МИНОБРНАУКИ РОССИИ
САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ
ЭЛЕКТРОТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
«ЛЭТИ» ИМ. В.И. УЛЬЯНОВА (ЛЕНИНА)
Кафедра МО ЭВМ

ОТЧЕТ

по описанию предполагаемого решения задачи

ТЕМА: МОДЕЛИ И МЕТОДЫ ОБНАРУЖЕНИЯ DDOS-АТАК В ОБЛАЧНЫХ ВЫЧИСЛИТЕЛЬНЫХ СРЕДАХ НА ОСНОВЕ ТЕХНОЛОГИИ ИНТЕЛЛЕКТУАЛЬНОГО АНАЛИЗА ДАННЫХ

Студент гр. 3304 _____ Сандин А.В.

Санкт-Петербург
2018

Цель работы.

Целью работы является описание предполагаемых моделей и методов обнаружения DDoS-атак в облачных вычислительных средах на основе технологии интеллектуального анализа данных.

Формулировка задачи.

Описать метод предполагаемого решения задачи, указать преимущества данного метода над другими.

Выполнение.

Метод обнаружения сетевых атак в облачных вычислительных средах состоит из трех этапов: подготовительного, первичного обучения, запуска системы защиты. После выбора точек расположения компонентов системы защиты и их установки оператор запускает первичное обучение компонентов обнаружения вредоносной активности. Это необходимо, так как в основе процесса обнаружения лежат модели интеллектуального анализа данных. Алгоритм обнаружения состоит из двух уровней для сокращения потребления ресурсов. На первом уровне проверяется наличие вредоносного трафике в вычислительной среде. Если модель классифицировала трафик как вредоносной, то активируется второй уровень глубинного анализа, на котором определяются источники атак и их жертвы. После первичного обучения моделей, они внедряются в систему, после чего система может работать в автоматическом режиме.

В условиях высоконагруженных облачных вычислительных сред в качестве данных для принятия решений по классификации трафика были выбраны данные о потоках трафика, а не о каждом пакете. Это позволяет существенно сократить время обработки трафика и генерации входных векторов для моделей интеллектуального анализа данных.

Для моделирования вредоносного и легитимного трафика был создан полигон, включающий в себя методы натурного и имитационного моделирования. Сценарии поведения клиентов задаются программно. Было создано 9 типов атак, сценарии для которых можно задать в конфигурационном файле. На любом участке имитируемой сети можно установить компонент защиты, сбора трафика, что дает возможность тестировать архитектурно-зависимые методы защиты. В качестве сценариев для легитимного трафика могут быть использованы сценарии атак, к пример, HTTP Flooding, с меньшими нагрузками и частой запросов от одного клиента.

В качестве базовых типов атак в облачных вычислительных средах были выбраны следующие атаки: SYN Flooding, HTTP Flooding, NTP Flooding. Они являются основными атаками, которые используются на сегодняшний день, а также по данным о потоках трафика похожи на многие другие типы атаки, такие как Chargen, UDP Flooding и т.д.

Для разработки системы защиты и ее тестирования была выбрана платформа OpenStack. OpenStack является системой с открытым кодом и широко поддерживается в сообществе. Также данная система предлагает системный подход управления комплексными услугами платформы облачных вычислений, которые включают в себя: обеспечение безопасности, систему хранения данных, межсетевое взаимодействие, управление работой виртуальных машин, отслеживание действий, происходящих внутри проекта, при помощи информационной панели.