УДК 004.056.2

МЕТОД ОБНАРУЖЕНИЯ СЕТЕВЫХ АТАК С ИСПОЛЬЗОВАНИЕМ ДВУХЭТАПНОГО АНАЛИЗА

Колесников Н. Д. (Университет ИТМО)

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

Введение. На сегодняшний день технология сегментации сетей быстро распространяется среди крупных организаций, однако процесс внедрения данной технологии является крайне трудоемким и время затратным. Согласно отчету Akamai [1] 89% опрошенных внедрили, внедряют или планируют внедрить сегментацию в сеть своих организаций, но согласно этому же опросу процесс полного перехода от классической сетевой архитектуры к сегментированной может занимать 2 и более лет (44% организаций, среди опрошенных, начали процесс сегментирования сетей 2 и более лет назад, но завершили этот процесс к 2021 году – 25%, к 2023 – 30%). Таким образом, в течение довольно длительного промежутка времени в организациях присутствует смешенная сетевая архитектура, где одновременно функционируют классические сети и сегментированные, что осложняет работу используемых там средств защиты информации (далее СЗИ), работа которых основывается на анализе сетевого трафика (подразумеваются системы, основанные на выявлении аномалий, а не на поиске сигнатур).

Помимо этого имеет место тенденция увеличения числа атак, совершаемых на корпоративные сети организаций, что можно увидеть в ежегодных отчетах Check Point Research [2-3].

Таким образом, наличие данных проблем порождает необходимость исследования области выявления сетевых атак в смешанных компьютерных сетях

Основная часть. В ходе данной работы была рассмотрено применение двухэтапного анализа в рамках задачи обнаружения сетевых атак. Двухэтапный анализ сетевого трафика подразумевает следующие шаги:

– применение легковесной модели для первичного анализа сетевого трафика (отсеивание части записей, относящихся к легитимному трафику);
– применение тяжеловесной модели для более глубокого анализа оставшихся данных.

В ходе экспериментального исследования было рассмотрено применение моделей машинного и глубокого обучения на каждом из двух этапов, с целью определить наиболее производительную (как с точки зрения точности обнаружения, так и с точки зрения затрачиваемых вычислительных ресурсов) комбинацию. В рамках экспериментального исследования решались следующие задачи:

– оценка легковесных моделей с использованием метрики качества recall и затрачиваемого времени на обучение и классификацию (обучение и классификация оцениваются отдельно);
– оценка тяжеловесных моделей с использованием метрики качества F1-score;
– оценка совместного применения легковесных и тяжеловесных моделей с использованием F1-score и затрачиваемого времени на обучение и классификацию (обучение и классификация оцениваются отдельно).

Выводы. В данной работе были представлены результаты исследования о применении двухэтапного анализа в рамках задачи обнаружения сетевых атак.

По результатам экспериментального исследования был представлен метод обнаружения сетевых атак с использованием наиболее производительной (точность вычисления и затраты вычислительных ресурсов) комбинации моделей.

Применение двухэтапного анализа сетевого трафика для выявления сетевых атак позволяет снизить вычислительную нагрузку (что является ключевым фактором при использовании методов обнаружения атак в высоконагруженных сетях, характерных для крупных компаний в общем и смешанных компьютерных сетей в частности) при сохранении в достаточной степени высокой точности классификации (что также является необходимым при применении в смешанных сетях, где базовая точность снижается за счет исключения подверженных влиянию характеристик сетевого трафика [4]).

Список использованных источников:

1) Akamai. The State of Segmentation 2023: Overcoming deployment obstacles proves to be transformational. – [Электронный ресурс]. – Режим доступа: https://www.akamai.com/resources/white-paper/2023-state-of-segmentation;

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

3) Check Point Research. Check Point Research Reports a 38% Increase in 2022 Global Cyberattacks. – [Электронный ресурс]. – URL: https://blog.checkpoint.com/2023/01/05/38-increase-in-2022-global-cyberattacks/;

4) Колесников Н.Д. Анализ влияния сегментации на характеристики сетевого трафика в процессе обнаружения сетевых атак // Наукосфера - 2024. - № 6(2). - С. 21-27.