УДК - 004.056

РАЗРАБОТКА ПРОГРАММНОГО МОДУЛЯ ОБНАРУЖЕНИЯ ГОРИЗОНТАЛЬНОГО ПЕРЕМЕЩЕНИЯ В КОМПЬЮТЕРНЫХ СЕТЯХ С ИСПОЛЬЗОВАНИЕМ МАШИННОГО ОБУЧЕНИЯ

Харченко А.А. (студент)
Научный руководитель – инженер Савков С.В.
Университет ИТМО

Введение. Горизонтальное перемещение – один из этапов атаки на организацию, во время которого злоумышленник, уже сумевший проникнуть внутрь корпоративной инфраструктуры и закрепиться в ней, начинает продвигаться по сети от точки входа к другим объектам [1]. Первичное проникновение обычно происходит сравнительно быстро, тогда как основная часть атаки – это длительное нахождение и передвижение во внутренней сети, которое может растягиваться на дни и месяцы, а также часто сопровождается использованием легитимных инструментов и учетных данных. В результате даже при наличии традиционных средств мониторинга, систем обнаружения вторжений, остается необходимость в методах, которые умеют учитывать контекст поведения сети и выделять аномальные внутренние связи в потоке событий. Учитывая специфику поставленной задачи, перспективными выглядят средства машинного обучения, способные адаптироваться к новым условиям и актуальным данным. Целью работы является повышение полноты обнаружения атак за счет использования модуля на базе машинного обучения, ориентированного на выявление горизонтального перемещения.

Основная часть. В первой главе рассматриваются существующие подходы обнаружения горизонтального перемещения. Выделяются следующие классы решений: сигнатурные средства (IDS – системы обнаружения вторжений), доменные средства (NDR/EDR - системы обнаружения и реагирования на сетевые угрозы и угрозы на конечных устройствах), а также средства машинного обучения (ML-подходы). В ходе анализа выявляются основные преимущества и недостатки каждого класса. Фокус исследования направлен на применение средств машинного обучения, поскольку они позволяют выявлять аномальные связи и последовательности действий без привязки к фиксированным сигнатурам. В рамках исследования необходим способ представления сетевой инфраструктуры, с которым модель сможет работать и эффективно улавливать контекст внутренних взаимодействий [2]. Одним из подобных способов является граф знаний (knowledge graph). В частности, в работе рассматривается базовая графовая модель (graph foundation model) Ultra, которая определяет оценку вероятности появления ребра в графе, при этом не требуя дополнительного обучения на целевых данных [3]. На основе данной модели разрабатывается алгоритм для выявления нетипичных взаимодействий между узлами графа в рамках временного окна фиксированной величины. Результатом работы алгоритма является ранжированный список событий в рамках временного окна, где события, получившие большую оценку, с большей вероятностью могут являться техниками горизонтального перемещения. Для тестирования алгоритма используется датасет LANL, который содержит обезличенные события корпоративной внутренней сети, собранные из пяти источников данных [4]. В него входят события аутентификации Windows, запуск и остановка процессов, DNS-запросы, сетевые потоки и размеченные события команды тестирования на проникновение. На основании данных строится модель графа, с которой будет работать программа. В качестве целевых метрик оценки работоспособности модели были выбраны полнота и площадь под ROC-кривой. Полученные значения метрик превышают показатели аналогичных решений [5].

Выводы. Горизонтальное перемещение может быть представлено как возникновение нетипичных связей между узлами графа. Для решения задачи обнаружения таких ребер целесообразно применять графовые нейронные сети. Рассмотренный в ходе исследования алгоритм на базе модели Ultra демонстрирует высокие показатели площади под ROC-кривой и полноты. Описанный подход будет положен в основу разрабатываемого программного модуля обнаружения горизонтального перемещения.

Литература

1. Энциклопедия Касперского [Электронный ресурс] – Режим доступа: https://encyclopedia.kaspersky.ru/glossary/lateral-movement/ (Дата обращения 13.01.2026)
2. M. Nicho, O. Adelaiye, C. D. McDermott, S. Girija Enhanced Detection of APT Vector Lateral Movement in Organizational Networks Using Lightweight Machine Learning // CMC – 2025. – Т. 83. – №. 1. – С. 282-305
3. Mikhail Galkin, Xinyu Yuan, Hesham Mostafa, Jian Tang, Zhaocheng Zhu Towards Foundation Models for Knowledge Graph Reasoning // ICLR – 2024
4. Набор данных Los Alamos National Laboratory // https://lanl.ma.ic.ac.uk/data/cyber1/
5. Jiacen Xu, Xiaokui Shu, Zhou Li Understanding and Bridging the Gap Between Unsupervised Network Representation Learning and Security Analytics // IEEE – 2024