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
_____ Серов В.В.
(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 на тему “методы обнаружения и защиты от DDoS-атак”

- 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 методами обнаружения и защиты от DDoS-атак.
2. На основе полученных знаний написать отчет по практике о проделанной работе.

Методы обнаружения и защиты от DDoS-атак.

Аннотация:

В рассматриваемой работе предлагается анализ различных методов обнаружения DDoS-атак. Показаны основные методы защиты от DDoS-атак. Выполнена классификация методов обнаружения и предотвращения DDoS-атак. Приведены последствия от DDoS-атаки, а также рекомендации по предотвращению атак данного типа.

Введение:

Распространение в интернете атак типа «отказ в обслуживании» делает актуальным как никогда потребность в разработке методов защиты и обнаружения атак данного типа. Существует огромное множество типов DDoS-атак, однако, как правило их принято делить на три основные категории:

1) Поток или объемные атаки. Этот тип атак направлен на использование всей доступной полосы пропускания центра обработки данных или сети, такого как наводнения по протоколу пользовательских дейтаграмм (UDP), наводнения по протоколу управляющих сообщений Интернета (ICMP) и система доменных имен (DNS) отражение. В результате законный пользователь больше не может подключаться или получать доступ к нужным серверам или приложениям.

2) Атаки состояния подключения. Все сетевые устройства или системы имеют внутренние таблицы с некоторыми ограниченными ресурсами/возможностями, которые используются для отслеживания активных или отключенных соединений. При таком типе атаки таблица заполняется множеством соединений, поэтому новый пользователь не может установить соединение. Иногда эти атаки приводят к сбоям устройства, в результате чего все активные пользователи теряют соединение.

3) Атаки на уровне приложений – при этих типах атак серверы приложений перегружены таким количеством запросов на ресурсы, что используются все доступные ресурсы.

Основные методы защиты от DDoS-атак:

1. Предотвращение - необходимо проводить профилактику причин, которая приводят к необходимости тем или иным лицам предпринимать DDoS-атаки. Личная неприязнь, конкуренция, религиозные или иные разногласия, а также многие другие факторы могут стать причиной такой атаки. Если вовремя устранить причины таких атак и сделать соответствующие выводы, то в дальнейшем удастся избежать повторения ситуации. Данный метод нацелен на защиту от любых DDoS-атак. Это является управленческим, а не техническим решением.
2. Ответные меры - необходимо проводить активные меры по воздействию на источники или организатора атак, используя как технические, так и организационно-правовые методы. Некоторые компании предоставляют сервис поиска организатора атак, который позволяет вычислить не только человека, проводящего атаку, но и заказчика данной атаки.
3. Специализированное программное и аппаратное обеспечение - сейчас многие производители программного и аппаратного обеспечения предлагают готовые решения для защиты от DDoS-атак. Это может выглядеть как небольшой сервер, который позволяет защититься от слабых и средних DDoS-атак, нацеленных на малый и средний бизнес, так и целый комплекс, позволяющий защитить от серьезных атак крупные предприятия и правительственные госорганы.
4. Фильтрация - фильтрация и блокировка трафика, исходящего от атакующих компьютеров позволяет снизить или вовсе загасить атаку. При использовании этого метода входящий трафик фильтруется в соответствии с теми или иными правилами, заданными при установке фильтров. Можно

выделить 2 способа фильтрации: маршрутизация по спискам ACL и использование межсетевых экранов.

Использование списков ACL позволяет фильтровать второстепенные протоколы, не затрагивая при этом протоколы TCP и не замедляя скорость работы пользователей с ресурсом. Однако, при использовании злоумышленниками первостепенных запросов или ботнета, данный способ фильтрации окажется неэффективным. Обычно межсетевые экраны являются крайне эффективным способом защиты от DDoS-атак. Однако они применимы исключительно для защиты частных сетей.

5. Обратный DDoS - перенаправление трафика на атакующего при достаточных серверных мощностях позволяет не только успешно преодолеть атаку, но и вывести из строя оборудование атакующего. Данный тип защиты невозможно применить при ошибках в программном коде ОС, системных служб или веб-приложений.

6. Устранение уязвимостей - данный тип защиты нацелен на устранение ошибок в тех или иных системах или службах. Такой метод защиты не работает против флуд-атак, для которых «уязвимостью» является конечность тех или иных системных ресурсов.

7. Наращивание ресурсов - не дает абсолютной защиты, но позволяет использовать другие виды защиты от DDoS-атак. Имея современное программное и аппаратное обеспечение, можно удачно справиться с DDoS-атакой, направленной на конечность системных ресурсов.

8. Построение распределенных систем – построение распределенных и дублирующих систем позволяет обслуживать пользователей, даже если некоторые узлы становятся недоступны из-за DDoS-атак. Рекомендуется строить распределенные системы, используя не только различное сетевое или серверное оборудование, но и физически разносить сервисы по разным Дата-центрам. Также возможна установка дублирующей системы на территории других государств, что позволит сохранить важную информацию.

9. Уклонение - вывод непосредственной цели атаки от других ресурсов, которые также могут подвергаться атаки вместе с целью. В таком случае необходимо разделить атакуемые ресурсы и другие рабочие ресурсы, которые расположены на одной площадке. Оптимальным является решение по разделению на внешние и внутренние ресурсы и вывод внешних ресурсов на другое сетевое оборудование. Это позволит сохранить внутреннюю ИТ-структуру даже при самой интенсивной DDoS-атаке на внешние ресурсы.
10. Мониторинг - установка системы мониторинга и оповещения, которая позволит вычислить DDoS-атаку по определенным критериям. Мониторинг напрямую не может защитить атакуемую систему, но позволяет вовремя среагировать и принять соответствующие меры.
11. Приобретение сервиса по защите от DDoS-атак - сейчас многие крупные компании предлагают предоставление как постоянного, так и временного сервиса по защите от DDoS-атак. Данный метод позволяет защититься от многих типов DDoS-атак, используя целый комплекс механизмов фильтрации нежелательного трафика к атакующим серверам.

Методы обнаружения и предотвращения DDoS-атак

Обнаружение является одним из ключевых шагов в защите от DDoS атак. Однако из-за большого числа типов DDoS-атак обнаружение таких атак становится проблематичным. Качественный метод обнаружения должен иметь малое время работы и низкий процент ложных срабатываний. Обнаружение DDoS-атак зачастую представляет собой часть более широкой системы обнаружения вторжений (IDS). IDS можно определить как программное или аппаратное обеспечение, используемое для обнаружения несанкционированного трафика или действий, которые противоречат разрешенной политике данной сети. IDS могут быть классифицированы на основе расположения источника аудита как основанные на хосте, основанные на сети или как комбинация обоих. В первом варианте выполняется мониторинг данных аудита, таких как лог-файлы приложений и операционной системы, и IDS располагается на каждом хосте. Во втором

варианте выполняется мониторинг сетевого трафика, и IDS располагается на машине отдельно от хостов, которые она защищает. Гибридные системы обнаружения вторжений объединяют оба описанных типа.

Обзор систем обнаружения вторжений.

Сетевые IDS обычно классифицируются на основе используемого метода обнаружения: метод на основе сигнатур или на основе обнаружения аномалий. Первый метод позволяет выявить атаку, сравнивая известные сигнатуры атак или шаблоны с отслеживаемым трафиком. Совпадение сигнализирует о потенциальной атаке. Этот метод имеет малое время работы, позволяет обнаруживать большинство известных атак, и, как правило, имеет низкую частоту ложных срабатываний, иначе говоря, не создает сигнал тревоги для легального трафика. Однако IDS на основе аномалий, также известные как основанные на поведении, работают, сравнивая поведение сетевого трафика с предыдущим «нормальным» поведением трафика. Любое отклонение считается признаком атаки. Система приобретает нормальный профиль трафика обычно посредством обучения и отслеживает трафик на предмет любых различий с нормальным профилем. Обученный трафик используется для определения порогового значения для будущего обнаружения. Выявленные аномалии помогают обнаружить неизвестные атаки; однако применение этого метода приводит к более частым ложным срабатываниям, чем сигнатур-основанные системы. На практике системы могут сочетать как сигнатурные, так и аномальные методы.

Методы обнаружения DDoS-атак.

Одним из ключевых параметров методики обнаружения DDoS является время обнаружения. Механизм обнаружения должен обнаружить атаку, прежде чем сервис начнет деградировать. Однако пакеты DDoS-трафика часто неотличимы от пакетов пользователей. Это затрудняет обнаружение и увеличивает шансы ложного срабатывания, что является критической проблемой в обнаружении атаки. Качественный метод обнаружения должен реагировать быстро и иметь низкую частоту ложных срабатываний. В общем

случае классификация систем обнаружения DDoS атак аналогична классификации систем обнаружения вторжений.

Обнаружение атак на основе сигнатур. Идентификация на основе сигнатур обычно используется для идентификации известных типов атак. Для обнаружения атаки не требуется какое-либо описание типичных действий при ней, однако для обнаружения этих видов атак необходима база данных с известными сигнатурами атак. Для обнаружения вируса или червя не требуется подробное описание его действий: как червь находит цель, как он распространяет себя или какие участки памяти он использует. При обнаружении на основе сигнатур полезная нагрузка исследуется и обрабатывается независимо от того, содержит ли она червя. Один огромный тест системы обнаружения вторжений на основе сигнатур состоит в том, что для каждой сигнатуры требуется раздел в базе данных, поэтому вся база данных может содержать сотни или даже тысячи сигнатур. Каждый пакет должен быть сопоставлен с идентичным в базе данных. Этот процесс может быть очень ресурсоемким, он может использовать всю пропускную способность и сделает данный тип обнаружения уязвимым.

Обнаружение атак на основе аномалий. Методы обнаружения вторжений, основанные на противоречивости, распознают необычную активность и создают предупреждения аномалий в действиях системы или действиях приложений. Обычные специфические действия, которые могли бы быть перехвачены, включают: 1) злоупотребление системными соглашениями, например, скрытие интервала IP-адресов и выполнение стандартного соглашения на скрытом порту; 2) уникальные паттерны трафика, например, больше UDP-пакетов по сравнению с TCP; 3) подозрительные примеры в полезных данных приложения. Наибольшие трудности в использовании методов обнаружения на основе аномалий заключаются в определении типичного поведения системы, выборе предела для срабатывания предупреждения и предотвращении ложных предупреждений. Пользователи системы, как правило, люди, и их поведение трудно предвидеть. В том

случае, если обычная модель не будет охарактеризована подробным образом, возникнет множество ложных срабатываний, и система обнаружения будет испытывать негативные последствия неверного исполнения. В связи с развитием средств машинного обучения на сегодняшний день многие исследователи предпочитают применять алгоритмы машинного обучения и искусственные нейронные сети для обнаружения различных угроз.

Классификация архитектур предотвращения DDoS-атак в соответствии с местом их развертывания.

При обнаружении DDoS-атаки нельзя сделать ничего иного, кроме как вручную устранить проблему и отключить систему-жертву от сети. DDoS-атаки блокируют многие ресурсы, например, ограничивают мощность процессора и пропускную способность сети, память, время обработки и т. д. Основная цель любого механизма защиты от DDoS-атак – как можно скорее обнаружить DDoS-атаки и остановить их как можно ближе к их источникам. Схемы защиты от DDoS подразделяют на четыре класса в зависимости от места развертывания: источник, жертва, промежуточные маршрутизаторы и распределенный или гибридный защитный механизм.

Механизмы защиты, устанавливаемые на стороне источника атаки. В данном типе механизмов защиты от DDoS средства развернуты на стороне источника атаки, чтобы предотвратить создание DDoS-атак пользователями сети. При таком подходе устройства-источники идентифицируют вредоносные пакеты в исходящем трафике и фильтруют или ограничивают трафик. Обнаружение и предотвращение DDoS-атаки на источнике является наилучшей возможной защитой, поскольку легальному трафику наносится минимальный ущерб, однако недостатком данного механизма является то, что обнаружить саму DDoS-атаку является сложной задачей, так как источники широко распределены по сети, и один из источников может передавать обычный трафик. Также неприятным фактом является сложность развертывания системы на каждом источнике.

Механизмы защиты, устанавливаемые на стороне жертвы атаки. В этом типе механизмов защиты от DDoS жертва обнаруживает, фильтрует или ограничивает скорость вредоносного входящего трафика на маршрутизаторах сетей жертвы, т. е. сетей, предоставляющих веб-службы. Легальный и атакующий трафик можно четко определить, используя либо обнаружение вторжений на основе неправильного использования, либо обнаружение вторжений на основе аномалий. Однако трафик атаки, достигающий жертвы, может отказать или ухудшить качество услуг и резко сократить ширину полосы пропускания.

Механизмы защиты, устанавливаемые на промежуточных маршрутизаторах. Любой маршрутизатор в сети может независимо попытаться определить вредоносный трафик и фильтровать или ограничить скорость трафика. Он также может настраивать баланс между точностью обнаружения и потреблением полосы пропускания атаки. Обнаружение и отслеживание источников атак становится простым благодаря совместной работе нескольких маршрутизаторов сети. В этой точке защиты весь трафик объединяется, т. е. и атакующие, и легитимные пакеты прибывают в маршрутизатор, и это лучшее место для ограничения скорости всего трафика.

Распределенные или гибридные механизмы защиты. Данный тип защиты может быть лучшей стратегией против DDoS-атак. Механизмы гибридной защиты развертываются в нескольких местах, таких как источник атаки, жертвы или промежуточные сети, и обычно между точками развертывания осуществляется взаимодействие. Механизмы маршрутизаторов лучше всего подходят для ограничения скорости всех видов трафика, тогда как механизмы на стороне жертвы могут точно обнаружить трафик атаки в комбинации легитимных и атакующих пакетов. Поэтому использование данной стратегии защиты от DDoS может быть более выгодным.

Воздействие DDoS-атаки может иметь разрушительные последствия для организации с точки зрения финансов и бренда. Несколько часов отключения сети могут стоить миллионы долларов и разозлить тысячи

клиентов, которые полагаются на онлайн-сервисы. Прямые потери доходов могут быть высокими для организаций, которые в значительной степени полагаются на общедоступные услуги. DDoS-атаки еще более эффективны, когда они используются в сочетании с другими видами преступлений. Последствия DDoS-атаки могут включать в себя:

1) Ущерб бренду и репутации.

2) Нарушение договора и нарушение соглашений об уровне обслуживания.

3) Потеря доверия акционеров.

4) Прерывание обслуживания, приводящее, например, к выдаче клиентских кредитов, трудности возобновления бизнеса и потерянным продажам.

5) Расходы на маркетинг и рекламу, связанные с контролем ущерба.

Учитывая необычайные и быстрые изменения в методах DDoS-атак, традиционные решения для предотвращения DDoS-атак
более не являются достаточными для обнаружения и защиты сети или приложений организации от сложных DDoS-атак. Наиболее экономически эффективный подход к смягчению атак DDoS состоит в том, чтобы заплатить Интернет-провайдеру за обнаружение и смягчение атак до того, как они достигнут интернет-ресурсов организации (например, веб-серверов, серверов электронной почты). Ключевым моментом здесь является поставщик услуг Интернета с точки зрения его зрелости предлагаемых услуг, направленных на большинство форм атак DDoS. Кроме того, существует множество организаций, которые предоставляют услуги по снижению уровня DDoS и играют роль посредников. Их предложения включают такие вещи, как перенаправление DNS на изменения маршрута протокола пограничного шлюза (BGP), при котором входящий интернет-трафик проходит через них, и они обнаруживают атаки и выполняют очистку/фильтрацию в своих интернет-центрах обработки данных. В результате их клиенты получают фильтрованный и чистый интернет-трафик.

Различные поставщики систем безопасности предоставляют решения на

основе устройств для защиты от DDoS-атак. Они обнаруживают и обеспечивают защиту от широкого спектра DDoS-атак. Многие поставщики заявляют о решениях с различными моделями устройств и предлагают пропускную способность от 12 Мбит/с до решений корпоративного уровня. Кроме того, эти устройства интегрированы с пакетом центрального управления, предоставляя пользователям единую точку контроля и полный обзор событий безопасности. Поскольку DDoS-угрозы развиваются каждый день, эти специализированные поставщики, вероятно, будут быстрее реагировать с помощью инновационных решений, чем поставщики, которые предлагают базовую защиту от DDoS, встроенную в межсетевой экран и предложения ISP.

Успешное предотвращение DDoS-атак подразумевает наличие круглосуточных технологий непрерывного мониторинга и возможностей для выявления и обнаружения атак, позволяя легитимному трафику достигать места назначения. Кроме того, для надлежащего решения проблем в режиме реального времени необходимо разработать надежный и проверенный план и процедуры реагирования на инциденты. Ключевые технологии, лучшие практики и процессы включают в себя:

1) Централизованный сбор и анализ данных. Организациям необходимо создавать централизованные панели мониторинга, которые позволяют им видеть всю сеть, системы и схемы трафика в одном месте, а группа экспертов постоянно и непрерывно следит за ними.

2) Многоуровневый подход защиты. Цель должна состоять в том, чтобы разрешить в сеть только законный трафик и исключить весь нежелательный трафик.

3) Масштабируемая и гибкая инфраструктура. Чтобы обеспечить правильную работу систем даже в условиях атаки, организации должны иметь легко масштабируемую и гибкую инфраструктуру с емкостью по требованию.

4) Регулярное решение проблем приложений и конфигурации. DDoS-атаки

стали более изощренными и трудными для обнаружения на уровне приложений. Нужно знать и понимать, что делает каждое приложение, его использование и модель использования, как выглядит обычный запрос приложения, а также нормальный уровень транзакций для каждого компонента приложения.

Вывод.

Одним из важнейших факторов борьбы с DDoS-атаками является их своевременное обнаружение, однако ввиду огромно числа разновидностей типов данной атаки, зачастую своевременное обнаружение невозможно.

В данной работе были выделены основные методы защиты от DDoS-атак, предложена классификация методов обнаружения DDoS-атак, классификация архитектур предотвращения DDoS-атак в соответствии с местом их развертывания, приведены примеры последствий DDoS-атак, и предложены.

Заключение

Для достижения данной цели, в процессе прохождения учебной (по получению первичных профессиональных умений и навыков, в том числе первичных умений и навыков научно-исследовательской деятельности) практики ознакомился с методами обнаружения и защиты от DDoS-атака.

Также были изучены требования к написанию отчета по практике. В результате прохождения практики был составлен отчет по практике, соответствующий предъявленным требованиям.

В ходе прохождения практики все задачи были выполнены, а цель достигнута.

Список используемых источников

1) **МЕТОДЫ ОБНАРУЖЕНИЯ И ПРЕДОТВРАЩЕНИЯ DDOS-АТАК**

Автор:

Руслан Рамилевич Кадыров

МГТУ им. Н.Э.Баумана, Москва, Российская Федерация

https://www.elibrary.ru/item.asp?id=39242642

2) **ВИДЫ DDOS АТАК И МЕТОДЫ ЗАЩИТЫ РАСПРЕДЕЛЕННОЙ СЕТИ**

Автор:

Дмитрий Александрович Зебров

Донской государственный технический Университет

https://www.elibrary.ru/item.asp?id=44545629

3) **РЕКОМЕНДУЕМЫЕ МЕТОДЫ И СТРАТЕГИИ ДЛЯ БЛОКИРОВКИ DDOS-АТАКИ**

Авторы:

Донкан Кристина Максимовна,

Дудоладова Полина Геннадьевна

МГУ им. Г.И. Невельского

https://www.elibrary.ru/item.asp?id=43309512

4) **СОВРЕМЕННОЕ СОСТОЯНИЕ ОБНАРУЖЕНИЯ DDOS-АТАК И ПРОТИВОДЕЙСТВИЕ К НИМ**

Авторы:

Кульмамиров Серик Алгожаевич, Баймаманова Айнур Аскаткызы

Казахский национальный университет имени аль-Фараби

https://www.elibrary.ru/item.asp?id=43055120

5) **ПРИЧИНЫ ВОЗНИКНОВЕНИЯ DDOS-АТАК И ИХ КЛАССИФИКАЦИЯ**

Авторы:

Кульмамиров Серик Алгожаевич, Баймаманова Айнур Аскаткызы

Казахский национальный университет имени аль-Фараби

https://www.elibrary.ru/item.asp?id=43055119

6) **An Efficient Detection Mechanism for Distributed Denial of Service (DDoS) Attack**

Авторы:

Saravanan Kumarasamy, Dr.R.Asokan

https://arxiv.org/abs/1302.5158