УДК 004.056.2

ВЛИЯНИЕ СЕГМЕНТАЦИИ КОМПЬЮТЕРНЫХ СЕТЕЙ НА ХАРАКТЕРИСТИКИ СЕТЕВОГО ТРАФИКА

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 были рассмотрены существующие подходы к сетевой сегментации, а именно макросегментация (например, технологии VLAN и VRF) и микросегментация (например, технология SDN). Также в ходе экспериментальных исследований были выявлены характеристики сетевого трафика, которые подвержены влиянию в результате перехода от классической сетевой архитектуры к сегментированной (статистика собиралась о сетевых пакетах, проходящих через маршрутизатор на границе подсети), а именно:

- увеличилось количество сетевых пакетов;
- увеличился объем сетевого трафика (в байтах);
- изменилось значение статистических характеристик, связанных с количеством сетевых пакетов (например, соотношение протоколов передачи данных, средний размер сетевых пакетов и др.).

В рамках дальнейшего исследования было выявлено, что подверженные влиянию характеристики сетевого трафика часто применяются в рамках задачи обнаружения сетевых атак, что делает подавляющее большинство существующих на сегодняшний день методов малоэффективными при работе в смешанных сетях.

Таким образом, в качестве основного решения снижения влияния сегментации на результаты анализа сетевого трафика было принято исключить подверженные влиянию характеристики из анализа, однако, как показала выполненная в рамках работы оценка, данное действие негативным образом сказывается на точности обнаружения сетевых атак.

Выводы. В данной работе были представлены результаты исследования о влиянии сегментации на характеристики сетевого трафика, что было выполнено в рамках области обнаружения сетевых атак в компьютерных сетях.

В рамках работы был определен ряд ключевых проблем:

– процесс сегментации сетей может занимать 2 и более лет, что на весь этот период порождает в организации смешанную сеть;
– сегментация оказывает влияние на ряд характеристик сетевого трафика, популярных в области выявления сетевых атак, что приводит к необходимости исключать данные характеристики из анализа;
– исключение подверженных влиянию характеристик сетевого трафика негативно сказывается на точности обнаружения сетевых атак.

Тамим образом, обозначенные выше проблемы определяют ключевую задачу для будущей работы в рамках области обнаружения сетевых атак в компьютерных сетях, основанных на сегментации, а именно – рассмотрение существующих методов предобработки сетевого трафика, выявления аномалий и классификации с целью дальнейшей разработки метода, позволяющего повысить точность обнаружения сетевых атак в смешанных сетях.

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/.