Сигнатурные методы обнаружения компьютерных кибератак в информационных системах

УДК 004.056.53

Толюпа С.В.[1], Самохвалов Ю.Я.[2]

КНУ им. Тараса Шевченко, [1]tolupa@i.ua, [2]yu1953@ukr.net

Системы обнаружения сетевых вторжений и выявления признаков кибератак на информационные системы уже давно применяются как один из необходимых рубежей обороны информационных систем. Исследования в области обнаружения кибератак ведутся за рубежом уже больше четверти века. Исследуются признаки кибератак, разрабатываются и эксплуатируются методы и средства обнаружения попыток несанкционированного проникновения через системы защиты, как межсетевой, так и локальной на логическом и даже на физическом уровнях. В действительности, сюда можно отнести даже исследования в области

На сегодня системы обнаружения вторжений и кибератак обычно представляют собой программные или аппаратно-программные решения, которые автоматизируют процесс контроля событий, протекающих в компьютерной системе или сети, а также самостоятельно анализируют эти события в поисках признаков проблем безопасности. Поскольку количество различных типов и способов организации несанкционированных проникновений в чужие сети за последние годы значительно увеличилось, системы обнаружения кибератак (СОКа) стали необходимым компонентом инфраструктуры безопасности большинства организаций. Этому способствуют и огромное количество литературы по данному вопросу, которую потенциальные злоумышленники внимательно изучают, и все более изощренные методы и сложные и подходы к обнаружению попыток взлома информационных систем.

Системы обнаружения кибератак, как и большинство современных программных продуктов, должны удовлетворять ряду требований. Это и современные технологии разработки, и ориентировка на особенности современных информационных сетей, и совместимость с другими программами. Чтобы понять, как правильно использовать СОКа, нужно четко представлять, как они работают и каковы их уязвимые места.

Если не учитывать различные несущественные инновации в области обнаружения компьютерных атак, то можно смело утверждать, что существуют две основные технологии построения СОКа. Суть их заключается в том, что СОКа обладают некоторым набором знаний либо о методах вторжений, либо о нормальном поведении наблюдаемого объекта.

Системы обнаружения аномального поведения основаны на том, что СОКа известны некоторые признаки, характеризующие правильное или допустимое поведение объекта наблюдения. Под нормальным или правильным поведением понимаются действия, выполняемые объектом и не противоречащие политике безопасности. Предлагается использовать сигнатурное описание кибератаки.

Сигнатурные методы позволяют описать кибератаку набором правил или с помощью формальной модели (рис. 1), в качестве которой может применяться символьная строка, семантическое выражение на специальном языке и т.п. Суть данного метода заключается в использовании специализированной базы данных шаблонов (сигнатур) кибератак для поиска действий, подпадающих под определение "кибератака".

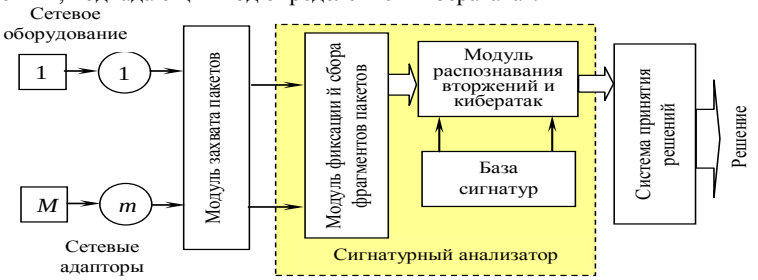

Рис. 1. Структура статистичного анализатора

Сигнатурный метод может защитить от вирусной или хакерской кибератаки, когда уже известна сигнатура кибератаки и она внесена в базу данных СОКа. То есть, когда сеть переживает первое нападение извне, первое заражение еще неизвестным вирусом и в базе попросту отсутствует сигнатура для его поиска, сигнатурная СОКа не сможет сигнализировать об опасности, поскольку сочтет атакующую деятельность легитимной.

Большинство существующих программных продуктов, заявляющих об использовании сигнатурного метода, на самом деле реализуют как раз наиболее примитивный способ сигнатурного распознавания. Многие системы позиционируются как предназначенные для выявления атак в информационных системах на основе интеллектуального анализа сетевых пакетов. На самом же деле сигнатурный метод реализован как алгоритм, исследующий лишь динамику развития кибератаки, основанный на автомате состояний для оценки сценария развития атаки. По замыслу такой подход должен позволить отследить динамику развития кибератаки в соответствии с действиями злоумышленника, при этом в качестве модуля сбора данных могут использоваться даже сами системы обнаружения кибератак.

Таким образом, эффективность работы сигнатурной СОКа определяется тремя основными факторами: оперативностью пополнения сигнутарной базы, ее полнотой с точки зрения определения сигнатур кибератак, а также наличием интеллектуальных алгоритмов сведения действий атакующих к некоторым базовым шагам, в рамках которых происходит сравнение с сигнатурами.

Литература:

1. Бугров Ю. Г. Системные основы оценивания и защиты информации: Учеб. пособие / Воронеж: Воронеж. гос. техн. ун-т, 2005. – 354 с.

2. В.Л. Бурячок, С.В. Толюпа, А.О. Аносов “Системний аналіз та прийняття рішень в інформаційній безпеці”. - К. : ДУТ, 2015. – с. 345.