1. Министерство образования и науки Российской Федерации
2. Санкт-Петербургский Политехнический Университет Петра Великого
3. Институт компьютерных наук и кибербезопасности

**ЛАБОРАТОРНАЯ РАБОТА № 4**

1. «Защита от встраиваемых потайных ходов»
2. по дисциплине «Основы информационной безопасности»
3. Выполнил
4. студент гр. 5151001/40001 Волошкевич М.А

<*подпись*>

1. Преподаватель
2. ст. преподаватель Орёл Е.М

<*подпись*>

1. Санкт-Петербург
2. 2025

**1. ЦЕЛЬ РАБОТЫ**

Приобрести навыки по анализу структуры, функциональности и угроз специального встраиваемого дефекта программного продукта – потайного хода(backdoor).

**2. ЗАДАЧИ**

2.1 Реализовать клиент-серверную программу, использующую для сетевого соединения, для удаления файла на компьютере жертвы.

2.2 Добавить процедуру маскировки для программы.

* 1. Провести тестирование программы
  2. Проанализировать порты, которые использует программа.

**3. ВВЕДЕНИЕ**

3.1 Задача заключается в том, чтобы научиться защищаться от клиент-серверных приложений, которые маскируется в системе

**4. ОСНОВНАЯ ЧАСТЬ**

4.1 Теория

Программа-шпион(spyware) – программное обеспечение, скрытно собирающее информацию о пользователе (персональные данные, настройки ос, статистику работы и пр.) Большинство шпионских программ не уведомляют об этом пользователей, эксплуатируя встроенные в программу дефекты – потайные ходы(backdoor).

**5. ОПИСАНИЕ РЕШЕНИЯ**

Создал клиент-серверную программу на языке программирования python. Сервер соединяется с клиентом и передает ему имя файла, который должен быть удалён. Удаление файла реализовал с помощью библиотеки os. Для того, чтобы программа автоматически запускалась при запуске ос, добавили её в реестр автозагрузки. Для этого импортировал библиотеку winreg.

Открыл раздел реестра, отвечающий за раздел автозагрузки: winreg.OpenKey()

Добавил значение в раздел реестра: winreg.SetValueEx()

Закрыл раздел реестра: winreg.CloseKey()

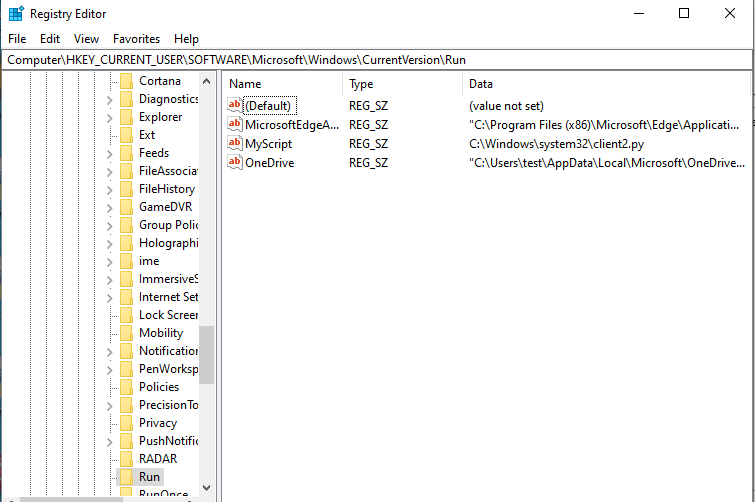


Рисунок 1. Раздел реестра с автозапуском

Для того, чтобы скрыть окно выполняемой программы, воспользуемся утилитой pyinstaller в которой пропишем, чтобы код клиента был в одном файле без консоли(аргументы --noconsole, --onefile). Копирование файла в системную директорию реализовано с помощью библиотеки shutil и os. При запуске программы проверяется: есть ли файл клиента в системной директории, в случае отсутствия — копирует сама себя с помощью функции shutil.copy(). Путь до системной директории находится с помощью значения списка os.environ[‘SystemRoot’]

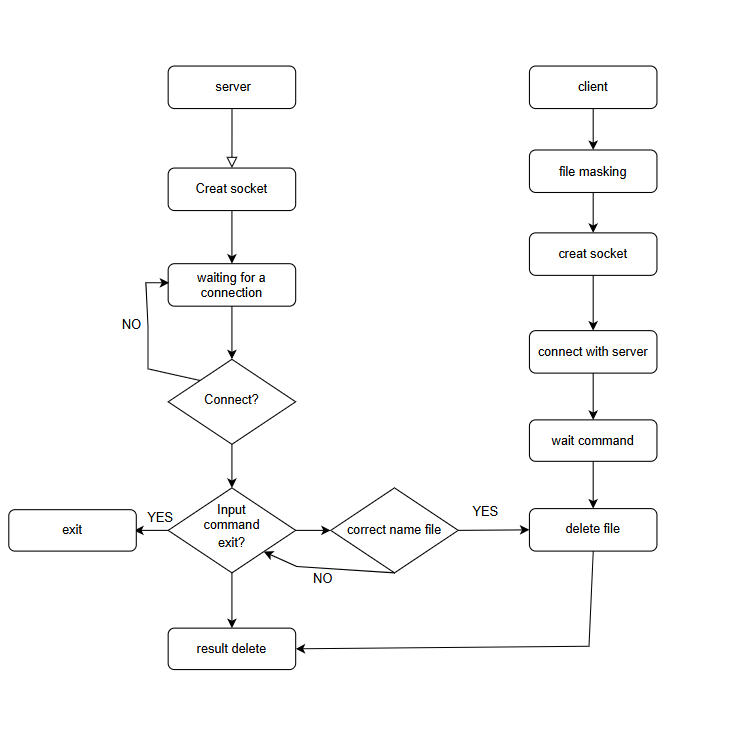


Рисунок 2. Блок-схема клиент-серверного приложения

Установив приложение межсетевого экрана, просмотрим открытые порты. Большее внимание уделяем порту, который открывает клиент в нашем приложении. Его статус – SYN\_SENT. Это означает, что клиент отправил запрос серверу на установление соединения и ожидает ответ.



Рисунок 3. Открытые порты

Запустив сервер, статус порта поменялся на ESTABILISHED. Это означает, что порт подключен.

Средствами межсетевого экрана заблокируем данные сетевые порты. Попытавшись выполнить соединение сервера и клиента, результата не будет. После открытия порта и разблокирования соединения всё работает.



Рисунок 4. Блокировка порта

**6. ВЫВОДЫ**

В ходе лабораторной работы, были приобретены навыки по анализу структуры, функциональности и угроз специально встраиваемого дефекта программного продукта – потайного хода, а также были изучены методы защиты от уязвимости такого вида. Были реализованы программы сервера и клиента, при помощи которых было успешно проведено удаление файла на компьютере-клиенте.

**7. ОТВЕТЫ НА ВОПРОСЫ**

1. Какие угрозы несут потайные ходы?

-Потайной ход позволяет копировать файлы с пораженного компьютера и на него, получать удаленный доступ к реестру, выполнять системные операции (перезагрузку системы, создание новых сетевых ресурсов, модификацию паролей и т.п.)

2. Как можно обнаружить потайной ход, если он открывает порт только на короткие промежутки времени, которые заранее неизвестны?

-Установить программный межсетевой экран, а также не отключать антивирус.

3. Можно ли использовать потайные ходы для организации распределенной атаки типа «отказ в обслуживании»?

-Да, можно заставить клиентов(жертв) отправлять запросы на определенный сервер.

4. Каким образом можно удалить процесс программ-клиента из списка задач *Диспетчера задача*?

-Снять задачу в Диспетчере задача. Также существует еще способ. Win+R и ввести *regedit*, переместиться в *Software\Microsoft\Windows\CurrentVersion\Run* и удалить программу с автозагрузки.

5. Опишите схему потайного хода, использующего для удаления управления Telnet-сервер.

-Telnet (telecommunications network) — это сетевой протокол (работающий по TCP-соединению), предназначенный для ручного управления удаленными машинами с помощью команд консольного терминала. В код сервера встраиваются данные, например «admin:1234». Злоумышленник загружает включает в Telnet-server потайной ход и настраивает нестандартный порт, например, 12345( по умолчанию работает на 23 порту) .