УДК 004.056.57

МЕТОД ОБНАРУЖЕНИЯ И КЛАССИФИКАЦИИ СЕТЕВОГО СКАНИРОВАНИЯ ПО ПРИЗНАКУ ЛЕГИТИМНОСТИ С ПРИМЕНЕНИЕМ МАШИННОГО ОБУЧЕНИЯ

Лучинин К.А.
Научный руководитель – инженер-практикант Савков С.В.
Университет ИТМО

Введение

Сетевое сканирование является начальным этапом большинства кибератак и представляет собой процесс систематического анализа сетевой инфраструктуры для выявления активных хостов, открытых портов и запущенных сервисов. По данным компании RED Security, с января по июнь 2025 года число кибератак на российские компании превысило 63 тысячи, что на 27% больше, чем за аналогичный период 2024 года [1]. Современные системы обнаружения вторжений, такие как Suricata, Snort и Zeek, используют сигнатурные и эвристические методы для детектирования сканирования портов и других видов разведывательной активности.

Однако существенной проблемой традиционных IDS является высокий уровень ложноположительных срабатываний при детектировании легитимной активности в корпоративных сетях [2]. К такой активности относятся: систематическая инвентаризация активов с использованием систем управления ИТ-инфраструктурой (GLPI, Lansweeper), мониторинг состояния сервисов (Zabbix, Nagios, Prometheus), плановые сканирования уязвимостей (Nessus, OpenVAS), проверки соответствия стандартам безопасности и централизованное обновление программного обеспечения через WSUS или аналогичные системы. Все перечисленные процессы генерируют сетевой трафик, схожий по паттернам с вредоносным сканированием: множественные подключения к различным хостам, опрос портов, SNMP-запросы, баннер-граббинг.

Избыточные ложные срабатывания создают значительную нагрузку на аналитиков SOC, сокращая ресурсы на анализ реальных угроз. Существующие исследования в области обнаружения сетевого сканирования фокусируются преимущественно на бинарной классификации (сканирование / не сканирование) без анализа легитимности обнаруженной активности [3]. Это указывает на актуальность разработки метода, способного отличить реальное сканирование сети от схожей легитимной активности.

Основная часть

Предлагаемый метод представляет собой дополнительный классификационный слой для существующих IDS, функционирующий на основе алгоритмов машинного обучения. Метод реализуется в следующей последовательности: при срабатывании IDS на сетевое сканирование система генерирует лог-файлы в формате агрегированных потоков (eve.json для Suricata или conn.log для Zeek); из этих логов извлекаются признаки сетевой активности; обученная модель машинного обучения производит финальную классификацию трафика как легитимного или вредоносного сканирования.

В качестве источника данных используются агрегированные сетевые потоки, содержащие метаинформацию о соединениях: IP-адреса источника и назначения, используемые порты, протоколы, временные метки, объемы переданных данных, флаги TCP-соединений. Ключевыми признаками для классификации являются: частота и равномерность обращений к портам и хостам, количество запросов к несуществующим IP-адресам и закрытым портам, длительность и периодичность сессий, распределение

активности по протоколам, а также, возможно, контекстная информация о роли источника в сети.

Для обучения модели планируется использование следующих алгоритмов машинного обучения: деревья решений, случайный лес и метод опорных векторов. Выбор конкретного алгоритма будет осуществляться на основе экспериментальной оценки качества классификации на реальных и синтетических датасетах. Оценка эффективности метода производится с использованием стандартных метрик: общая точность модели (accuracy), точность (precision), полнота (recall) и F1-мера.

Выводы

Разработанный метод позволяет снизить количество ложноположительных срабатываний IDS за счет дифференциации легитимного и вредоносного сканирования на основе анализа признаков сетевых потоков. Ожидаемым результатом применения метода является снижение нагрузки на аналитиков SOC и повышение эффективности обнаружения реальных угроз на ранних стадиях атаки. Практическая значимость работы заключается в возможности интеграции разработанного решения в существующие системы обнаружения вторжений и SIEM-платформы в качестве дополнительного модуля классификации. Метод может быть адаптирован под специфику конкретной организации с учетом характерных для нее легитимных сценариев сканирования.

Дальнейшая работа предполагает расширение обучающего датасета за счет генерации синтетического трафика различных типов легитимной и вредоносной активности, проведение экспериментального тестирования выбранных алгоритмов машинного обучения на публичных и собственных датасетах, а также создание полноценного программного прототипа решения с интеграцией с системами обнаружения вторжений с открытым исходным кодом (Suricata, Zeek).

Литература

1. RED Security. RED Security SOC: характер кибератак меняется от массовых к целенаправленным [Электронный ресурс] // RED Security. ; Режим доступа: https://redsecurity.ru/news/red-security-soc-kharakter-kiberatak-menyaetsya-ot-massovykh-k-tselenapravlennym. —; Дата доступа: 15.02.2026.
2. Bada G. K., Nabare W. K., Quansah D. K. K. Comparative Analysis of the Performance of Network Intrusion Detection Systems: Snort, Suricata and Bro Intrusion Detection Systems in Perspective // International Journal of Computer Applications. 2020. Vol. 176, No. 40. P. 39-44.
3. Buczak, A. L., Guven E. A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection / A. L. Buczak, E. Guven // IEEE Communications Surveys & Tutorials. — 2016.— Volume 18, Issue 2. — P. 1153—1176.