Министерство образования Республики Беларусь
Учреждение образования
БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

КАФЕДРА ИНФОРМАТИКИ

Лабораторная работа № 3

Атаки при установке TCP-соединения и протоколов прикладного уровня

Выполнил:
студент гр. 753502
Василюк В. И.

Проверил :
Протько М.И.

Минск, 2020

1. Введение

Целью данной лабораторной было:

1) Изучитьтеоретическиесведения ( ) изучение адресации в сети Internet, базовых сетевых протоколов (IP, TCP), атак, которые производятся на протокол TCP и его участников
2) Создать приложение, реализующее атаки на протокол при установке TCP-соединения и в рамках заданного протокола прикладного уровня.

   В интерфейсе приложения должны быть наглядно представлены:
   - Исходные данные протокола (модули, ключи, флаги, иные данные);
   - Данные, передаваемые по сети каждой из сторон;
   - Проверки, выполняемые каждым из участников.

1. Теоретические сведения

Адресация в сети Internet.

Типы адресов:

1. **Физический (MAC-адрес)**
2. **Сетевой (IP-адрес)**
3. **Символьный (DNS-имя)**

Компьютер в сети TCP/IP может иметь адреса трех уровней (но не менее двух):

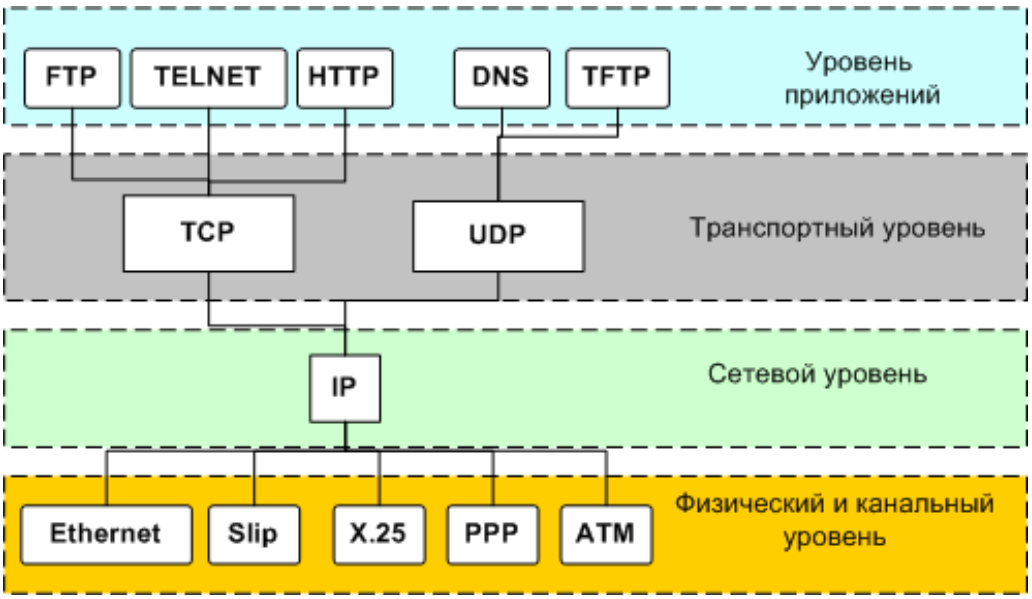
- Локальный адрес компьютера. Для узлов, входящих в локальные сети - это MAC-адрес сетевого адаптера. Эти адреса назначаются производителями оборудования и являются уникальными адресами.
- IP-адрес, состоящий из 4 байт, например, 109.26.17.100. Этот адрес используется на сетевом уровне. Он назначается администратором во время конфигурирования компьютеров и маршрутизаторов.
- Символьный идентификатор-имя (DNS), например, www.kstu.ru.

Базовые протоколы (IP, TCP)

Стек протоколов TCP/IP

TCP/IP - собирательное название для набора (стека) сетевых протоколов разных уровней, используемых в Интернет. Особенности TCP/IP:

- Открытые стандарты протоколов, разрабатываемые независимо от программного и аппаратного обеспечения;
- Независимость от физической среды передачи;
- Система уникальной адресации;
- Стандартизованные протоколы высокого уровня для распространенных пользовательских сервисов.



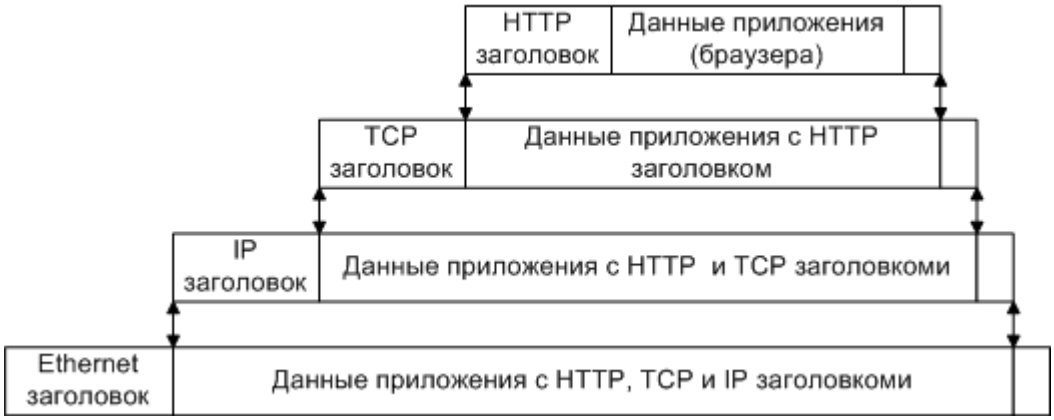
Стек протоколов TCP/IP

Стек протоколов TCP/IP делится на 4 уровня:

- Прикладной,
- Транспортный,
- Межсетевой,
- Физический и канальный.

Позже была принята 7-ми уровневая модель ISO.

Данные передаются в пакетах. Пакеты имеют заголовок и окончание, которые содержат служебную информацию. Данные, более верхних уровней вставляются, в пакеты нижних уровней.



Пример инкапсуляции пакетов в стеке TCP/IP

Физический и канальный уровень.

Стек TCP/IP не подразумевает использования каких-либо определенных протоколов уровня доступа к среде передачи и физических сред передачи данных. От уровня доступа к среде передачи требуется наличие интерфейса с модулем IP, обеспечивающего передачу IP-пакетов. Также требуется обеспечить преобразование IP-адреса узла сети, на который передается IP-пакет, в MAC-адрес. Часто в качестве уровня доступа к среде передачи могут выступать целые протокольные стеки, тогда говорят об IP поверх ATM, IP поверх IPX, IP поверх X.25 и т.п.

Межсетевой уровень и протокол IP.

Основу этого уровня составляет IP-протокол.

IP (Internet Protocol) – интернет протокол.

Первый стандарт IPv4 определен в RFC-760 (DoD standard Internet Protocol J. Postel Jan-01-1980)

Последняя версия IPv6 - RFC-2460 (Internet Protocol, Version 6 (IPv6) Specification S. Deering, R. Hinden December 1998).

Основные задачи:

- Адресация
- Маршрутизация
- Фрагментация датаграмм
- Передача данных

Транспортный уровень

Протоколы транспортного уровня обеспечивают прозрачную доставку данных между двумя прикладными процессами. Процесс, получающий или отправляющий данные с помощью транспортного уровня, идентифицируется на этом уровне номером, который называется номером порта. Таким образом, роль адреса отправителя и получателя на транспортном уровне выполняет номер порта (или проще - порт).

Анализируя заголовок своего пакета, полученного от межсетевого уровня, транспортный модуль определяет по номеру порта получателя, какому из прикладных процессов направлены данные, и передает эти данные соответствующему прикладному процессу. Номера портов получателя и отправителя записываются в заголовок транспортным модулем, отправляющим данные; заголовок транспортного уровня содержит также и

другую служебную информацию; формат заголовка зависит от используемого транспортного протокола.

На транспортном уровне работают два основных протокола: UDP и TCP.

Протокол надежной доставки сообщений TCP

TCP (Transfer Control Protocol) – протокол контроля передачи, протокол TCP применяется в тех случаях, когда требуется гарантированная доставка сообщений.

Первая и последняя версия TCP - RFC-793 (Transmission Control Protocol J. Postel Sep-01-1981).

Основные особенности:

- Устанавливается соединение.
- Данные передаются **сегментами**. Модуль TCP нарезает большие сообщения (файлы) на пакеты, каждый из которых передается отдельно, на приемнике наоборот файлы собираются. Для этого нужен **порядковый номер (Sequence Number - SN)** пакета.
- Посылает запрос на следующий пакет, указывая его номер в поле **"Номер подтверждения" (AS).** Тем самым, подтверждая получение предыдущего пакета.
- Делает проверку целостности данных, если пакет битый посылает повторный запрос.

Структура дейтограммы TCP. Слова по 32 бита.

Назначение портов

По номеру порта транспортные протоколы определяют, какому приложению передать содержимое пакетов.

Порты могут принимать значение от 0-65535 (два байта 2^16).

Номера портам присваиваются таким образом: имеются стандартные номера (например, номер 21 закреплен за сервисом FTP, 23 - за telnet, 80 - за HTTP), а менее известные приложения пользуются произвольно выбранными локальными номерами (как правило, больше>1024), некоторые из них также зарезервированы.

Программа Ping

Программа для проверки соединения и работы с удаленным хостом.

Программа TraceRoute - позволяет проверить маршрут до удаленного хоста.

Программа nmap - позволяет сканировать порты.

3. Атаки на протокол TCP и его участников

Слабость TCP в том, что реализация протокола предполагает «честное» поведение всех участников сети. В результате злоумышленник может получить доступ к передаваемым данным, выдать себя за другую сторону, привести систему в нерабочее состояние

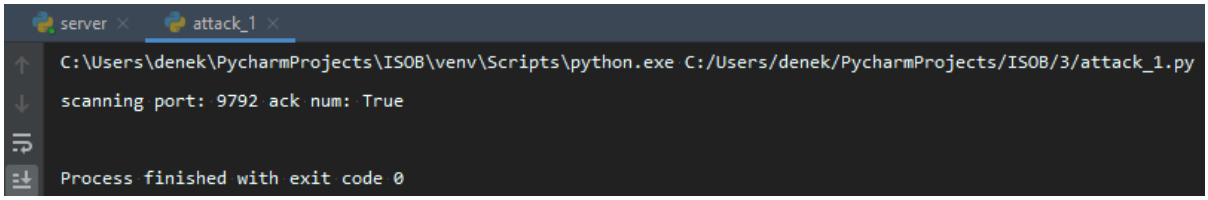
1) Passive scan -пассивное сканирование портов SYNc-(SYNs-ACKc)-RSTc и SYNc-RSTs. При достаточно умном поведении сканера (например, сканирование с низкой скоростью или проверка лишь конкретных портов) детектировать пассивное сканирование невозможно, поскольку оно ничем не отличается от обычных попыток установить соединение.

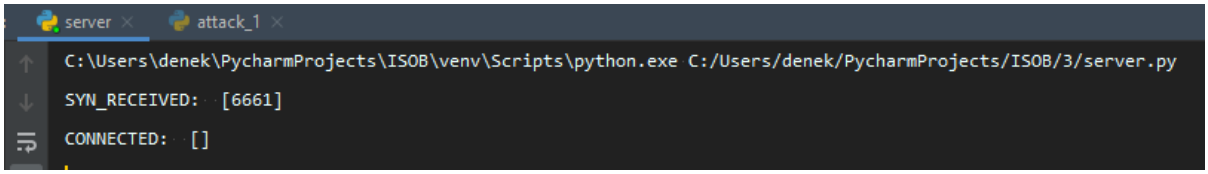
2) SYN Flooding –затопление полуоткрытыми сессиями, переполняющими очереди сервера, после чего сервер перестает отвечать на запросы легитимных клиентов. Зачастую достаточно 50-100 ложных сессий и сервер будет «тормозить»

3) TCP FullConnection Flooding.Атаку SYN flood удерживает большое число соединений на атакуемом узле в состоянии SYN-RECEIVED. Но, состояния множество ESTABLISHED и FIN-WAIT-1 также вызываютDoS.C сервером-жертвой создаётся множество легитимных полных троекратных TCP соединений с одного узла (до 65 000 штук по количеству портов для сокета), что истощит очередь сессий

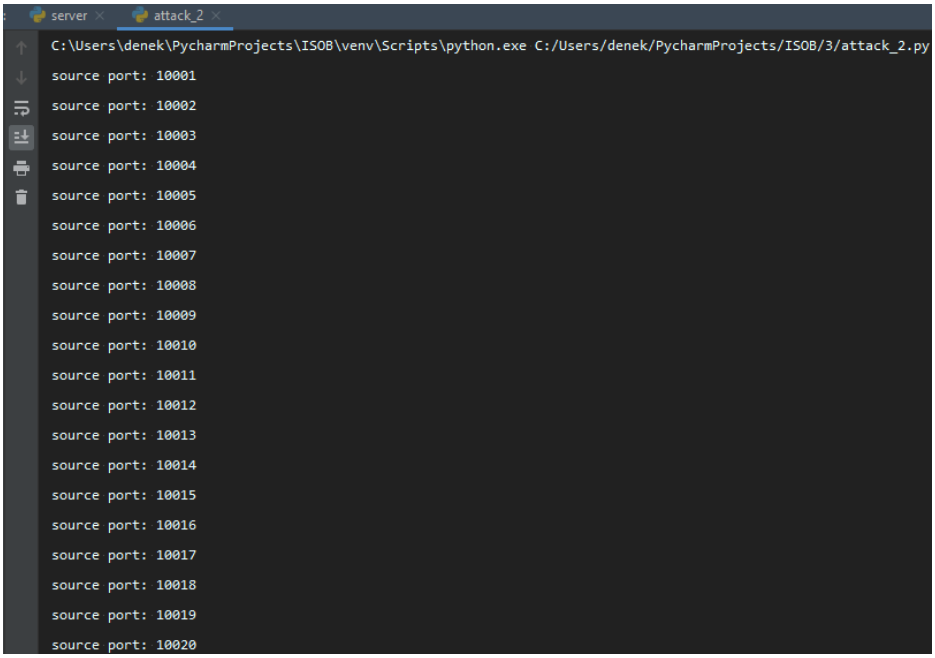
3. Атаки на протокол TCP и его участников

1) Passive scan





2) SYN Flooding



3) TCP Full Connection Flooding