УДК 004.4+004.41+004.62

Ван Синь, студент,
Институт компьютерных и инженерных наук,
Амурский государственный университет,
г. Благовещенск

Научный руководитель:
Бушманов А.В.
Амурский государственный университет,
г. Благовещенск

ОБЗОР ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ И ОПТИМИЗАЦИИ РЕАГИРОВАНИЯ НА ОСНОВЕ ТЕОРИИ ИГР
OVERVIEW OF INTRUSION DETECTION AND RESPONSE OPTIMIZATION BASED ON GAME THEORY

Аннотация: В настоящее время масштабы сети резко возросли, а различные процессы вторжения постепенно превратились в тенденцию усложнения и диверсификации. Потери, вызванные кибератаками, становятся все более серьезными, и становится все труднее обнаруживать, обнаруживать, расследовать и реагировать на различные инциденты безопасности. Технологии обнаружения вторжений и реагирования на них приобретают все большее значение для быстрого выявления и реагирования на различные инциденты кибербезопасности. Способность системы обнаружения вторжений (IDS) выявлять сложные шаблоны атак и анализировать большие объемы сетевого трафика зависит в основном от ее точности и конфигурации, что делает оптимизацию обнаружения вторжений и реагирования на них важным требованием к безопасности сети и системы, и стало активной темой исследований.

Abstract: At present, the scale of the network has increased dramatically, and various intrusion processes have gradually developed into a trend of complexity and diversification. The losses caused by cyber attacks are becoming more and more serious, and it is becoming increasingly difficult to detect, detect, investigate and respond to various security incidents. Intrusion detection and response technologies are becoming increasingly important in order to quickly identify and respond to various cybersecurity incidents. The ability of an intrusion detection system (IDS) to identify complex attack patterns and analyze large amounts of network traffic depends mainly on its precision and configuration, which makes the optimization of intrusion detection and response an important requirement for network and system security, and has become an active research topic.

Ключевые слова: обнаружение вторжений; реакция на вторжение; многоагентное обучение с подкреплением; кибербезопасность

Keywords: game theory; intrusion detection; intrusion response; multi-agent reinforcement learning; cyber security

В связи со стремительным развитием интернета масштабы сети постепенно расширялись, а также значительно возросло количество атак на сеть. В то время как жизнь людей стала более неотделимой от интернета, вопросы кибербезопасности также влияют на стабильность целых стран и обществ. В результате обеспечение безопасности сетевых систем стало сложной задачей. Однако традиционные решения кибербезопасности, такие как межсетевые экраны и антивирусные системы, уже не в состоянии справиться со сложными кибератаками. Для решения этих проблем и смягчения неизвестных угроз система обнаружения вторжений была развернута в качестве логического дополнения к технологии

межсетевых экранов и быстро стала важным компонентом информационной системы защиты, улучшая возможности управления безопасностью системы управления сетевой безопасностью.

Обнаружение вторжений – это технология, которая идентифицирует вторжения, которые произошли, находятся в процессе и вот-вот произойдут. Он собирает и анализирует критически важную информацию о компьютерной сети или операционной системе для выявления нарушений политики безопасности и следов атак. Специальная технология обнаружения вторжений, останавливает атаки до того, как они достигнут системы. Предотвращение вторжений отличается от общего обнаружения вторжений, оно может не только выявлять потенциальные угрозы, но и быстро реагировать, а также является технологией безопасности, которая может отслеживать поведение передачи данных по сети и предотвращать ненормальное или вредное поведение сети. Методика автоматизации контрмер и реакции на вторжение целиком и полностью называется реакцией на вторжение. Обнаружение вторжений и реагирование на них открывает замкнутую систему защиты от обнаружения, обнаружения, раннего предупреждения и реагирования, а также улучшает возможности защиты системы. Текущие системы здравоохранения в различных странах предлагают разнообразные решения для онлайн-консультаций, самообслуживания пациентов и доступа к личной медицинской информации. В России многие системы сталкиваются с проблемами сложности интерфейсов, недостатка комплексного охвата и слабо развитой интеграции с традиционными медицинскими учреждениями. В то же время в других странах, особенно в технологически развитых, онлайн-системы здравоохранения активно развиваются и используются для повседневной медицинской помощи, облегчая пациентам доступ к консультациям и сведениям о состоянии здоровья.

Самая большая проблема при обнаружении вторжений – это сложность анализа тысяч оповещений. Классификация оповещений в порядке важности является важным шагом, необходимым для инициирования соответствующего реагирования и смягчения киберугроз. Во многих исследовательских работах были достигнуты эффективные результаты в повышении эффективности обнаружения интрузий, но в этих работах не было уделено внимания оптимизации детектирования интрузий. Теория игр дает нам новый взгляд на безопасность: безопасность – это не отсутствие угроз, а то, что атака на систему обходится дороже, чем ее отсутствие. Исследователи применяют теорию игр для оптимизации обнаружения вторжений, чтобы обеспечить наилучший компромисс для данной проблемы при определенных ограничениях ресурсов, таких как выбор сетевых узлов, которые должны быть приоритетными для мониторинга, или лучший выбор для развертывания системы предотвращения вторжений после атаки. Создание системы управления здоровьем на базе Java предоставляет значительные возможности для повышения удобства и эффективности такой платформы. Технология Java предлагает широкий выбор библиотек и инструментов для создания гибких и масштабируемых решений. Использование Java позволяет разрабатывать системы с возможностью дальнейшего расширения, чтобы включить дополнительные функции, такие как анализ данных, автоматизированные оповещения и интеграция с другими сервисами.

Технология обнаружения вторжений – это технология информационной безопасности, предназначенная для обеспечения безопасности компьютерных сетей и операционных систем, которая может своевременно обнаруживать несанкционированное и аномальное поведение в системе. Он может не только выявлять внешние атаки на компьютерные сети, но и обнаруживать некоторые несанкционированные сетевые действия внутри. После десятилетий развития технология обнаружения вторжений прошла путь от простой исследовательской идеи и теоретической модели до широкого спектра прототипов систем и коммерческих продуктов.

Список литературы:

1. Ли Яньпэн, Дэн Айчжэнь, Хэ Сичун и др. Проектирование и внедрение системы управления бронированием отелей на базе.NET.DOI:10.15966/j.cnki.dnydx.2019.07.011.

2. Ван Цзэю. Проектирование и внедрение системы управления отелем. DOI:10.27131/d.cnki.ghugc.2018.000100.

3. Лю Фэнчжи и Му Баолян. Разработка и внедрение системы бронирования номеров в гостиницах малого и среднего размера на основе B/S.