Молдавский Государственный Университет
Факультет Математики и Информатики
Департамент Информатики

Лабораторная работа №6
по курсу “Securitatea Sistemelor Informatice”

Тема: “Обнаружение и предотвращение вторжений в компьютерные системы. Системы защиты от вредоносного ПО и журналирования. IDS/IPS (Intrusion Detection Systems / Intrusion Prevention Systems) (Windows, Linux и т. д.)”

Выполнил: Slavov Constantin,
студент группы I2302
Проверила: L. Novac,
doctor conferențiar universitar

Кишинев, 2024

- Введение: В этой лабораторной работе я буду изучать характеристики и принципы работы систем обнаружения и предотвращения вторжений (IDS/IPS). По ходу выполнения я проанализирую основные параметры этих систем, чтобы лучше понять, как они работают и насколько они эффективны в разных условиях.

Также я сравню несколько IDS/IPS систем из предложенного списка. Особое внимание будет уделено их совместимости с операционными системами, такими как Windows, Linux и iOS, а также возможности управления через мобильные устройства, например телефоны и планшеты.

Кроме того, я рассмотрю, как эти системы работают, и попробую классифицировать их по популярности и эффективности. Это поможет мне выделить наиболее удобные и полезные решения.

- Ход работы:

- Общая характеристика систем обнаружения вторжений (IDS). Классификация систем IDS

IDS отслеживают активность в сети или на устройствах для выявления угроз. Основные виды:

- Сигнатурные – ищут известные угрозы по базам сигнатур.
- **Аномалийные** – выявляют отклонения от нормального поведения.
- **Гибридные** – совмещают оба подхода для повышения эффективности.

- Типичные механизмы обнаружения вторжений. Распространенные типы систем IDS

Механизмы:

- Сигнатурное обнаружение – поиск совпадений с шаблонами атак.
- **Анализ аномалий** – обнаружение отклонений в поведении.

Типы систем:
- **Сетевые (NIDS)** – мониторят сетевой трафик.
- **Хостовые (HIDS)** – следят за активностью конкретного устройства.

- Характеристики решений IDS, важные для практического применения. Смешанные системы

Важные параметры:

- Точность – снижение ложных срабатываний.

- **Скалируемость** – работа с большими объемами данных.

Смешанные IDS объединяют сигнатурный и аномалийный подходы для более точной и гибкой защиты.

Сравнение IDS и IPS:

- Назначение

IDS (система обнаружения вторжений) используется для выявления подозрительных действий в сети и отправки уведомлений администраторам. IPS (система предотвращения вторжений) не только обнаруживает угрозы, но и автоматически блокирует их в реальном времени.

- Методы работы

IDS анализирует сетевой трафик с помощью сигнатурного анализа (поиск известных угроз) и поведенческого подхода (выявление аномалий). IPS использует аналогичные методы, но также имеет возможность вмешиваться в сетевой трафик.

- Реакция на угрозы

IDS фиксирует угрозы и отправляет уведомления, не блокируя действия. IPS активно предотвращает атаки, прерывая соединения или изменяя сетевые правила.

- Влияние на сеть

IDS не влияет на производительность сети, так как только анализирует данные. IPS может вызывать задержки или ложные срабатывания из-за вмешательства в сетевой трафик.

- Примеры

Примерами IDS являются Snort, Zeek (Bro) и NetworkMiner. К примерам IPS относятся Palo Alto Networks, FortiGate и Wireshark.

IDS подходит для анализа и выявления угроз, предоставляя подробную информацию о подозрительных действиях, а IPS обеспечивает проактивную защиту, блокируя атаки в реальном времени. Вместе они создают комплексную систему безопасности.

Для более подробного сравнительного анализа систем IDS были взять следующие системы:

Сравнение Wireshark и NetworkMiner

Критерий	*Wireshark*	*NetworkMiner*
Условия использования	Бесплатное ПО с открытым исходным кодом (GPL).	Бесплатная версия с ограниченными функциями, платная версия для расширенного функционала.
Совместимость с ОС	Поддержка Windows, macOS, Linux, UNIX.	Поддержка Windows; возможно, работает через Wine на Linux, но официально не поддерживается.
Предлагаемые услуги/принципы работы	Анализ сетевого трафика в реальном времени; мощные инструменты фильтрации и декодирования.	Анализ захваченных пакетов, фокус на восстановлении файлов и данных из сетевых сессий.
Преимущества	- Мощный и гибкий анализ трафика. - Поддерживает тысячи протоколов. - Огромное сообщество.	- Простота для анализа pcap-файлов. - Поддержка восстановления данных (например, изображений).
Недостатки	- Крутая кривая обучения для новичков. - Может быть ресурсоемким.	- Ограниченная функциональность в бесплатной версии. - Ограниченная поддержка ОС.
Интерфейс/удобство	Графический интерфейс. Поддержка работы с командной строкой.	Удобный графический интерфейс, но без CLI.
Степень безопасности	Высокий уровень безопасности, но возможны ошибки анализа, если данные повреждены.	Минимальный риск ложных тревог, но ограничен в реальном времени.

Популярность/категории пользователей	Популярен среди сетевых инженеров, исследователей.	Используется исследователями кибербезопасности, экспертами по анализу данных.
Общая простота использования	Высокая сложность для новичков, но огромный потенциал для анализа.	Прост в освоении, особенно для восстановления файлов или анализа содержимого.

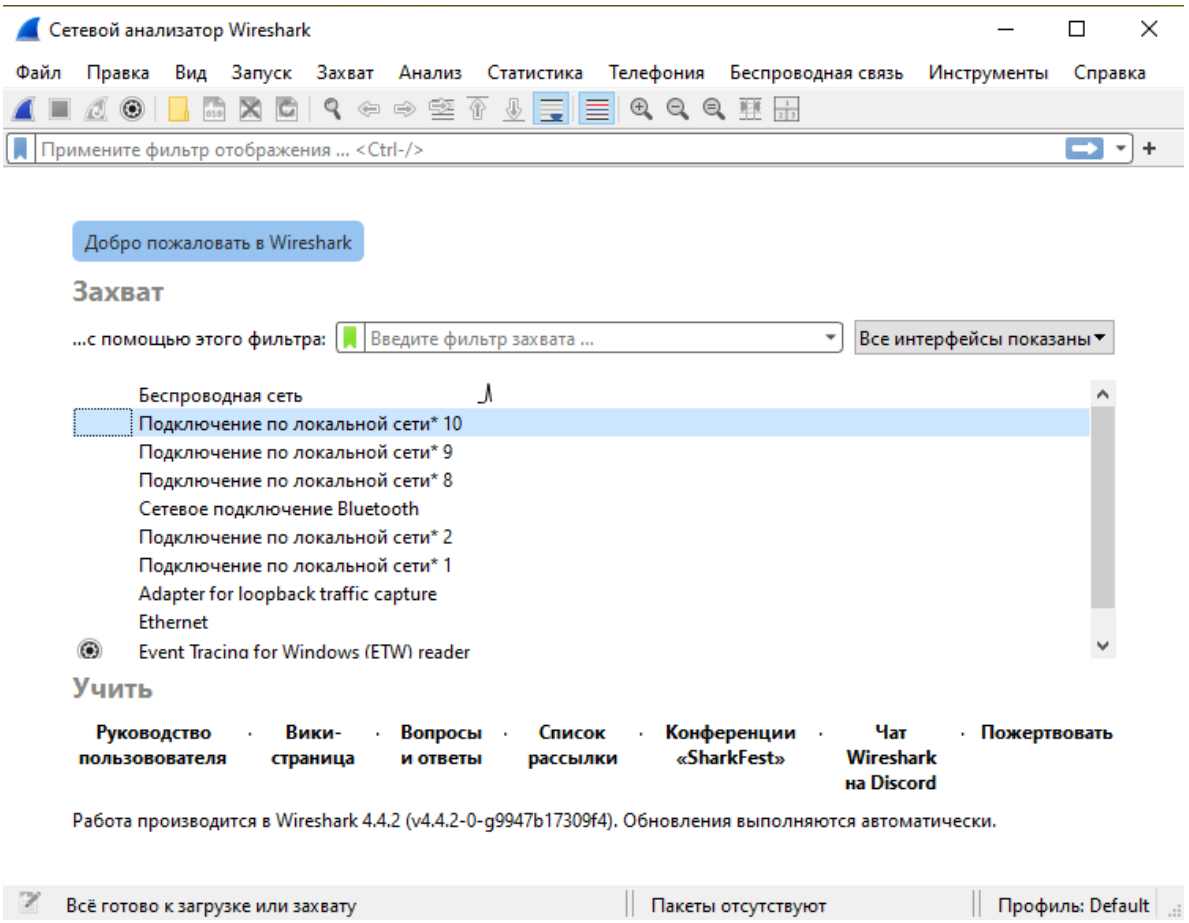
Wireshark и NetworkMiner имеют разные подходы к анализу сетевого трафика. Wireshark подходит для детального анализа трафика в реальном времени, предоставляя мощные инструменты декодирования, но требует высокой квалификации. NetworkMiner, напротив, более удобен для восстановления данных из уже захваченных пакетов, отличается простотой в использовании, но ограничен функционально и поддержкой ОС. Выбор между ними зависит от конкретных задач: глубокий анализ в реальном времени или восстановление данных из сессий.

- Перейдем к обзору программ:

Работа в программе **WireShark:**

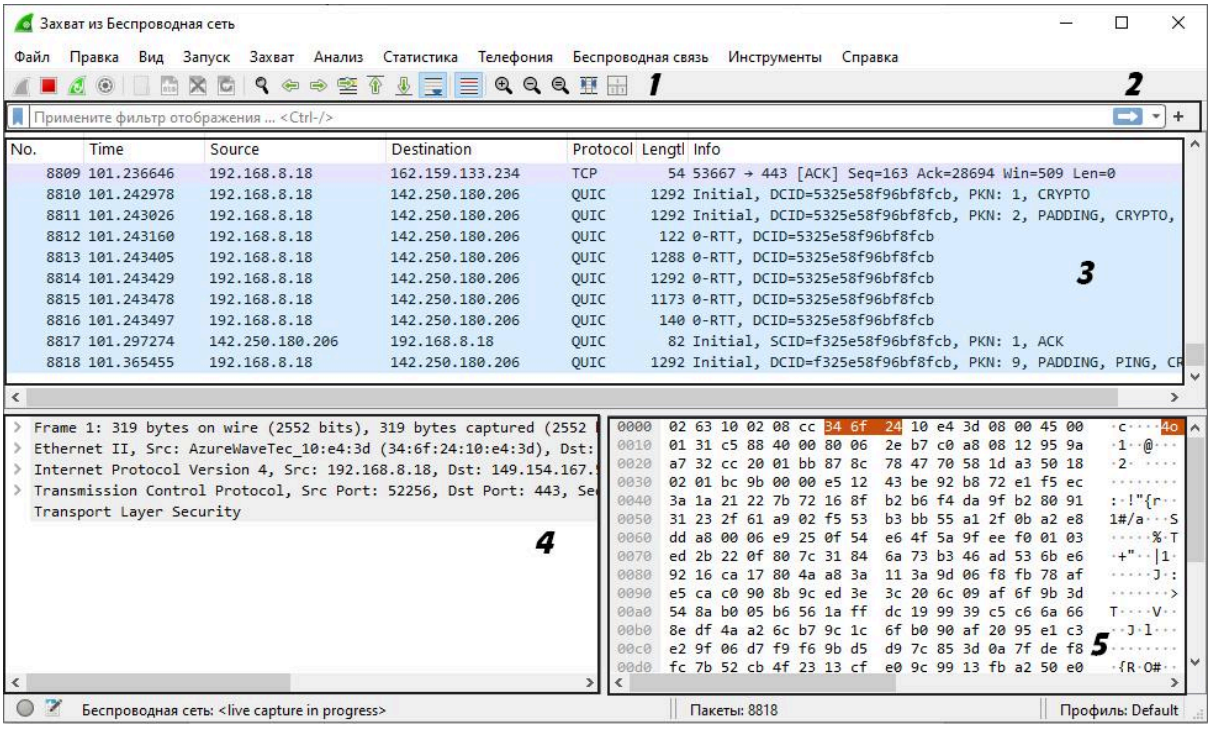
Данное программное обеспечение можно скачать с официального сайта разработчика, после чего установить его на свой компьютер. После установки требуется перезагрузка компьютера. Затем, можно начинать работы в самой программе.

После открытия программы, предоставляется возможность выбрать отображение желаемого интерфейса:



В моем случае, я выберу беспроводную сеть, потому что это тот сетевой интерфейс, к которому подключен мой компьютер.

После выбора подходящего интерфейса, появляется следующее окно. Пройдемся подробнее по его функционалу:



1. **Панель фильтров**

В верхней части интерфейса расположена панель, позволяющая применять фильтры для поиска необходимой информации. Фильтрация помогает сузить выборку отображаемых данных. Подробнее об этой функции можно узнать в соответствующем разделе руководства.

2. **Панель наименований**

Эта панель отображает заголовки столбцов с ключевой информацией о каждом пакете: номер, время с начала захвата, исходный и конечный адреса, используемый протокол, длину пакета и краткое описание содержимого.

3. **Панель пакетов**

Обновляется в реальном времени, отображая список всех захваченных пакетов. Информация в этой панели представлена в столбцах, которые соответствуют заголовкам на панели наименований.

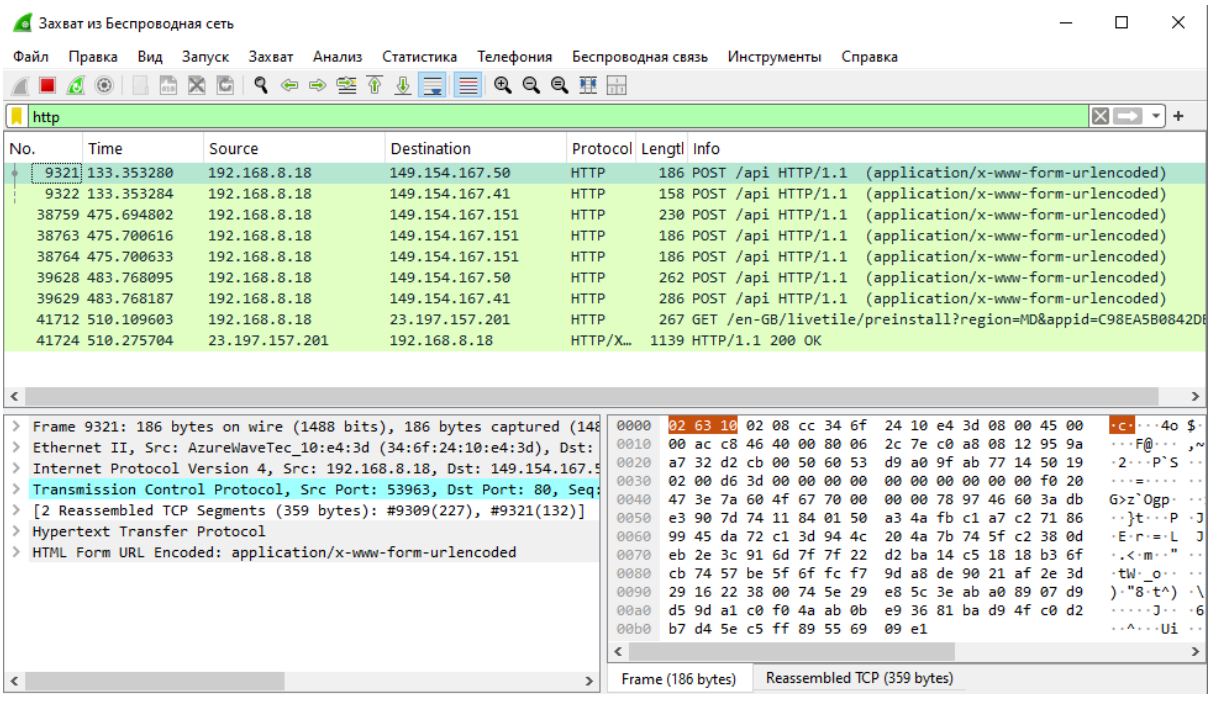
4. **Панель уровней**

Эта область описывает содержимое выбранного пакета с точки зрения уровней модели OSI. Здесь отображаются такие данные, как заголовки Ethernet, IP, TCP/UDP и других протоколов.

5. **Панель метаданных**

В нижней части интерфейса расположена панель, отображающая содержимое выбранного пакета в шестнадцатеричном коде и текстовом представлении. Это позволяет детально анализировать данные пакета.

Для анализа трафика был использован фильтр **http**, который позволил выделить HTTP-запросы, содержащие потенциально подозрительные действия. В процессе анализа пакетов важно уделять внимание необычным IP-адресам и типам запросов, которые могут указывать на возможные аномалии или угрозы.



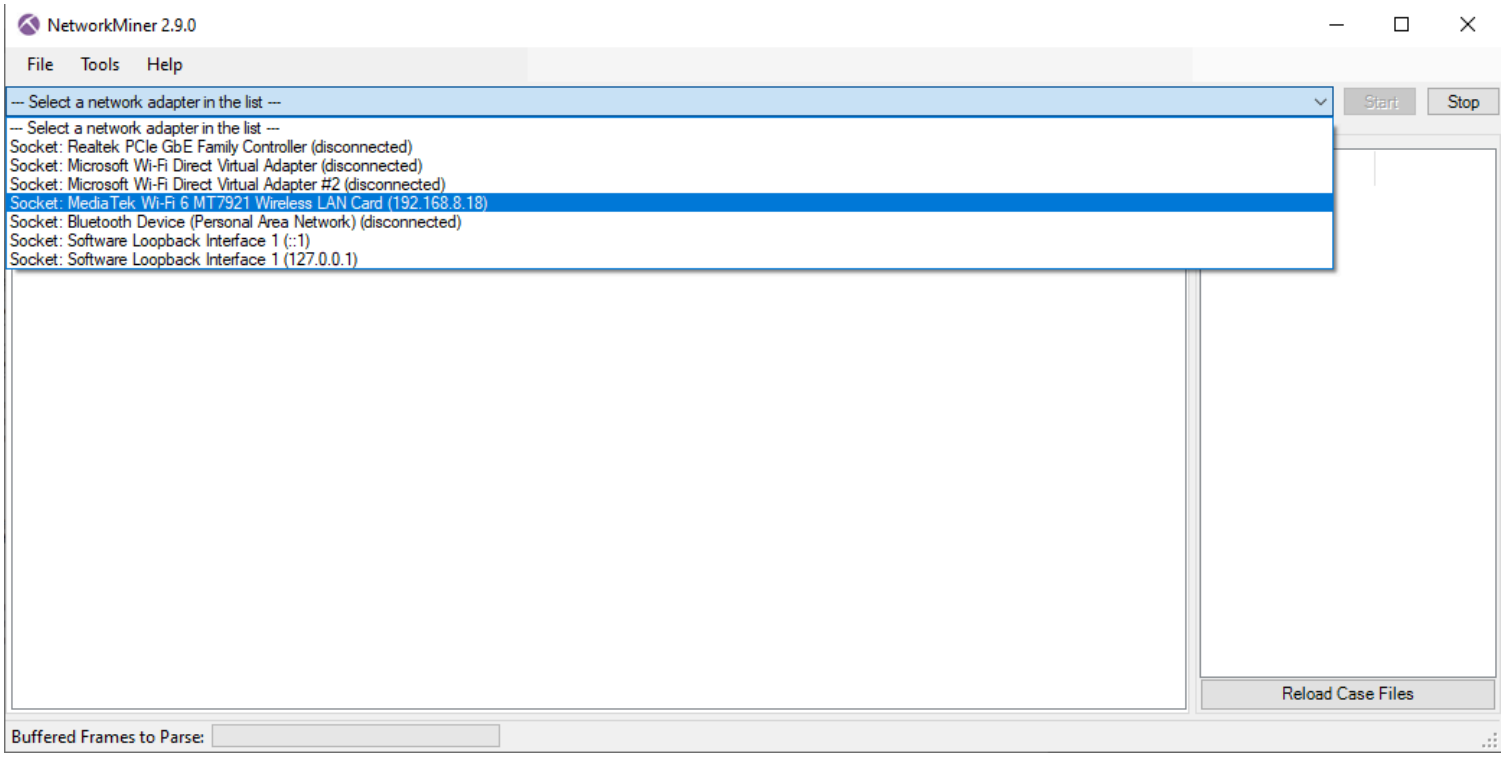
Вывод по работе с программой:

Работа с программой, такой как Wireshark, позволяет эффективно анализировать сетевой трафик, выявлять потенциальные угрозы и отслеживать подозрительную активность. Использование фильтров, например для выделения HTTP-запросов, значительно упрощает поиск нужной информации среди большого объема данных. Анализ пакетов предоставляет детальную информацию о сетевом взаимодействии, что помогает идентифицировать необычные IP-адреса, нестандартные типы запросов и возможные попытки атак. Программа является мощным инструментом для диагностики сети, но требует внимания к деталям и базовых знаний сетевых протоколов для правильного интерпретирования полученных данных.

- Работа в программе **Network Miner:**

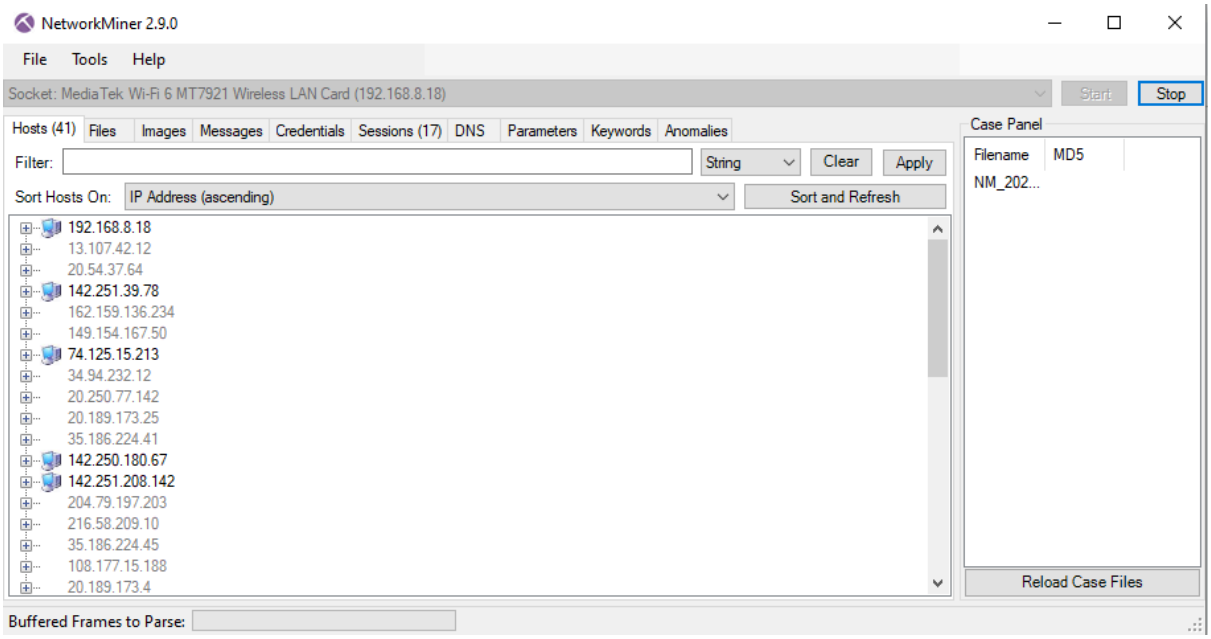
Это программное обеспечение также необходимо скачать с официального сайта разработчика, однако, его не нужно устанавливать. На компьютер скачивается уже готовый для работы .exe-файл.

После открытия программы, необходимо выбрать нужный интерфейс для его анализа. В моем случае, выбираю свою беспроводную сеть Wi-Fi.



После выбора нужного интерфейса, нажимаю кнопку **“Start”** для запуска анализа, после чего начинается сбор данных, отображая все хосты, соединения и трафик.

Во вкладке **“Hosts”** отображаются все устройства, подключенные к сети, с указанием их IP-адресов, MAC-адресов и общей информации о соединениях. Вкладка **“Files”** показывает файлы, передаваемые в сети, что позволяет анализировать переданные документы на наличие подозрительных данных. Во вкладке **“Credentials”** программа автоматически извлекает учетные данные, переданные через незащищенные протоколы, что помогает выявить возможные риски безопасности.



В итоге я проверил, не появились ли неизвестные устройства в списке хостов, и проанализировал подозрительные соединения, в которых передавался большой объем данных или использовались необычные порты. Также я обратил внимание на активность, связанную с нестандартными IP-адресами, и проверил, не происходило ли передач данных через незащищенные протоколы, что могло бы указывать на потенциальные угрозы безопасности.

- Вывод по программе:
Network Miner — это удобный инструмент для анализа захваченного сетевого трафика, который позволяет восстанавливать файлы и извлекать

полезные данные, такие как учетные записи и метаданные. Программа проста в использовании и особенно полезна для анализа содержимого сетевых пакетов. Однако ее функционал ограничен в бесплатной версии, что может сужать возможности более глубокого исследования.

- **Вывод:** В процессе выполнения лабораторной работы я изучил принципы работы систем обнаружения и предотвращения вторжений (IDS/IPS), их основные задачи и значимость в обеспечении информационной безопасности. Эти системы играют ключевую роль в выявлении угроз и защите сетевых ресурсов от несанкционированного доступа.

Я провел анализ сетевого трафика с использованием инструментов Wireshark и NetworkMiner. Wireshark предоставил возможность изучать трафик в реальном времени, фильтровать данные по протоколам и выявлять подозрительные действия на уровне пакетов. NetworkMiner оказался удобным для анализа уже захваченных данных, включая восстановление файлов, учетных записей и метаданных, что значительно упростило поиск потенциальных угроз.

Работа с этими инструментами позволила глубже понять, как осуществляется мониторинг сетевого трафика, как идентифицировать угрозы и учитывать важные данные при анализе. Особое внимание было уделено анализу нестандартных соединений, передаче больших объемов данных через необычные порты и проверке новых устройств в сети. Полученные знания о системах IDS/IPS и методах анализа сетевого трафика сформировали прочную базу для дальнейшего изучения информационной безопасности и использования подобных инструментов в реальной практике.

- Библиография:

1. https://habr.com/ru/articles/204274//
2. https://selectel.ru/blog/ips-and-ids/
3. https://www.wireshark.org/download.html
4. https://www.netresec.com/?page=NetworkMiner
5. https://spy-soft.net/networkminer/