УДК 004.056.2

РАЗРАБОТКА МЕТОДА ОБНАРУЖЕНИЯ И ОПРЕДЕЛЕНИЯ ХАРАКТЕРА АНОМАЛЬНОГО ПОВЕДЕНИЯ УСТРОЙСТВ В ЛОКАЛЬНЫХ СЕТЯХ С ПРИМЕНЕНИЕМ МИКРОСЕГМЕНТАЦИИ

Устин Д.А. (Университет ИТМО), **Колесников Н.Д.** (Университет ИТМО), **Есипов Д.А.** (Университет ИТМО)

Научный руководитель – доцент, кандидат технических наук Попов И.Ю. (Университет ИТМО)

Введение. На сегодняшний день как никогда стремительно развиваются технологии, в том числе, связанные с построением сетевой инфраструктуры организаций. Крупные российские компании начинают все чаще применять микросегментацию при построении своих сетей. Необходимо отметить, что под микросегментацией поднимается разделение сети на ряд сегментов с использованием технологии VLAN (деление, как правило, производится по типу устройства, однако может выполняться и по другим признакам, например, разделение может быть по отделам организации). Применение микросегментации приводит к изменению характера сетевого трафика (например, появляется дублирование сетевых пакетов на коммутаторах, а также увеличивается количество пакетов, проходящих через маршрутизаторы), что приводит к усложнению его анализа, а, следовательно, и к снижению точности средств защиты данный анализ выполняющих.

Помимо этого, на фоне участившихся атак на корпоративные сети организаций [1], актуальной проблемой является выявление подмены устройств во внутреннем сегменте сети (подменяется, как правило, VoIP телефон или принтер на подготовленное устройство, например, на базе RasverryPi). Сложность выявления связана с тем, что опытный злоумышленник при такой подмене может применять MAC-spoofing с целью обхода port security, может использовать средства генерации сетевого трафика, характерного для конкретного типа устройств (например, vgetty в случае подмены VoIP телефона), а также может применять рукописное ПО для обхода signature based IDS.

В результате применения микросегментации снижается количество и качество источников сетевого трафика, что отражается на точности работы систем обнаружения вторжений, а применение злоумышленниками описанных выше техник при выполнении атак с подменой устройств существенно снижает вероятность обнаружения их с использованием signature и anomaly based IDS. Таким образом, разработка решения способного решить данные проблемы является крайне актуальной задачей.

Основная часть. В данной работе для решения проблем обнаружения аномального поведения устройств в локальных сетях с применением микросегментации предполагается использовать раздельный анализ межсетевых взаимодействий и взаимодействий в рамках сегментов, а также выполнять анализ сетевого трафика не в исходном виде (в формате сетевых пакетов, либо потоков), а в виде соединений (формат, получаемый в результате преобразования собранного сетевого трафика к форме, описывающей взаимодействие хоста с другими хостами и его характеристики).

Предполагаемый метод обнаружения и определения характера аномального поведения устройств в локальных сетях с применением микросегментации включает в себя следующие этапы:

1) сбор и предобработка сетевого трафика;
2) анализ межсетевых взаимодействий;
3) анализ взаимодействий в рамках сегмента;
4) классификация сетевых атак.

В ходе анализа взаимодействий будет производится определение предполагаемой группы устройств, участвующих в взаимодействии (выполнять данное действие предполагается с использованием соотнесения пары IP-адрес / MAC-адрес с ожидаемой группой, либо путем выбора наиболее близкой группы исходя из характеристик соединения).

Классификацию сетевых атак предполагается выполнять в случае обнаружения аномального сетевого трафика в ходе анализа межсетевых взаимодействий и взаимодействий в рамках сегмента с использованием метода машинного обучения с учителем, поскольку данный подход продемонстрировал хорошие результаты в прошлом [2-4].

Выводы. В данной работе представлен метод обнаружения и определения характера аномального поведения устройств в локальных сетях с применением микросегментации. В дальнейшей работе предполагается выбор наиболее подходящего для решения задачи классификации сетевых атак метода машинного обучения с учителем, а также программная реализация разрабатываемого метода с целью оценки его точности обнаружения аномального поведения устройств в локальной сети организации.

Список использованных источников:

1) Check Point Research. Cyber Attacks Increased 50% Year over Year. – [Электронный ресурс]. – Режим доступа: https://blog.checkpoint.com/2022/01/10/check-point-research-cyber-attacks-increased-50-year-over-year/.

2) Mol P. R., Mary C. I. Classification of Network Intrusion Attacks Using Machine Learning and Deep Learning^ //Annals of the Romanian Society for Cell Biology. – 2021. – С. 1927-1943.

3) Tait K. A. et al. Intrusion detection using machine learning techniques: an experimental comparison //2021 International Congress of Advanced Technology and Engineering (ICOTEN). – IEEE, 2021. – С. 1-10.

4) Khatib A., Hamlich M., Hamad D. Machine Learning based Intrusion Detection for Cyber-Security in IoT Networks //E3S Web of Conferences. – EDP Sciences, 2021. – Т. 297.