***А. Е. Котович, А. М. Шабалин***
*Тюменский государственный университет, г. Тюмень*
**УДК 004.732**

# ОРГАНИЗАЦИЯ СИСТЕМЫ ОБНАРУЖЕНИЯ И ПРЕДОТВРАЩЕНИЯ ВТОРЖЕНИЙ СРЕДСТВАМИ РЕШЕНИЙ OPEN SOURCE

**Аннотация.** В статье рассмотрены особенности внедрения системы предотвращения и обнаружения вторжений средствами решений Open Source, а также проведен анализ и сравнение существующих систем. Результатом исследования стала практическая модель применения системы обнаружения и предотвращения вторжений в современной среде эмуляции.
**Ключевые слова:** IDS, IPS, EVE-NG, Snort, Pfsense.

**Введение.** В настоящее время с развитием информационных технологий вопрос информационной безопасности стоит остро, так как методы и действия злоумышленников, направленные на получение несанкционированного доступа к сетевой инфраструктуре, компрометацию данных и устройств, внедрение вредоносных программ и т. п., становятся все более быстрыми и эффективными [1], увеличивается число сетевых атак, в связи с ростом количества информационных систем и устройств [2]. Существующие базовые системы безопасности (например, межсетевые экраны и антивирусы) не способны обеспечить должную защиту [3].

При такой ситуации существующим инфраструктурам требуется система, позволяющая автоматизировать процесс анализа опасного трафика, обнаруживать и предотвращать попытки несанкционированного доступа или внедрения вредоносных программ [4], а также сообщать обо всех. В таких случаях используется IDS/IPS, которая представляет собой технологию обнаружения и блокирования как известных, так и еще не известных угроз [5].

**Проблема исследования.** Современные Open Source-решения предлагают эффективное и доступное решение для предотвращения вторжений в компьютерные сети и минимизации рисков, связанных с нарушением безопасности. Для организации такой системы в сети предприятия были поставлены следующие задачи:

1) проанализировать современные технологии, которые существуют в IDS/IPS-системах;

2) сделать краткий обзор существующих систем и сравнить по основным параметрам;

3) смоделировать компьютерную сеть для демонстрации работы IDPS.

**Материалы и методы.** Для исследования использовались такие методы, как наблюдение, сравнение, эксперимент, измерение и абстрагирование. Для эмуляции компьютерной сети было выбрано программное средство EVE-NG 5.0.1-19.

**Результаты.** Современные IDS/IPS в своей работе используют разные технологии и методы, которые позволяют повысить эффективность работы и точность обнаружения инцидентов. Вот некоторые технологии, которыми оперируют IDPS:

1. Обнаружение на основе сигнатур: данный подход предполагает сравнение сетевого трафика с базой данных известных сигнатур или шаблонов атак. Если есть совпадение, то система выдает предупреждение или предпринимает другие действия для блокировки атаки.

2. Обнаружение на основе аномалий: метод направлен на выявление статистически аномального трафика, не являющегося нормой. Система сравнивает модель трафика со статической моделью, предупреждая администратора, если обнаружено отклонение.

3. Поведенческий анализ: метод, предполагающий отслеживание сетевого трафика в течение определенного времени для выявления «нормальной» активности. Отклонение от «нормы» будет рассматриваться как потенциально подозрительное.

4. Машинное обучение: этот новый подход использует алгоритм и искусственный интеллект для распознавания моделей вредоносной активности и обучения системы реагировать соответственно.

Существует две Open-source системы обнаружения и предотвращения вторжений — Snort и Suricata. Наибольшую популярность имеет Snort — это система обнаружения и предотвращения вторжений, которая работает на основе сигнатур. Она анализирует сетевой трафик, захватывая и анализируя пакеты, чтобы определить, является

ли трафик легитимным или злонамеренным, используя сигнатуры известных атак. В случае злонамеренного трафика система предпринимает превентивные меры в соответствии с заранее определенными правилами.

Для демонстрации работы IDPS была спроектирована топология (рис. 1), включающая в себя Pfsense, внешнюю сеть и две машины Kali Linux

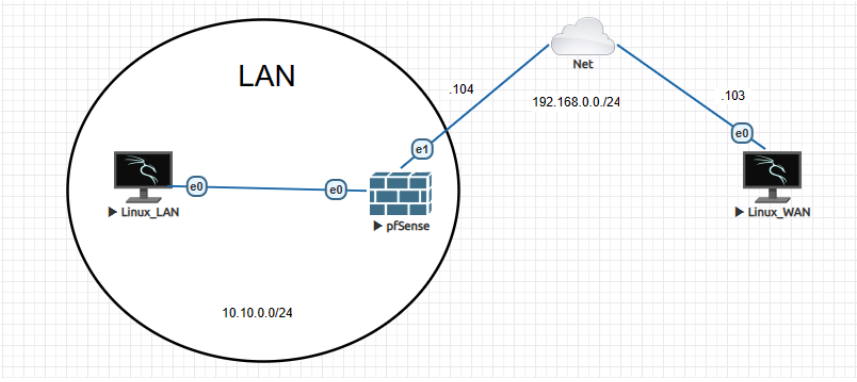


*Рис. 1.* Топология сети

На Linux_LAN был организован веб-сервер Apache. Используя утилиту hping3, с Linux_WAN была проведена DoS-атака на МСЭ PfSense, с установленной IDS/IPS Snort. Во время атаки Snort, используя собственные правила, были созданы предупредительные сообщения (рис. 2).

Most Recent 250 Entries from Active Log

| Date | Action | Pri | Proto | Class | Source IP | SPort | Destination IP | DPort |
|---|---|---|---|---|---|---|---|---|
| 2023-05-07 09:29:47 | ⚠ | 2 | TCP | Detection of a Non-Standard Protocol or Event | 192.168.0.102 | 22 | 192.168.0.104 | 80 |
| 2023-05-07 09:29:47 | ⚠ | 2 | TCP | Detection of a Non-Standard Protocol or Event | 192.168.0.102 | 22 | 192.168.0.104 | 80 |
| 2023-05-07 09:29:47 | ⚠ | 2 | TCP | Detection of a Non-Standard Protocol or Event | 192.168.0.102 | 22 | 192.168.0.104 | 80 |
| 2023-05-07 09:29:46 | ⚠ | 2 | TCP | Detection of a Non-Standard Protocol or Event | 192.168.0.102 | 22 | 192.168.0.104 | 80 |
| 2023-05-07 09:29:46 | ⚠ | 2 | TCP | Detection of a Non-Standard Protocol or Event | 192.168.0.102 | 22 | 192.168.0.104 | 80 |

*Рис. 2.* Сигнализация программы Snort об атаках

Так как в системе присутствует IPS, то, основываясь на созданных им сообщениях, она заблокировала атакующий IP-адрес (рис. 3).


*Рис. 3.* Заблокированный хост

Если впоследствии попытаться зайти на веб-сервер, то ничего не получится, поскольку хост заблокирован (рис. 4).

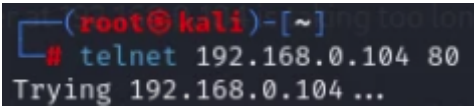


*Рис. 4.* Вариант проверки доступности через Telnet

**Заключение.** В статье рассматриваются особенности организации системы обнаружения и предотвращения вторжений в компьютерной сети. Также были сделаны выводы об использовании Open Source-решений, проанализированы технологии, существующие в IDS/IPS. В результате проведенной работы была смоделирована работа IDS/IPS системы в современной среде эмуляции.

## СПИСОК ЛИТЕРАТУРЫ

1. Пиксаева, А. А. Применение оптимального стека алгоритмов для системы обнаружения вторжений / М. В. Жаркова. — Текст: электронный // Юность и Знания — Гарантия Успеха — 2022. — 2022. — С. 234-240. — URL: https://www.elibrary.ru/item.asp?id=49556780 (дата обращения: 30.04.2023).
2. Смирнов, Е. Ю. Системы обнаружения вторжении как важная часть защиты корпоративной сети / Е. Ю. Смирнов. — Текст: элетронный // Информационные технологии в науке, бизнесе и образовании. — 2020. — С. 293-297. — URL: https://www.elibrary.ru/item.asp?id=43100643 (дата обращения: 30.04.2023).
3. Глущенко, М. В. IDS / IPS — системы обнаружения и предотвращения вторжений / М. В. Глущенко, А. А. Ширяев, С. А. Глушенко. — Текст:

электронный // Концепция «Общества знаний2 в современной науке. — 2019. — С. 115-117. — URL: https://www.elibrary.ru/item.asp?id=41328677 (дата обращения: 30.04.2023).
4. Кумага, Н. К. Проектирование и внедрение системы обнаружения и предотвращения вторжений IDS/IPS в корпоративной сети УГТУ / Н. К. Кумага, А. В. Григорьевых. — Текст: электронный // Информационные технологии в управлении и экономике. — 2022. — № 2(27). — С. 44-52. — URL: https://www.elibrary.ru/item.asp?id=48660794 (дата обращения: 30.04.2023).
5. Shevchenko, T. N. IDS/IPS Technologies for the detection and prevention of intrusion of telecommunications infrastructure / T. N. Shevchenko, I. V. Zimin. — Текст: электронный // Известия Кыргызского государственного технического университета им. И. Раззакова. — 2017. — No. 2(42). — P. 26-32. — URL: https://www.elibrary.ru/item.asp?id=30273969 (дата обращения: 30.04.2023).