БАЗАРОВА И. А.
АНАЛИЗ СРАВНИТЕЛЬНЫХ ХАРАКТЕРИСТИК СИСТЕМ ЗАЩИТЫ СЕТЕЙ IDS И IPS

УДК 004.056.5, ВАК 05.13.11, ГРНТИ 49.33.35

Анализ сравнительных характеристик систем защиты сетей IDS и IPS

Analysis of comparative characteristics of IDS and IPS network protection systems

И. А. Базарова

Ухтинский государственный технический университет, г. Ухта

I. A. Bazarova

Ukhta State Technical University, Ukhta

В статье представлен обзор и анализ сравнительных характеристик систем защиты сетей IDS и IPS, описание сетевых уязвимостей, способы отслеживания вторжений, недостатки систем защиты. Кроме того, приведены отличия от классических межсетевых экранов.

The article provides an overview and analysis of the comparative characteristics of security systems for IDS and IPS networks, a description of network vulnerabilities, methods of tracking intrusions, and shortcomings of security systems. In addition, the differences from classic firewalls are shown.

Ключевые слова: *кибератаки, защита сетей, IDS, IPS, сетевое вторжение, сетевой трафик, отслеживание вторжений.*

Keywords: *cyber attacks, network protection, IDS, IPS, network intrusion, network traffic, intrusion tracking.*

Введение

Кибератаки - одна из основных проблем современного мира, с которой сталкиваются любые владельцы информационных ресурсов. Даже популярные антивирусные программы и брандмауэры эффективны лишь для защиты очевидных мест доступа к сетям. Однако киберпреступники находят пути обхода и уязвимые сервисы даже в самых совершенных системах безопасности. Актуальность защиты сетей топливно-энергетического комплекса, передающих стратегически важную информацию, особенно велика. И неудивительно, что зарубежные и российские UTM-решения получают все более широкую популярность среди организаций, желающих исключить возможность вторжения и распространения вредоносного программного обеспечения.

В статье производится сравнительный обзор систем защиты сетей IDS и IPS на примерах характеристик вторжения и различных векторов атак, которые киберпреступники могут использовать для компрометации сетевой безопасности.

Основное различие между системами обнаружения вторжений (Intrusion Detection System, IDS) и системами предотвращения вторжений (Intrusion Prevention System, IPS) заключается в том, что IDS выполняет задачи по мониторингу и оповещению, а IPS выполняют задачи по мониторингу и противодействию. IDS не изменяет сетевой трафик, в то время как IPS предотвращает доставку пакетов в зависимости от содержимого пакета, подобно тому, как файервол фильтрует трафик [1].

IDS используют для мониторинга сетей и отправки предупреждений при обнаружении подозрительной активности в системе или сети, в то время как IPS реагирует на кибератаки в режиме реального времени с целью предотвращения проникновения злоумышленников в целевые системы и сети. IDS и IPS способны обнаруживать сигнатуры атак, а главное отличие заключается в их реакции на атаку: как IDS, так и IPS могут реализовывать одни и те же методы мониторинга и обнаружения.

Сетевое вторжение – это любое несанкционированное действие в компьютерной сети. Обнаружение вторжения зависит от понимания сетевой активности и общих угроз безопасности. Правильно спроектированные и развернутые IDS и IPS могут помочь заблокировать активность злоумышленников, которые стремятся украсть конфиденциальные данные, вызвать утечки данных и установить вредоносное ПО.

Сети и конечные точки могут быть уязвимы для вторжений со стороны злоумышленников, которые могут находиться в любой точке мира.

К распространенным сетевым уязвимостям относятся [2]:

1. Вредоносное ПО - это любая программа или файл, наносящий вред пользователю компьютера. Типы вредоносных программ включают компьютерные вирусы, черви, троянские программы, шпионское ПО, рекламное ПО и программы-вымогатели.

2. Социальная инженерия - вектор атаки, который использует человеческую психологию и восприимчивость, чтобы манипулировать жертвами с целью разглашения конфиденциальной информации и конфиденциальных данных или выполнения действий, нарушающих стандарты безопасности. Общие примеры социальной инженерии включают фишинг, целевой фишинг и whaling-атаки.

3. Устаревшее или неисправное программное и аппаратное обеспечение - известные уязвимости, подобные тем, которые указаны в CVE (Common Vulnerabilities and Exposures, база данных общеизвестных уязвимостей информационной безопасности).

4. Устройства хранения данных - портативные устройства хранения, такие как USB и внешние жесткие диски, могут приводить к проникновению вредоносных программ в сеть.

IDS - это устройство или ПО, которое отслеживает сеть или систему на предмет злонамеренных действий и нарушений политик безопасности. О любом вредоносном трафике или нарушении обычно сообщается администратору. Данная

информация собирается централизованно с помощью систем управления информацией и событиями безопасности (Security Information and Event Management, SIEM).

Существует три распространенных варианта, которые IDS использует для отслеживания вторжений [2]:

1. Обнаружение на основе сигнатур - обнаружение атак путем поиска определенных шаблонов, таких как последовательности байтов в сетевом трафике, или поиск сигнатур (известных последовательностей инструкций), используемых вредоносным ПО. IDS на основе сигнатур могут легко обнаруживать известные кибератаки, однако они не способны обнаружить новые виды атак.

2. Обнаружение на основе аномалий - мониторинг активности системы и классификации этой активности, как нормальной или аномальной. Этот тип обнаружения был разработан для обнаружения неизвестных атак. Базовым подходом является использование машинное обучение для создания эталонной модели поведения, заслуживающей доверия, и сравнения нового поведения с эталонной моделью. Поскольку эти модели можно обучать, опираясь на конкретные приложения и конфигурации оборудования, они обладают более универсальными свойствами по сравнению с традиционными IDS на основе сигнатур. Однако, такому типу обнаружения свойственно большое количество ложных срабатываний.

3. Обнаружение на основе репутации - распознает потенциальные киберугрозы на основе оценок репутации.

IPS или системы обнаружения и предотвращения вторжений (Intrusion Detection and Prevention System, IDPS) - это приложения сетевой безопасности, целью которых является выявление возможных злонамеренных действий, логирование активности и оповещение администраторов о попытках вторжения и попытках их предотвращения. Системы IPS часто находятся непосредственно за межсетевым экраном. Для предотвращения вторжения IPS может изменить среду безопасности, перенастроив брандмауэр или изменив содержание сетевых пакетов.

Многие рассматривают IPS, как расширение IDS, поскольку они отслеживают сетевой трафик и действия внутри систем на предмет злонамеренных действий.

Существует три варианта, которые IPS использует для отслеживания вторжений [4]:

1. Обнаружение на основе сигнатур пакетов - отслеживание пакетов в сети и сравнение их с предварительно настроенными и заранее определенными шаблонами атак, известными как сигнатуры.

2. Статистическое обнаружение аномалий - отслеживание сетевого трафика и сравнивает его с базовым трафиком. Базовый трафик используется для определения того, что является «нормальным» в сети, например, какие протоколы используются чаще всего. Этот тип обнаружения аномалий хорош для выявления

новых угроз, однако он может генерировать ложные срабатывания, когда допустимое использование полосы пропускания превышает базовый уровень или когда базовые показатели настроены некорректно.

3. Анализ протоколов с сохранением состояния - метод выявляет отклонения в состояниях протокола путем сравнения наблюдаемых событий с заранее определенными профилями общепринятых определений полезной нагрузки.

После обнаружения девиации в реальном времени IPS выполняет проверку каждого пакета, который проходит в сети, и, если подозрительная активность не прекращается, IPS выполняет одно или несколько из следующих действий [4]:

1. Отключение использующегося TCP-коннекта.

2. Блокировка IP-адреса, со стороны которого исходит активность, или учетную запись пользователя от доступа к любому приложению, хосту или сетевому ресурсу.

3. Перепрограммирование или перенастройка брандмауэра с целью предотвращения подобной атаки в будущем.

4. Удаление вредоносного контента, остающегося после атаки, путем переупаковывания полезной нагрузки, удаления информации из заголовков пакетов или уничтожения зараженных файлов.

При правильном развертывании это позволяет IPS предотвращать серьезные повреждения, вызванные вредоносными или нежелательными пакетами, а также рядом других киберугроз, включая DDOS, эксплойты, компьютерные черви, вирусы, bruteforce-атаки.

На основе проанализированных характеристик какие мы можем выявить недостатки IDS и IPS?

1. Наличие ложных срабатываний - нередко количество реальных атак затмевается количеством ложных срабатываний, что может привести к тому, что настоящие атаки будут проигнорированы. Например, это может произойти по причине наличия шума - пакетов, созданных из-за ошибок ПО, например, содержащих поврежденные данных DNS.

2. Зависимость от баз данных сигнатур - многие атаки используют известные уязвимости, что означает, что библиотека сигнатур должна постоянно обновляться, чтобы быть эффективной. Устаревшие базы данных сигнатур могут сделать уязвимыми сети и системы для новых стратегий атак.

3. Ограниченная защита от ненадежной системы идентификации и аутентификации - злоумышленник может получить доступ из-за плохой защиты паролем, тогда IDS/IPS может быть не в состоянии предотвратить действия злоумышленника.

4. Отсутствие обработки зашифрованных пакетов - большинство IDS/IPS не обрабатывают зашифрованные пакеты, что означает, что шифрованные пакеты могут использоваться для вторжения в сеть.

5. Зависимость от атрибута IP - многие IDS/IPS анализируют информацию на основе сетевого адреса. Это полезно, если IP-пакет приходит от доверенного источника, но доверенный источник можно подделать.

Определим разница между IPS и IDS? Основное отличие состоит в том, что IDS - это система мониторинга, а IPS - это система управления. Оба вида систем анализируют сетевые пакеты и сравнивают их содержимое с базой данных известных угроз или базовой активности. Однако IDS не изменяет сетевые пакеты, в то время как IPS может препятствовать доставке пакетов в зависимости от их содержимого, как это делает брандмауэр.

IDS анализирует и отслеживает трафик на предмет наличия признаков, которые могут указывать на вторжение или кражу данных. IDS сравнивает текущую сетевую активность с известными угрозами, нарушениями политики безопасности и сканированием открытых портов. IDS требует, чтобы человек или система анализировали результаты ее активности и определяли, как реагировать, что делает их эффективным инструментом расследования киберпреступлений после их совершения. Кроме того, IDS не нуждается в том, чтобы быть встроенной в сетевую архитектуру, что не уменьшает скорость трафика.

IPS также имеет возможности обнаружения, но ключевое отличие заключается в возможности блокировки сетевого трафика, если он представляет собой известную угрозу безопасности. Это свойство делает IPS эффективным инструментом предотвращения вторжений.

IDS и IPS могут быть настроены на совместную работу. Многие современные производители сочетают IDS и IPS с межсетевыми экранами [3]. Этот тип технологии называется межсетевым экраном нового поколения (Next-generation firewall, NGFW) или универсальной системой сетевой безопасности (Unified Threat Management, UTM).

А чем IDS и IPS отличаются от классических межсетевых экранов?

Традиционные сетевые брандмауэры используют статический набор правил для разрешения или запрета сетевых подключений. Это может предотвратить вторжения, если заранее известно, как фильтровать трафик. Основная функция брандмауэров заключается в ограничении доступа из внешней сети для предотвращения вторжений, но не для предотвращения атак изнутри сети. IDS и IPS отправляют предупреждения, когда обнаруживают вторжение, а также отслеживают атаки изнутри сети [3].

Выводы

Итак, почему IDS и IPS так важны? Команды обеспечения безопасности крупных компаний сталкиваются с постоянно растущим списком проблем безопасности - от потери и утечек данных до штрафов за несоблюдение нормативов, но при этом они все еще ограничены бюджетом и корпоративной политикой. Именно технологии IDS и IPS призваны помочь охватить и решить важные задачи управления безопасностью сетей, а следовательно, информации.

Список использованных источников и литературы

1. Официальный сайт Cisco Systems американского транснационального технологического конгломерата, статья [Электронный ресурс]. – Режим доступа: https://www.cisco.com/c/en/us/td/docs/security/ips/6-0/installtion/guide/hwguide/hwAIM.html (дата обращения: 03.11.2020).

2. Официальный сайт InfoSec Institute - компания, занимающаяся обучением в сфере технологий [Электронный ресурс]. – Режим доступа: https://resources.infosecinstitute.com/topic/network-design-firewall-idsips/ (дата обращения: 05.11.2020).

3. Официальный сайт американской компании TechTarget, которая предлагает услуги по информационной безопасности, статья “Система предотвращения вторжений” [Электронный ресурс]. – Режим доступа: https://searchsecurity.techtarget.com/definition/intrusion-prevention (дата обращения: 09.11.2020).

4. Англоязычный публичный ресурс сообщества Zentyal, статья “Настройка IDS / IPS с Zentyal” [Электронный ресурс]. – Режим доступа: https://doc.zentyal.org/en/ids.html (дата обращения: 10.11.2020).

5. Англоязычный электронный словарь “TechTerms” терминов computer science, определение “intrusion prevention system” [Электронный ресурс]. – Режим доступа: https://techterms.com/definition/ips (дата обращения: 12.11.2020).

List of references

1. Official site Cisco Systems, Inc. - американского транснационального технологического конгломерата, статья “Cisco Intrusion Prevention System Appliance and Module Installation Guide for IPS 6.0”: https://www.cisco.com/c/en/us/td/docs/security/ips/6-0/installtion/guide/hwguide/hwAIM.html [Electronic resource] (date of the application 03.11.2020).

2. InfoSec Institute, “Network Design: Firewall, IDS/IPS”: https://resources.infosecinstitute.com/topic/network-design-firewall-idsips/ [Electronic resource] - (date of the application 05.11.2020).

3. TechTarget, “Intrusion prevention system (IPS)”: https://searchsecurity.techtarget.com/definition/intrusion-prevention [Electronic resource] (date of the application 09.11.2020).

4. Zentyal, “Configuring an IDS/IPS with Zentyal”: https://doc.zentyal.org/en/ids.html [Electronic resource] (date of the application 10.11.2020).

5. “TechTerms”, “intrusion prevention system”: https://techterms.com/definition/ips [Electronic resource] (date of the application 12.11.2020).