УДК 004.75

АНАЛИЗ СЕТЕВОГО ТРАФИКА. МЕТОДЫ СБОРА СЕТЕВЫХ ПРИЗНАКОВ И ПРЕДУПРЕЖДЕНИЙ ДЛЯ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ

Грибович А.А., Клепцов Ю.В., Грищук А.А. магистранты гр.267041

Белорусский государственный университет информатики и радиоэлектроники[1]
г. Минск, Республика Беларусь

Медведев С.А. – канд. технич. наук

Аннотация. Рассматривается задача сбора и анализа сетевых признаков и предупреждений для выявления аномалий и вредоносной активности, улучшения диагностики, восстановления и устранения причинных факторов. Рассмотрена концепция сетевого мониторинга безопасности (NSM) и методы сбора данных.

Ключевые слова. Сетевой мониторинг безопасности, сбор сетевых данных, обнаружение на конечных точках.

Введение. В современном мире безопасность сетей становится все более приоритетной, особенно в условиях нарастающих угроз в интернете. Эффективные

методы сбора данных о сетевой активности играют решающую роль в обнаружении и реагировании на потенциальные атаки.

Концепция сетевого мониторинга безопасности (NSM) включает в себя сбор, анализ и реагирование на признаки вторжений [1]. Необходимость сбора сетевых данных обусловлена выявлением аномалий и вредоносной активности, что предоставляет ценную информацию о возможных угрозах. Каждый из методов сбора данных имеет свои преимущества и недостатки, и их выбор зависит от конкретных требований и целей. В данной работе мы рассмотрим каждый из них в контексте обеспечения безопасности сети.

Важно отметить, что мониторинг сетевых данных и активности пользователей играет важную роль в обеспечении безопасности сети. Постоянное обновление политик безопасности и тщательная проверка конфигураций конечных точек являются неотъемлемой частью защиты сети от вредоносных атак.

Основная часть. Мониторинг сетевой безопасности (NSM) - это сбор, анализ и эскалация признаков и предупреждений для обнаружения и реагирования на вторжения. Данный подход неявно обращается к планированию деятельности или попыткам сопротивления вторжениям. Все четыре фазы цикла безопасности – планирование, сопротивление, обнаружение и реагирование необходимы при защите сети организации от угроз. Первым шагом в построении операционной модели является описание взаимосвязей между планированием, сопротивлением, обнаружением и реагированием, как показано на рисунке 1.

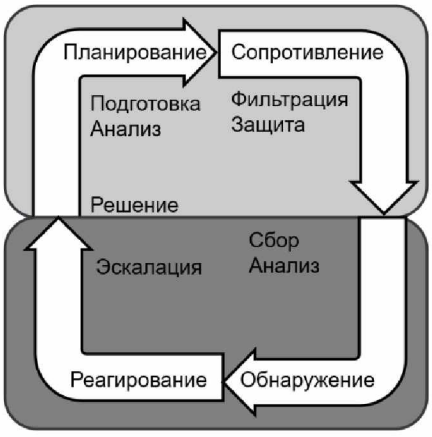

Рисунок 1 – Цикл обеспечения безопасности

IT-команды и команды по безопасности планируют новые защитные меры, в то время как существующие компоненты противодействия отражают некоторых злоумышленников. В то время как одна группа занимается обнаружением одних злоумышленников, реагируя на них, команды инцидентного реагирования по безопасности уже реагируют на других злоумышленников, уже проникших в организацию.

Фаза планирования. Команды IT и безопасности подготавливаются и анализируют текущую ситуацию, нацеливаясь на оптимальное сопротивление вторжениям и уязвимостям. В рамках этой фазы проводятся бюджетирование, аудит, проверка соответствия, обучение и разработка безопасного программного обеспечения. К примерам работы по оценке относятся симуляция атак, тестирование на проникновение и практика проведения атакующих операций.

Фаза сопротивления. Команды IT и безопасности осуществляют фильтрацию и защиту данных. Здесь применяется автоматизированное противодействие, такое как брандмауэры, антивирусное программное обеспечение и защита от утечки данных. Также проводятся обучение по безопасности и управление конфигурацией и уязвимостями.

Фазы обнаружения и реагирования включают в себя сбор, анализ и эскалацию, которые являются основой цикла безопасности предприятия. Аналитики занимаются обнаружением и реагированием на вторжения.

Сбор данных, которые нам необходимы для принятия решения о том, является ли деятельность нормальной, подозрительной или вредоносной. Включает в себя различные процессы, которые собирают информацию, как техническую, так и не техническую.

Технические процессы включают в себя сбор данных с конечных точек или хостов (таких как компьютеры, серверы, планшеты, мобильные устройства и т. д.), сети и логов (созданных приложениями, устройствами и другими источниками).

Нетехнические процессы сбора включают запись информации от сторонних лиц (внешних участников, таких как партнеры, правоохранительные органы, разведывательные агентства и т. д.) и пользователей. Индикатор компроментации (IOC) – это признак компрометации, который указывает на наличие инцидента безопасности или активности злоумышленников в сети или системе. IOC может включать в себя различные типы данных, такие как IP-адреса, URL-адреса, хэши файлов, паттерны сетевого трафика, аномальные действия пользователей и другие сигналы, которые могут указывать на наличие угрозы безопасности.

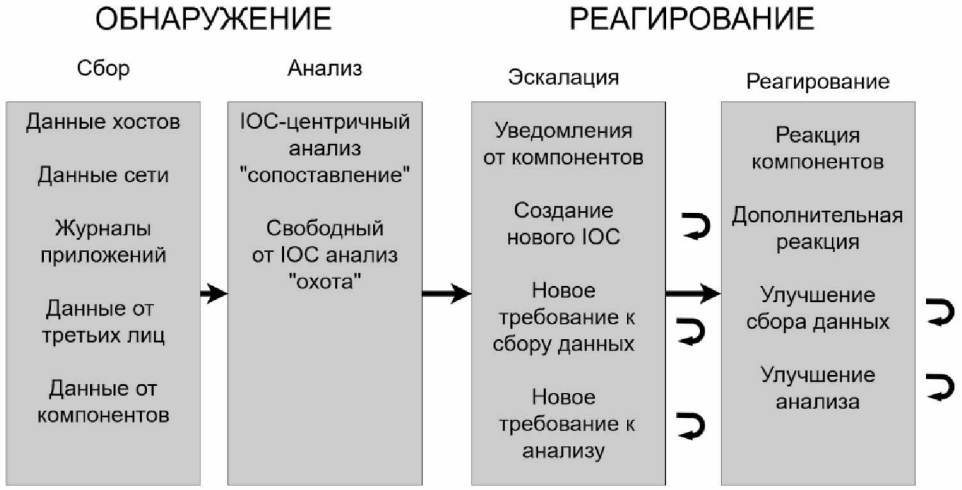

Рисунок 2 – Процесс сетевого управления безопасностью

Сбор данных происходит с помощью комбинации аппаратных и программных средств, которые используются для генерации и сбора данных для обнаружения и анализа NSM [2].

Большинство организаций можно отнести к одной из трех категорий:

- Организации без установленной инфраструктуры NSM, которые только начинают определять свои потребности в сборе данных.
- Организации, которые уже занимаются обнаружением вторжений, но никогда подробно не изучали данные, которые они собирают.
- Организации, которые вложили много времени в определение своей стратегии сбора данных и постоянно совершенствуют эту стратегию в рамках цикла NSM.

Сбор сетевых данных может помочь выявить закономерности, и необходим для обнаружения аномальной или вредоносной активности в сети. Предоставляет полезную информацию о вторжениях для улучшения диагностики, восстановления и устранения причинных факторов. Вот несколько методов:

1. Захват пакетов: Используйте инструменты захвата пакетов, такие как Wireshark, tcpdump или Snort, для захвата сетевых пакетов, проходящих по сети. Захват пакетов

позволяет вам осмотреть содержимое отдельных пакетов, включая исходные и конечные IP-адреса, порты, протоколы и данные полезной нагрузки.

Процесс сниффинга пакетов включает в себя взаимодействие программного и аппаратного обеспечения и состоит из трех этапов:

Сбор данных: Сначала сниффер пакетов собирает сырые двоичные данные с провода, переключая выбранный сетевой интерфейс в режим promiscuous. Это позволяет прослушивать весь трафик на сегменте сети.

Преобразование: Захваченные двоичные данные преобразуются в читаемый формат. Большинство продвинутых снифферов ограничиваются этим этапом, оставляя анализ для пользователя.

Анализ: Сниффер пакетов анализирует захваченные данные, проверяя протокол сетевых данных и выявляя его особенности [3].

PCAP представляет собой формат файла, используемый для хранения данных, захваченных при сниффинге пакетов. PCAP - это важный инструмент для системных администраторов и команд по безопасности, предоставляющий глубокое понимание сети [4]. Он увеличивает видимость сети, позволяет мониторить в реальном времени и прост в использовании. Однако есть и недостатки:

- Не обнаруживает угрозы, не связанные с сетью, такие как атаки на аппаратный уровень.
- Не преодолевает шифрование, что делает невозможным анализ зашифрованных коммуникаций.
- Расположение сниффера пакетов влияет на видимость, так как он не может видеть всю активность по сети.

2. Анализ сетевого потока: Собирает данные сетевого потока, которые предоставляют краткую информацию о потоках сетевого трафика. Данные потока включают в себя такие детали, как исходные и конечные IP-адреса, порты, протоколы и метки времени. Инструменты, такие как NetFlow, sFlow или IPFIX, могут использоваться для экспорта данных потока из маршрутизаторов, коммутаторов или сетевых устройств.

Строго говоря, поток – это серия пакетов, которые имеют одни и те же исходные и конечные IP-адреса, исходные и конечные порты, а также IP-протокол [5]. Это также называется пятикратным IP-потоком. Термин "поток" иногда также используется для обозначения агрегации отдельных потоков. Запись потока – это сводная информация о потоке, записывающая, какие хосты общались с какими другими хостами, когда происходила эта связь, как трафик передавался, и другая основная информация о сетевом общении. Система анализа потока собирает информацию о потоках и предоставляет вам систему для поиска, фильтрации и печати информации о потоках. Записи потока подводят итоги каждого соединения в вашей сети.

Архитектура потоковой системы включает три компонента:

- Сенсор (зонд): Устройство, которое прослушивает сеть и захватывает данные о трафике. Это может быть коммутатор, маршрутизатор или программное обеспечение, которое слушает сетевой трафик. Сенсор отслеживает сетевые соединения и передает данные после завершения соединения или по истечении тайм-аута.
- Коллектор: Программное обеспечение, которое получает записи сенсора и сохраняет их на диск. Коллектор является критической частью инфраструктуры управления потоками, хотя формат хранения данных может отличаться.
- Система отчетности: Читает файлы коллектора и создает удобные для анализа отчеты. Система должна быть совместима с форматом файла, используемым коллектором.

3. Обнаружение вторжений (IDS) - это процесс мониторинга событий в компьютерной системе или сети и анализа их на наличие признаков вторжений, таких как попытки компрометации конфиденциальности, целостности и доступности данных, а также обход механизмов безопасности [6]. Эти события могут быть вызваны злоумышленниками, получающими доступ из Интернета, авторизованными пользователями, пытающимися получить несанкционированные привилегии, или авторизованными пользователями, злоупотребляющими своими привилегиями.

Цели использования IDS:

- Предотвращение проблемного поведения путем увеличения риска обнаружения и наказания злоумышленников.
- Обнаружение атак и других нарушений безопасности, которые не удается предотвратить другими мерами безопасности.
- Обнаружение и реагирование на предвестники атак, такие как сетевые запросы и другие аномалии.
- Документирование существующих угроз для организации.
- Контроль качества проектирования и администрирования безопасности, особенно в крупных и сложных предприятиях.

4. Управление информацией и событиями безопасности (SIEM). SIEM используется для централизации и корреляции журнальных данных с различных сетевых устройств и средств безопасности. Платформы SIEM собирают журналы от брандмауэров, маршрутизаторов, коммутаторов, сенсоров IDS/IPS, серверов и других сетевых устройств, и применяют правила корреляции для выявления потенциальных инцидентов безопасности.

5. Журналирование на DNS и DHCP серверах для мониторинга разрешений доменных имен и выделений IP-адресов. Анализ журналов DNS и DHCP может помочь выявить подозрительные доменные имена, IP-адреса или имена хостов, связанные с злонамеренной деятельностью.

6. Журналы прокси-серверов и веб-серверов. Используются для мониторинга веб-активности пользователей и доступа к внешним сайтам. Журналы прокси-серверов и веб-серверов могут предоставить информацию о шаблонах веб-трафика, поведении пользователей и потенциальных угрозах безопасности, таких как доступ к вредоносным веб-сайтам или загрузка подозрительных файлов. Включите журналирование на сетевых устройствах, таких как брандмауэры, маршрутизаторы и коммутаторы, чтобы записывать события и активности.

6. Сетевые тапы/Зеркалирование портов сети. Используется для копирования сетевого трафика с одного сегмента сети на другой. Это позволяет вам мониторить сетевой трафик, не нарушая поток данных. Сетевые тапы и зеркалирование могут быть особенно полезны для захвата трафика на высокоскоростных или критически важных сетевых каналах.

7. Обнаружение и ответ на события на конечных точках (EDR). Интегрируются решения безопасности конечных точек с возможностями мониторинга сети для сбора данных с конечных точек о сетевых подключениях, трафике и связи. Решения EDR предоставляют информацию о сетевой активности конечной точки и могут помочь выявить аномальное или злонамеренное поведение, свидетельствующее о угрозах безопасности.

По мере присоединения, изменения и выхода устройств из наших сетей, они приобретают динамичные характеристики, сравнимые с фильмом, а не статичным снимком [7]. Наш подход к сети, особенно к ее периметру, должен быть адаптивным и постоянно ориентированным на динамическую природу сети. Это требует от нас не только моментальных снимков, но и всестороннего обеспечения доверительности всех подключаемых к нам конечных точек.

С учетом разнообразия методов подключения устройств к нашим сетям, конечная точка становится ключевым периметром, который необходимо защитить. Хотя у нас есть сетевые брандмауэры, контролирующие широкомасштабный доступ к сети, основная угроза исходит от мелких нарушений доступа, таких как небольшие вирусы, попадающие в сеть через пользовательские конечные точки.

Путем анализа данных с этих сетевых источников организации могут обнаружить и оперативно реагировать на аномальную или вредоносную активность на своих сетях, чтобы минимизировать потенциальные угрозы безопасности.

Как минимум, предпочтительно избежать следующего: вирусов, червей, незаконного программного обеспечения, шпионских программ, неавторизованных пользователей, неавторизованных конечных точек [8].

Каждая конечная точка должна выполнять следующее: обеспечить целостность операционной системы, проверить конфигурацию системы, быть удаленно управляемой.

Успешное удаленное управление требует строгой политики, которая обеспечивает соблюдение минимальной конфигурации для всех подключенных конечных точек, независимо от возражений пользователей. Это важно, поскольку даже одна несоответствующая система может привести к серьезным проблемам в сети.

На рисунке 3 показан процесс коррекции наших правил, включая в них принципы восстановления и компартментализации. Важно понять, может ли сеть может доверять каждой из конечных точек.

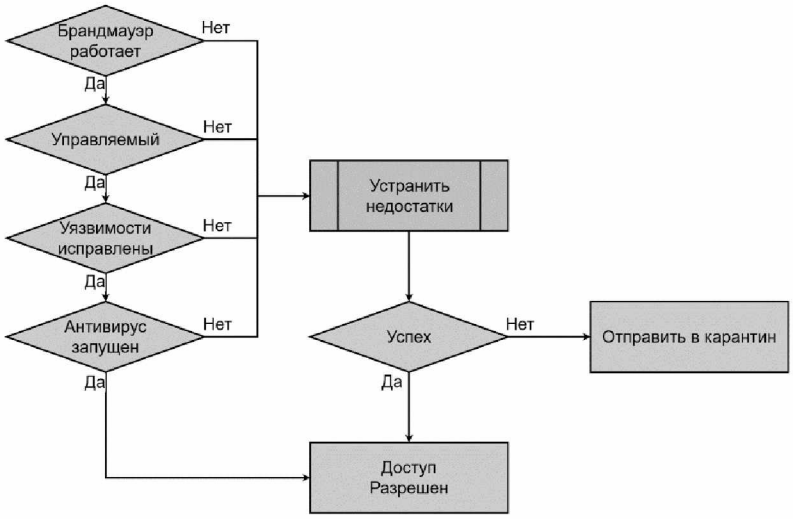

Рисунок 3 – Конечная точка должна быть помещена в карантин, если не проходит четыре простых теста

Заключение. В современном мире, где угрозы в интернете продолжают расти, мониторинг сетевых данных и активности пользователей играет ключевую роль в обеспечении безопасности сети. Разнообразные методы сбора данных имеют свои преимущества и недостатки, и выбор конкретного метода зависит от требований и целей организации. Однако, независимо от выбранного метода, важно понимать необходимость постоянного обновления политик безопасности и строгой проверки конфигураций конечных точек, хостов и других узлов сети, как неотъемлемой части защиты от вредоносных атак.

Список использованных источников:

1. Richard Bejtlich // The Practice of Network Security Monitoring: Understanding Incident Detection and Response, 2013. P. 185-189.

2. Chris Sanders, Jason Smith, and Liam Randall // Applied Network Security Monitoring: Collection, Detection, and Analysis, 2014. P. 74-75.

3. Крис Сандерс // Анализ пакетов: Практическое руководство по использованию Wireshark и tcpdump для решения реальных проблем в локальных сетях, 2017. P. 23-26.

4. What Is PCAP? Packet Capture Explained [Electronic resource]. URL: www.forbes.com/advisor/business/software/what-is-pcap. (date of access: 05.02.2024).

5. Michael W. Lucas // Network Flow Analysis, 2010. P. 10-12.

6. *Rebecca Bace, Peter Mell // Intrusion Detection Systems, 1999. P. 5-6.*
7. *Mark Kadrich // Endpoint Security, 2007. P. 15.*
8. *Mark Kadrich // Endpoint Security, 2007. P. 73-74.*