Министерство образования Республики Беларусь

Учреждение образования

«Брестский Государственный технический университет»

Кафедра ИИТ

Реферат

По дисциплине «Современные методы защиты компьютерных систем»

Выполнил:

Студент 4 курса

Группы ИИ-21

Шпак И.С.

Проверила:

Хацкевич М. В.

Брест 2024

Вариант 2

1. SOC
2. FW/NGFW
3. IDS/IPS
4. NTA

1.SOC

SOC (Security Operations Center, Центр управления безопасностью) — это организационная единица или структура, предназначенная для мониторинга, анализа и защиты систем и данных от киберугроз. Однако SOC в криптографии и информационной безопасности чаще рассматривается как часть более широкой экосистемы управления безопасностью.

Основные задачи SOC:

1. **Мониторинг в реальном времени:** Отслеживание событий и активности в сети, чтобы обнаружить подозрительное поведение или возможные атаки.
2. **Обнаружение угроз:** Использование систем анализа событий безопасности (SIEM) для идентификации потенциальных инцидентов.
3. **Реагирование на инциденты:** Быстрое реагирование на выявленные угрозы и устранение их последствий.
4. **Анализ уязвимостей:** Проверка систем на наличие слабых мест и их устранение.
5. **Интеграция криптографических методов:** Обеспечение надёжного шифрования данных и безопасного обмена ключами.

SOC активно использует криптографические методы для защиты данных и повышения безопасности:

- **Шифрование данных** (например, с помощью AES, RSA).
- **Электронная подпись** для проверки подлинности данных.
- **Управление ключами** для безопасной работы с криптографическими протоколами.

2. FW/NGFW

FW (Firewall) — это межсетевой экран, используемый для фильтрации входящего и исходящего трафика в сети на основе заранее определённых

правил безопасности. Основная задача FW — защита сети или устройства от несанкционированного доступа, вредоносного трафика и других угроз.

Основные функции классического FW:

1. **Фильтрация пакетов:** Проверяет сетевые пакеты на соответствие заданным правилам (например, блокировка пакетов с определённого IP-адреса).
2. **Маршрутизация:** Управляет трафиком между различными сетями (например, внутренней и внешней).
3. **Контроль доступа:** Позволяет ограничивать доступ к определённым портам, службам или приложениям.

NGFW (Next-Generation Firewall) — это межсетевой экран нового поколения, который включает в себя функции классического FW, но расширен дополнительными возможностями для борьбы с современными угрозами.

Отличия NGFW от традиционного FW:

1. **Анализ на уровне приложений:** NGFW способен понимать, какие приложения используют сеть, и применять правила безопасности на уровне приложений (например, блокировать Facebook, но разрешать WhatsApp).
2. **Интеграция с системами предотвращения вторжений (IPS):** NGFW может обнаруживать и предотвращать атаки в реальном времени.
3. **Детальная фильтрация содержимого:** Проверяет не только пакеты данных, но и их содержимое, чтобы блокировать вредоносный контент (например, вирусы, трояны).
4. **Поддержка SSL/TLS-декрипции:** NGFW может расшифровывать зашифрованный трафик для проверки на наличие угроз.
5. **Идентификация пользователей:** Учитывает не только IP-адрес, но и конкретного пользователя (например, блокировка определённого сотрудника на доступ к сайтам).
6. **Обновляемая защита:** Использует облачные базы данных для обнаружения новых угроз.

Примеры использования:

- **FW:** Используется для базовой защиты сети, например, в домашних маршрутизаторах.

- **NGFW:** Применяется в корпоративных сетях, где требуется более сложная защита от целевых атак, шифрованного вредоносного трафика и утечек данных.

Популярные решения NGFW: Cisco Firepower, Palo Alto Networks, Fortinet FortiGate, Check Point.

3.IDS/IPS

IDS (Intrusion Detection System) и **IPS (Intrusion Prevention System)** — это системы, используемые для защиты компьютерных сетей от несанкционированного доступа, атак и других угроз. Несмотря на схожесть названий, они выполняют разные функции:

IDS (Intrusion Detection System):

IDS — это система обнаружения вторжений. Она **анализирует сетевой трафик или события на устройствах, чтобы выявить подозрительную активность**.

Основные характеристики IDS:

1. **Обнаружение атак:**
   - Анализирует данные и события в сети, чтобы выявить угрозы (например, DDoS-атаки, попытки эксплуатации уязвимостей).
2. **Реагирование:**
   - Не вмешивается в трафик, а только уведомляет администратора о подозрительных действиях (например, срабатывание тревоги, создание отчёта).
3. **Типы IDS:**
   - **HIDS (Host-based IDS):** Установлена на конкретном устройстве и анализирует его журналы событий, процессы и сетевой трафик.
   - **NIDS (Network-based IDS):** Работает на уровне сети, анализируя сетевой трафик.

Преимущества IDS:

- Выявляет сложные атаки (в том числе многослойные).
- Не влияет на производительность сети, так как не вмешивается в поток данных.

Недостатки IDS:

- Может генерировать ложные срабатывания.
- Только обнаруживает атаки, но не предотвращает их.

IPS (Intrusion Prevention System)

IPS — это система предотвращения вторжений. Она **не только обнаруживает угрозы, но и активно блокирует или предотвращает их**.

Основные характеристики IPS:

1. **Обнаружение и предотвращение:**
   - Анализирует трафик в режиме реального времени, как IDS, но дополнительно блокирует подозрительные действия.
2. **Автоматическая реакция:**
   - Может сбрасывать соединения, блокировать IP-адреса или запретить доступ к определённым ресурсам.
3. **Типы IPS:**
   - **HIPS (Host-based IPS):** Защищает отдельное устройство.
   - **NIPS (Network-based IPS):** Применяется на уровне сети.

Преимущества IPS:

- Автоматически предотвращает атаки, снижая риск повреждения сети.
- Уменьшает зависимость от ручного вмешательства администратора.

Недостатки IPS:

- Может блокировать легитимный трафик из-за ложных срабатываний.
- Требует тонкой настройки, чтобы не снижать производительность сети.

Основные отличия IDS и IPS:

Характеристика	IDS	IPS
Функция	Обнаруживает угрозы	Обнаруживает и блокирует угрозы
Реакция	Оповещение или отчёт	Автоматическое вмешательство
Расположение	После передачи данных	В потоке трафика
Влияние на сеть	Не влияет	Может замедлить работу сети

Совместное использование:

IDS и IPS часто используются вместе, чтобы объединить преимущества обеих систем. IDS предупреждает администраторов о потенциальных угрозах, а IPS автоматически блокирует их в реальном времени.

Примеры систем IDS/IPS:

- **Snort** (открытое решение для IDS/IPS).
- **Suricata**.
- **Cisco Firepower**.
- **Palo Alto Networks**.

4.NTA

NTA (Network Traffic Analysis) — это анализ сетевого трафика для выявления аномалий, угроз и подозрительных действий. Основная цель NTA — **мониторинг и обнаружение угроз** в сетевой инфраструктуре, включая сложные атаки, которые могут пройти незамеченными традиционными средствами защиты, такими как IDS/IPS или NGFW.

Основные функции NTA:

1. **Сбор сетевого трафика:**
    - Захватывает данные о сетевой активности, включая пакеты, сессии, и метаданные, с использованием технологий, таких как NetFlow, IPFIX, sFlow и других.
2. **Выявление аномалий:**
    - Анализирует поведение сетевых устройств и пользователей в режиме реального времени для выявления отклонений от нормальной активности.
3. **Обнаружение угроз:**
    - Использует методы машинного обучения, эвристики и поведенческого анализа для выявления сложных атак (например, скрытых APT — Advanced Persistent Threats).
4. **Контекстуализация событий:**
    - Позволяет связать выявленные аномалии с конкретными устройствами, пользователями или приложениями.
5. **Обнаружение атак без сигнатур:**
    - NTA эффективно выявляет атаки, которые ещё не имеют известных сигнатур (например, нулевые дни).

Основные возможности NTA:

- **Мониторинг в реальном времени:** Постоянное наблюдение за всей сетевой активностью.
- **Обнаружение аномалий:** Поиск необычного поведения, например:
    - Необычно большое количество пакетов.
    - Подозрительные соединения с редкими IP-адресами.
    - Попытки обхода политик безопасности.

- **Поддержка расследования инцидентов:** Хранение записей сетевого трафика для последующего анализа.
- **Интеграция с другими системами безопасности:** NTA может работать совместно с SIEM, SOC и IPS/IDS для более комплексного подхода.

Где применяется NTA:

1. **Обнаружение скрытых угроз:** Например, утечка данных, внутренние атаки или вредоносный трафик.
2. **Мониторинг облачной инфраструктуры:** Выявление аномалий в гибридных и облачных сетях.
3. **Защита IoT-устройств:** Анализ активности устройств Интернета вещей для выявления подозрительного поведения.
4. **Защита от APT-атак:** Обнаружение сложных атак, таких как скрытые перемещения внутри сети (lateral movement) или эксфильтрация данных.

Преимущества NTA:

- Обнаружение угроз, которые невозможно выявить с помощью сигнатурных методов.
- Поддержка сложных инфраструктур (гибридные облака, IoT).
- Обнаружение аномалий в зашифрованном трафике (без расшифровки).

Недостатки:

- Требует мощных вычислительных ресурсов для анализа больших объёмов данных.
- Возможны ложные срабатывания, особенно в сложных сетях без правильно настроенных базовых моделей поведения.

Примеры решений для NTA:

- **Darktrace**
- **Cisco Stealthwatch**
- **Extrahop**
- **Vectra AI**
- **Corelight**

NTA является ключевым инструментом для современных команд по обеспечению кибербезопасности, дополняя традиционные средства защиты (IDS, IPS, SIEM) и позволяя выявлять угрозы, которые могут оставаться незамеченными в классических системах.