Министерство образования и науки Российской Федерации

1. Санкт-Петербургский Политехнический Университет Петра Великого
2. —
3. Институткибербезопасности и защиты информации

**ЛАБОРАТОРНАЯ РАБОТА № 4**

**Защита от встраиваемых потайных ходов**

по дисциплине «Основы информационной безопасности»

1. Выполнил
2. студент гр. 4851003/10002 Лобов Е.А

1. Ассистент
   1. преподавателя ЗубковЕ.А.

Санкт-Петербург

1. 2022

## **ПОСТАНОВКА ЗАДАЧИ**

Задача данной 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.

Для её достижения были выполнены следующие подзадачи:

1. Реализовать потайной ход, использующий сокеты для сетевого соединения.
2. С помощью разработанных программ удалённо выполнить удаление файла на компьютере, на котором установлена программа – клиент.
3. Расширить функциональность программ путём добавления маскировки для программы-клиента и осуществления регулярных попыток соединения с программой-сервером.
4. Заблокировать сетевые порты и изучить изменение работы программ.

## **ХОД РАБОТЫ**

### **Реализация потайного хода**

Потайной ход (backdoor) – это программное обеспечение, основным назначением которого является скрытное управление компьютером. Потайные ходы можно условно подразделить на следующие категории:

1. Построенные по технологии клиент-сервер. Такой потайной ход состоит минимум из двух программ — небольшой программы, скрытно устанавливаемой на поражаемый компьютер с программы управления, устанавливаемой на компьютер злоумышленника;
2. Использующие для удаленного управления встроенный Telnet-, Web- или IRC-сервер. Для управления таким потайным ходом не требуется специальное клиентское программное обеспечение. Примером может служить потайной ход, который подключается к заданному IRС-серверу и использует его для обмена информацией и командами управления со злоумышленником.

Для выполнения поставленных задач был реализован потайной ход из первой категории.Для его работы были использованы сокеты. Сокеты — название программного интерфейса для обеспечения обмена данными между процессами. Процессы при таком обмене могут исполняться как на одной ЭВМ, так и на различных ЭВМ, связанных между собой сетью. Сокет — абстрактный объект, представляющий конечную точку соединения. Существуют клиентские и серверные сокеты. Клиентское приложение (например, браузер) использует только клиентские сокеты, а серверное (например, веб-сервер, которому браузер посылает запросы) — как клиентские, так и серверные сокеты.

В качестве клиента была использована виртуальная машина, сервер запускался на основной ОС. Основной цикл работы с потайным ходом выглядел следующим образом:

1. После запуска «Server.exe» сервер ожидает подключения со стороны клиента.
2. После запуска на виртуальной машине «Client.exe» происходит установка соединения
3. В программе «Server.exe» «злоумышленник» указывает путь к файлу на машине клиента, который необходимо удалить (Рисунок 1)
4. Файл по данному пути удаляется, соединение закрывается

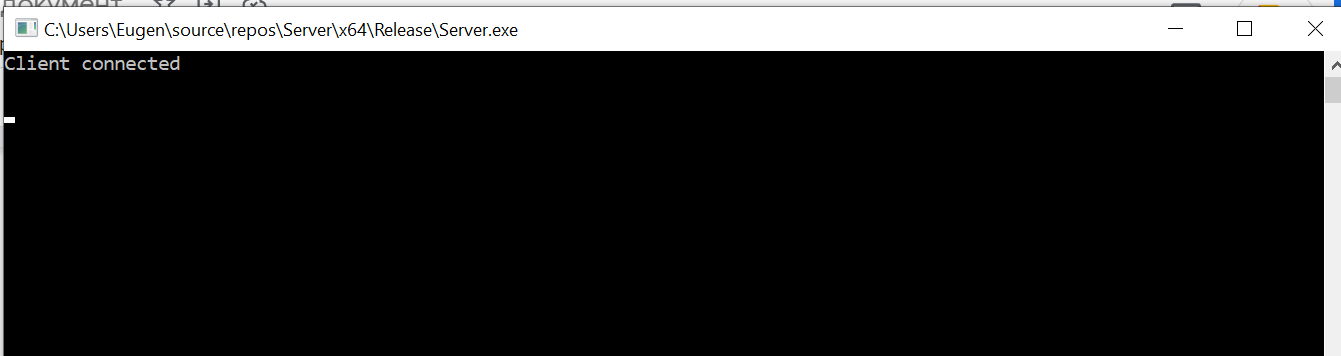


Рисунок 1 – Ожидание название файла после успешного соединения.

### **2. Маскировка программы-клиента**

Разработанный тайный ход успешно выполнял свою главную функцию – удалённое удаление файла на компьютере – жертве, но в исходной реализации присутствовали проблемы с программой-клиентом. Так, при её работе открывалась консоль, а для её запуска нужно было каждый раз самостоятельно открывать нужный файл.

В связи с этими недочётами был проведён ряд модификаций, связанный с маскировкой программы-клиента на компьютере жертвы:

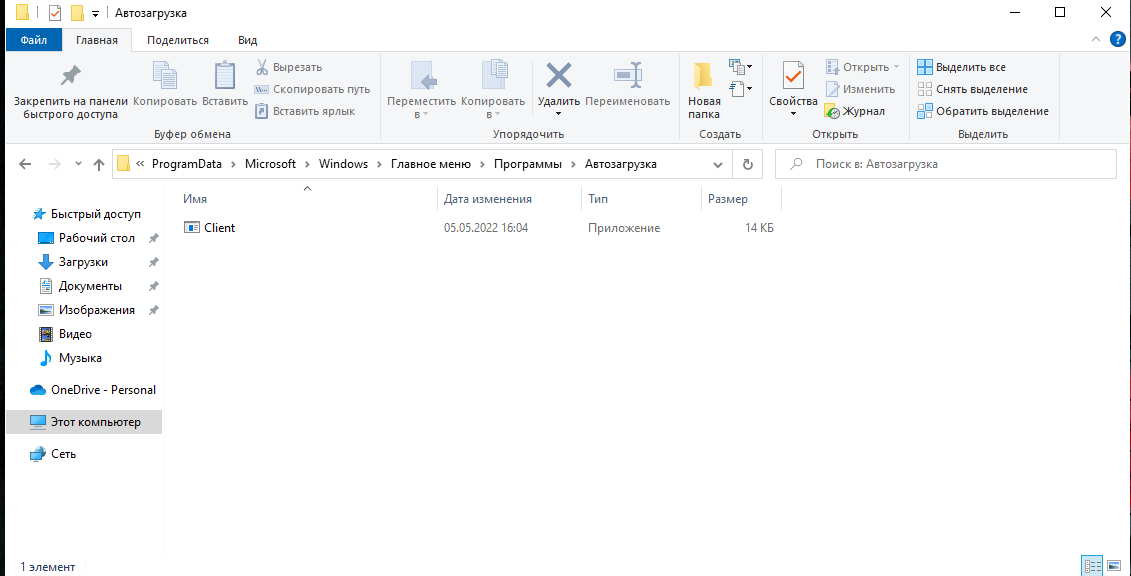
* Копирует себя в папку автозагрузки, таким образом автоматически запускается при старте ОС
* Не имеет окна
* В бесконечном цикле самостоятельно осуществляет попытки соединения с программой-сервером

Рисунок 2 – Папка автозагрузки после добавления программы-клиента (Client.exe).

### **3. Работа с межсетевым экраном**

Далее было рассмотрено использование межсетевого экрана для защиты от подобных потайных ходов. С помощью программы CurrPorts было выяснено, что запускающаяся автоматически программа-клиент действительно ждёт соединение по 1111порту (Рисунок 3).

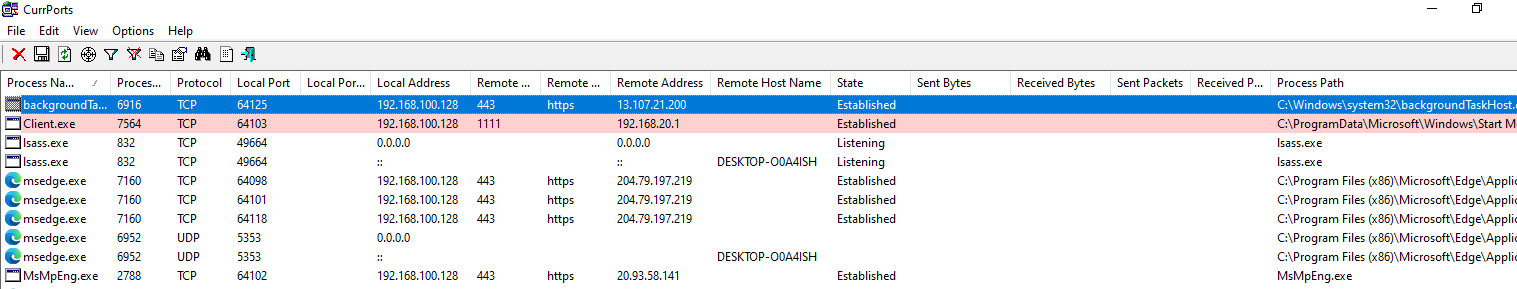


Рисунок 3 – Часть списка открытых портов.

В качестве решения были заблокированы соединения, использующие в качестве удалённого порта вышеуказанный. Проводилось это с использованием встроенного в Windows 10 ПО – Windows Defender Firewall (Рисунок 4):

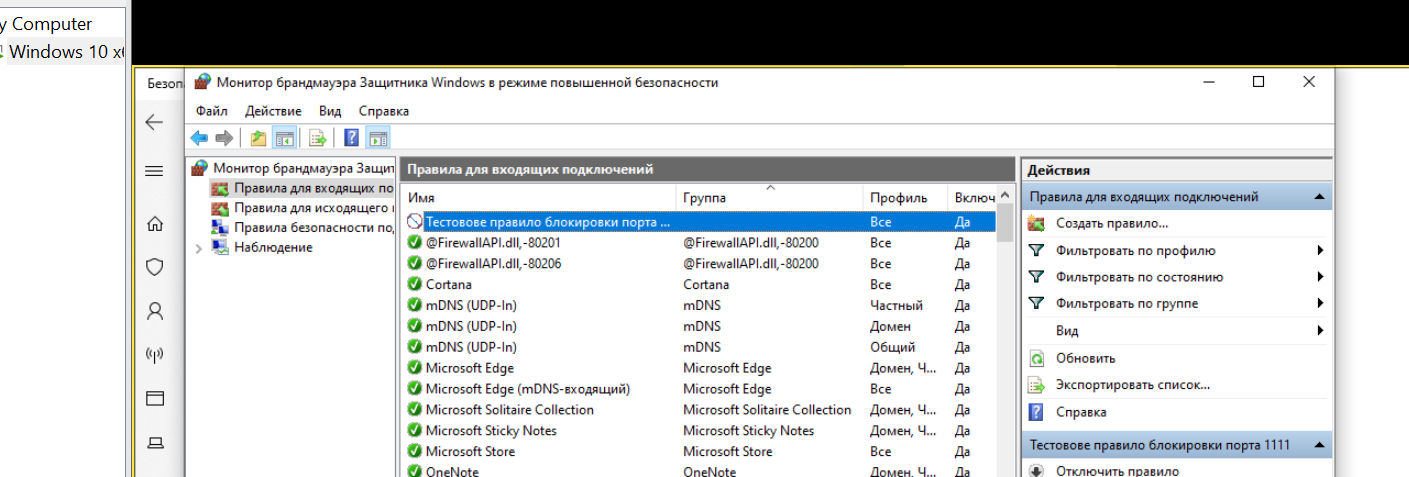


Рисунок 4 – Работа с межсетевым экраном.

После создания данного запрета клиент перестал подключаться к серверу вплоть до возвращения настроек межсетевого экрана к исходным.

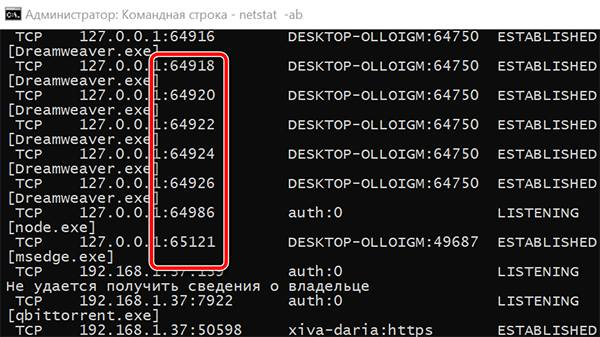
# Контрольные вопросы

1. Какие угрозы несут потайные ходы?

Благодаря потайным ходам злоумышленник может получить практически полный доступ к компьютеру.

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

Например благодаря утилите TCPView или через сравнение нескольких вызовов -netstat ab (функция cmd). Интересуют порты с префиксом «192.168.xxx.xxx», который является IP-адресом. Это означает, что процессы прослушивают сообщения из удаленных Интернет-узлов (например, веб-сайтов). Номер порта – это номер после двоеточия.



3.Можно ли использовать потайные ходы для организации распределенной DOS-атаки?

Да и это достаточно распространенный способ проведения DOS-атак. Сети из таких компьютеров называется ботнет.

4.Опишите схему работы потайного хода, использующего для удаленного управление Telnet-сервер.

Для управления таким потайным ходом не требуется специальное клиентское программное обеспечение, т.к оно уже входит в состав операционных систем или пакетов прикладных программ,установленных на компьютерах пользователей.

**ВЫВОД**

В ходе данной работы были приобретены навыки по анализу структуры, функциональности и угроз специально встраиваемого дефекта программного продукта – потайного хода (backdoor), а также изучены методы защиты от уязвимости такого вида.

С помощью реализованного потайного хода была осуществлена имитация действий злоумышленников, которые были успешно заблокированы с помощью специального ПО, называющегося межсетевым экраном. Было выяснено, что для того, чтобы обнаружить потайной ход, нужно регулярно осуществлять проверку открытых портов, а также установить специальную программу-монитор (например, Commodo Internet Security) которая позволяет обнаруживать такие программы.

Потайной ход позволяет копировать, удалять файлы с пораженного компьютера, позволяет получить удаленный доступ к реестру, производить системные операции: создание новых сетевых ресурсов, модификацию паролей и т.д. Также потайные ходы относятся к классу шпионским программных обеспечений (spyware) т.к. с их помощью можно собирать информацию с компьютера пользователя. Таким образом, потайной ход представляет серьезную угрозу безопасности системы в целом.