Министерство образования и науки Российской Федерации

Санкт-Петербургский Политехнический Университет Петра Великого

Институт кибербезопасности и защиты информации

**ЛАБОРАТОРНАЯ РАБОТА № 4**

**Защита от встраиваемых потайных ходов**

по дисциплине «Основы информационной безопасности»

Выполнил

Студент гр. 4851003/10002 Билан Н.С.

Руководитель

ст. преподаватель Зубков Е.А.

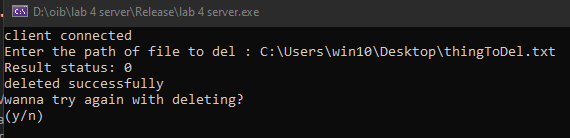
1. **ЦЕЛЬ РАБОТЫ**

Цель работы – приобретение навыков по анализу структуры, функциональности и угроз специально встраиваемого дефекта программного продукта – потайного хода (backdoor), а также изучение методов защиты от уязвимости такого вида**.**

1. **ЗАДАЧИ**
2. Реализовать клиент-серверную программу, использующую сокеты для сетевого соединения, с помощью которой можно дистанционно выполнить удаление файла с компьютера клиента.
3. Модифицировать программу клиент таким образом, чтобы она копировала себя в системный каталог, автоматически запускалась при старте операционной системы и не имела окна.
4. С помощью программного межсетевого экрана разорвать соединение между сервером и клиентом.

**3. ХОД РАБОТЫ**

Была реализована клиент-серверная программа, использующая сокеты для сетевого соединения. Клиент при запуске открывает определённый порт и ожидает входящего соединения. Сервер соединяется с клиентом и передаёт ему имя файла, который должен быть удалён (рис. 1):



**Рис. 1 - Пример работы программы**

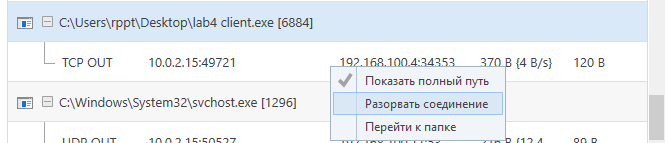
Далее была реализована процедура маскировки программы-клиента: самокопирование в системный каталог, автозапуск при старте операционной системы (рис 2.), отсутствие окна:



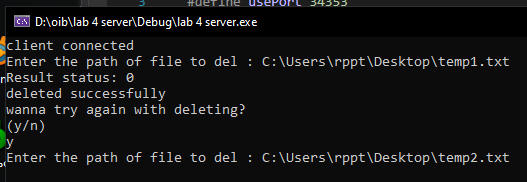
**Рис. 2 - Программа-клиент в автозагрузке**

Далее функционал программы-клиента был изменён таким образом, чтобы при её запуске она самостоятельно осуществляла регулярные попытки соединения с программой-сервером.

С помощью межсетевого экрана Comodo Internet Security было зафиксировано и разорвано соединение программы-сервера и программы-клиента. Дальнейшее удаление файлов оказалось невозможным (рис. 3, 4)



**Рис. 3 - Разрыв соединения**



**Рис. 4 - Пример работы программы**

1. **ВЫВОД**

Специально встраиваемый дефект программного продукта типа *backdoor* способен нанести ущерб системе и может быть использован для хакерских атак. В ходе выполнения работы были изучены структура, функциональность и угрозы данного дефекта, а также методы защиты от уязвимости такого вида. В общей сложности на выполнение работы было потрачено ~ 10 часов.

1. **КОНТРОЛЬНЫЕ ВОПРОСЫ**
2. Какие угрозы несут потайные ходы?

Потайные ходы позволяют копировать, удалять файлы с поражённого компьютера, позволяют получить удалённый доступ к реестру, производить системные операции: создание новых сетевых ресурсов, модификацию паролей и т.д.

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

Для того, чтобы обнаружить потайной ход, нужно регулярно осуществлять проверку открытых портов, а также установить специальную программу-монитор (например, Comodo Internet Security), которая позволяет обнаруживать такие порты.

1. Можно ли использовать потайные ходы для организации распределённой атаки типа “отказ в обслуживании”?

Да, например, осуществить массовую рассылку спам-сообщений, или многократно скопировать мусорные файлы.

1. Каким образом можно удалить процесс программы-клиента из списка Диспетчера задач?

Для удаления процесса программы-клиента из списка Диспетчера задач необходимо снять задачу с активного процесса программы-клиента и удалить его из автозагрузки.

1. Опишите схему работы потайного хода, использующего для удаленного управления Telnet-сервер.

При различных манипуляциях с системой поражённого компьютера с помощью потайного хода, использующего для удалённого управления Telnet-сервер устанавливается соединение компьютера взломщика с атакованным компьютером. Затем требуемые команды направляются на поражённый компьютер, а результаты их выполнения — обратно.