УДК 004.056

СОВРЕМЕННЫЕ МЕТОДЫ ПРОТИВОДЕЙСТВИЯ СЕТЕВЫМ АТАКАМ НА ОСНОВЕ АНАЛИЗА АНОМАЛИЙ ТРАФИКА

Коротин В.О., преподаватель СПО кафедры ИБ
Прокопенко Е.В., заведующий кафедрой ИБ
Луцык Е.М., студент гр. ИБт-221 кафедры ИБ
Скачкова А.И., студент гр. ИБт-221 кафедры ИБ
Кузбасский государственный технический университет имени Т.Ф. Горбачева
Россия, г. Кемерово

Современный этап цифровой трансформации характеризуется тотальной зависимостью бизнес-процессов, государственного управления и социальной сферы от стабильного и безопасного функционирования компьютерных сетей. Параллельно с ростом сложности и масштаба сетевой инфраструктуры наблюдается стремительная эволюция методов и средств их несанкционированной эксплуатации. Под сетевыми атаками в контексте данной статьи понимаются целенаправленные действия злоумышленника, нацеленные на компрометацию конфиденциальности, целостности или доступности информационных ресурсов, осуществляемые через каналы сетевого взаимодействия [1].

Классические средства защиты, такие как межсетевые экраны (Firewalls) и системы обнаружения вторжений (Intrusion Detection Systems, IDS) сигнатурного типа, долгое время являлись основой периметровой безопасности. Однако их фундаментальный недостаток – реактивный характер – делает их уязвимыми перед новыми, неизвестными угрозами (APT-атаки, полиморфные вредоносы, атаки «нулевого дня») [2]. В связи с этим, все более востребованными становятся проактивные подходы, способные выявлять отклонения от нормального поведения сети, даже если атака ранее не была документирована.

Одним из таких перспективных направлений является построение систем обнаружения вторжений на основе анализа аномалий (Anomaly-Based Intrusion Detection Systems, A-IDS). Данный подход предполагает формирование модели «нормального» поведения сети или системы и последующее выявление событий, существенно отклоняющихся от этой модели [3]. В качестве источника данных для анализа наиболее информативным является сетевой трафик, так как он аккумулирует в себе информацию о всех взаимодействиях между узлами сети.

Целью статьи является разработка и экспериментальная оценка эффективности многоуровневой модели обнаружения сетевых атак на основе комплексного анализа аномалий сетевого трафика с применением методов машинного обучения.

Для достижения поставленной цели необходимо решить следующие задачи:

1. Провести анализ существующих методов классификации и обнаружения аномалий в сетевом трафике.

2. Разработать многоуровневую архитектуру системы обнаружения, интегрирующую анализ на уровне пакетов, потоков и хостов.

3. Исследовать применимость различных алгоритмов машинного обучения для задач классификации сетевых аномалий.

4. Оценить эффективность предложенного подхода на синтезированных данных.

Все методы обнаружения аномалий в сетевом трафике можно условно разделить на несколько крупных классов.

Статистические методы. Данные методы основаны на вычислении статистических показателей сетевой активности за определенный временной интервал и сравнении их с пороговыми значениями или историческими данными. К таким показателям относятся: средняя интенсивность пакетов, объем передаваемых данных, количество уникальных IP-адресов в сегменте сети, распределение портов и протоколов [4]. Преимуществом статистических методов является их относительная простота и низкие вычислительные затраты. Недостатком – сложность настройки пороговых значений и низкая эффективность против низкоинтенсивных и распределенных атак (например, DDoS с медленным темпом).

Методы, основанные на машинном обучении. Данная группа методов в последние годы получает наибольшее развитие в связи с ростом вычислительных мощностей и доступности данных.

- Кластеризация (неконтролируемое обучение). Алгоритмы, такие как k-means, DBSCAN или метод ожидания максимизации (Expectation-Maximization, EM), используются для группировки сетевых событий (например, NetFlow records) в кластеры без предварительного присвоения меток. События, не попавшие ни в один из крупных кластеров, или образующие небольшие изолированные кластеры, рассматриваются как аномалии [5]. Этот подход не требует размеченных данных об атаках, что является его ключевым преимуществом.
- Классификация (контролируемое обучение). Алгоритмы, включая решающие деревья, метод опорных векторов (SVM) и глубокие нейронные сети, обучаются на размеченных наборах данных, где каждому сетевому событию присвоена метка «норма» или «атака» (с указанием типа). После обучения модель способна классифицировать новые, ранее не виданные события [6]. Эффективность этого метода напрямую зависит от качества и репрезентативности обучающей выборки.
- Глубокое обучение (Deep Learning). Сверточные нейронные сети (CNN) и рекуррентные нейронные сети (RNN), в частности, сети с долгой краткосрочной памятью (LSTM), показали высокую эффективность в анализе последовательностей сетевых пакетов и выявлении сложных временных зависимостей, характерных для многостадийных атак [7].

Предлагаемая многоуровневая архитектура системы обнаружения

Для преодоления ограничений одноуровневых подходов предлагается многоуровневая архитектура A-IDS, осуществляющая анализ на трех взаимодополняющих уровнях.

Уровень 1: Анализ сетевых пакетов (Packet-Level Analysis). На данном уровне производится глубокая проверка пакетов (Deep Packet Inspection, DPI). Анализируются не только заголовки, но и содержимое пакетов на предмет наличия известных шаблонов эксплойтов, скрытых каналов передачи данных и признаков сканирования. Для этого могут применяться быстрые сигнатурные методы в сочетании с анализом энтропии содержимого пакетов (высокая энтропия может указывать на шифрование или упаковку вредоносного кода).

Уровень 2: Анализ метаданных потоков (Flow-Level Analysis). Этот уровень оперирует агрегированными данными о сетевых потоках (например, в формате NetFlow или IPFIX). Анализируются такие признаки, как:

- Продолжительность потока.
- Объем переданных данных (в байтах и пакетах).
- Протокол транспортного уровня (TCP/UDP).
- Номера портов источника и назначения.
- Флаги TCP.
- Биты per second (bps) и packets per second (pps).

На этом уровне наиболее эффективно применяются методы машинного обучения для кластеризации и классификации. Например, короткие TCP-потоки с множеством SYN-пакетов и малым объемом данных могут быть признаком сканирования портов.

Уровень 3: Анализ поведенческих паттернов хостов (Host-Level Analysis). Уровень фокусируется на поведении отдельных узлов сети. Собирается и анализируется информация о:

- Количестве установленных сетевых соединений за единицу времени.
- «Горизонте общения» хоста (количество уникальных IP-адресов, с которыми он взаимодействует).
- Протокольном разнообразии исходящих соединений.
- Периодичности сетевой активности.

Резкие изменения в этих поведенческих паттернах, например, попытка хоста, обычно работающего в дневное время, установить сотни соединений ночью, являются сильным индикатором компрометации.

Корреляционный движок, являющийся ядром системы, агрегирует события и оценки риска со всех трех уровней. Решение о наличии атаки принимается на основе совокупности свидетельств, что позволяет значительно снизить уровень ложных срабатываний по сравнению с использованием каждого уровня в отдельности.

Для проверки эффективности предложенного подхода было проведено моделирование работы системы.

В качестве тестовой среды использовалась виртуальная сеть, развернутая с помощью среды моделирования GNS3. Сеть включала 50 виртуальных хостов, маршрутизаторы и коммутаторы. Для генерации фонового

«нормального» трафика применялись инструменты iPerf и скрипты на Python, имитирующие работу пользователей (веб-серфинг, почта, файловый обмен). Атаки генерировались с помощью фреймворков Metasploit и Scapy и включали:

- Сканирование сети и портов (Nmap).
- Атаки типа «отказ в обслуживании» (DDoS UDP-flood).
- Эксплуатация уязвимостей для получения удаленного доступа.
- Горизонтальное перемещение внутри сети.

Сбор данных осуществлялся с помощью утилиты tcpdump и экспорта NetFlow с маршрутизаторов. Общий объем собранных данных составил более 5 миллионов сетевых событий, из которых примерно 2% были помечены как атаки.

Для уровней 2 и 3 был реализован пайплайн обработки данных на языке Python с использованием библиотек scikit-learn и pandas. Из метаданных потоков были извлечены 15 числовых признаков. Для задачи классификации были протестированы следующие алгоритмы:

- Решающее дерево (Decision Tree).
- Случайный лес (Random Forest).
- Метод опорных векторов (SVM).
- Многослойный перцептрон (MLP).

Оценка проводилась с использованием метрик Precision, Recall и F1-score на основе 5-кратной перекрестной проверки.

Результаты и их обсуждение

Результаты классификации для основных типов атак представлены в Таблице 1.

Таблица 1 Результаты классификации сетевых атак

Тип атаки	Precision	Recall	F1-score
Сканирование портов	0.98	0.96	0.97
DDoS UDP-flood	0.99	0.99	0.99
Эксплуатация RCE	0.87	0.82	0.84
Перемещение в сети	0.85	0.79	0.82
Среднее взвешенное	**0.96**	**0.95**	**0.95**

Как видно из таблицы, атаки, связанные с большими объемами трафика (DDoS) или ярко выраженными шаблонами (сканирование), детектируются с очень высокой точностью. Более сложные и низкоинтенсивные атаки, такие как удаленное выполнение кода (RCE) и горизонтальное перемещение,

обнаруживаются несколько хуже, однако показатели F1-score выше 0.8 свидетельствуют о практической применимости метода.

Интеграция данных с уровня анализа поведенческих паттернов хостов позволила дополнительно повысить Recall для атак типа RCE на 8%, так как после успешной эксплуатации наблюдалась аномальная сетевая активность скомпрометированного хоста.

Общий коэффициент обнаружения (True Positive Rate) для предложенной многоуровневой архитектуры составил 94,5%, при уровне ложных срабатываний (False Positive Rate) 2,1%, что является приемлемым для систем данного класса.

В ходе проведенного исследования была подтверждена гипотеза о высокой эффективности комплексного подхода к обнаружению сетевых атак, основанного на анализе аномалий на нескольких уровнях сетевого взаимодействия. Предложенная многоуровневая архитектура A-IDS, сочетающая анализ пакетов, метаданных потоков и поведенческих паттернов хостов, позволяет достичь высоких показателей обнаружения как известных, так и ранее не встречавшихся угроз.

Ключевым преимуществом является использование методов машинного обучения, в частности, алгоритма «Случайный лес», который продемонстрировал стабильно высокие результаты по метрикам Precision, Recall и F1-score для различных классов атак.

Перспективами дальнейших исследований является интеграция в систему методов глубокого обучения для анализа сырого трафика (LSTM-сети) в реальном времени, а также разработка механизмов автоматического реагирования (переход к Intrusion Prevention System, IPS) на основе оценок корреляционного движка. Внедрение подобных систем позволит существенно повысить устойчивость корпоративных и государственных информационных инфраструктур к современным киберугрозам.

Список литературы:

1. Stallings, W. Cryptography and Network Security: Principles and Practice [Текст] / W. Stallings. – 7th ed. – Pearson, 2017. – 768 p.

2. Scarfone, K. Guide to Intrusion Detection and Prevention Systems (IDPS) [Текст] / K. Scarfone, P. Mell // NIST Special Publication 800-94. – 2012. – 127 p.

3. Chandola, V. Anomaly Detection: A Survey [Текст] / V. Chandola, A. Banerjee, V. Kumar // ACM Computing Surveys. – 2009. – Vol. 41, № 3. – P. 1–58.

4. Garcia-Teodoro, P. Anomaly-based network intrusion detection: Techniques, systems and challenges [Текст] / P. Garcia-Teodoro, J. Diaz-Verdejo, G. Maciá-Fernández // Computers & Security. – 2009. – Vol. 28, № 1-2. – P. 18–28.

5. Zuev, D. Network Anomaly Detection Based on Statistical Traffic Analysis [Текст] / D. Zuev // Proceedings of the 10th International Conference on Security of Information and Networks. – 2017. – P. 175–180.

6. Sommer, R. Outside the Closed World: On Using Machine Learning for Network Intrusion Detection [Текст] / R. Sommer, V. Paxson // IEEE Symposium on Security and Privacy. – 2010. – P. 305–316.

7. Yin, C. A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks [Текст] / C. Yin, Y. Zhu, J. Fei // IEEE Access. – 2017. – Vol. 5. – P. 21954–21961.