1. Министерство науки и высшего образования Российской Федерации
2. Санкт-Петербургский Политехнический Университет Петра Великого
3. —
4. Высшая школа кибербезопасности

**ЛАБОРАТОРНАЯ РАБОТА № 3**

1. **«Функционирование потайного хода с использованием netcat и windump»**
2. по дисциплине «Программно-аппаратные средства обеспечения информационной безопасности»
3. Выполнил
4. студент гр. 5151004/10101 Плохотникова М.С.

<*подпись*>

1. Проверил
2. преподаватель Семенов П.О.

<*подпись*>

1. Санкт-Петербург
2. 2024

# Цель работы

В ходе выполнения лабораторной работы необходимо проанализировать tcp-соединение и предложить способы обнаружения потайного хода.

# ход решения

## Анализ tcp-соединения

На виртуальной машине с помощью утилиты netcat был запущен сервер, прослушивающий 9000 порт.

nc -l 9000 > data.txt

С хоста был отправлен файл на 13КБ.

ncat 192.168.1.138 9000 < D:\poly\course\_4\sem\_7\ПАСОИБ\data.txt

В wireshark был зафиксирован процесс передачи файла.

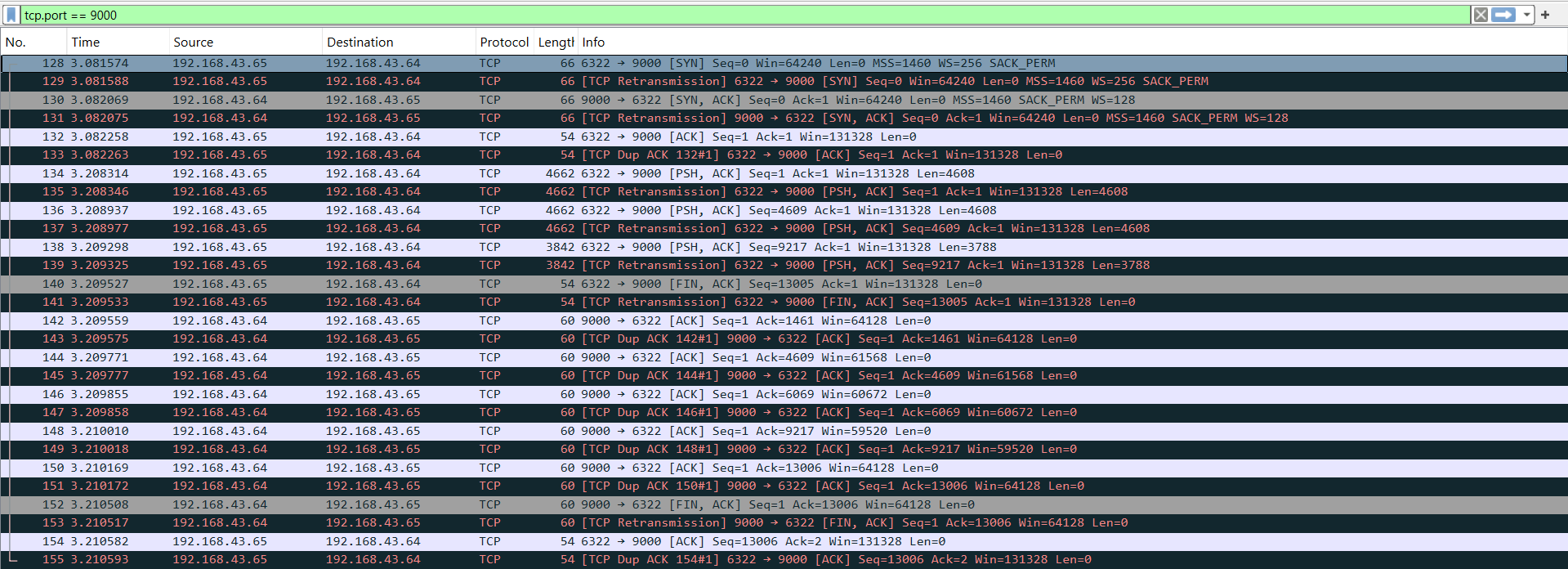


Рисунок 1 – Процесс передачи данных

Значение параметров и полей tcp-пакетов представлены в таблице ниже.

Таблица 1 – Заголовок tcp-пакета

| Параметр | Описание |
| --- | --- |
| Src port | Порт источника |
| Dst port | Порт назначения |
| Sequence number | Номер первого байта сегмента данных гарантирует, что данные принимаются в надлежащем порядке путем упорядоченного сегментирования и повторной сборки их на принимающей стороне. |
| Acknowledge number | Содержит следующий ожидаемый номер и подтверждает обратную связь вплоть до этого. |
| Data offset | Определяет размер заголовка пакета TCP в 4-байтных (4-октетных) словах. |
| Control Flags (9 bits):   * URG * ACK * PSH * RST * SYN * FIN | Управляющие флаги для регулирования обмена данными. Некоторые из важных флагов включают в себя:  SYN: отвечает за соединение отправителя и получателя.  ACK: подтверждение того, что отправитель получил данные.  FIN: сообщает, завершено ли TCP-соединение или нет.  RST: используется для сброса соединения при возникновении ошибки. |
| TCP Window | Количество байт данных начиная с последнего номера подтверждения, которые может принять отправитель данного пакета. |
| Checksum | Показывает, был ли заголовок поврежден во время транспортировки. |
| Urgent pointer | 16-битовое значение положительного смещения от порядкового номера в данном сегменте. Это поле указывает порядковый номер октета, которым заканчиваются важные (urgent) данные. Поле принимается во внимание только для пакетов с установленным флагом URG. |
| Options | Могут применяться в некоторых случаях для расширения протокола. |
| Data | Передаваемые данные |

## Способы обнаружения потайного хода

Обнаружить потайные ходы можно с помощью анализа сетевой активности: логгирования и сканирования открытых портов, открывающихся соединений, сопоставления портов с использующими их приложениями. Также необходимо проверять записи в планировщике, автозагрузке, смотреть запускаемые в ОС сервисы, чтобы выявить потенциальные вредоносные программы, которые могут запускаться незаметно. Для обнаружения потайного хода следует проводить аудит и использовать актуальный антивирус с обновленными базами сигнатур.

# Выводы

В ходе лабораторной работы была исследована передача файла между двумя ПК при помощи утилит netcat. С помощью wireshark был осуществлен захват tcp-траффика.