Федеральное государственное автономное образовательное учреждение высшего образования

«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ «ВЫСШАЯ ШКОЛА ЭКОНОМИКИ»

Московский институт электроники и математики им. Тихонова

Департамент электронной инженерии

ОТЧЕТ

О ПРАКТИЧЕСКОЙ РАБОТЕ №1

по дисциплине «Безопасность операционный систем»

«Обход защиты ОС»

Студент гр. БИБ201

Шадрунов Алексей

Дата выполнения: 14 декабря 2023 г.

Преподаватель:

Смирнов Данил Вадимович

«___» _____ 2023 г.

Москва, 2023

Содержание

1 Цель работы

Целью работы ставится получение знаний о механизмах обеспечения безопасности ОС Windows, а также навыков эксплуатации уязвимостей повышения привилегий.

2 Ход работы

2.1 Подготовка виртуальной машины

Для выполнения работы подготовим виртуальную машину Windows 10 с установленным Process Monitor.

2.2 Подготовка программы

Запустим Process Monitor. Установим фильтр по имени процесса (Рисунок 1):

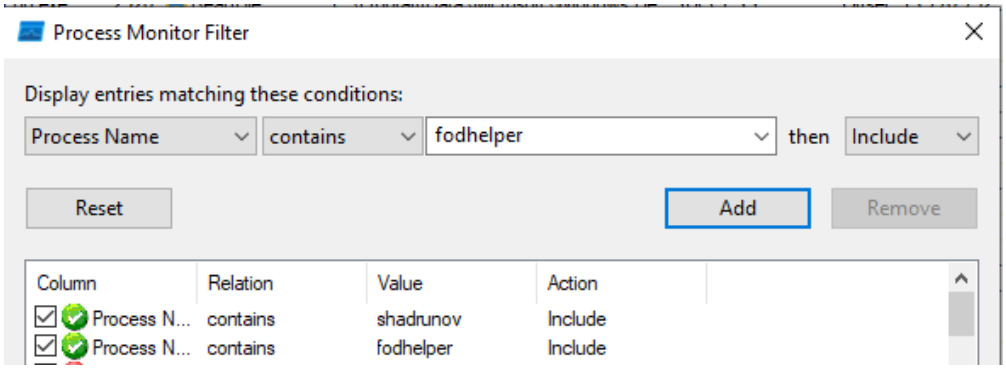

Рисунок 1 – Фильтр по имени процесса

Запустим fodhelper.exe. В списке событий этого процесса видим, что fodhelper.exe обращается к ветке реестра HKCU\Software\Classes\ms-settings\Shell\Open\Command.

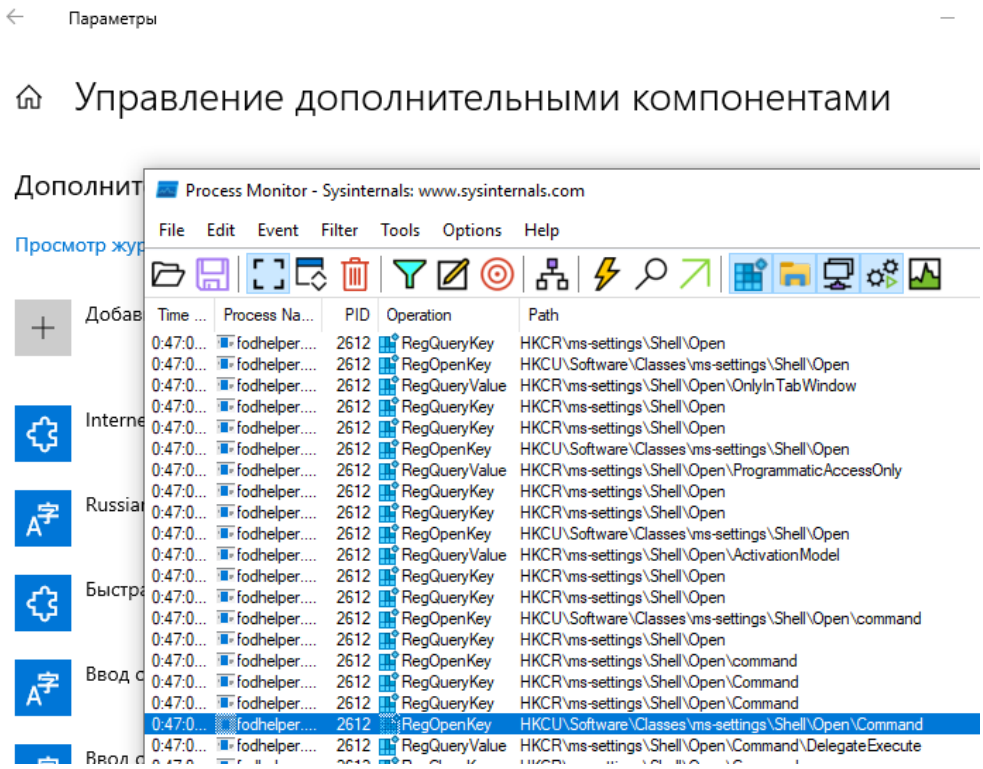

Рисунок 2 – Обращение к реестру

Создадим нужный куст в реестре в разделе HKEY_CURRENT_USER (Рисунок 3). По нужному пути разместим значение исполняемого файла (C:\Users\alex\shadrunov.exe) и строковое значение DelegateExecute.

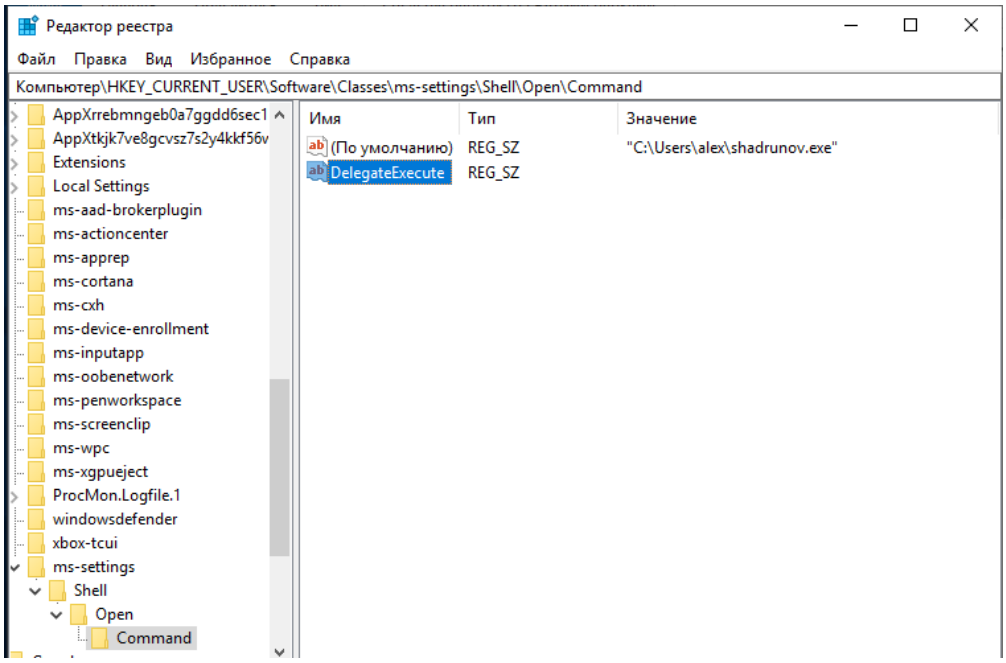

Рисунок 3 – Новый куст

Созданный куст отображается также и в разделе HKEY_CURRENT_CLASSES (Рисунок 4).

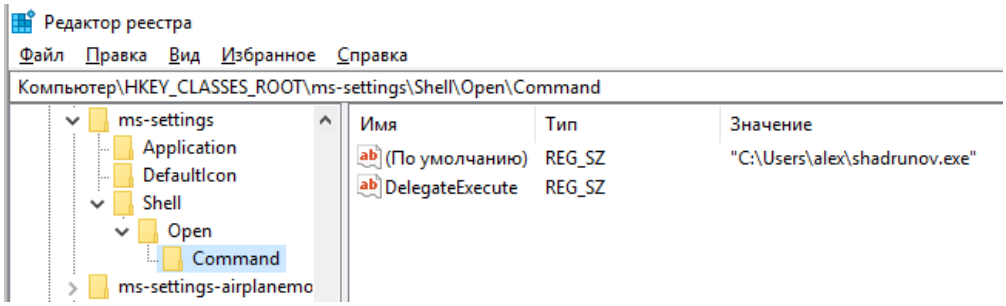

Рисунок 4 – Куст в другом дереве

Снова запустим fodhelper.exe. Открывается командная строка (Рисунок 5).

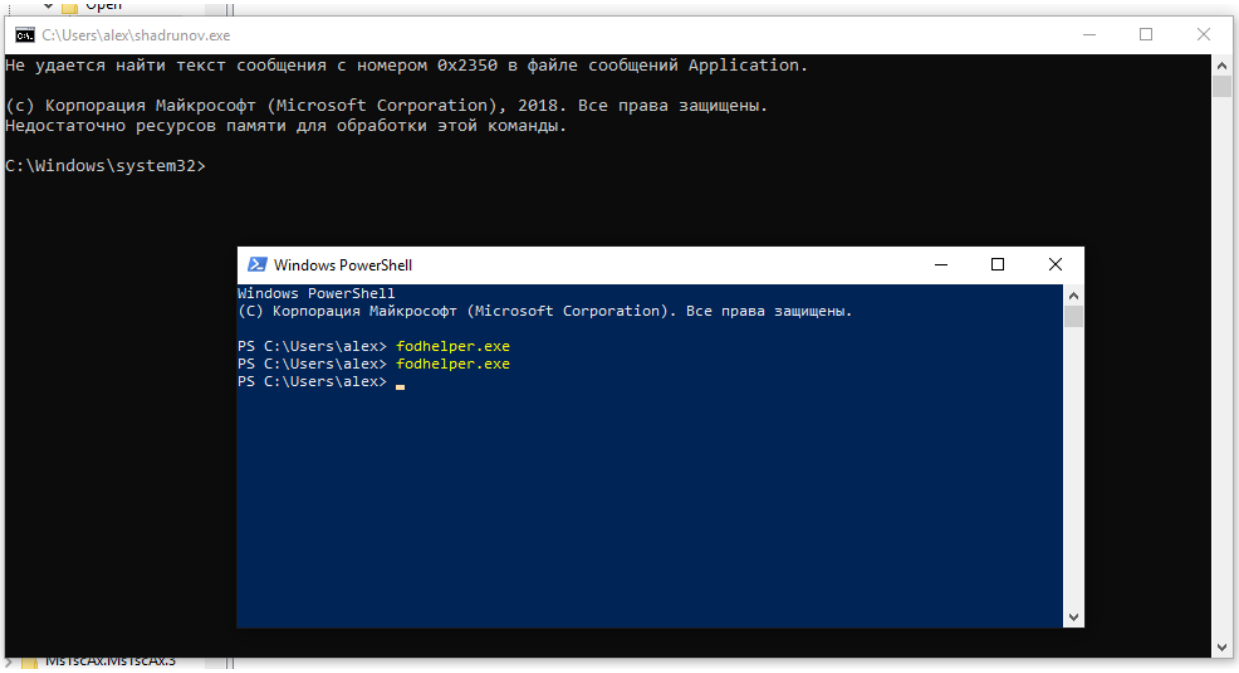

Рисунок 5 – Эксплуатация

Проверим привилегии дочернего процесса. Process Monitor отображает его как процесс с высоким уровнем целостности (рисунки 6-7).

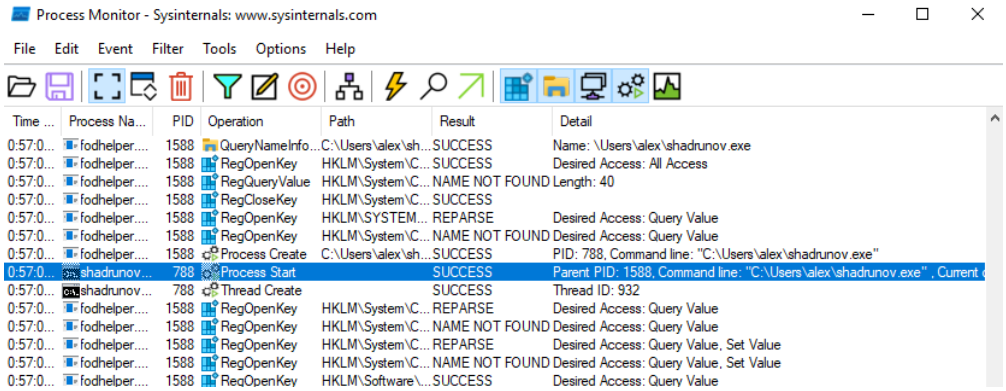

Рисунок 6 – Создание дочернего процесса

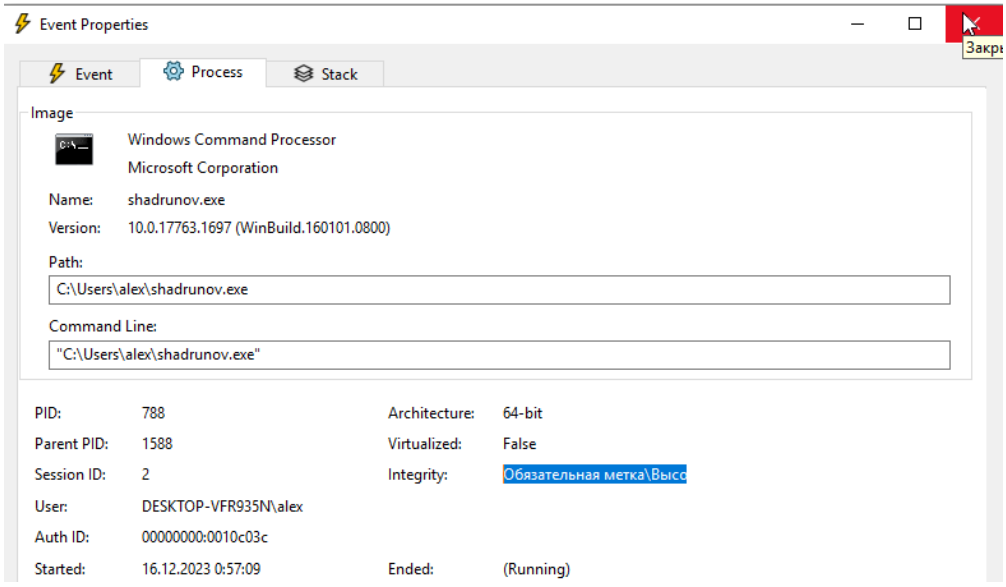

Рисунок 7 – Высокий уровень целостности

Проверим административный доступ процесса. Для этого создадим файл на диске C: (операция, требующая повышенных привилегий). Видно, что обычной консоли в доступе отказано (рисунки 8-9).

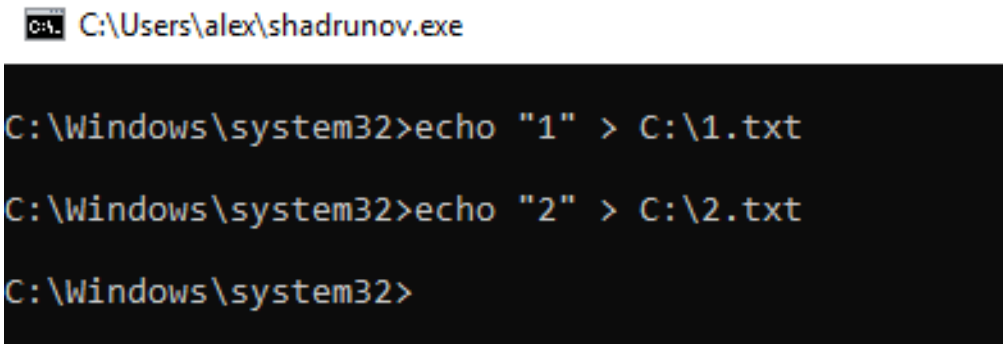

Рисунок 8 – Дочерний процесс может записывать на диск C:

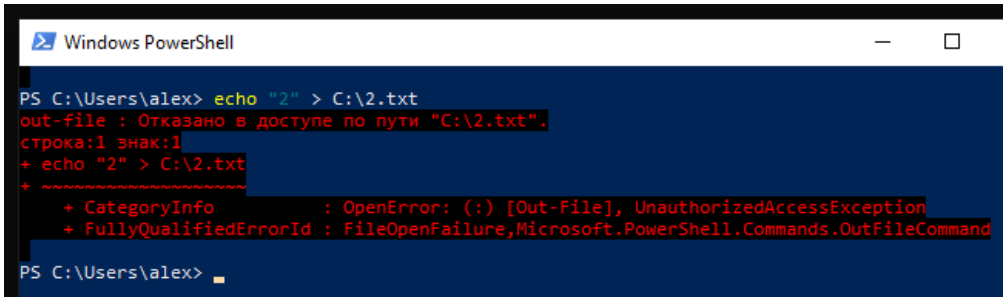

Рисунок 9 – Обычная консоль не может записывать на диск C:

3 Выводы о проделанной работе

В рамках данной работы получены знания о механизмах обеспечения безопасности ОС Windows, а также навыки эксплуатации уязвимостей повышения привилегий.