УДК 004

АЛГОРИТМЫ НЕЙРОННЫХ СЕТЕЙ ДЛЯ КЛАССИФИКАЦИИ ЛЕГИТИМНОСТИ СЕТЕВОГО ТРАФИКА.

Чумаков В.Е.

Студент 2 курса напр. «Интеллектуальные системы и технологии»,

ИСОиП (филиал) ДГТУ г. Шахты

Россия, Шахты

Аннотация

В статье рассмотрены возможности проведения анализа трафика в полосе пропускания. Также приведены два типа нейронных сетей для обнаружения атак типа Dos и DDos. Была раскрыта их структура, назначение и принцип работы. Был приведен пример моделирования аномального трафика. Рассмотрен пример использования эксплойта.

Ключевые слова: безопасность сетевого трафика, карты Кохонена, многослойный персептрон, эксплойты.

THE ALGORITHMS OF NEURAL NETWORKS FOR THE CLASSIFICATION OF THE LEGITIMACY OF NETWORK TRAFFIC.

Chumakov V. E.

2nd year student e.g. "Intelligent systems and technologies»,

Isoip (branch) of DSTU Shakhty

Russia, Shakhty

Annotation

The article considers the possibilities of traffic analysis in the bandwidth. There are also two types of neural networks for detecting Dos and DDos attacks. Their

structure, purpose and principle of operation were revealed. An example of abnormal traffic simulation was given. An example of using an exploit is considered.
Keywords: network traffic security, Kohonen maps, multilayer perceptron, exploits.

В настоящее время, программные и аппаратно–программные средства не имеют возможности обеспечить полную защиту от атак типа Dos (Denial of Service «отказ в обслуживании) и DDos (Distributed Denial of Service «распределенный отказ в обслуживании») в компьютерных сетях предприятий. Межсетевые экраны, являются одним из эффективных средств для защиты от перечисленных угроз, но также в свою очередь они вызывают определенные трудности, так как возникает необходимость определять легитимность поступающих пакетов в сети. Также эффективным инструментом считаются системы обнаружения вторжений, которые используют предприятия с большой сетевой инфраструктурой. Такие системы руководствуются двумя основными подходами, а именно сигнатурным и поведенческим [1].

Сигнатурный позволяет анализировать проходящий сетевой трафик и сравнивать его с имеющейся базой сигнатур о вредоносных программах и оповещать ответственное лицо о возможном обнаружении вредоносного объекта.

Поведенческий позволяет исследовать нормальное поведение пользователя и различных приложений в сети и обнаруживать аномальное поведение перечисленных объектов.

Тем самым, вредоносное программное обеспечение может избежать обнаружения, пока его сигнатура не внесена в базу системы обнаружений вторжений. Для повышения эффективности защиты сети предприятия используют нейросетевые технологии, поскольку они не имеют в своём составе баз, которые необходимо пополнять, после обнаружения нового вида

атаки, а обучаются обнаружению, на уже ранее проведенных тестовых наборах. В статье будут рассмотрены нейросети типа многослойный персептрон и гибридная нейросеть, состоящая из многослойного персептрона и самоорганизующейся сети Коханена. Перейдем к рассмотрению перечисленных технологий.

Многослойный персептрон – это нейронная сеть прямого распространения, входной сигнал которой распространяется от слоя к слою и состоит из следующих элементов [2]:

- входные данные, которые составляют входной слой;
- один или несколько скрытых слоёв;
- один выходной слой.

В сети с многослойным персептроном выход обеспечивается путём срабатывания функции активации типа гиперболического тангенса, тем самым выходной нейрон превращается в сумму всех весов связей между скрытыми уровнями и выходным уровнем нейронной сети. Примером входа для сети обнаружения атак может служить набор разных пакетов, например, TCP,UDP,IP за определенный промежуток времени без определения легитимности рассматриваемых пакетов. Целью данной сети является минимизация ошибки работы многослойного персептрона, тем самым выход может быть получен при использовании алгоритма обратного распространения, который заключается в уменьшении разницы между выходными данными, полученными в процессе обучения и необходимыми выходными данными.

Алгоритм работы такой сети можно представить в виде блок-схемы, проиллюстрированной на рисунке 1.

Рисунок 1 – Иллюстрация алгоритма работы сети с многослойным персептроном.

Теперь необходимо рассмотреть нейросети с применением карт Кохонена. Такие карты группируют аналогичные события по своей структуре в нейросети и позволяют собирать сгруппированные события в отдельные кластеры. Примером входного вектора такой сети могут служить адрес передающегося пакета и порт, по которому он передаётся. Следующим этапом может служить группировка входных пакетов, тем самым принадлежность пакета должна быть заранее известна к тому или иному кластеру. После чего устанавливается многослойный персептрон, который способен выявить возможные неправильно заполненные заголовки пакетов, тем самым уведомить ответственное лицо о возможной атаке на определенную компьютерную машину. Процесс работы рассматриваемой сети представлен на рисунке 2.

Рисунок 2 – Модель работы гибридной нейросети

Рассматриваемая сеть способна обнаружить Dos и DDos атаку, так как позволяет произвести анализ отдельных узлов каждого кластера в сети Кохонена, которые в свою очередь являются одним из сценариев возможной атаки и обнаружить различные перепады сетевого трафика, проходящего через коммутационное оборудование, чтобы выявить перепад в нагрузке полосы пропускания, ведь именно эти два параметра позволяют с уверенностью сказать, что происходит атака типа Dos. Для проверки работы такой сети необходимо смоделировать два трафика. Первый характеризует обычное поведение сетевого трафика в инфраструктуре предприятия, второй характеризует аномальное поведение сетевых приложений и проходящего сетевого трафика. Смоделировать аномальный трафик можно различными методами, одним из эффективных и управляемых ответственным лицом методов, является запуск эксплойта на машине, которая является атакующим звеном.

Эксплойт – это подвид вредоносного программного обеспечения, который способен нанести вред машине, подверженной атаке, при использовании ранее найденных уязвимостей в каких-либо службах или приложениях, установленных на этой машине [3].

Для примера моделирования аномального трафика можно воспользоваться эксплойтом Angler Exploit kit [4]. Например, такой эксплойт может воспользоваться уязвимостью операционных систем типа Windows и OS X и самопроизвольно запустить код во Flash – версии приложений или самопроизвольно отключить ASLR, который является своего рода защитным механизмом и позволяет случайным образом заменять в адресном пространстве важные структуры данных, например, исполняемые файлы различных приложений или библиотеки, необходимые для стабильной работоспособности таких приложений, тем самым можно смоделировать аномальный трафик для проведения проверки работоспособности алгоритма нейросети.

Таким образом, можно сделать вывод, что нейросетевые технологии обладают высокой производительностью, более тонкой настройкой и минимальным уровнем ошибок при обнаружении такого рода атак, тем самым нейросетевые технологии занимают лидирующее место в компьютерной индустрии, как средства по обнаружению возможных атак на компьютерную сеть предприятия.

Библиографический список

1. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. –М.,2016. – 592с.
2. Ерёмин И.А. Портал искусственного интеллекта [Электронный ресурс]. – Режим доступа - URL: http://www.aiportal.ru/articles/neuralnetworks/multiperceptron (дата обращения 25.09.2019)
3. Калмыков С.И. Защита от эксплойтов [Электронный ресурс]. – Режим доступа - URL: https://www.avast.ru/c-exploits (дата обращения 27.09.2019)
4. Захарья А.С. Способ установки эксплойтов [Электронный ресурс]. – Режим доступа - URL: https://heimdalsecurity.com/blog/ultimate-guide-angler-exploit-kit-non-technical-people/ (дата обращения 29.09.2019)

Оригинальность 98%