Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники

УДК_____

Недведский
Александр Юрьевич

АНАЛИЗ DNS ПАКЕТОВ С ЦЕЛЬЮ ОБНАРУЖЕНИЯ ПОПЫТКИ ПЕРЕДАЧИ НЕСАНКЦИОНИРОВАННОГО ТРАФИКА ПОСРЕДСТВОМ ТУННЕЛИРОВАНИЯ DNS

АВТОРЕФЕРАТ
на соискание академической степени магистра информатики и вычислительной техники

по специальности 1-40 81 04 – Обработка больших объемов информации

_____

Научный руководитель
Калабухов Е. В.
ст. преподаватель

_____

Минск 2017

КРАТКОЕ ВВЕДЕНИЕ

Повсеместное распространение различных вычислительных устройств и развитие сетей передачи данных, связывающие эти устройства, изменило наш мир. Глубокая интеграция этой развитой инфраструктуры в повседневную жизнь каждого отдельного человека остро ставит вопрос об информационной безопасности. И поэтому одним из ключевых аспектов по обеспечению функционирования развитой инфраструктуры вычислительных устройств является гарантирование безопасности ее работы в целом и отдельных ее узлов в частности.

Со времен первого объединения нескольких компьютеров в единую сеть было сделано очень многое для достижения этой цели. Возможно, главной движущей силой по обеспечению безопасности работы сети являются межсетевые экраны – программные или программно-аппаратные элементы компьютерной сети, осуществляющие контроль и фильтрацию проходящего через них сетевого трафика в соответствии с заданными правилами. Благодаря межсетевым экранам можно обеспечить защиту отдельных сегментов локальной сети от несанкционированного доступа с использованием уязвимых мест в протоколах сетевых моделей. Межсетевые экраны осуществляют фильтрацию трафика на основании заданных правил и шаблонов.

Протокол DNS (Domain Name System) отвечает за получение информации о доменных именах. В частности, за преобразование символьного имени ресурса сети Интернет, такого как example.com в его IP адрес. Протокол DNS предусматривает возможность передачи и приема пакетов определенного типа. Такие пакеты позволяют инкапсулировать в них зашифрованные данные, что в свою очередь делает возможным организацию туннеля на основе протокола DNS. Так как протокол DNS не предназначен для передачи пользовательского трафика, содержимое пакетов данного протокола часто не анализируется на наличие вредоносного трафика или установленных каналов связи. И более того, одним из ограничений межсетевых экранов является невозможность анализа туннелированного трафика, поэтому подобная уязвимость протокола DNS может использоваться злоумышленниками для эксфильтрации данных.

Решение проблемы состоит в анализе поступающих DNS запросов на предмет аномального поведения. Причем сегодня данная задача может быть решена с применением последних достижений в области обработки больших объемов информации. Обработка больших объемов информации достигается за счет распределения нагрузки среди множества вычислительных устройств и реализации соответствующих парадигм программирования. Такие системы, как правило, преследуют одну единственную цель – обработка постоянно поступающих данных за приемлемое время.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы магистерской диссертации

Туннелирование DNS – это техника, которая может быть использована для обхода межсетевых экранов и получения доступа к ресурсам сети. Она предполагает инкапсуляцию данных в обычные DNS пакеты. Одним из примеров использования этой техники является передача несанкционированного трафика, с целью контроля над ботнетом, что предполагает использование незащищённого канала связи. Таким образом, туннелирование DNS представляет серьезную угрозу безопасности сети.

Цель и задачи исследования

Целью диссертационной работы является проведения полного анализа методов, алгоритмов и программного обеспечения для обнаружения передачи по компьютерной сети несанкционированного трафика, которая предполагает использование техники туннелирования DNS.

Для достижения поставленной цели необходимо решить следующие задачи:

1) Провести всесторонний анализ системы DNS.

2) Провести всесторонний анализ техники туннелирования DNS.

3) Выявить причины, позволяющие использовать системы DNS для передачи несанкционированного трафика.

4) Проанализировать существующие решения в области обнаружения использования техники туннелирования DNS.

5) Определить их основные характеристики и ограничения.

6) Проанализировать методы и алгоритмы обнаружения использования техники туннелирования DNS с использованием возможностей, предоставляемых Big Data.

Объектом исследования являются система DNS и техника туннелирования DNS.

Предметом исследования являются методы, алгоритмы и программное обеспечение компьютерных систем для решения задач обнаружения передачи несанкционированного трафика по компьютерной сети посредством туннелирования DNS.

Основной *гипотезой*, положенной в основу диссертационной работы, является возможность использования различных подходов и методов для обнаружения передачи несанкционированного трафика посредством туннелирования DNS. Поскольку протокол DNS не предназначен для передачи пользовательского трафика, чаще всего он не рассматривается сетевыми

администраторами как средство для передачи вредоносных сообщений. Поэтому в большинстве сетей DNS не подвергается контролю и фильтрации межсетевыми экранами. Используя современные подходы к обработке больших объемов информации, можно добиться высоких показателей эффективности и обеспечить безопасность работы компьютерной сети.

Связь работы с приоритетными направлениями научных исследований и запросами реального сектора экономики

В связи с быстрым ростом сферы информационных технологий большое распространение получили компьютерные сети передачи данных. Компьютерные сети служат для объединения вычислительных устройств, обеспечивая обмен данными и распределение вычислительных ресурсов. Безопасность компьютерных сетей играет ключевую роль в гарантировании неприкосновенности личности каждого отдельного человека, которая сводится к защите личных данных. Кроме того, обеспечение безопасности компьютерной сети является ключевым фактором, необходимым для нормального функционирование любой компании.

Несовершенство средств защиты и уязвимости протоколов, используемых в компьютерных сетях, могут приводить к нарушению безопасности компьютерных сетей, что в свою очередь может стать причиной многомилионных убытков и упущенной прибыли.

С учетом всего выше сказанного, в реальном секторе экономики существует реальная необходимость разработки методов обеспечения безопасности работы сети в целом и отдельных ее компонент в частности.

Личный вклад соискателя

Результаты, приведенные в диссертации, получены соискателем лично. Вклад научного руководителя Е. В. Калабухова, заключается в формулировке целей и задач исследования. Вклад соавторов опубликованных статей В. В. Масензова и Ф. В. Якубовича заключается в формулировке требований, выдвигаемых к системам, реализующим обработку большого объема данных.

Опубликованность результатов диссертации

По теме диссертации опубликовано 2 печатные работы, из них 2 работы в международном журнале «Наука, образование и культура»

Структура и объем диссертации

Диссертация состоит из введения, общей характеристики работы, трех глав, заключения, списка использованных источников. В первой главе представлен анализ предметной области и существующих моделей, выявлены основные проблемы в рамках тематики исследования, показаны направления их решения. Вторая глава посвящена анализу существующих инструментов и методов, предоставляемых различными подходами по обработке больших объемов информации. Также в данной главе приведены основные требования, выдвигаемые к подобным системам, а также приведено их сравнение в контексте используемых архитектурных решений. В третьей главе происходит описание реализаций предложенных ранее методов и алгоритмов, приводятся результаты проведения испытаний реализованных методов. В данной главе также рассматриваются реализация анализируемой системы при помощи различных инструментов и методов по обработке больших объемов информации, сравнивается ее эффективность с результатами, полученными при реализации системы с использованием классических подходов.

Общий объем работы составляет 69 страниц, из которых основного текста – 45 страниц, 18 рисунков на 9 страницах, 1 таблицы на 2 страницах и список использованных источников из 48 наименований на 3 страницах.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

DNS это широко используемый сервис. Поэтому он представляет собой заманчивую цель для злоумышленников. В частности, DNS протокол часто используется для настройки туннеля. При помощи DNS туннеля, можно передавать сообщения других протоколов под видом DNS пакетов. DNS туннель может быть использован для передачи команд, эксфильтрации данных или туннелирования любого другого IP трафика.

Большинство инструментов для создания и эксплуатация туннелей на основе протокола DNS работают за счет того, что содержимое DNS пакетов чаще всего не анализируется, так как протокол DNS не предназначен для передачи пользовательского трафика. Исходя из этого, все методы для обнаружения использования техники туннелирования DNS можно условно разделить на две категории:

1) Методы, предполагающие анализ содержимого DNS пакета.

2) Методы, предполагающие общий анализ DNS трафика.

К первой категории относятся методы, на основе анализа содержимого DNS запросов и ответов, ко второй же – на основе анализа частоты, количества определенных пакетов и других атрибутов DNS трафика.

Обработка больших объемов данных достигается за счет распределения нагрузки среди множества вычислительных устройств и реализации соответствующих парадигм программирования. Причем требования к системам, которые занимаются обработкой больших объемов информации постоянно растут. Такие системы, как правило, преследуют одну единственную цель – обработка постоянно поступающих данных за приемлемое время.

Касательно рассматриваемой темы, применение технологий обработки больших данных данных является критическим условием. Протокол DNS это широко используемый протокол, задержка в работе которого может отрицательно повлиять на большое число конечных узлов. Кроме этого, от результата выполнения DNS запроса зависит работа других протоколов сети Интернет.

Для выполнения анализа DNS трафика с использованием средств предоставляемых BigData была разработана архитектура приложения, запуск которого предполагается выполнять с использованием фреймворка Apache Storm.

Разработанная архитектура является модульной и позволяет легко расширять функциональность системы и выполнять оптимизацию каждого из его компонент.

ЗАКЛЮЧЕНИЕ

DNS туннели могут использоваться злоумышленниками для сокрытия своей деятельности и представляют серьезную угрозу безопасности сети. Существует большое количество утилит для эксплуатации данной уязвимости протокола DNS. Некоторые из них были разработаны достаточно давно, другие же появились совсем недавно и предлагают расширенную функциональность по созданию и использованию DNS туннелей. Например, Heyoka, использует IP спуфинг для сокрытия IP адреса клиента DNS туннеля.

Разнообразие инструментов для эксплуатации уязвимости протокола DNS, их широкое распространение и простота использования представляют серьезную угрозу для безопасности личных данных отдельных пользователей и корпоративной информации различных организаций. DNS туннели могут применятся для удаленного контроля зараженного компьютера, а также эксфильтрации передаваемых по туннелю данных.

Для обнаружения передачи несанкционированного трафика посредством туннелирования DNS могут быть использованы методы анализа полезной нагрузки DNS пакета и методы, предполагающие общий анализ DNS трафика. Методы анализа полезной нагрузки DNS пакета предполагают рассмотрение различных специфичных характеристик присущих утилитам для создания DNS туннелей. Подобные методы могут быть особенно эффективны в случае их использования для детектирования применения хорошо изученных инструментов для туннелирования DNS. Методы, основанные на общем анализе DNS трафика, оказываются более универсальными и демонстрируют свою эффективность в независимости от класса используемых утилит. Реализация подобных методов была продемонстрирована в данной работе.

Большие объемы информации могут быть обработаны благодаря распределению нагрузки среди множества вычислительных узлов. В данной работе были проанализированы требования и основные подходы к обработке больших объемов информации. Введены основные понятия в области пакетной и поточной обработки данных. Рассмотрены основные фреймворки по обработке больших объемов информации, реализующие оба этих подхода. Проанализированы их архитектуры и основные концепции, лежащие в основе их программных моделей. Так, фреймворк MapReduce позволяет обрабатывать большие объемы сохраненных данных, а Apache Spark – производить обработку поточных данных.

В контексте рассматриваемой темы, в данной работе был продемонстрирован один из вариантов архитектура системы для выполнения анализа DNS трафика с использованием возможностей предоставляемых методами обработки больших объемов информации. Выявлены основные

критерии, которые могут быть использованы в качестве признаков для обнаружения передачи несанкционированного трафика.

Однако, полученные результаты не могут считаться достаточными для формирования окончательных выводов по данной теме. Так, необходимо провести более обширное тестирование предложенных в данной работе методов. Необходимо развернуть предложенную архитектуру приложения в реальной среде для формирования полноценных результатов ее работы в рамках анализа повседневного трафика и в условиях полной нагрузки. Также в рамках расширения функциональности рассмотренной системы, возможно выделение дополнительных признаков детектирования DNS туннелей. Кроме этого, применение нейронных сетей для настройки классификатора и обучения построенной модели может помочь улучшить точность получаемых результатов. Таким образом, в результате работы над данной диссертацией создана плодотворная почва для проведения дальнейших исследований по данной теме. Планируется проведение дополнительных испытаний рассмотренных методов и расширении класса задач, решаемых с их помощью.

СПИСОК ОПУБЛИКОВАННЫХ РАБОТ

1) Обнаружение передачи несанкционированного траффика посредством туннелирования DNS. Калабухов Е.В., Недведский А.Ю., Масензов В.В., Якубович Ф.В. Номер 05(20) 2017 года журнала «Наука, образование и культура».

2) Технология HealthCloud на базе одноименной CRM-системы Salesforce. Калабухов Е.В., Масензов В.В.,Недведский А.Ю., Якубович Ф.В. Номер 05(20) 2017 года журнала «Наука, образование и культура».