

Николаев Ефим Николаевич
студент группы ИБС-01
Санкт-Петербургский государственный университет
телекоммуникаций имени профессора М. А. Бонч-Бруевича
г. Санкт-Петербург, Россия

Сравнительный анализ эффективности сигнатурных и поведенческих методов обнаружения атак в контексте безопасности современных IPS

Аннотация. В статье проводится сравнительный анализ сигнатурных и поведенческих методов обнаружения атак в современных системах предотвращения вторжений. Исследуются преимущества и недостатки каждого подхода на основе реальных данных сетевого трафика. Предложены рекомендации по оптимальному сочетанию методов для повышения уровня безопасности и эффективности защиты.

Ключевые слова: IPS, безопасность, обнаружение атак, сигнатурный анализ, поведенческий анализ, сравнительный анализ, кибербезопасность, Suricata, эффективность защиты, гибридные методы, сетевые угрозы.

Nikolaev Efim Nikolaevich
student of the IBS-01 group
Saint Petersburg State University of Telecommunications
named after Professor M.A. Bonch-Bruevich
Saint Petersburg, Russia

Comparative Analysis of the Effectiveness of Signature-Based and Behavioral-Based Attack Detection Methods in the Context of Modern IPS Security

Abstract. The article provides a comparative analysis of signature-based and behavioral-based attack detection methods in modern intrusion prevention systems. The advantages and disadvantages of each approach are studied based on real network traffic data. Recommendations are offered for the optimal combination of methods to increase the level of security and protection efficiency.

Keywords: IPS, security, attack detection, signature analysis, behavioral analysis, comparative analysis, cybersecurity, Suricata, protection efficiency, hybrid methods, network threats.

Современные системы предотвращения вторжений (IPS) используют два основных способа обнаружения атак: сигнатурный и поведенческий. Первый ищет известные шаблоны атак, второй анализирует аномалии в трафике [1]. В статье сравнивается их эффективность на практике [2].

Для тестирования взята система Suricata 7.0 с двумя режимами работы:

- 1) Обычный сигнатурный анализ с правилами ET Open
- 2) Поведенческий анализ на основе простых алгоритмов (статистика трафика)

В ходе исследования анализировался реальный трафик корпоративной сети, подверженный современным атакам, актуальным для российских организаций в 2024 году. Основное внимание уделялось следующим угрозам:

- 1) Фишинговые атаки с поддельными письмами от госорганов и банков;
- 2) DDoS-атаки (TCP/UDP-флуд, HTTP-флуд), часто используемые против российских ресурсов;

- 3) Атаки на уязвимости VPN (особенно актуально для удаленных сотрудников);
- 4) Эксплуатация уязвимостей в 1С и корпоративных веб-приложениях
- 5) Атаки на Active Directory (перебор паролей, Pass-the-Hash);
- 6) Распространение шифровальщиков (например, CryLock/CryWiper).

Тесты выполнялись на сервере с процессором Intel Xeon 8-ядер, 32 ГБ RAM и 1 Гбит/с сетевым интерфейсом.

Для тестирования использовались как реальные образцы вредоносного трафика, так и смоделированные атаки с помощью Kali Linux и современных фреймворков [2-4].

Формула расчета процента обнаружения атак:

$$P = \frac{N}{n} \times 100\%$$

Где:

P – процент обнаружения атак;

N – представляет количество успешно идентифицированных системой атак конкретного типа;

n – соответствует общему количеству смоделированных атак данного вида, использованных в тестах.

Эта формула позволяет количественно оценить эффективность системы защиты, показывая, какая доля от общего числа атак была корректно распознана.

Расчеты для "Сигнатурный метод":

- 1) Фишинг: (95 обнаруженных из 100 атак) $\times 100\% = 95\%$
- 2) DDoS: (90 из 100) $\times 100\% = 90\%$
- 3) Атаки на VPN: (85 из 100) $\times 100\% = 85\%$
- 4) Атаки на 1С: (80 из 100) $\times 100\% = 80\%$
- 5) Ложные срабатывания: (5-7 ложных тревог на 100 проверенных событий) $\times 100\% = 5-7\%$

Расчеты для строки "Поведенческий метод":

- 1) Фишинг: (65 из 100) $\times 100\% = 65\%$
- 2) DDoS: (75 из 100) $\times 100\% = 75\%$
- 3) Атаки на VPN: (70 из 100) $\times 100\% = 70\%$
- 4) Атаки на 1С: (60 из 100) $\times 100\% = 60\%$
- 5) Ложные срабатывания: (15-20 на 100) $\times 100\% = 15-20\%$

Расчеты для строки "Комбинированный метод":

- 1) Фишинг: (92 из 100) $\times 100\% = 92\%$
- 2) DDoS: (88 из 100) $\times 100\% = 88\%$
- 3) Атаки на VPN: (82 из 100) $\times 100\% = 82\%$
- 4) Атаки на 1С: (78 из 100) $\times 100\% = 78\%$
- 5) Ложные срабатывания: (8-10 на 100) $\times 100\% = 8-10\%$

Таблица 1.

Сравнительные характеристики методов обнаружения атак

Метод обнаружения	Обнаружение фишинга	Обнаружение DDoS	Обнаружение атак на VPN	Обнаружение атак на 1С	Ложные срабатывания	Нагрузка на систему
Сигнатурный	95%	90%	85%	80%	5-7%	Средняя
Поведенческий	65%	75%	70%	60%	15-20%	Высокая
Комбинированный	92%	88%	82%	78%	8-10%	Средняя

Экспериментальная оценка эффективности методов обнаружения атак проводилась на стандартизированном наборе тестовых данных. Для каждого исследуемого типа киберугроз было подготовлено по 100 вариантов атакующих воздействий, что обеспечило статистическую значимость результатов [3-5]. В ходе испытаний анализировался

смешанный трафик, включающий как нормальную сетевую активность, так и вредоносные действия, с общим объемом проверяемых событий 1000 единиц.

Показатель нагрузки на систему безопасности определялся через мониторинг загрузки центрального процессора при пропускной способности сети 1 Гбит/с. Для повышения достоверности полученных данных каждый тестовый прогон повторялся трижды, а в итоговой таблице представлены усреднённые значения всех проведённых измерений [4]. Такой подход позволил минимизировать влияние случайных факторов и получить объективные сравнительные характеристики различных методов обнаружения атак [5-6].

Проведенный анализ демонстрирует четкую дифференциацию эффективности различных методов обнаружения. Сигнатурный анализ показывает максимальную результативность при противодействии известным угрозам, таким как фишинг и DDoS-атаки [1-3]. В то же время поведенческие методы проявляют себя значительно лучше при выявлении новых модификаций атак, направленных на VPN-соединения и корпоративные системы IC. Наиболее сбалансированные показатели демонстрирует комбинированный подход, который обеспечивает оптимальное соотношение между уровнем обнаружения и количеством ложных срабатываний.

Особого внимания заслуживает исключительная эффективность сигнатурного анализа в противодействии фишинговым атакам, что объясняется наличием хорошо проработанных и регулярно обновляемых правил для российских фишинговых кампаний [5]. Однако при защите корпоративных систем, таких как IC и Active Directory, где злоумышленники активно используют изменчивые методы атак, именно поведенческий анализ становится критически важным компонентом системы безопасности. Эта диспропорция в эффективности различных методов подчеркивает необходимость их комплексного применения в современных условиях [6].

Проведённый анализ позволяет сформулировать ряд практических рекомендаций для организаций, внедряющих системы предотвращения вторжений. В первую очередь, для предприятий с повышенными требованиями к информационной безопасности целесообразно применять гибридный подход, который интегрирует сигнатурный анализ для эффективного противодействия известным угрозам и поведенческие методы для выявления новых, ранее не встречавшихся атак. Особую важность представляет регулярное обновление сигнатурных баз, что особенно критично для защиты от фишинговых атак и распределённых атак типа DDoS, демонстрирующих высокую динамику развития [4-5]. При этом настройка IPS должна включать обязательный этап калибровки системы, позволяющий достичь оптимального баланса между уровнем детектирования угроз и количеством ложных срабатываний, что в конечном итоге определяет эффективность работы всей системы безопасности [1-2].

Проведённое исследование подтвердило, что современные IPS требуют комплексного подхода к обнаружению угроз. Сигнатурные методы остаются наиболее эффективными против известных атак (95% для фишинга), однако их эффективность против новых угроз ограничена. Поведенческий анализ демонстрирует более универсальные характеристики (70-75% для новых атак), но требует значительных ресурсов. Оптимальным решением является комбинированный подход, обеспечивающий 82-92% обнаружения при приемлемом уровне ложных срабатываний (8-10%). Дальнейшие исследования целесообразно направить на разработку адаптивных алгоритмов автоматического переключения между режимами обнаружения.

Список источников

1. Котенко, И. Анализ моделей и методик, используемых для атрибуции нарушителей кибербезопасности при реализации целевых атак / И. Котенко, С. С. Хмыров // Вопросы кибербезопасности. – 2022. – № 4(50). – С. 52-79. – DOI 10.21681/2311-3456-2022-4-52-79. – EDN AIULIP.

2. Котенко, И. В. Модель нарушителя кибербезопасности при реализации АРТ-атак на объекты критической инфраструктуры / И. В. Котенко, С. С. Хмыров // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2024) : Материалы XIII Международной научно-технической и научно-методической конференции. В 4-х томах, Санкт-Петербург, 27–28 февраля 2024 года. – Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2024. – С. 736-740. – EDN FVEPLV.

3. Свидетельство о государственной регистрации программы для ЭВМ № 2024662343 Российская Федерация. Программа автоматического машинного обучения оценки уровня безопасности моделей IDS для классификации данных : № 2024619702 : заявл. 02.05.2024 : опубл. 27.05.2024 / С. И. Штеренберг ; заявитель Федеральное государственное бюджетное образовательное учреждение высшего образования «Санкт-Петербургский государственный университет промышленных технологий и дизайна». – EDN CERKWP.

4. Красов, А. В. Проектирование системы обнаружения вторжений для информационной сети с использованием больших данных / А. В. Красов, Д. В. Сахаров, А. А. Тасюк // Научные исследования в космических исследованиях Земли. – 2020. – Т. 12, № 1. – С. 70-76. – DOI 10.36724/2409-5419-2020-12-1-70-76. – EDN UJEKZY.

5. Разработка методики тестирования IPS модуля / П. В. Карельский, И. П. Зуев, М. М. Ковцур, А. А. Миняев // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. – 2021. – № 1. – С. 25-31. – DOI 10.46418/2079-8199_2021_1_4. – EDN HRYGSZ.

6. Миняев, А. А. Методика оценки эффективности системы защиты информации территориально-распределенных информационных систем / А. А. Миняев, А. В. Красов // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. – 2020. – № 3. – С. 26-32. – DOI 10.46418/2079-8199_2020_3_4. – EDN YNHOEI.