/C++;
* разрабатываемая программа не должна использовать готовые обертки над Windows API;
* программа должна уметь выводить список активных задач и их статус;
* создайте правило, уведомляющее пользователя о внесении изменений в механизмы безопасности Windows: в работу встроенного антивируса Windows Defender, изменении любых настроек брандмауэра;
* создайте правило, уведомляющее пользователя, когда брандмауэр Windows блокирует ping-запрос с определенного IP-адреса;
* поддержка ОС Windows 7 – 10.

1. Ход работы

Работа была выполнена на виртуальной машине Windows 10 Pro.

Планировщик задач Window открывается с помощью вызова Win+X -> Computer Manager -> Task Sheduler.

Изображение выглядит как текст, снимок экрана, программное обеспечение, Значок на компьютере

Автоматически созданное описание

Рисунок 1 – Открытие планировщика задач

Изображение выглядит как текст, снимок экрана, Шрифт, программное обеспечение

Автоматически созданное описание

Рисунок 2 – Запуск программы

Изображение выглядит как текст, снимок экрана, программное обеспечение, Значок на компьютере

Автоматически созданное описание

Рисунок 3 – Отображение запущенных задач в Планировщике заданий

Изображение выглядит как текст, снимок экрана, программное обеспечение, веб-страница

Автоматически созданное описание

Рисунок 4 – Изменение настроек фаервола

Изображение выглядит как текст, снимок экрана, Шрифт, число

Автоматически созданное описание

Рисунок 5 – Изменение настроек антивируса

Утилита auditpol отображает сведения о функциях для управления политиками аудита.

Для блокировки ping необходимо запустить следующие команды (для отключения можно запустить disable):

auditpol /get /category:\*

auditpol /set /subcategory:"Filtering Platform Packet Drop" /success:enable /failure:enable

auditpol /set /subcategory:"Filtering Platform Connection" /success:enable /failure:enable

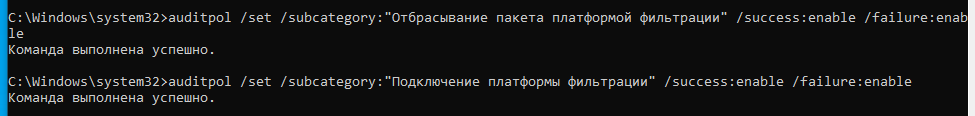


Рисунок 6 – Запуск команд

Изображение выглядит как текст, снимок экрана, Шрифт, линия

Автоматически созданное описание

Рисунок 7 – Включение

Отбрасывание пакетов платформой фильтрации аудита определяет, генерирует ли операционная система события аудита при отбрасывании пакетов платформой фильтрации Windows.

Платформа фильтрации Windows (WFP) позволяет независимым поставщикам программного обеспечения (ISV) фильтровать и изменять пакеты TCP/ IP, отслеживать или разрешать подключения, фильтровать трафик, защищенный IPSec (Internet Protocol Security), и фильтровать вызовы удаленных процедур (RPC).

Брандмауэр Windows в режиме повышенной безопасности можно отслеживать созданные правила.

Изображение выглядит как текст, снимок экрана, программное обеспечение, Значок на компьютере

Автоматически созданное описание

Рисунок 8 – Брандмауэр Windows в режиме повышенной безопасности

Изображение выглядит как снимок экрана, текст, программное обеспечение, Мультимедийное программное обеспечение

Автоматически созданное описание

Рисунок 9 – Созданное правило

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

Рисунок 10 – Блокирование ping

1. Выводы

В ходе выполнения данной лабораторной работы была написана программа для управления планировщиком задач в ОС Windows, использующая возможности Windows API.

1. Контрольные вопросы
2. **Опишите, зачем нужен планировщик задач ОС Windows и какие есть альтернативы данному инструменту.**

Планировщик задач **–** компонент Microsoft Windows, который предоставляет возможность запланировать запуск программ или скриптов в определённые моменты времени или через заданные временные интервалы. Он позволяет пользователям и системным администраторам настроить автоматический запуск программ, выполнение скриптов, отправку электронных писем, создание резервных копий, а также другие действия в определенное время или при наступлении определенных событий. Это улучшает продуктивность и помогает поддерживать систему в рабочем состоянии без необходимости вмешательства пользователя.

Альтернативы:

1. Windows PowerShell позволяет создавать задачи с использованием скриптов и планировать их выполнение через командную строку.
2. Apache Airflow – ПО для создания, выполнения, мониторинга и оркестровки потоков операций по обработке данных.
3. VisualCron – коммерческое решение для планирования задач в Windows, предоставляющее расширенные возможности автоматизации и интеграции.
4. Cron (в Unix-системах) – классический демон, использующийся для периодического выполнения заданий в определённое время.
5. Асинхронный или анахроничный cron. Anacron в отличие от cron не поддерживает запуск заданий по расписанию, вместо этого задания запускаются с заданным интервалом времени.
6. **Какие триггеры существуют во встроенном планировщике задач ОС Windows?**

Планировщик задач имеет два вида триггеров: “триггер, зависящий от времени” и “триггер, основанный на событии”.

Триггеры на основе времени запускают задачи в указанное время. Сюда входит запуск задачи один раз в определенное время или несколько раз в ежедневном, еженедельном, ежемесячном или ежемесячном расписании.

Триггеры на основе событий запускают задачу в ответ на определенные системные события. Например, триггеры на основе событий можно настроить для запуска задачи при запуске системы, при входе пользователя на локальный компьютер или при бездействии системы.

1. **Какие ограничения накладываются на задачи?**

Разрешения: Для выполнения задач могут требоваться административные права. Задачи, требующие выполнения с повышенными привилегиями, должны быть настроены соответствующим образом.

Контекст пользователя: Задачи могут быть настроены для выполнения от имени определенного пользователя, и могут не работать, если учетная запись пользователя неактивна или имеет ограниченные права.

Окружение выполнения: Некоторые задачи могут требовать определенной конфигурации окружения (например, наличие сети или конкретных ресурсов).

Ресурсы: Если задача требует значительных системных ресурсов, это может повлиять на производительность системы и других задач.

Периодичность: Слишком частое выполнение задачи может создать нагрузку на систему.

1. **Перечислите типы задач, которые могут быть запущены с помощью планировщика.**

Запуск приложений и программ: Запускать исполняемые файлы (.exe), сценарии (.bat, .cmd, .ps1) и другие приложения.

Отправка электронных писем: Отправка уведомлений по электронной почте при наступлении определенных условий.

Отображение сообщений: Показ всплывающих уведомлений или сообщений пользователю.

1. **Опишите механизмы безопасности Windows, которые задействованы при регистрации новых задач**

Права доступа: Для создания и управления задачами могут потребоваться административные права. Операционная система проверяет, имеет ли пользователь соответствующие привилегии.

Аутентификация: При создании задачи, выполняемой от имени другого пользователя, необходимо указать его учетные данные, которые проверяются системой.

Контроль учетных записей (UAC): Если задача требует выполнения с повышенными правами, включается контроль учетных записей, который запрашивает подтверждение от пользователя.

Шифрование данных: Учетные данные, использованные для выполнения задач, хранятся в зашифрованном виде.

Журналирование: Все действия, связанные с созданием, изменением и выполнением задач, регистрируются в журнале событий Windows, что позволяет отслеживать и анализировать их.

Политики безопасности: Могут применяться групповые политики, ограничивающие возможность создания и выполнения задач для определенных пользователей или групп.