Андреева Я.А, Василевский К.А. Анализ современных систем обнаружения вторжений // Международный журнал информационных технологий и энергоэффективности. – 2023. – Т. 8 № 6(32) с. 134–141

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 004

АНАЛИЗ СОВРЕМЕННЫХ СИСТЕМ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ

[1]Андреева Я.А., [2]Василевский К.А.
Ордена Трудового Красного Знамени ФГБОУ ВО «Московский технический университет связи и информатики» (МТУСИ), Москва, Россия (123423, Москва, ул. Народного Ополчения, 32), e-mail: [1]andreevaya.00@mail.ru, [2]alaxtver@yandex.ru.

В настоящее время, параллельно со стремительным развитием технологий постоянно растет количество различного рода атак злоумышленников, а также скорость генерации новых способов проникновения в системы. Злоумышленники постоянно разрабатывают новые механизмы вторжения и вредоносные программы, а это значит, что вопрос обеспечения информационной безопасности останется актуальным еще долгое время. На данный момент ключевым элементом обеспечения информационной безопасности являются системы обнаружения вторжений (СОВ). В данной статье представлен обзор архитектуры современных СОВ, а также дан сравнительный анализ некоторых открытых средств обнаружения вторжений.

Ключевые слова: информационная безопасность, вторжения, системы обнаружения вторжений, СОВ.

ANALYSIS OF MODERN INTRUSION DETECTION SYSTEMS

[1]Andreeva Ya.A., [2]Vasilevsky K.A.
MTUCI, Moscow, Russia (123423, Moscow, Narodnogo Opolcheniya st., 32), e-mail: [1]andreevaya.00@mail.ru, [2]alaxtver@yandex.ru.

Nowadays, in parallel with the rapid development of technology, the number of various kinds of attacks by intruders is constantly growing, as well as the speed of generating new ways to penetrate systems. Attackers are constantly developing new intrusion mechanisms, which means that the issue of ensuring information security will remain relevant for a long time. At the moment, intrusion detection systems (IDS) are a key element of ensuring information security. This article provides an overview of the architecture of modern IDS, as well as a comparative analysis of some open intrusion detection tools.

Keywords: information security, intrusions, intrusion detection systems, IDS.

Программные продукты всех производителей имеют уязвимости, которые могут представлять угрозу информационной безопасности. Вредоносное программное обеспечение используется в качестве основного инструмента для эксплуатации этих уязвимостей.

В наши дни скорость генерации вредоносных программ очень высока. Это связано с тем, что злоумышленники владеют различными механизмами, позволяющими им генерировать новые варианты вредоносных программ, то есть создавать мутации. Например, полиморфные и метаморфические механизмы модифицируют некоторые части исходного кода вредоносного ПО, вследствие чего антивирусное программное обеспечение не в состоянии его обнаруживать.

Исторически люди использовали системы обнаружения вторжений (СОВ) для защиты своих сетей от злонамеренных воздействий. Традиционные системы обнаружения вторжений включают в себя мониторинг сети и обнаружение сетевых атак с помощью сигнатур. Такие СОВ успешно справляются с задачей обнаружения известных атак, но терпят неудачу в случае возникновения новых. Кроме того, появление новых шаблонов требует обновления базы данных сигнатур, содержащей определение атак, что увеличивает потенциальное окно злонамеренного воздействия.

В методическом документе ФСТЭК России представлено следующее определение СОВ: «система обнаружения вторжений — программное или программно-техническое средство, реализующие функции автоматизированного обнаружения (блокирования) действий в информационной системе, направленных на преднамеренный доступ к информации, специальные воздействия на информацию (носители информации) в целях ее добывания, уничтожения, искажения и блокирования доступа к ней [1]».

Другими словами, системы обнаружения вторжений (англ. Intrusion Detection System (IDS)) — это программные или аппаратные средства, которые позволяют обнаруживать и реагировать на попытки несанкционированного доступа к компьютерной системе или сети.

IDS-системы бывают двух типов: сетевые IDS и хост-IDS. Сетевые IDS используются для мониторинга трафика на сетях. Они работают, просматривая пакеты данных, которые передаются по сети, и обнаруживая аномалии в этом трафике. Сетевые IDS могут быть установлены на маршрутизаторах или коммутаторах, чтобы мониторить весь трафик, проходящий через них. Также могут быть установлены на специальном сервере, который будет мониторить весь трафик в сети. Хост-IDS работают на уровне операционной системы и отслеживают активность на конкретном компьютере. Они могут обнаруживать попытки взлома, вирусы, трояны и другие виды вредоносного программного обеспечения, которы е могут появиться на компьютере. IDS-системы могут быть настроены на обнаружение различных типов атак: попытки взлома паролей, DoS-атаки, сканирование портов и другие. Когда IDS обнаруживает атаку, он может сгенерировать оповещение администратору системы или автоматически запустить процедуры реагирования на эту атаку.

IDS-системы являются важной частью защиты компьютерных систем и сетей от кибератак. Они позволяют быстро обнаруживать аномалии в трафике и предпринимать соответствующие меры для защиты системы.

Анализ обобщенной архитектуры СОВ

На рисунке 1 представлена обобщенная структура СОВ.

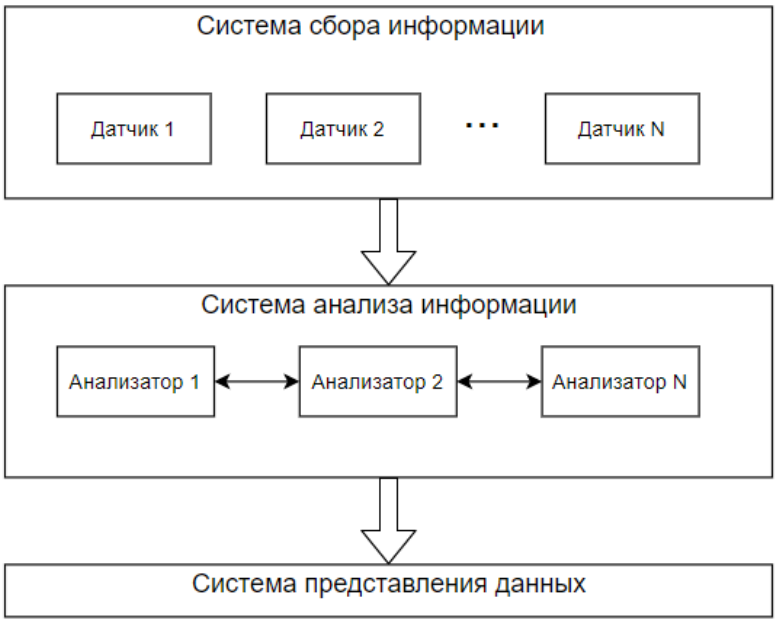

Рисунок 1 – Структурная схема СОВ

В структуре современных СОВ выделяют три главных элемента, представленных на рисунке 2.

Рисунок 2 – Основные элементы СОВ

Система сбора информации собирает информацию о работе объекта защиты. Для сбора информации используются автономные модули – датчики. Количество используемых датчиков различно и зависит от специфики защищаемой системы.

Система анализа состоит из одного или более модулей анализа, которые принято называть анализаторами. Для повышения эффективности обнаружения вторжений, в некоторых системах применяется несколько различных анализаторов.

В качестве входных данных анализаторов выступает информация из системы сбора информации или от других анализаторов.

Результатом работы системы анализа информации является индикация о состоянии защищаемой системы. В случае, если анализатором обнаружено злонамеренное действие, на его выходе появляется некоторая дополнительная информация о зафиксированном нарушении.

Подсистема представления данных выполняет функцию информирования пользователей СОВ о состоянии объекта защиты.

Таким образом, анализаторы являются ключевыми элементами СОВ, которые выполняют роль классификаторов входных данных. Именно анализаторы принимают решение об отнесении поданной на вход информации к какому-либо классу.

Обзор открытых средств обнаружения вторжений

Рассмотрим некоторые СОВ с открытым исходным кодом.

Несмотря на широкое распространение и возрастающую потребность в защите информации, открытых систем обнаружения вторжений крайне мало.

Всего будет рассмотрено 6 наиболее распространенных открытых СОВ. Их краткое описание представлено в таблице 1.

Таблица 1 – Краткое описание открытых СОВ

Наименование СОВ	Ссылка
AAFID	http://www.cs.purdue.edu/coast/projects/autonomousagents.html
ASAX	http://www.ja.net/CERT/Software/asax/
NetSTAT	http://www.cs.ucsb.edu/~kemm/netstat.html/
Prelude	http://www.prelude-ids.org/
SHADOW	http://www.nswc.navy.mil/ISSEC/CID
Snort	http://www.snort.org/

Важнейшим критерием оценки СОВ в рамках данного сравнения является адаптивность к неизвестным атакам. Этот критерий определяет способность СОВ обнаруживать атаки «нулевого дня».

Адаптивность к неизвестным атакам, как и эффективность СОВ зависит от применяемых методов анализа полученной информации.

Большинство существующих систем используют эвристические методы обнаружения атак, которые позволяют детектировать и производить классификацию атак, опираясь на неполные данные и порой неверную классификацию.

Системы, рассмотренные в рамках данного сравнительного анализа, применяются для выявления различного класса атак. Некоторые из них подходят для обнаружения локальных атак и применяют в этих целях журналы систем аудита, журналы регистрации приложений, ОС. К такому типу СОВ относятся AAFID и ASAX.

Для обнаружения сетевых атак наиболее подходящими будут системы, которые используют в качестве источников сетевой трафик. К системам с данным подходом можно отнести Snort, SnortNet и SHADOW.

Остальные СОВ являются гибридными и способны детектировать как локальные, так и внешние атаки.

AAFID (Advanced Anti-Fraud and Intrusion Detection System) — это полностью распределенная СОВ. Система включает ряд агентов, которые для выявления вторжений используют характеристики атак, заданные вручную. Агенты – это программные модули с четко описанными признаками атак, для обнаружения которых они предназначены,

написанные на алгоритмическом языке общего назначения. Отсюда следует, что подобная организация трудно расширяемая и не подходит для обнаружения неизвестных атак.

Агенты могут применять фильтры для аккумулирования данных о поведении объектов.

В своей работе система использует современные методы машинного обучения и анализа данных, которые позволяют ей анализировать большие объемы данных и выявлять аномалии в поведении пользователей и устройств в сети. Она также использует технологии искусственного интеллекта для автоматического обнаружения новых угроз и атак.

AAFID имеет модульную структуру, которая позволяет ей работать с различными типами устройств и операционных систем. Она может быть настроена для работы с любыми типами данных и протоколов связи.

СОВ AAFID имеет широкий спектр функций, включая мониторинг сетевой активности, обнаружение вторжений, предотвращение атак, реагирование на инциденты и генерацию отчетов. Она также может интегрироваться с другими системами безопасности и управления рисками.

В целом, система AAFID является одной из самых передовых систем обнаружения вторжений, которая обеспечивает высокий уровень защиты компьютерных систем от кибератак.

В работе системы обнаружения ворожений ASAX применяется язык описания сценариев атак, эквивалентный по описательной мощности алгоритмическому языку C [2].

NetSTAT (Network Statistics) — это утилита командной строки в операционных системах Windows и Unix, которая позволяет отображать информацию о сетевых соединениях, портах и протоколах. С помощью NetSTAT можно узнать, какие сетевые соединения установлены на компьютере, какие порты используются и какой статус имеет каждое соединение.

С помощью NetSTAT можно выполнить следующие задачи:

- отобразить список всех открытых сетевых соединений на компьютере, включая IP-адреса, порты и статусы соединений;
- отобразить список всех открытых портов на компьютере, включая номер порта, протокол и приложение, которое использует этот порт;
- отобразить статистику использования сетевых интерфейсов, такую как количество отправленных и полученных пакетов данных.

NetSTAT может быть полезен для диагностики сетевых проблем, таких как блокировки портов или неправильно настроенные сетевые соединения. Кроме того, NetSTAT может использоваться для обнаружения вредоносных программ, которые могут использовать открытые порты для передачи данных или получения удаленного доступа к компьютеру. [3].

Система Prelude работает с базой сигнатур известных сетевых атак и с журналами. Для анализа сетевого трафика имеется возможность импорта системы Snort. Также система позволяет интегрировать набор специализированных модулей для детектирования таких атак, как сканирование портов, некорректные ARP-пакеты.

Система обнаружения вторжений SHADOW состоит из двух основных типов компонентов – сенсоров сетевого трафика и анализаторов. СОВ использует язык Perl для описания различных фильтров. В анализаторах системы хранится база знаний разработчиков системы о том, какие пакеты могут свидетельствовать о наличии атаки.

Одной из самых популярных систем обнаружения вторжений является утилита Snort. Snort — это бесплатная и открытая СОВ, которая используется для мониторинга сетевого

трафика и обнаружения потенциальных угроз безопасности. Она может работать на различных операционных системах, включая Windows, Linux и macOS.

С помощью Snort можно настраивать правила, определяющие типы атак, которые нужно обнаруживать. Эти правила могут быть созданы самостоятельно или загружены из общедоступных баз данных, таких как OpenAppID и Emerging Threats.

Snort может работать в режиме обнаружения вторжений (IDS) и в режиме предотвращения вторжений (IPS), что позволяет не только обнаруживать угрозы, но и блокировать их.

Кроме того, Snort имеет множество дополнительных модулей и расширений, которые позволяют расширить его функциональность, такие как Snorby, Barnyard2 и PulledPork.

Snort является одним из самых популярных инструментов IDS в мире и широко используется в крупных организациях и правительственных учреждениях для защиты своих сетей.

В работе [5] было впервые предложено использовать деревья решений вместо обычного модуля обнаружения в системе Snort. Эксперименты были проведены на устаревшем датасете DARPA [6]. В данном исследовании авторы смогли доказать, что использование деревьев решений дает возможность увеличить скорости обработки сетевых пакетов более чем на 40%.

Другими широко применяемыми подходами машинного обучения являются алгоритмы кластеризации и регрессии.

В исследовании [7] автор анализирует вопросы, связанные с эффективностью применения систем машинного обучения для задач обнаружения атак «нулевого дня». Автор высказал предположение, что сочетание методов классификации и кластеризации способно привести к лучшим результатам и защитит от ложноположительных срабатываний.

В 2009 году авторы исследования [8] предложили модель нейронной сети с прямой связью для создания СОВ, которая для обучения использует алгоритм обратного распространения ошибки. Авторы также провели тестирование на датасете DARPA KDD’98. По результатам тестирования сеть имела точность 76% на тестовом наборе данных, состоящем из 100 экземпляров.

В исследовании [9] авторы проверили потенциальную возможность применения глубокой нейронной сети в качестве классификатора различных типов атак. Для этой задачи многослойная нейронная сеть прямой связи была обучена с использованием набора данных KDD. В исследовании сообщается о точности обучения составила 99%.

В работе [10] построили классификатор на основе модели глубокой нейронной сети для системы обнаружения вторжений в среде SDN и обучили модель с помощью набора данных NSL-KDD. Исследователи ограничили признаковое пространство до 6 признаков. Результаты показали, что нейронные сети позволяют получить приемлемую скорость обнаружения вторжений только с использованием ограниченного числа признаков.

Выводы

В данной статье представлен обзор обобщенной архитектуры средств обнаружения вторжений, из которого видно, что ключевым элементов СОВ являются анализаторы, которые выполняют роль классификаторов входных данных. Именно анализаторы принимают решение об отнесении поданной на вход информации к какому-либо классу.

Стоит отметить, что СОВ не являются идеальным решением для защиты от всех видов атак. Некоторые виды атак могут обойти СОВ, например, если они используют шифрование или маскировку. Кроме того, системы обнаружения вторжений могут давать ложные срабатывания, что может приводить к перегрузке системы уведомлениями о ложных атаках.

Для максимальной эффективности, СОВ должны быть использованы в сочетании с другими средствами защиты, такими как брандмауэры, антивирусное программное обеспечение и системы аутентификации. Это позволяет создать комплексную систему защиты, которая будет максимально эффективна против различных типов атак.

В целом, IDS-системы являются неотъемлемой частью безопасности компьютерных систем и сетей. Они позволяют быстро обнаруживать и реагировать на атаки, что позволяет минимизировать возможный ущерб и сохранить целостность системы. Поэтому, при разработке системы безопасности, следует уделить особое внимание выбору и настройке СОВ.

Проведенный анализ нескольких распространенных систем обнаружения вторжений с открытым исходным кодом показал, что на сегодняшний день нет открытой и общедоступной СОВ, которая могла бы в режиме реального времени адаптироваться к неизвестным атакам. Наиболее распространенные методы обнаружения вторжений способны обнаружить неизвестные атаки лишь после явного указания их описания в базе знаний системы. Еще одним недостатком рассмотренных систем является необходимость в их постоянной поддержке.

На основании проведенного обзора можно сделать вывод, что наиболее перспективными в сфере обнаружения вторжений являются методы машинного и глубокого обучения, а разработка системы обнаружения вторжений в компьютерную сеть, способной обнаруживать неизвестные ранее аномалии, является актуальной и востребованной задачей.

Список литературы

1. ИТ.СОВ.У5.ПЗ. Методический документ ФСТЭК России. Профиль защиты систем обнаружения вторжений уровня узла пятого класса защиты“ (утв. ФСТЭК России 06.03.2012).
2. Mounji A. “Languages and Tools for Rule-Based Distributed Intrusion Detection“ / A. Mounji // Computer Science - 1997.
3. Khraisat A. “Survey of Intrusion Detection Systems: tTechniques, Datasets and Challenges“ / A. Khraisat, I. Gondal, P. Vamplew // Cybersecurity – 2019.
4. Zhang, “Research on IDS Snort Based on Classic Clustering Algorithm“ / Zhang, Gongguo, Li // International Conference on Urban Engineering and Management Science (ICUEMS) – 2020 – PP. 673-676.
5. Kruegel C. “Using Decision Trees to Improve Signature-Based Intrusion Detection“ / C. Kruegel, T. Toth // Recent Advances in Intrusion Detection - 2003 -PP. 173–191.
6. “DARPA Intrusion Detection Data Sets“ (Интернет ресурс, дата обращения 26.04.2022) - [https://www.ll.mit.edu/ideval/data].
7. Miller M. “Are we protected yet? developing a machine learning detection system to combat zero-day malware attacks” / M. Miller // IEEE International Conference on Big Data (Big Data) - 2018.
8. Shun J. “Network Intrusion Detection System Using Neural Networks” / J. Shun, A. Malki // Fourth Int. Conf. Nat. Comput. - 2009 - vol. 5 - PP. 242–246.

9. Roy S. “A deep learning based artificial neural network approach for intrusion detection,” / S. Roy, A. Mallik, R. Gulati // Communications in Computer and Information Science - 2017.
10. Tang T. “Deep learning approach for Network Intrusion Detection in Software Defined Networking” / T. Tang, L. Mhamdi, D. McLernon // International Conference on Wireless Networks and Mobile Communications, WINCOM – 2016

References

1. IT.SOV.U5.PZ. Methodological document of the FSTEC of Russia. Protection profile of intrusion detection systems at the node level of the fifth protection class” (approved by the FSTEC of Russia on 03/06/2012).
2. Mounji A. “Languages and Tools for Rule-Based Distributed Intrusion Detection“ / A. Mounji // Computer Science - 1997.
3. Khraisat A. “Survey of Intrusion Detection Systems: tTechniques, Datasets and Challenges“ / A. Khraisat, I. Gondal, P. Vamplew // Cybersecurity - 2019.
4. Zhang, “Research on IDS Snort Based on Classic Clustering Algorithm“ / Zhang, Gongguo, Li // International Conference on Urban Engineering and Management Science (ICUEMS) – 2020 – PP. 673-676.
5. Kruegel C. “Using Decision Trees to Improve Signature-Based Intrusion Detection“ / C. Kruegel, T. Toth // Recent Advances in Intrusion Detection - 2003 - PP. 173–191.
6. “DARPA Intrusion Detection Data Sets“ (Internet resource, accessed 26.04.2022) - [https://www.ll.mit.edu/ideval/data].
7. Miller M. Are we protected yet? developing a machine learning detection system to combat zero-day malware attacks” / M. Miller // IEEE International Conference on Big Data (Big Data) - 2018.
8. Shun J. “Network Intrusion Detection System Using Neural Networks” / J. Shun, A. Malki // Fourth Int. Conf. Nat. Comput. - 2009 - vol. 5-PP. 242–246.
9. Roy S. “A deep learning based artificial neural network approach for intrusion detection,” / S. Roy, A. Mallik, R. Gulati // Communications in Computer and Information Science - 2017.
10. Tang T. “Deep learning approach for Network Intrusion Detection in Software Defined Networking” / T. Tang, L. Mhamdi, D. McLernon // International Conference on Wireless Networks and Mobile Communications, WINCOM – 2016