ПОВЫШЕНИЕ КАЧЕСТВА ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПУТЕМ ВНЕДРЕНИЯ ПРОГРАММЫ WIRESHARK В ПРОЦЕСС ОБУЧЕНИЯ СПЕЦИАЛИСТОВ СВЯЗИ

Михно К.В.

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

Федоренко В.А.

Аннотация. Данный тезис объясняет необходимость внедрения программы Wireshark в учебный процесс специалистов связи.

Сегодня стало очевидным, что использование инновационных технологий эффективно влияет на подготовку специалистов в области коммуникаций. Тема проблем повышения эффективности образовательного процесса на базе информационных технологий очень актуальна. С потрясающей быстротой происходит компьютеризация мирового сообщества, создаются сложнейшие образцы вооружения и техники, требующей подготовки военных кадров на совершенно ином уровне. В мире современных технологий невозможно представить любой процесс без применения электронных программ и других современных информационных технологий. Так, внедрение программ для возможности считывания и перехвата информационного трафика в учебный процесс обеспечивает актуальность получаемых знаний, и увеличивает спектр возможных для выполнения работ специалистов связи.

Wireshark – это широко распространённый инструмент для захвата и анализа сетевого трафика, который активно используется как для образовательных целей, так и для устранения неполадок на компьютере или в сети. Wireshark работает практически со всеми протоколами модели OSI, обладает понятным для обычного пользователя интерфейсом и удобной системой фильтрации данных [1]. Помимо всего этого, программа является кроссплатформенной и поддерживает следующие операционные системы:

- Windows;
- Linux;
- Mac OS X;
- Solaris;
- FreeBSD;
- NetBSD;
- OpenBSD.

Wireshark имеет комфортный и понятный графический пользовательский интерфейс, который показывает детальную информацию о каждом поле протокола любого уровня. Также она поддерживает различные статистические и графические функции для анализа сетевой активности.

В данной программе есть три основных режима захвата:

- Режим общения;
- Мониторинга;
- Нормальный режим.

Каждый из них выполняет определенные функции и позволяет выполнять конкретные задачи. Анализ трафика может решать большое количество проблем для сети. Чтобы понять на что в первую очередь обратить внимание, нужно четко понимать цель анализа.

Передача данных в глобальной сети Интернет является небезопасной, особенно если никак не защищать их. В современных браузерах используется протокол SSL/TLS, который шифрует информацию и позволяет безопасно передать её.

Иногда пользователю или системного администратору необходимо проверить трафик на наличие подозрительной активности или на корректную работу программы.

Перехват трафика Wireshark относится к инструментам диагностики сети, который можно использовать и для пассивного анализа сетевой инфраструктуры. Например, выяснить детали сетевой топологии или имена и адреса серверов, обычно недоступных пользователям.

Исходя из полученных из этого внедрение программы в процесс обучения позволить обучить специалистов связи методам решения разных задач:

- Диагностики сетевых проблем, которые могут возникать в ходе эксплуатации средств инфокоммуникации или применения на их средств подавления;
- Совершенствование сетевой безопасности;
- Проверка сетевых приложений на наличие считывания трафика и передачи его;
- Отладки реализаций сетевых протоколов;

Программа также может быть полезна и в многих других случая, но все это обеспечивается благодаря внушительному функционалу:

- Захват сетевых пакетов в реальном времени;

- Сохранение захваченных пакетов;
- Открытие файлов, содержащих данные пакетов, которые были захвачены;
- Импорт пакетов из текстовых файлов, содержащих шестнадцатеричные дампы сетевых пакетов;
- Отображение содержимого пакетов с подробной информацией об их структуре;
- Экспорт некоторых или всех пакетов в различные форматы файлов для захвата;
- Фильтрация пакетов на основе заданных условий;
- Поиск пакетов на основе заданных условий;
- Создание различных статистик.

Однако функционал подобных Wireshark инструментальных средств выходит далеко за пределы простого захвата и анализа трафика. Они позволяют восстанавливать пароли для ОС Windows, производить атаки для получения потерянных учетных данных, углубленно изучать пакеты и данные в сети, анализировать маршрутизацию пакетов и многое другое[2].

В Wireshark имеются диссекторы протоколов (или декодеры, как их называют в других продуктах) для большого числа протоколов.

Диссектор протокола – это компонент программного обеспечения, который анализирует и интерпретирует байты, передаваемые по сети, в соответствии с определенным сетевым протоколом. В анализаторах сетевого трафика, таких как Wireshark, диссекторы протоколов используются для разбора сетевых пакетов и представления их содержимого в удобочитаемом виде.

Каждый диссектор протокола специализируется на конкретном протоколе или группе протоколов и может выделять из сетевых пакетов различные поля, атрибуты и значения, которые затем могут быть показаны пользователю или использованы для дальнейшего анализа[3].

Кроме того, программа имеет открытый исходный код и распространяется под лицензией GNU General Public License (GPL). Именно поэтому ее можно не только свободно использовать на любом количестве компьютеров, не заботясь о лицензионных ключах, платежах или чем-либо подобном, но и легко добавлять в Wireshark новые протоколы. Это можно сделать либо через плагины, либо интегрировав их прямо в исходный код.

Wireshark не является системой обнаружения вторжений (IDS, Intrusion Detection System). Утилита не предупредит вас, если кто-то будет делать в вашей сети что-то необычное или несанкционированное. Однако, если происходит что-то странное, Wireshark может помочь вам разобраться, в чем дело.

Общеизвестно и признано, что для повышения качества управления необходимо систематически повышать квалификацию персонала, поэтому актуальной становится задача разработки, использования и внедрения инновационных программ компьютерной подготовки, электронных учебников и специализированных компьютерных тренажеров в подготовке специалистов. Разработки в этой области позволяют проводит обучение персонала, снизить затраты на приобретение дорогостоящего оборудования, а оператору изучить особенности управления автоматизированными комплексами связи, каналообразующими средствами, приобрести опыт работы в чрезвычайных ситуациях и др. Практическое обучение помогает отработать полученные навыки в безопасной виртуальной среде. Компьютерные обучающие системы позволяют выбрать не только индивидуальный подход к обучению, но и удобный и гибкий режим обучения. Таким образом, компьютерное обучение требует переосмысления всей концепции обучения. Однако это не означает, что классические методы преподавания должны быть разбиты на части. Весь классический метод является блестящим примером. На сегодняшний день уже стал очевидным тот факт, что использование инновационных технологий эффективно влияет на обучение специалистов связи. Предпочтение отдается обучающим программам, электронным моделям и тренажерам, которые совмещают в себе эффективность, качество обучения, экономичность в создании, эргономичность в использовании и позволяют осуществить переход к индивидуальному обучению, обеспечить эффективную самостоятельную работу каждого обучающегося, а также изменить характер деятельности преподавателя. Главным является выполнение условия по внедрению в процесс обучения программ перехвата и анализа сетевого трафика и захвата пакетов коммутации, позволяющих имитировать прохождение сигнала через местность с учетом ее топографических свойств на станциях радиорелейной связи и определять значения КИД для радиолиний, связывающих требуемые пункты связи в различных условиях, определяемых уровнями помех, видами модуляции. Таким образом внедрение данной программы в учебный процесс, значительно повысит уровень подготовки специалистов связи [4].

Список использованных источников:

1. Программы по изучению и технические средства обучения / Докучаев А.С.// – Минск, 2010. – 378 с..

2. Руководство по программе Wireshark – Электронные данные. – Режим доступа:[https://wireshark.wiki/?utm_source=yandex&utm_medium=cpc&utm_campaign=wireshark&yclid=14233624587790450687]

3. Повышение качества обучения студентов с использованием современных компьютерных технологий – [https://science-education.ru/ru/article/view?Id=23538]

4. Информационные технологии в образовательном процессе – [https://elib.bspu.by/bitstream/doc/27261/1/%D0%91%D1%8.pdf].