УДК 004

АКТУАЛЬНОСТЬ ПРОВЕДЕНИЯ АНАЛИЗА КОМПЬЮТЕРНЫХ СЕТЕЙ С ЦЕЛЬЮ ПОИСКА АНОМАЛЬНОГО ТРАФИКА

Пламадил О.А.

аспирант,

«Российский университет транспорта» (рут (МИИТ),

Москва, Россия

Аннотация

Данная статья посвящена актуальности проведения анализа компьютерных сетей с целью поиска аномального трафика. В статье рассмотрены проблемы, к которым привело бурное развитие компьютерных сетей. Представлены инструменты мониторинга и анализа сетей. Приведены примеры сетей безопасности. Рассмотрены плюсы и минусы данных систем. Рассмотрены способы обнаружения аномального трафика. Приведены примеры данных методов. Сделаны соответствующие выводы.

Ключевые слова: компьютерная сеть, анализ компьютерной сети, аномальный трафик, сеть безопасности, мониторинг сети, анализ сети.

THE RELEVANCE OF ANALYSIS OF COMPUTER NETWORKS FOR THE PURPOSE OF SEARCHING FOR ANOMAL TRAFFIC

Plamadil O.A.

Postgraduate student,

Russian University of Transport (MIIT),

Moscow, Russia

Abstract

This article is devoted to the relevance of analyzing computer networks in order to search for anomalous traffic. The article discusses the problems that have resulted from

the rapid development of computer networks. Network monitoring and analysis tools are presented. Examples of security networks are given. The pros and cons of these systems are considered. Methods for detecting anomalous traffic are considered. Examples of these methods are given. Relevant conclusions have been drawn
Keywords: computer network, computer network analysis, abnormal traffic, security network, network monitoring, network analysis.

Обработка информации, а также ее хранение привели к обмену данными между теми, кто принимает участие в данном процессе.

В 70-х годах появилось большое количество новых сетей, в том числе оборудование и устройства сети. Сети локального и глобального масштабов продолжают свое развитие и в наше время. На сегодняшний день появляются новые и новые протоколы передачи информации, возможностей сетевого оборудования становится все больше, количество абонентов увеличивается, вместе с этим постоянно растут объемы трафика.

Активное развитие компьютерных сетей приводит к различного рода проблемам. К примеру, быстрый рост потребителей в услугах информационного характера требует лучшего сетевого оборудования, а также обслуживания по высшему разряду.

Другая проблема состоит в важности охраны информации, находящейся внутри сети.

Проблемы и вопросы данного типа могут быть решены на базе проведения подробного анализа трафика, который поможет выявить и разрешить проблемы на этапе их появления. Оборудование остается неподверженным простою, длящемуся долгое время.

Передача информации по сети - это непрерывный процесс, поэтому, если обслуживание сети находится не в порядке, то организацию и компанию ожидают убытки.

Движение сетевого трафика должно отслеживаться в обязательном порядке, производительность сети должна подвергаться контролю, все недочеты должны отслеживаться политикой безопасности.

Инструменты отслеживания и проведения анализа сетей вычислительного характера делятся на:

1. Системы управления сетью: это общего рода собирательные системы данных по оборудованию сетевого характера, а также системы собирательного характера о трафике в сети. Информация системы помимо отслеживания и проведения анализа может осуществлять управление сетью. Чтобы управлять сетью, необходимо:

- правильно ее настраивать, менять таблицы адресов на коммутаторах и т.д.;

- подключать и отключать порты оборудования.

2. Диагностика и управление, которые встроены в систему. Сюда входит модуль программ и модуль аппарата, их можно установить на оборудовании коммуникации или встроить в операционную систему. Данные, которые находятся в системе, являются очень важными для управления системой.

3. Методы, применяемые при установки системы. Их деятельность схожа с функциями управления, но в этом случае могут быть задействованы несколько объектов. Системы могут иметь схожие функции.

4. Анализ протоколов представляет собой специальное устройство или оборудование (персональный компьютер) с картой сети и подходящим программным обеспечением. Хороший анализатор может захватывать и декорировать пакеты протоколов в большом количестве, применяемые в сетях. Данные устройства работают логично с целью захвата пакетов и их декодирования. На этапе проектирования сети имеют большое значение количественные характеристики.

5. Устройства диагностики и сертификации кабельных систем в оборудовании.

6. Экспертные системы. Созданы для того, чтобы выявлять аномальную сеть и восстанавливать ее. Некоторые подсистемы могут справиться с данными функциями.

7. Оборудование, предназначенное для анализа и диагностики аномалий.

Представленные системы, защищающие информацию, имеют свое значение в работе с уязвимыми системами. Нежелательные воздействия можно устранить путем специальных систем обнаружения. Данные системы часто использует политика безопасности. Данными системами являются такие:

1. Система, обнаруживающая вторжение. Это программный аппарат, выявляющий реальные факты доступа в систему, аппарат не выдает себя при входе в сеть.

2. Система предотвращения вторжений. Призвана следить за сетью или системой с целью выявления и блокировки активной деятельности вируса. Данная система может как выявить вторжение, так и защитить от нежелательного вторжения. Цель данной системы - отслеживание атак нежелательного характера. СПВ призвана определять вторжения в режиме реального времени, в том числе, когда атака уже началась. Работает система с помощью:

- сброса соединения с сетью;
- внутренней защиты сети;
- подачи сигнала оперативной системе.

Кроме того, системы могут выводить пакеты, а также изменять их некоторые части.

Системы проводят автоматизацию сложного процесса контроля над событиями, происходящими в сети или на персональном компьютере, и анализируют набор событий, чтобы определить проблемы, которые касаются безопасности сети.

В наше время существует очень много способов, а также разновидностей проникновений в сеть, не являющихся санкционированными. В результате этого

обнаружение вторжений стало обязательным во всей системе безопасности для большинства организаций и предприятий. В этом и состоит актуальность проведения анализа компьютерных сетей с целью поиска аномального трафика.

Данные события происходят потому, что попытки вторжения в сеть расширяют свои способы и приводят к более тонким попыткам в поиске методов, приводящих к проникновению информационных систем. Системы, которые находят вторжения в сеть, на сегодняшний день имеют сложную схему. Их направленность может быть локальной и сетевой.

Системы сети должны быть установлены на специальных компьютерах в особом порядке. Системы должны проводить тщательный анализ трафика, который отслеживается в местной сети вычисления.

Системы местного уровня должны находиться на таких компьютерах, для которых очень важна защита и которые подвергают исследованиям события определенного характера.

СОВ отличаются не только архитектурным устройством, но и по методам обнаружения:

- по поиску поведения аномального характера;

- по поиску поведения злого умысла.

Чтобы обнаружить аномальное поведение или поведение злоумышленников, существуют некоторые методы.

Системы, которые создаются для определения поведения аномального характера, основаны на определении СОВ признаков, которые характеризуют поведение объекта как правильное или допустимое. Правильным (соответствующим норме) считается поведение, которое не идет вразрез с политикой безопасности.

Системы, которые способны выявить поведение злоумышленного характера, базируются на заранее известных и хорошо знакомых признаках, из которых складывается поведение злоумышленников. Такими системами чаще всего выступают системы экспертного характера.

К примеру, очень часто поступают жалобы на сайт и приложение РЖД. Данный сайт действительно подвергается очень часто атакам со стороны хакеров, по этой причине очень часто остаются недоступны многие сервисы сайта. Поэтому и билеты РЖД часто приходится приобретать в режиме реального времени в кассе, а не онлайн. Тем не менее сайт РЖД имеет эшелонированную систему защиты, которая состоит из решений ведущего характера, которые открыто представлены на рынке по безопасности информации в России.

Системе безопасности информации ОАО "РЖД" приходится обрабатывать более сорока шести тысяч событий каждую секунду. Узлы системы подвергаются атакам каждый месяц, сегмент сервера, наоборот, чаще одного раза в неделю. Система контроля защиты использует программные и аппаратные решения, которые базируются на продуктах российской разработки. Широкий аудит уязвимостей критического характера IT-инфраструктуры РЖД производится постоянно. В 2020 году, к примеру, проводилось большее число аудитов из-за перевода на работу в удаленном режиме более ста тысяч сотрудников организации [5].

В 2020 году было зарегистрировано 28094 случая заражения вирусами. Более тысячи атак, связанных с информационной системой, были задержаны. Самыми опасными атаками оказались атаки, связанные с финансовой системой и деятельностью производственного характера. В последнее время участились атаки DDoS. Тип таких атак обязательно имеет свой план, злоумышленники часто останавливаются в инфраструктуре и оставляют доступ к системе длительный период. Целью финансовой атаки ОАО "РЖД" было получение логинов и паролей к доступу отправки денежных средств, а также к бухгалтерской отчетности. Бизнес-процессы РЖД остались незатронутыми [5].

Однажды сеть по передаче данных РЖД была взломана, в связи с чем взломщикаи стало доступно видеонаблюдение на вокзалах.

Факт доступа к данным был неоднократно подтвержден. Появилась уязвимость в настройке маршрутизатора, который обеспечивает соединение Интернета и сегмента системы информационного характера.

Подробный план действий, а также угрозы, которые могут возникнуть, привлекли большое внимание хакеров к сети РЖД. Это спровоцировало атаки массового характера на информационную систему российских железных дорог. Под удар попали миллионы пассажиров, пользующихся услугами российских железных дорог. На ухудшение ситуации повлияло появление данных об этом в средствах массовой информации.

Остается открытым вопрос о специально оставленной уязвимости в сети РЖД. Данным вопросом занимается служба безопасности российских железных дорог. Официальные заявления РЖД говорят о том, что данное событие не имеет никакой связи с организацией перевозок, в тот момент угрозы безопасности движению поездов не было выявлено, личные данные клиентов холдинга не имеют статуса пострадавших.

Резервная копия данных РЖД была видна в открытом доступе. Была известна информация об электронных адресах тех людей, которые пользовались сайтом. Это стало возможным по вине администратора организации подряда, которая работала над сайтом.

На данный момент разрабатываются методы приобщения внешних пользователей к проверке того, насколько уязвимой является сеть. Будет внедряться дополнительная линия центра звонков, которая поможет собрать воедино звонки о разных «находках» на внешнем уровне сети корпорации профильным специалистам в организации Российских железных дорог.

На верхнем уровне управления в организации стоит задача – проанализировать имеющиеся кейсы и скорректировать политику информационной безопасности на уровне всего холдинга с целью исключения повтора события. Перевод процессов на цифровой уровень становится основным вектором развития Российских железных дорог. Но перевод в цифровой вид

большого количества данных повышает опасность утечки этих данных в результате умышленного взлома системы или сбоя в работе её охраны.

Постоянно производятся как организационные, так и технические мероприятия по соблюдению требований законодательства Российской Федерации в сфере охраны информации. Большое внимание на сегодняшний день уделяется охране объектов критической инфраструктуры информационного характера, прежде всего связанных с процессами бизнеса на производстве. Менеджмент управления в сфере информационной безопасности основан на принципах рискованного подхода и является входящим в систему управления рисками контроля ОАО «РЖД» внутри организации. Центром можно считать централизованную систему управления безопасностью в сфере информации, основанную на сети ОАО «РЖД» и представляющую собой комплекс мероприятий в системе обеспечения, контроля и быстрого реагирования на случаи, связанные с информационной безопасностью.

Информационная безопасность компании стоит на основе принципов комплексной защиты от внешнего проникновения и внутреннего, которые не являются несанкционированными. В ОАО "РЖД" ведется отслеживание и контроль за возможными точками проникновения в инфраструктуру, с помощью которых можно за короткий промежуток времени выявить действия злоумышленников. С этой целью сегодня активно используются технологии различного рода, в том числе DLP-системы (от англ. Data Loss Prevention) [2].

Система, которая предотвращает уход информации, способна собрать воедино данные с различных источников, которые располагаются на границе с сетью Интернет. Система способна отобразить обнаруженные в источниках признаки аномалий поведения пользователей, попытки утечки информации, детектирует сложные целевые атаки на инфраструктуру компании, когда злоумышленники внешней среды находятся в сговоре со злоумышленниками внутреннего уровня.

К технологиям детектирования атак данного вида можно отнести выполнение проверок всех файлов исполнения в инфраструктуре облака на базе технологии машинного обучения. В этом же случае выявляются активности подозрительного и вредоносного характера объектов информации на базе анализа их поведения в изолированной среде: сообщения на почте, документы и файлы различного рода. Проводится анализ файлов с применением ранее созданных сигнатур пользователя. В том числе ведутся списки репутации по вредоносным и фишинговым ресурсам, по адресам узлов управления ПО, в котором есть вирус, по адресам хакерских группировок [1].

Чтобы сделать минимальными риски, которые связаны с внутренними угрозами, в организации РЖД постоянно производят контроль каналов, по которым передается информация. Это позволяет выявлять действия неправомерного характера сотрудников компании, обнаруживать недоступные к публикации данные в открытом доступе на местных и сетевых ресурсах организации, а также тщательно анализировать поведения сотрудников, также выявлять признаки действий, которые являются противоправными и противозаконными.

Комплексное использование технических решений различного рода в области обеспечения информационной безопасности позволяет очень быстро реагировать на угрозы, связанные с безопасностью информации в режиме автоматизации [3].

Существуют специальные технологии, которые могут обнаружить деятельность аномального трафика. К данным технологиям относят датчики сенсорного характера аномалий, которые способны выявить поведение нестандартного характера, то есть аномалии, происходящие в каком-либо работающем на данный момент объекте. Трудность при их применении в практических условиях состоит в нестабильной защите объектов внутренней среды и объектов внешней среды, связанных с ними. Объектом наблюдения в этом случае может выступать сеть, компьютер или что-то иное. Устройства

могут сработать в том случае, если нападение имеет отличие от деятельности законного характера [4].

Методы обнаружения аномалий являются следующими:

1. Способ обнаружения с помощью порогового значения: объект отслеживается с помощью интервалов сети. Аномальное поведение признается в том случае, если выход осуществился за пределы интервала. К параметрам наблюдения относятся:

- число файлов, которые показывают посещения пользователя за какой-либо период времени;

- попытки входа в систему, которые нельзя считать удачными.

Пороги могут быть неизменяемыми и считаются в этом случае статистическими, а могут изменяться, подстраиваясь под какую-либо систему, тогда они считаются динамическими.

Пороги параметрического характера способны выявлять атаки с помощью построения специального "профиля нормальной системы" на основе заранее выстроенных шаблонов.

Непараметрические пороги характеризуют профиль на основе наблюдения за объектом именно в тот момент, когда он обучается.

Статистическими мерами описывается тот промежуток времени, когда атака имеет подтверждение с помощью большого объема данных, которые были собраны заранее и обработаны с помощью методов статистики.

Меры на основе правил имеют схожесть с непараметрическими мерами статистического характера. Обучение помогает составить верное представление о поведении объекта, которое можно считать нормальным, записанное с помощью цепочки условий "специального" характера.

Иными мерами считаются сети нейронного состава, алгоритмы генетического характера, которые помогают собрать в классификацию ряд признаков, которые видит сенсор-датчик.

Системы современного устройства определяют аномалии с помощью первых двух методов. Применение данной технологии имеет свои особенности:

1. Обнаружение поведения аномального характера, которое не является атакой;

2. Пропуск случайным образом и пропуск атаки, которую нельзя отнести к атакам аномального поведения. Здесь специалистам приходится решать задачи нестандартного характера:

1) Необходимо обнаружить пограничные значения поведения, которое характеризует субъект, чтобы снизить риск появления крайних случаев, которые могут произойти;

2) Важно выстроить профиль объекта. Данная задача требует определенных затрат во времени, приложение от специалиста больших усилий, опыта и высокой квалификации.

Системы, которые могут выявить активность аномального характера, применяют журналы специальной регистрации и деятельность, которую ведет пользователь в данный промежуток времени как источник информации для проведения анализа.

Положительными характеристиками, способными определить атаки на базе технологии, которая может определить поведения аномального характера, можно считать:

1. Они не требуют обновления правил по обнаружению атак;

2. Способны обнаружить новые виды атак, сигнатур по которым еще не существует;

3. Имеют связь с информацией, которая применяется при обнаружении поведения злоумышленниками.

Минусы систем:

1. Часто генерируют ошибки второго рода;

2. Работа с ними требует продолжительного обучения высокого качества;

3. Имеют медленный темп работы;

4. Содержат требования к большому количеству ресурсов вычисления.

Для того, чтобы вычислить аномальное поведение, используют метод статистического анализа. С помощью датчиков статистического характера производится сбор информации о том, как ведет себя объект в типичных условиях, а также собирается вся информация в профиль. Профилем является набор параметров, которые дают характеристику поведению объекта типичного вида. Базой данного профиля является статистика объекта, за которым наблюдают с помощью методов статистики математики (метод сумм взвешивания). В первую очередь формируется первичный профиль, далее производят сравнение с параметрами соответствия. Начало атаки сигнализирует об отклонениях.

Группы профильных параметров следующие:

1. Параметры категорий:

- наименования файлов;

- команды от пользователя и т.д.

2. Параметры числовых значений:

- число данных, которые были переданы по протоколам;

- количество файлов, в которые производился вход и т.д.

3. Характеристики иного рода.

В профилях существуют механизмы изменения динамического характера. Их цель: полное описание поведения объекта, которое постоянно подвергается изменениям.

Плюсами систем с методами статистики являются:

1. У них нет необходимости в постоянном обновлении базы сигнатур атак;

2. Системы имеют возможность приспособиться к постоянно изменяющемуся поведению пользователя (попытки вторжения с помощью них определяются скорей, чем их определит человек);

3. Данные системы находят атаки неизвестного происхождения до написания сигнатур;

4. С помощью этих систем распознаются атаки уровней большой сложности.

Но у данных систем есть и минусы:

1. Статистические методы могут выдавать ложные сообщения;

2. Не всегда предоставляется возможным задать пороговое значение;

3. Изменения в действиях пользователя могут обрабатываться некорректно;

4. Адаптация к поведению может не распознать атаку;

5. Если шаблон поведения невозможно описать, то атака со стороны субъектов может остаться неопознанной;

6. Методы, основанные на статистике, должны иметь основную базу заданных параметров;

7. Порядок следования событий у статистических данных может быть нарушен.

Данные проблемы, безусловно, могут быть решены, но со временем. Статистический метод на сегодняшний день занимает лидирующие позиции распознавания аномального поведения трафика.

Системы, которые обнаруживают проблемы, делятся на системы поиска следующего рода:

1. Сигнатуры узнаваемых атак;

2. Аномалии, которые имеют связь с контролируемыми объектами;

3. Информация по профилю, которая искажена.

На сегодняшний день почти нельзя найти гибридных систем, а также систем пространственного характера или временного. Метод распознавания, который используется, является сигнатурным, и именно он распознает аномалии, происходящие в сети.

Имитация атаки у систем, применяемых в наше время, отсутствует. Конфигурационные параметры в сети можно распознать далеко не всегда. Средство данного характера дано давать возможность повторить работу

обеспечения программы вируса, атак на отрицание в обслуживании и атак с той задачей, чтобы повысить плюсы записи учетного характера, атаки отправления трафика и присвоения данных ложного характера. При этом важно, чтобы средство программного обеспечения могло производить генерацию атаки характера распределения. Так как ситуация может иметь различный характер, то может появиться необходимость в соединении нескольких агентов разных классов в один момент. В данном случае система архитектуры может приспособиться к сетевой реконфигурации, различному трафику и его изменениям, а также к абсолютно неизвестным типам угроз с помощью опыта предыдущего времени.

Системы различных агентов можно считать необычной разработкой. Но в отечественной литературе об этом ничего не сказано.

Существуют действительные минусы таких систем обнаружения атак и трафика аномального характера:

1. Простая характеристика поиска сигнатуры;

2. Низкий результат при находке сложных атак;

3. Низкая степень соединения информации на уровне сети для выявления комбинации атак, в том числе вторжений, которые являются несанкционированными;

4. Высокое количество операций вычисления для обычного деления принадлежности события на "свой-чужой";

5. Невозможность откорректировать и проработать все данные, которые поступают в настоящее время на ПК по причине низкой скорости обработки событийного трафика. По этой причине аномальный трафик не будет вычислен вовремя, и, следовательно, не сработает система защиты. Здесь методы, которые используются для того, чтобы найти атаки могут считаться только сбором информации всех пунктов атаки для изучения в дальнейшем.

6. Программная система или программно-аппаратная система того или иного характера не имеют режима "замены горячих клавиш", которая позволяет

в одно мгновение при выведения какой-либо системы их строя быстро восстановить информацию по сети [7].

Но существующие средства защиты постоянно обновляются и совершенствуются.

Таким образом, актуальность проведения анализа сетей компьютера с целью поиска аномального трафика для охраны от воздействия несанкционированного характера обоснована. Методы решения данных вопросов имеют свое существование. Системы управления в данной области развиваются следующим образом:

1. Функции управления сетями и системами соединяются в едином продукте;

2. Система управления имеет четкое распределение, происходит сбор информации об устройствах, а также подсистемах, которые выдают действия управления.

Большое количество систем имеют узкую специализацию и стремятся хорошо выполнить свои функции. Чтобы исключить высокую уязвимость сети, важно соединить несколько продуктов. При этом система отслеживания и учета трафика проверяют, может ли оборудование и сеть работать хорошо, может ли система запретить вторжения нежелательного характера. Выявляется угроза в сети и снаружи [6].

Но, к сожалению, несмотря на все способы обнаружения и контроля нежелательных вторжений, система остается несовершенной.

На сегодняшний день существует около десяти систем обнаружения и предотвращения вторжений, но, к сожалению, вторжения совершенствуются и имеющиеся системы не всегда способны их распознать.

Важно создавать новые системы обнаружения и защиты, к чему отечественные производители недостаточно готовы.

Библиографический список

1. Официальный сайт сетевого протокола Cisco NetFlow [Электронный ресурс]. Режим доступа - http://www.cisco.com/go/netflow/ (Дата обращения: 10.01. 2012).
2. Платов В. В. Исследование самоподобной структуры телетрафика беспроводной сети // Радиотехнические тетради. 2022. № 30. С. 58-62.
3. Гальцев А.А., Сухов А.М., Кузнецова Н.Ю., Первицкий А.К. Функция распределения задержки пакетов в глобальной сети для задач теории управления // Телекоммуникации. 2020. №12. С. 10-16.
4. Титенко Е.А., Стариков Ф.А. Продукционный подход к проектированию экспертных систем // Известия Курского государственного технического университета, 2002. №2. С.86-88.
5. Цифровая инфраструктура привлекает злоумышленников // Гудок. №22(27116). 10.02.2021
6. Чернышевская Е.И., Селянина И.Ю. Метод обеспечения гарантированного качества обслуживания в IP-сетях // Век качества. 2010. № 6. С.70-72.
7. Шрейдер Ю.А. Системы и модели. - М.: Радио и связь. 2022. С. 152.

Оригинальность 89%