МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное
учреждение высшего образования
Дальневосточный федеральный университет

ШКОЛА ЕСТЕСТВЕННЫХ НАУК

Кафедра информационной безопасности

О Т Ч Е Т

о прохождении учебной (по получению первичных профессиональных умений и навыков, в том числе первичных умений и навыков научно-исследовательской деятельности) практики

Выполнил студент
гр. С8118-10.05.01-1СПЕЦ
_____ Площинский В.Ю.
(подпись)

Отчет защищен с оценкой

_____
_____ С.С. Зотов
(подпись) (И.О. Фамилия)
« 31 » июля 2021 г.

Руководитель практики
Старший преподаватель кафедры
информационной безопасности ШЕН
_____ С.С. Зотов
(подпись) (И.О. Фамилия)

Регистрационный № _____
« 31 » июля 2021 г.

_____ Е.В. Третьяк
(подпись) (И.О. Фамилия)

Практика пройдена в срок
с « 19 » июля 2021 г.
по « 31 » июля 2021 г.
на предприятии
Кафедра информационной безопасности ШЕН ДВФУ

г. Владивосток
2021

Оглавление

Задание на практику

- Проведение исследования DDoS и примерах защиты от него.

- Написание отчета по практике о проделанной работе.

Введение

Учебная (по получению первичных профессиональных умений и навыков, в том числе первичных умений и навыков научно-исследовательской деятельности) практика проходила на кафедре информационной безопасности ШЕН ДВФУ в период с 19 июля 2021 года по 31 июля 2021 года.

Целью прохождения практики является приобретение практических и теоретических навыков по специальности, а также навыков оформления проведенного исследования в отчетной форме.

Задачи практики:

1. Ознакомиться с DDoS и защитой от них.

2. Ознакомиться с методами защиты от DDoS атак и рассмотреть один из них.

3. На основе полученных знаний написать отчет по практике о проделанной работе.

Пример реализации защиты от DDoS-атаки принципом псевдослучайной смены сетевого адреса внутри сессии

Аннотация:

В рассматриваемой работе предлагается способ защиты от распределенных атак типа «отказ в обслуживании», основанный на механизмах защиты на уровне протоколов.

Введение:

Атака типа «отказ в обслуживании» (DoS) характеризуется как явная попытка предотвратить легитимное использование службы; распределенная атака типа «отказ в обслуживании» (DDoS) подразумевает участие нескольких атакующих лиц для достижения этой цели. Такой результат достигается путем специальных действий атакующей стороны, результатом которых становится исчерпывание ограниченных ресурсов жертвы атаки. В качестве этих ресурсов может быть выбрана пропускная способность сети жертвы, вычислительные возможности и так далее.

Принцип псевдослучайной смены сетевого адреса внутри сессии

Для обеспечения снижения нагрузки на сервер от производящих атаку «ботов» и исключения блокировки пакетов от легитимного клиента используется смена адреса сервера по расписанию, известному только авторизованному пользователю. Боты не получают достоверной информации о расписании смены адресов и не могут посылать запросы на адрес сервера, таким образом, теряя возможность создать значительную нагрузку, нарушающую нормальное функционирование ресурса.

Предлагаемое решение аналогично тому, как делается это в радиотехнических системах с перескоком частоты. Приемник и передатчик в течение интервала передачи одного сообщения переходят с одной частоты на другую синхронно, тем самым обеспечивая непрерывный процесс передачи информации. Передатчик злоумышленника, пытающийся поставить помеху приемнику или прослушать канал, не знает расписания смены частот и потому не может создать значительного ущерба работе, защищенной с помощью перескока частоты радиолинии. В данном случае роль частоты играет IP-адрес, и клиент должен знать, по какому расписанию он изменяется у сервера. При этом расписание не должно быть открытым для внешних наблюдателей.

Принцип замены адреса в принимаемых пакетах применяется в настоящее время в маршрутизаторах Интернет при использовании технологии Network Address Translation (NAT). В отличие от предлагаемого способа эта замена осуществляется путем назначения соответствия переменного внешнего адреса устройства на период сессии из пула адресов внутреннему постоянному адресу. Этот механизм используется для обеспечения коллективного использования внешних сетевых адресов большим числом устройств, не имеющих необходимости постоянного соединения через Интернет. Все пакеты, поступающие к устройству, должны иметь одинаковый IP-адрес в течение всей сессии, поэтому такое использование преобразования адресов не решает поставленной в данной работе задачи.

Способ защиты от атак, основанный на прыгающей адресации Интернет-ресурса, включает в себя то, что DNS-серверы содержат записи не об IP-адресе защищаемого ресурса, а об IP-адресе сервера авторизации. Для того чтобы получить доступ к Интернет-серверу, клиент должен пройти авторизацию на предмет того, является ли он доверенным для этого сервиса. Если авторизация, которая может быть основана не только на проверке установленного у пользователя соответствующего сертификата, но и на наличии подписки на сервис, пройдена успешно, то терминалу клиента сообщается IP-адрес сервера, который выполняет роль контроллера расширенных защищенных соединений Интернет-сервиса и подключенных к нему клиентов. В данной работе под такими соединениями понимаются сессии передачи данных между терминалом пользователя и Интернет-ресурсом, которые проводятся при помощи динамической смены адресов назначения и отправителя передаваемых пакетов. Авторизованный пользователь устанавливает зашифрованное соединение с контроллером, по которому ему передается пул IP-адресов или ключ генерации псевдослучайной последовательности адресов для осуществления прыгающей адресации. После получения или генерирования этого набора IP-адресов клиент начинает обращение к Интернет-ресурсу по какому-то зафиксированному «инициальному» адресу. Но при этом адрес назначения каждого следующего отправляемого пакета определяется терминалом пользователя динамически из полученного пула адресов путем расчета специальной хэш-функции, которая отображает значение поля timestamps в заголовке TCP-протокола передаваемого пакета и идентификатора текущей расширенной защищенной сессии. Этот идентификатор может быть определен как по private key сертификата, установленного на терминале, так и передан контроллером сессий. Таким образом, осуществляется изменение адреса получателя TCP-пакетов, отправляемых от клиента к Интернет-ресурсу, с фиксированного «инициального» адреса на виртуальный, рассчитанный по псевдослучайному закону.

Упоминающийся здесь пул IP-адресов не содержит адреса Интернет-сервера, защита которого осуществляется посредством предлагаемого метода. Этот набор формируется из адресов, которые принадлежат одному или более высокопроизводительному маршрутизатору в Автономной системе или подсети, которые имеют соответствующее соглашение об использовании своих ресурсов для реализации предлагаемой системы. Контроллер защищенных сессий сообщает каждому такому роутеру идентификатор новой сессии и адрес клиента, с которым должно поддерживаться это расширенное соединение. Когда роутер получает пакет от такого клиента, производится расчет хэшфункции, отображающей идентификатор этой сессии и поле timestamps в заголовке TCP-протокола этого пакета. Если рассчитанный IP-адрес совпадает с адресом назначения принятого пакета, то этот пакет перенаправляется на реальный адрес Интернет-ресурса. В противном случае пакет отбрасывается. Ответы Интернет-ресурса подвергаются такой же процедуре, но не с адресом назначения пакета, а с адресом отправителя. При получении этих пакетов терминалом клиента виртуальный адрес заменяется на его инициальный IP-адрес.

В итоге получается, что для внешнего наблюдателя сессии передачи данных между Интернет-ресурсом и авторизованным клиентом IP-адрес Интернет-сервиса регулярно меняется. Замена IP-адреса защищаемого сервера происходит с каждым инкрементом значения поля timestamps, что обычно соответствует одной миллисекунде.

Предсказание IP-адреса назначения следующего пакета крайне затруднено для стороннего терминала и зависит от параметров псевдослучайной последовательности, по закону которой изменяется виртуальный адрес защищенного сервера для данного конкретного терминала доверенного пользователя.

Выигрыш в устойчивости к атаке для такого метода можно оценить исходя из следующих соображений. Пусть атакующая сторона располагает ресурсами для силовой атаки интенсивностью N (ГБ/с). Если атака будет

направлена на известный сетевой адрес сервера-жертвы, то вся эта интенсивность должна быть обработана сервером как нагрузка, если необходимо обеспечить его функционирование в условиях атаки. В соответствии с данным методом атака на любой из адресов пула, состоящего из m адресов, будет иметь интенсивность не более чем N/m (ГБ/с). Следовательно, можно считать, что сервер будет оставаться в режиме функционирования, если сможет обработать такую нагрузку, в m раз меньше, чем мощность атаки. Таким образом, величина размера пула адресов для реализации описываемого метода может считаться оценкой выигрыша устойчивости к силовой атаке. Работая в сетях с адресацией IP v6, можно иметь пулы размером в несколько тысяч адресов, что будет означать выигрыши в устойчивости в десятки и сотни раз, что может позволить снова опередить возможности атакующей стороны в процессе борьбы «брони и снаряда» на данном этапе.

Если пул IP-адресов прыгающей адресации недостаточно велик, то боты могут осуществить атаку на каждый из адресов этого пула, используя IP-спуфинг для того, чтобы замаскировать злокачественный трафик под трафик реального пользователя. В этом случае роутеры перенаправят часть потока пакетов, включая легитимные и нелегитимные, на защищаемый Интернет-сервер. Для борьбы с этой уязвимостью описываемый метод от атак предполагает следующее:

Как было описано выше, пул IP-адресов, использующихся для прыгающей адресации, достаточно велик, чтобы сделать такую избыточную атаку крайне ресурсоемкой и неэффективной для атакующей стороны.

Сети Интернет-провайдеров, через которые передается трафик от легитимного пользователя к Интернет-ресурсу, должны осуществлять фильтрацию пакетов, которые подверглись IP-спуфингу.

В итоге, предлагаемый метод позволяет присваивать каждому или группе серверов пул сетевых адресов достаточно большого размера и изменять текущий адрес сервера при передаче каждого или группы пакетов по

псевдослучайному закону. Авторизованные клиенты получают ключ к последовательности адресов и производят установление соединения по стандартным протоколам типа TCP, тогда как неавторизованные клиенты и боты могут проводить атаку только в целом на пул адресов, что снижает эффективность атаки или вероятность перехвата трафика в число раз пропорциональное размеру пула.

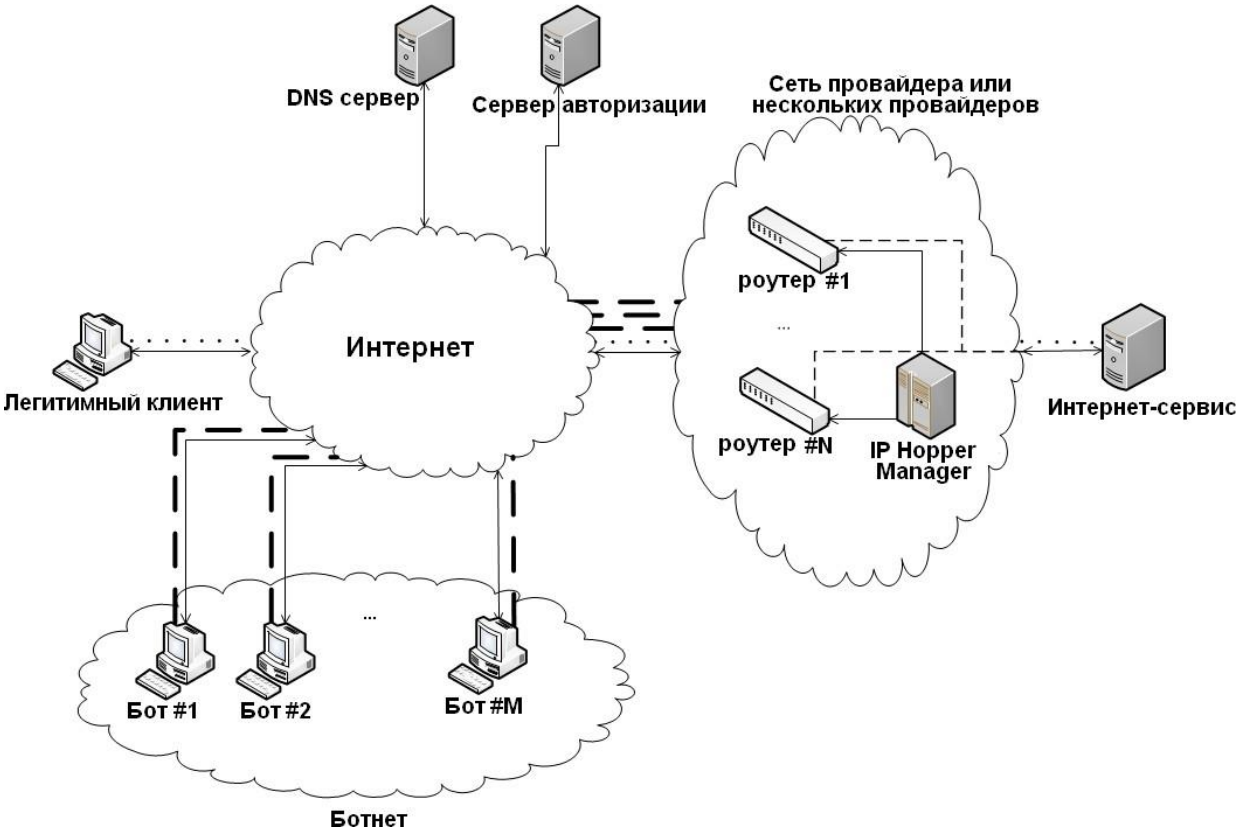
Имплементация прототипа

Как описывалось ранее, одним из основных принципов построения системы защиты от атак является принцип применимости на практике. Поэтому предлагаемую реализацию механизма осуществления прыгающей адресации IP-адресов создадим в виде модуля ядра операционной системы GNU/Linux. В этом случае для разворачивания такой системы будет достаточно установить на роутеры, построенные на базе операционной системы GNU/Linux, этот модуль ядра и настроить его работу соответствующим образом. В данном исследовании такие роутеры будут представлять собой компьютеры с несколькими сетевыми интерфейсами под управлением системы Debian.

Ядро Linux содержит в себе встроенный межсетевой экран (брандмауэр) — Netfilter, который осуществляет фильтрацию и перенаправление пакетов, согласно установленным пользователем набором правил при помощи утилиты iptables.

Основная идея реализации метода заключается в следующем: IP Hopper Manager, осуществляющий управление расширенными защищенными соединениями, при помощи утилиты netfilter добавляет новый набор правил в цепочку PREROUTING для каждого роутера, участвующего в поддержке процесса обмена пакетами между сервером и клиентом по алгоритму

прыгающей адресации



Простейшее представление схемы атаки на защищенный по описанному методу Интернет-сервер

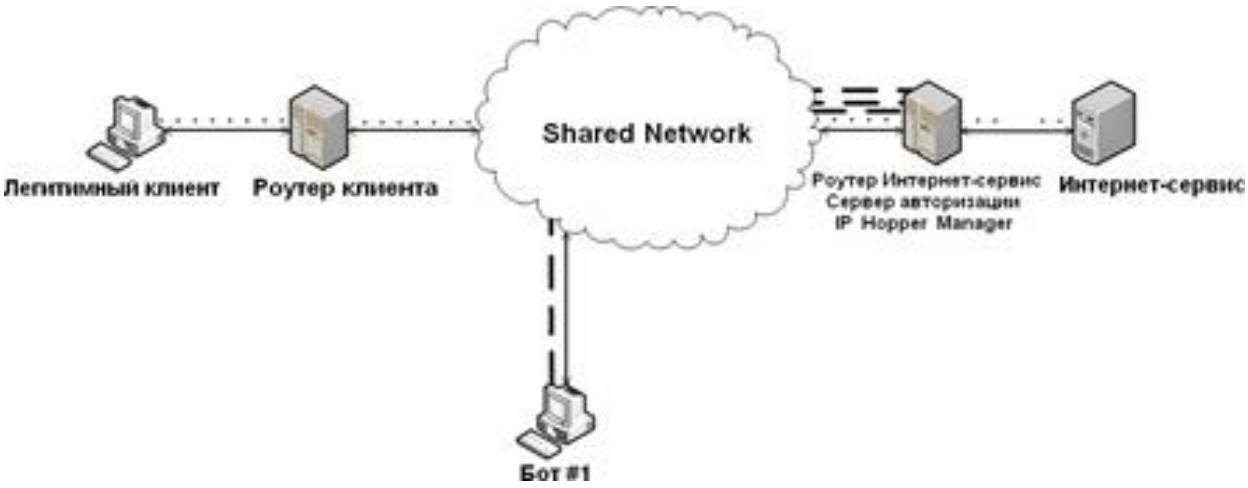
Этот новый набор правил осуществляет проверку того, что полученный пакет адресован на корректный виртуальный IP-адрес сервера. Если поле адреса назначения удовлетворяет этому условию, то пакет перенаправляется на физический адрес защищаемого сервера, иначе пакет отбрасывается. Для всех отправляемых сервером клиенту пакетов этот же набор правил осуществляет замену IP-адреса источника на корректный виртуальный адрес сервера для конкретного значение timestamps этого пакета.

Такое расширение netfilter требует создания нового модуля ядра Linux, который производит описанные выше операции с получаемыми и отправляемыми пакетами.

Результаты тестирования прототипа

Первая реализация метода прыгающей адресации Интернет-сервиса была протестирована на стенде, построенном на виртуальных машинах под управлением операционной системы Debian. Целью этого испытания являлась демонстрация того, что применение динамической смены IP-адреса защищаемого севера по описанным правилам позволит существенным образом уменьшить нагрузку на жертву путем исключения из входящего трафика потока запросов от нелегитимных пользователей.

Используемый тестовый стенд можно изобразить следующим образом:



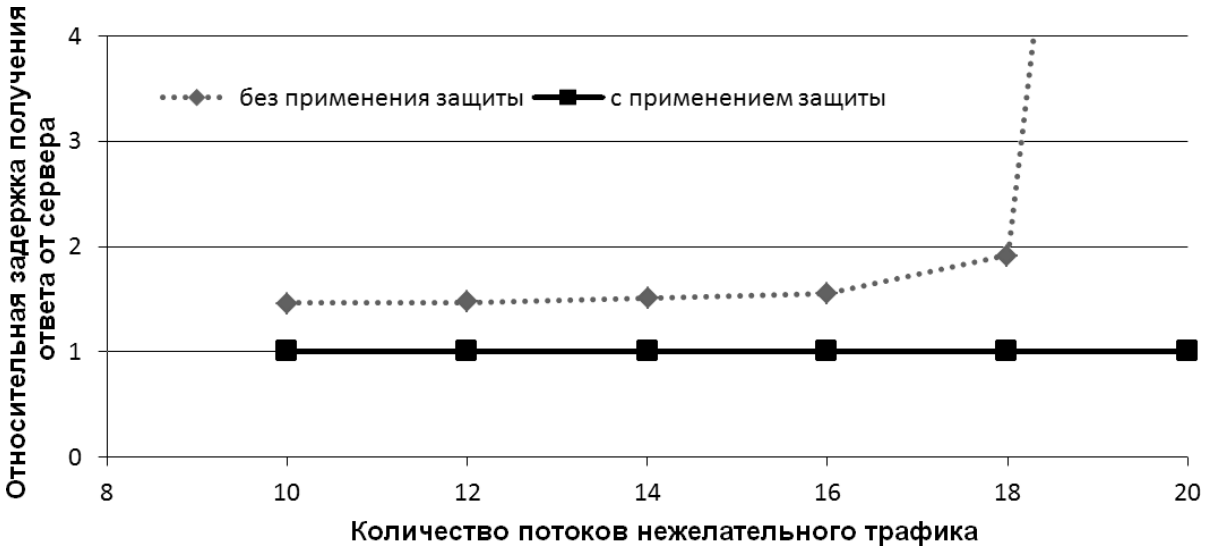
Тестовый стенд

Для упрощения процесса тестирования и снижения требований, выставляемых к техническим характеристикам компьютера, на котором запускается эта экспериментальная система, атака типа «отказ в обслуживании» осуществляется только с одного «бота». Это упрощение по-прежнему позволяет пронаблюдать эффективность фильтрации трафика в случае простейших атак на защищаемый сервер. В эксперименте атака проводилась при помощи программного продукта LOIQ, которая предоставляет удобный инструментарий для нагрузочного тестирования и атак.

В данном эксперименте сеанс передачи информации между легитимным клиентом и защищаемым сервером был симулирован путем открытия клиентом обновляемой автоматически HTML-страницы, что обеспечивало

постоянный обмен TCP-пакетами между машиной легитимного клиента и сервером. Объем входящего полезного трафика для сервера составлял порядка 8 Кб/сек.

Для наблюдения эффекта, вызываемого маломощной атакой в рамках построенного тестового стенда, активировали LOIQ во время передачи данных между клиентом и сервером, постепенно увеличивая количество одновременных потоков атаки от 10 до 20. В итоге можно было наблюдать, что нагрузка на сетевой интерфейс и скорость ответа сервера на запросы пользователя существенно возросла. Полученные результаты приведены на графике.



Сравнение время отклика сервера в случае атаки с применением предлагаемого метода защиты и без нее.

Если же в рамках этого тестового стенда применить метод динамической адресации, то IP-адрес виртуальной машины, играющей роль сервера-жертвы, станет недоступен для всех внешних клиентов, кроме авторизованного легитимного пользователя. Поэтому, когда повторили эти же тесты с использованием рассматриваемого метода, то проявления атаки на сервер не наблюдались.

При анализе полученных результатов надо учитывать, что весь стенд был запущен на одном физическом компьютере с использованием только одного роутера, построенного на базе виртуальной машины под управлением операционной системы Debian. Очевидно, что этот маршрутизатор,

осуществляющий фильтрацию нежелательного трафика, обладает ограниченной невысокой производительностью, что оказывает существенное влияние на наблюдаемые эффекты при проведении атаки на сервер с использованием порядка 20 потоков.

В ходе проведенного тестирования видно, что способ эффективно фильтрует нежелательный трафик в ходе атак на защищаемый сервер.

Заключение

Рассмотрен метод псевдослучайной замены адресов Интернет-ресурса для повышения устойчивости Интернет-серверов к атакам и перехвату трафика сторонними наблюдателями. Предложенная система скрывает реальный IP-адрес сервера за большим числом «виртуальных» IP-адресов. Соответствие между реальным IP-адресом и каким-либо «виртуальным» определяется динамически для каждой конкретной сессии передачи данных в каждый конкретный момент времени, и это установленное соответствие меняется каждую миллисекунду. Представленный подход является распределенным, разделяя весь трафик от легитимных пользователей и производящих атаку ботов на отдельные потоки, что также позволяет снизить нагрузку на сетевое оборудование в ходе, действующей атаки.

Список используемых источников

1) Saravanan Kumarasamy, R. Asokan, «Distributed Denial of Service (DDoS) Attacks Detection Mechanism» [Электронный ресурс] – Электрон. дан. – Режим доступа: https://arxiv.org/abs/1201.2007

2) Saravanan Kumarasamy, R. Asokan «An Efficient Detection Mechanism for Distributed Denial of Service (DDoS) Attack» [Электронный ресурс] – Электрон. дан. – Режим доступа: https://arxiv.org/abs/1302.5158

3) Краснов Андрей Евгеньевич, Надеждин Евгений Николаевич, Никольский Дмитрий Николаевич, Галяев Владимир Сергеевич, Зыкова Евгения Андреевна «Способ защиты от атак на основе классификации трафика» [Электронный ресурс] – Электрон. дан. – Режим доступа: https://www.elibrary.ru/item.asp?id=41323806

4) Семён Владимирович Камышев, Игорь Николаевич Карманов «Проблемы атак в современной IT-индустрии методы защиты от них» [Электронный ресурс] – Электрон. дан. – Режим доступа: https://www.elibrary.ru/item.asp?id=35661015

5) В. В. Крылов, К. Н. Кравцов «Защита IP-подсетей от DDoS-атак и несанкционированного доступа методом псевдослучайной смены сетевых адресов» [Электронный ресурс] – Электрон. дан. – Режим доступа: https://www.elibrary.ru/item.asp?id=22485189