УДК 004.056

Булыгин Дмитрий Константинович студент
5 курс, Санкт-Петербургский государственный университет
телекоммуникаций им. проф. М.А. Бонч-Бруевича
Россия, г. Санкт-Петербург

АНАЛИЗ СЕТЕВОГО ТРАФИКА КАК МЕТОД РАССЛЕДОВАНИЯ КИБЕРПРЕСТУПЛЕНИЙ

Аннотация: *В статье рассматривается анализ сетевого трафика как эффективный метод расследования киберпреступлений. Описаны определение сетевого трафика, его компоненты и различные типы, такие как TCP/IP и UDP, а также инструменты для его захвата и анализа. Рассмотрена роль этого метода в выявлении аномалий, установлении источников атак и сборе доказательств. Так же приведен пример применения анализа сетевого трафика для обнаружения инцидента, что демонстрирует практическую значимость данного подхода. Работа направлена на углубление понимания методов расследования киберпреступлений и подчеркивает важность анализа сетевого трафика в обеспечении информационной безопасности.*

Ключевые слова: *информационные технологии, информационная безопасность, кибербезопасность, анализ сетевого трафика, цифровая компьютерная криминалистика.*

Annotation: *The article examines network traffic analysis as an effective method for investigating cybercrimes. It describes the definition of network traffic, its components, and various types such as TCP/IP and UDP, as well as the tools used for capturing and analyzing it. The role of this method in detecting anomalies, identifying attack sources, and collecting evidence is discussed. Additionally, an example of using network traffic analysis to detect an incident is provided, demonstrating the practical significance of this approach. The work aims to deepen*

the understanding of cybercrime investigation methods and emphasizes the importance of network traffic analysis in ensuring information security.

Key words: information technology, information security, cybersecurity, network traffic analysis, digital computer forensics.

В современном мире, где цифровая трансформация охватывает все сферы жизни, киберпреступления становятся одной из наиболее острых проблем для общества, бизнеса и государственных структур. Актуальность анализа сетевого трафика как метода расследования киберпреступлений обусловлена несколькими ключевыми факторами:

Количество кибератак продолжает расти с каждым годом. Наблюдается значительное увеличение случаев использования фишинга, вредоносного ПО и других форм киберугроз. Это создает необходимость в эффективных методах расследования, таких как анализ сетевого трафика, который позволяет выявлять и предотвращать подобные атаки.

Киберпреступления становятся все более сложными и изощренными. Злоумышленники используют продвинутые технологии и методы шифрования, что затрудняет их обнаружение и расследование. Анализ сетевого трафика предоставляет возможность отслеживать аномалии и подозрительную активность в реальном времени, что критически важно для успешного расследования.

Анализ сетевого трафика представляет собой ключевой элемент в области кибербезопасности и расследования киберпреступлений, позволяя выявлять, отслеживать и предотвращать угрозы. Сетевой трафик - совокупность данных, передаваемых между устройствами в компьютерной сети. Он состоит из различных компонентов, включая пакеты данных, протоколы передачи и адресацию, которые обеспечивают взаимодействие между пользователями и системами. Каждый пакет содержит информацию о отправителе, получателе, а также о типе передаваемых данных.

Существует несколько типов сетевого трафика, наиболее распространенными из которых являются TCP/IP и UDP. Протокол TCP

(Transmission Control Protocol) обеспечивает надежную и последовательную передачу данных, что делает его идеальным для приложений, требующих гарантированной доставки, таких как веб-серфинг и электронная почта. В отличие от него, UDP (User Datagram Protocol) обеспечивает более быструю, но менее надежную передачу данных, что подходит для приложений в реальном времени, таких как видеоконференции и онлайн-игры. [1, с. 90].

Для захвата и анализа сетевого трафика используются различные инструменты и технологии. К ним относятся программные решения, такие как Wireshark, tcpdump и другие системы мониторинга сетевой активности. Эти инструменты позволяют исследователям перехватывать пакеты данных в реальном времени, анализировать их содержимое и выявлять аномалии или подозрительные действия. Таким образом, основы анализа сетевого трафика включают в себя понимание его компонентов, типов и применения соответствующих инструментов, что составляет фундамент для эффективного расследования киберпреступлений.

Анализ сетевого траффика состоит из нескольких этапов. Сначала выявляются аномалии, поскольку многие кибератаки характеризуются отклонениями от нормального поведения сети. Используя методы статистического анализа и машинного обучения, специалисты могут обнаруживать необычные паттерны трафика, такие как резкое увеличение объема данных, несанкционированные попытки доступа к ресурсам или нестандартные протоколы передачи. Эти аномалии могут служить ранними индикаторами потенциальных угроз и позволяют оперативно реагировать на инциденты.

Следующим этапом является установление отправителя и получателя атак для определения виновных и предотвращения дальнейших инцидентов. Анализ сетевого трафика позволяет отслеживать маршруты передачи данных, идентифицировать IP-адреса злоумышленников и сопоставлять их с известными базами данных угроз. Это не только способствует более

глубокому пониманию характера атаки, но и помогает в разработке стратегий защиты для предотвращения аналогичных инцидентов в будущем.

Наконец, сбор доказательств для судебных разбирательств является завершающим этапом анализа сетевого трафика. Полученные данные могут быть использованы в качестве ключевых улик в судебных процессах против киберпреступников. Пакеты данных, журналы сетевой активности и другие артефакты, собранные в ходе анализа, могут быть представлены в суде как доказательства, подтверждающие факты нарушения закона. Таким образом, анализ сетевого трафика не только способствует выявлению и предотвращению киберпреступлений, но и играет важную роль в правоприменительной практике, обеспечивая законность и справедливость в борьбе с киберугрозами.

Рассмотрим инцидент и как его можно проанализировать с помощью Wireshark, многофункционального анализатора сетевого трафика с открытым исходным кодом, который позволяет в режиме реального времени захватывать, декодировать и изучать сетевые пакеты. Используем гипотетический сценарий, в котором злоумышленник получает доступ к корпоративной сети и начинает выполнять атаку типа Brute Force. [2].

Microsoft Exchange и Office 365 являются широко используемыми решениями для корпоративной электронной почты. Злоумышленники могут воспользоваться этими сервисами для получения доступа к учетным записям пользователей Active Directory. Они используют метод, при котором сначала составляют список пользователей, а затем пытаются подобрать к ним пароли, чтобы избежать блокировки учетных записей. Вместо использования словаря паролей для каждого пользователя, они применяют один и тот же пароль для всех. Этот метод называется password spraying.

Если в инфраструктуре применяется аутентификация через Kerberos, для выявления попыток подбора паролей необходимо анализировать протокол, находить сессии с ошибками, указывающими на отсутствие

запрашиваемого пользователя, и отслеживать сессии с точностью до миллисекунд.

Если в сетевом трафике наблюдается множество сессий с ошибкой KDC_ERR_C_PRINCIPAL_UNKNOWN для различных учетных записей, это свидетельствует о том, что злоумышленники пытаются перебрать имена пользователей.

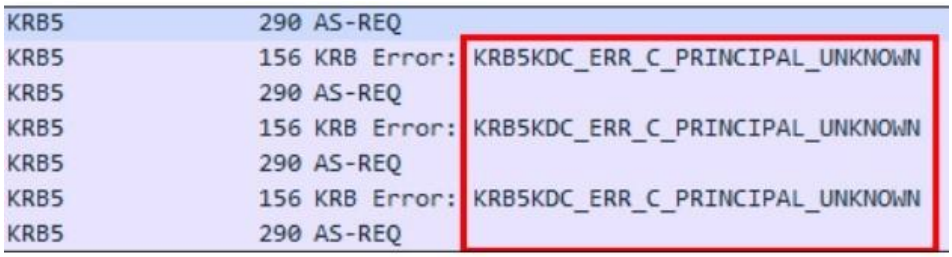


Рисунок 1. Пример сессии с ошибкой

Сессии с коротким временем отклика сервера (десятки миллисекунд) по сравнению с другими сессиями (сотни миллисекунд) указывают на успешный подбор паролей. В трафике также будут видны попытки входа с подобранными учетными записями и ошибки Kerberos. Сессии без ошибок, с успешными ответами AS_REP и выданными билетами указывают на то, какие учетные записи были успешно взломаны.

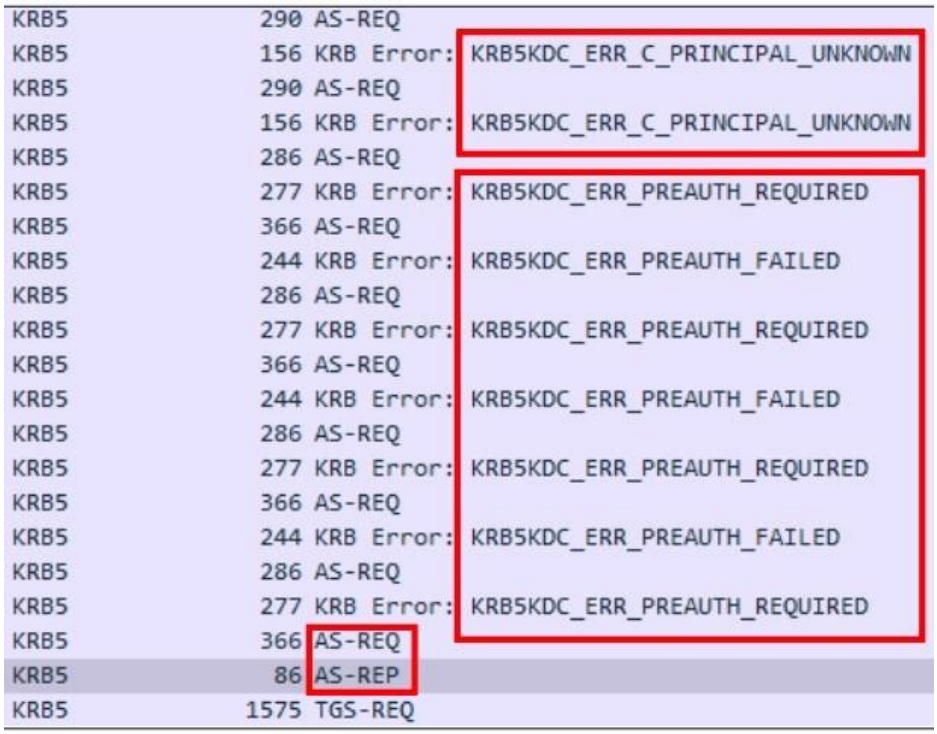


Рисунок 2. Успешный подбор пароля

Кроме того, можно заметить цикличность в именах пользователей, так как злоумышленники подбирают один и тот же пароль для всех учетных записей из списка. Перед атакой может быть сделан запрос на получение информации о политике паролей домена: сколько попыток неправильного ввода пароля разрешено и на какое время блокируется учетная запись.

Атаку, описанную выше, можно выявить и с помощью других методов, таких как SIEM и анализ журналов событий. На конечных устройствах можно обнаружить артефакты, указывающие на компрометацию, но для полного понимания цепочки атаки и определения первоначального вектора проникновения, а также для проверки гипотез в рамках охоты за угрозами, необходимо отслеживать действия злоумышленника в сети, выявлять соединения с командными серверами или узлами в Tor, а также находить и анализировать аномалии в сетевом трафике.

Стандартные решения для защиты конечных устройств и межсетевые экраны зачастую не обеспечивают необходимого уровня контроля, так как опытные хакеры могут адаптировать свои инструменты для их обхода. Анализ сетевого трафика станет полезным дополнением к уже проверенным методам обнаружения и расследования киберинцидентов. Копия сетевого трафика может помочь специалисту по информационной безопасности глубже разобраться в инциденте.

Использованные источники

1. Таненбаум, Э. С. Компьютерные сети / Таненбаум, Э. С. Фимстер Н. , Уэзеролл Д.— 6-е изд.— Москва : Питер, 2025.— 90 с.

2. Wireshark — подробное руководство по началу использования : Хабр. [Электронный ресурс]. URL: https://habr.com/ru/articles/735866/ (дата обращения: 26.11.2025).