**Слайд 1**

Добрый день, коллеги! Сегодня я хотел бы рассказать вам о Wireshark — одном из самых мощных и популярных инструментов для анализа сетевого трафика, который входит в состав Kali Linux.

**Слайд 2**

Wireshark — это бесплатная и открытая утилита для анализа сетевого трафика. Она позволяет нам перехватывать и подробно изучать пакеты данных, проходящие через нашу сеть. С поддержкой более 2000 протоколов Wireshark дает возможность детально анализировать практически любой тип сетевого трафика. Программа работает на различных операционных системах (Windows, Linux, MacOS) и имеет интуитивно понятный интерфейс, что делает ее доступной для широкого круга пользователей. Wireshark позволяет сохранять я и анализировать захваченные данные. За многие годы wireshark получил множество модификаций от сообщества в виде скриптов и плагинов

**Слайд 3**

Wireshark был создан в 1998 году Джеральдом Комбсом как альтернатива дорогим коммерческим анализаторам трафика. Вот что он говорил:

"В те годы на рынке абсолютно доминировал дорогой коммерческий сниффер от компании Network General, а альтернативной программы open source не существовало. Это и подтолкнуло меня к написанию утилиты для прослушивания трафика Ethernet и TCP/IP..."

Изначально программа называлась Ethereal, но в 2006 году была переименована в Wireshark из-за юридических вопросов с товарным знаком. Благодаря активному участию сообщества, Wireshark постоянно развивается и совершенствуется. Сегодня это один из стандартных инструментов в области сетевой безопасности и обучения.

**Слайд 4**

Wireshark предлагает обширный набор функций, делающих его незаменимым инструментом для анализа сети. Он позволяет перехватывать трафик в режиме реального времени или работать с сохраненными файлами. С помощью мощной системы фильтров мы можем быстро найти нужные пакеты среди тысяч других. Поддержка огромного количества протоколов и возможность расширения функциональности через плагины делают Wireshark гибким инструментом для различных задач.

**Слайд 5**

Одним из преимуществ использования Wireshark в Kali Linux является его готовность к работе сразу "из коробки". Kali Linux — это специализированный дистрибутив для тестирования на проникновение и цифровой криминалистики. Wireshark в этой среде интегрируется с другими инструментами, такими как Nmap и Metasploit, что позволяет создавать комплексные сценарии анализа и тестирования. Консольная версия TShark удобна для автоматизации задач и работы на удаленных серверах.

**Слайд 6**

На данном слайде представлен интерфейс Wireshark, где применяется фильтр ip.addr == 192.168.0.11. Этот фильтр позволяет из всего сетевого трафика выделить пакеты, связанные с указанным IP-адресом. Это полезно, когда нужно проанализировать действия определённого устройства или узла в сети.

**Слайд 7**

На этом слайде показан другой пример использования Wireshark, где используется фильтр http для анализа HTTP-трафика. Данный фильтр позволяет изучать обмен данными между клиентом и сервером, включая запросы GET и ответы сервера. Такой подход упрощает диагностику проблем на уровне веб-приложений.

**Слайд 8**

Здесь приведена таблица с примерами популярных фильтров в Wireshark. Например, фильтр http.cookie помогает находить пакеты, содержащие cookies, а http.content\_type contains "image" позволяет искать передачи изображений. Это существенно ускоряет работу с большим объёмом данных и помогает сфокусироваться на конкретных задачах.

**Слайд 9**

Wireshark находит применение в самых разных областях. Сетевые администраторы используют его для диагностики и решения проблем с сетью. Специалисты по безопасности — для обнаружения и анализа подозрительного трафика. Разработчики могут изучать взаимодействие своих приложений с сетью и оптимизировать производительность. В образовательных целях Wireshark помогает студентам и исследователям глубже понять принципы работы сетевых протоколов.

**Слайд 10**

Подводя итог, Wireshark является незаменимым инструментом для каждого, кто работает с сетями. Его возможности и интеграция с Kali Linux делают его идеальным выбором для анализа и обеспечения безопасности сетевого трафика. Благодаря активному сообществу и постоянному развитию, Wireshark остается актуальным и эффективным инструментом.

Спасибо за внимание!