DOI 10.37882/2223–2966.2020.06.23

АНАЛИЗ И КРИТЕРИИ ЭФФЕКТИВНОСТИ СОВРЕМЕННЫХ МЕТОДОВ И СПОСОБОВ ВЫЯВЛЕНИЯ ИНКАПСУЛИРОВАННЫХ ПАКЕТОВ TCP/IP-ТРАФИКА

ANALYSIS AND EFFICIENCY CRITERIA OF MODERN METHODS AND TECHNIQUE FOR DETECTING ENCAPSULATED TCP/IP TRAFFIC PACKETS

M. Makukha
S. Klyuev

Summary. One of the main methods of covert transmission of information from an attacked network is encapsulation within the existing network Protocol. Therefore, we consider the detection of encapsulated protocols to be an important direction for government agencies and civil organizations seeking to prevent the loss of valuable information. The paper considers modern methods and methods of organizing network protection, their advantages and disadvantages are noted. On the basis of the conducted research, efficiency criteria were proposed. The purpose of this study is a comparative analysis of methods and methods for detecting encapsulated TCP/IP traffic packets, as well as determining the criteria for their effectiveness for further use in network security systems and tools. The materials of this work are of theoretical value for further research in this field.

Keywords: methods for detecting abuse, methods for detecting anomalies, knowledge-based methods, behavioral methods, data mining methods.

Макуха Максим Юрьевич
Преподаватель, Краснодарский университет МВД России
mmkrdu@yandex.ru
Клюев Станислав Геннадьевич
К.т.н., доцент, Краснодарское высшее военное училище
s.g.klyuev@mail.ru

Аннотация. Одним из основных способов скрытой передачи информации из атакованной сети является инкапсулирование в рамках существующего сетевого протокола. Поэтому мы считаем обнаружение инкапсулированных протоколов важным направлением для государственных органов и гражданских организаций, стремящихся предотвратить потерю ценной информации. В работе рассматриваются современные способы и методы организации сетевой защиты, отмечены их достоинства и недостатки. На основе проведенного исследования были предложены критерии эффективности. Цель данного исследования — сравнительный анализ способов и методов выявления инкапсулированных пакетов TCP/IP трафика, а также определение критериев их эффективности для дальнейшего применения в системах и средствах сетевой защиты. Материалы работы представляют теоретическую ценность для дальнейших исследований в данной области.

Ключевые слова: Методы обнаружения злоупотреблений, методы обнаружения аномалий, методы на основе знаний, поведенческие методы, методы интеллектуального анализа данных.

Актуальность исследования определена тем, что в настоящее время к глобальной сети Интернет подключено более четырех с половиной миллиардов уникальных пользователей [1]. Подключение к сети открывает широкие возможности, например, позволяет банкам, магазинам и другим сервисам работать круглосуточно, давая клиентам возможность получения доступа к их услугам со своих устройств, таких как мобильные телефоны или планшеты. Однако, помимо больших возможностей, подключение к глобальной сети Интернет, также создает риски для безопасности корпоративных сетей. Даже устройства, косвенно подключенные к Интернету потенциально уязвимы, например, узлы, скрытые за устройствами безопасности. Несмотря на значительный прогресс в защите устройств и сетей от атак, существующие механизмы защиты несовершенны. Совокупность подключенных к защищаемой сети уязвимых устройств и устройств, на которых хранится/обрабатывается ценная информация обеспечивает благоприятные условия для реализации атаки Advanced Persistent Threat которая направлена на компрометацию сетей, принадлежащих государственным органам или коммерческим организациям с целью кражи информации.

Согласно докладу о глобальных рисках Всемирного экономического форума 2019 года, кибер-атаки занимают пятое место в списке глобальных рисков, с которыми

сталкивается каждая организация, что приравнивается к стихийным бедствиям [2].

В соответствии со статистикой «Лаборатории Касперского», в 2019 году в мире на 72% возросло число пользователей, атакованных программами для кражи паролей, что составляет почти два миллиона пользователей. Данные анонимизированной статистики были собраны на основе срабатывания решений «Лаборатории Касперского» за 2019 год [3].

В период с 2013–2015 годы группировкой Carbanak было атаковано более 300 IP-адресов почти в 30 странах мира и похищено в общей сложности порядка миллиарда долларов у десятков банков по всему миру. [4]

Эти и многие другие примеры показывают, что поддержание безопасности компьютерной сети на высоком уровне достаточно нетривиальный процесс. Это обусловлено уязвимостями программного обеспечения, а также несоблюдением оптимальных политик безопасности корпоративных сетей. Специалисты по сетевой безопасности вынуждены предполагать, что в конечном итоге злоумышленник сможет скомпрометировать их сеть. Исходя из этого задачей специалиста по сетевой безопасности, помимо предотвращения компрометации сети, является минимизация ущерба вследствие ее компрометации. На основе чего предпринимаются меры по обнаружению необычной активности, например, кражи информации из сети.

Как правило, атаки на сеть проводятся удаленно и для передачи полученной информации из сети жертвы злоумышленники применяют распространённый метод передачи украденной информации посредством туннелирования протоколов. Сущность метода заключается в инкапсуляции сообщений протокола некоторого уровня сетевой модели передачи данных в сообщения прикладного уровня стека TCP/IP, в результате чего средства защиты игнорируют неразрешенные протоколы, так как обрабатывают только внешний протокол, который как правило разрешенный, что приводит к реализации угрозы безопасности информации, а также указывает на неэффективность средств сетевой защиты к такому методу обхода защиты. Исходя из изложенного, проведение анализа и определение критериев эффективности современных методов и способов выявления инкапсулированных пакетов TCP/IP-трафика является актуальным.

Отечественными и зарубежными учеными проводятся активные научные исследования в области разработки методов и способов предотвращения сетевых угроз. В научных трудах Киселева П.Л, Гамаюнова Д. Ю., Ушакова Д.В, M. Mahoney, P. K. Chan [5–8] описываются основы обеспечения сетевой безопасности и принципы работы средств и систем сетевой защиты, однако не в полной мере рассмотрены способы и методы выявления инкапсулированных пакетов TCP/IP-трафика.

В общем виде системы обнаружения вторжений можно классифицировать по следующим признакам:

1. По способу реагирования:
   - активные;
   - пассивные.
2. По методу обнаружения атак:
   - системы обнаружения злоупотреблений;
   - системы обнаружения аномалий.
3. По способу сбора информации об атаке:
   - сетевые (network-based IDS, NIDS);
   - узловые (host-based IDS, HIDS).

В целях обеспечения контроля за нарушением безопасности сетей используются системы обнаружения вторжений типа (Intrusion Detection Systems) и системы предотвращения вторжений (Intrusion Prevention Systems). Системы IDS предназначены для обнаружения вредоносной активности в режиме реального времени и оповещении о ней сотрудников, ответственных за информационную безопасность, различными способами, например, письмом на электронную почту или отправкой SMS-сообщения на мобильный телефон. В результате чего сотрудники могут предпринять соответствующие меры по минимизации последствий обнаруженной вредоносной активности. Такие системы предназначены для пассивного мониторинга сетевого трафика. Преимуществом данных систем является то, что решение о блокировке трафика принимается оператором, однако, применение подобных систем предполагает наличие следующих недостатков: значительные трудозатраты и низкая оперативность в принятии решения.

К активным системам обнаружения вредоносной активности относятся системы предотвращения вторжений (IPS), которые автоматически предотвращают атаки, производя фильтрацию вредоносного трафика. Главными преимуществами являются: обеспечение своевременной защиты организации от проникновения, а также оптимизация деятельности оператора на принятие решения. В случае определения легитимного трафика как вредоносного и его блокирования IPS рискуют вызвать отказ в обслуживании (DoS), что является недостатком рассматриваемых систем.

Для проведения анализа и определения критериев эффективности методов выявления инкапсулированных пакетов TCP/IP-трафика из существующих методов выявления атак на системы распределенной обработки данных для проведения дальнейших исследований были отобраны методы обнаружения аномалий и методы обнаружения злоупотреблений.

Методы обнаружения злоупотреблений

Коммерческие устройства сетевой безопасности обычно используют метод обнаружения вторжений на основе сигнатур для сопоставления трафика с шаблоном известных атак и как следствие, они выполняют обнаружение злоупотреблений. Выбор данного подхода обуславливается достижением современными устройствами относительно низкого уровня ложных срабатываний при обнаружении атак. Некоторые NIDS выполняют глубокую проверку пакетов с отслеживанием трафика для извлечения файлов, отправленных по сети, а затем анализируют файлы с помощью сигнатур, что способствует снижению нагрузки и повышению точности обнаружения. Несмотря на это, системы обнаружения злоупотреблений обладают рядом ограничений:

1. *Ранее неизвестные типы атак.* Обнаружение ограничивается «известным вредоносным» трафиком. Злоумышленники могут обойти систему обнаружения злоупотреблений созданием нового вредоносного программного обеспечения, а также использованием уязвимости нулевого дня (0 day). Также к новому вредоносному программному обеспечению можно отнести существующие варианты вредоносного программного обеспечения, которые поддерживают методы полиморфизма и метаморфизма.
2. *Обфускация.* Злоумышленники могут избежать обнаружения путем разбиения, кодирования и шифрования трафика.
3. *Промежуток до создания сигнатур для новых угроз.* Средства обнаружения злоупотреблений основаны на использовании сигнатур, которые могут быть созданы только после того, как вредоносное программное обеспечение будет впервые обнаружено и изучено. Вероятнее всего, сигнатуры будут разрабатываться только для популярного вредоносного программного обеспечения нежели для программного обеспечения, разработанного индивидуально под определенную атаку и организацию. Также средствам обнаружения злоупотреблений постоянно необходимо обновление баз сигнатур.

К классу методов обнаружения злоупотреблений относятся методы на основе знаний, методы вычислительного интеллекта и методы машинного обучения.

К методам на основе знаний относятся: сигнатурный метод, языки описания сценариев, конечные автоматы, сети Петри, экспертные системы и метод проверки на модели. Основой работы данных методов является обнаружение атак по заданным признакам. Далее рассмотрим некоторые методы, относящиеся к данной группе.

Сигнатурные методы основаны на сравнении текущего состояния системы с образцом и проверке соответствия наблюдаемых событий с заданным множеством сигнатур атак. К преимуществу сигнатурного метода можно отнести низкое число ложных срабатываний так как производится идентификация с базой сигнатур и выявление полного соответствия существующим атакам. Недостатком метода является отсутствие возможности детектирования неизвестных атак и высокие требования к вычислительной мощности системы обнаружения для использования баз сигнатур большого объема.

Экспертные системы основаны на формализации знаний специалистов-экспертов в набор правил, на основании которых система принимает решение о наличии или отсутствии атаки. В общем виде правило представляет из себя конструкцию if-then, то есть, когда выполняются все условия, описанное в левой стороне правила, выполняются действия, описанные в правой стороне правила, которые могут активировать большое количество правил или идентифицировать возникновение вторжения.

Основным недостатком экспертных систем является то, что с помощью правил записанных в базу знаний системы отсутствует возможность выявления атак, не описанных правилами, хранящимися в данной базе. Из этого вытекает ряд недостатков, связанных с зависимостью системы от полноты базы, а также с ее обслуживанием и быстродействием системы в целом. Значительное влияние на эффективность данных систем оказывает компетентность экспертов, описывающих правила, которые будут эффективны в зависимости от квалификации эксперта.

Исходя из недостатков систем обнаружения злоупотреблений становится понятно, что применение данного метода для выявления инкапсулированных пакетов TCP/IP-трафика не имеет смысла, так как туннелированный трафик будет идентифицирован системой как разрешенный.

Методы обнаружения аномалий

В отличие от систем обнаружения злоупотреблений системы обнаружения аномалий имеют ряд преимуществ, которые заключаются в обнаружении новой, ранее неизвестной активности и, следственно, в способности обнаружения атак нулевого дня, не требуя их описания в шаблоне атак. Системы обнаружения аномалий также подходят для обнаружения обфускации и не зависят от времени создания баз сигнатур для

новых угроз. Иными словами, ограничения свойственные системам обнаружения злоупотреблений на них не распространяются. Это вызвано принципом работы данных систем, который заключается в моделировании «нормальной» активности сети, а затем определением любого последующего трафика, не соответствующего модели, как аномального и потенциально вредоносного.

Современные системы обнаружения аномалий также имеют ряд недостатков, основным из которых является высокий уровень ложного обнаружения, которые происходят, когда неестественный для сети, но «нормальный» определяется как «аномальный». Это вызвано неполной моделью трафика. Ложные обнаружения также могут возникать при изменении трафика, например, при подключении к сети новых узлов или сервисов.

К методам обнаружения аномалий можно отнести:

1. *Поведенческие методы*. Основаны на сравнении «нормального» состояния системы с состоянием наблюдаемого поведения.
2. *Методы машинного обучения*. Применяются как в системах обнаружения злоупотреблений, так и в системах обнаружения аномалий, учитывая, что в основе данных подходов, в качестве обучающей выборки, лежит применение шаблонов «нормального» трафика и аномального поведения. Преимуществом методов машинного обучения является возможность вычисления условных вероятностей наступления угрозы посредством оценки вероятностных отношений между рассматриваемыми событиями.
3. *Методы вычислительного интеллекта*: нейронные сети, генетические алгоритмы, нечетная логика, иммунные системы, метод опорных векторов, роевые алгоритмы.

Методы машинного обучения и вычислительного интеллекта также можно отнести к интеллектуальному анализу данных.

К *поведенческим методам* относятся вейвлет-анализ, статистический анализ, анализ энтропии, спектральный анализ, фрактальный анализ и кластерный анализ. Данная группа методов направлена на выявление атаки посредством построения нормальной работы системы и выявлении отклонений от нее. К недостаткам систем, использующих данный подход, стоит отнести наличие ложных срабатываний, а также временные затраты на формирование модели нормальной активности системы или пользователей, что в свою очередь является решающим фактором в отказе от данных систем нарушений безопасности в сети. Далее рассмотрим некоторые методы, относящиеся к данной группе.

Статистический анализ является основополагающим методом обнаружения аномалий. Стоит отметить, что важную роль в системах обнаружения вторжений, основанных на статистическом анализе, играет выбор параметров, указывающих на отличия нормального трафика от аномального.

Недостатком данного метода является наличие ложных срабатываний, а также пропуски атак, что обусловлено неполным или избыточным описанием модели «нормального» состояния системы.

Преимуществом статистических систем является способность выявления ранее неизвестных атак.

Анализ энтропии. Суть метода заключатся в построении модели, которая максимизировала бы значение энтропии. Для обнаружения аномалий в [9] энтропию конечной последовательности данных измеряют преобразованием этой последовательности в двоичную форму с последующим применением к ней алгоритмов сжатия. Величина энтропии в последовательности данных будет равна размеру сжатого таким образом объекта.

Методы машинного обучения наряду с системами вычислительного интеллекта применяются как при обнаружении аномалий, так и обнаружении злоупотреблений, так как данные методы используют для обучения сведения о нормальном и аномальном поведении в сети.

Методы машинного обучения могут использоваться для построения детальной модели нормального трафика основываясь на данных наблюдаемого трафика, в отличие от моделей, заданных экспертами и включающих только ожидаемый трафик, который может быть неполным или неправильным.

Применение методов машинного обучения для обнаружения злоупотреблений может расширить возможности по обнаружению посредством выявления деятельности аналогичной известному нарушению без необходимости точного описания таковой.

При расследовании инцидентов вторжения в сеть используются значительные ресурсы, определяющие степень поражения посредством изучения журналов узлов и сети экспертами. Однако, ни одна организация не будет инвестировать ресурсы на ежедневный мониторинг журналов в ожидании выявления новой атаки. Вместо этого сотрудники безопасности отслеживают предупреждения системы безопасности, основанные на выявлении злоупотреблений и ситуаций реагирования на них системами безопасности. Данный подход не может обеспечить должного уровня безопасности

Таблица 1. Результаты анализа методов обнаружения вторжений и критерии их эффективности.

Критерии Методы	Выявление ранее неизвестных атак	Противодействие обфускации	Зависимость от полноты и правильности базы сигнатур	Адаптивность	Способ сбора информации об атаке
Методы на основе знаний	-	-	+	-	Сетевые; Узловые
Поведенческие методы	+	+	-	+	Сетевые; Узловые
Методы интеллектуального анализа данных	+	+	-	+	Сетевые; Узловые

и уступает активному, который заключается в поиске угроз и предотвращении или уменьшении ущерба. Стоит отметить, что активный подход обладает значительным недостатком, который проявляется в привлечении большого числа опытных сотрудников. Этот недостаток можно компенсировать за счет повышения уровня автоматизации применением методов машинного обучения.

На основе проведенного исследования были сформулированы критерии эффективности методов выявления инкапсулированных пакетов TCP/IP-трафика. В таблице 1 приводятся результаты сравнительно анализа.

Из результатов анализа следует, что для выявления инкапсулированных пакетов TCP/IP-трафика наиболее эффективными являются методы интеллектуального анализа данных и поведенческие методы. Для обеспечения надлежащей защиты наиболее предпочтительными являются методы машинного обучения. Основными преимуществами данных методов являются: независимость от времени для создания новых баз сигнатур, способность выявления атак с применением обфускации, а также выявление ранее неизвестных атак.

Стоит отметить существование ряда сложностей применения методов машинного обучения для безопасности компьютерной сети, основным из которых является отсутствие возможности применения сетевого трафика непосредственно в качестве входных данных.

Также к специфичным сложностям применения машинного обучения для обеспечения безопасности компьютерной сети относятся:

- большой объем сетевого трафика;
- вредоносный трафик составляет лишь небольшую часть общего трафика;
- использование готовых наборов данных для обнаружения вторжений, таких как KDD-Cup 99, DARPA 1998/99 [10, 11] и т.д., на сегодняшний день не актуально в связи с их устареванием;
- сложность получения точно классифицированных данных обучения;
- разнообразие и развитие сетевого трафика.

Из перечисленных сложностей применения методов машинного обучения следует необходимость разработки автоматизированной среды идентификации и классификации угроз обеспечения безопасности компьютерной сети.

ЛИТЕРАТУРА

1. Digital 2020: 3.8 billion people use social media // We Are Social [Электронный ресурс]. URL: https://wearesocial.com/blog/2020/01/digital-2020–3–8-billion-people-use-social-media (дата обращения: 15.03.2020).
2. Weltwirtschaftsforum, Zurich Insurance Group Global risks 2019: insight report / Weltwirtschaftsforum, Zurich Insurance Group, 2019.
3. Новости | Лаборатория Касперского [Электронный ресурс]. URL: https://www.kaspersky.ru/about/press-releases/2020_pochti-dva-milliona-polzovatelei-bili-atakovani-programmami-dlya-krazhi-parolei-v-2019-godu (дата обращения: 15.03.2020).
4. Ограбление XXI века: группировка хакеров Carbanak похитила миллиард долларов [Электронный ресурс]. URL: https://www.kaspersky.ru/blog/billion-dollar-apt-carbanak/6950/ (дата обращения: 15.03.2020).
5. Киселёв П. Л. Модель и метод оценки эффективности комплексных систем защиты информации сетевых автоматизированных систем 2000.
6. Гамаюнов Д. Ю. Обнаружение компьютерных атак на основе анализа поведения сетевых объектов 2007.
7. Ушаков Д. В. Развитие принципов функционирования систем обнаружения сетевых вторжений на основе модели защищенной распределенной системы 2005.

8. Mahoney M.V., Chan P. K. Learning Models of Network Traffic for Detecting Novel Attacks C. 48.
9. Морозов Д. И. Энтропийный Метод Анализа Аномалий Сетевого Трафика В Ip-Сетях // Известия Трту. 2006. № 7 (62). С. 120–124.
10. KDD Cup 1999 Data [Электронный ресурс]. URL: https://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html (дата обращения: 17.04.2020).
11. 1998 DARPA Intrusion Detection Evaluation Dataset | MIT Lincoln Laboratory [Электронный ресурс]. URL: https://www.ll.mit.edu/r-d/datasets/1998-darpa-intrusion-detection-evaluation-dataset (дата обращения: 17.04.2020).

Журнал «Современная наука: актуальные проблемы теории и практики»

Г. Краснодар