Киреев Александр Павлович
Kireev Alexander Pavlovich
Студент Омского государственного технического университета, радиотехнический факультет.
Колмыков Дмитрий Витальевич
Kolmikov Dmitry Vitalevich
Студент Омского государственного технического университета, радиотехнический факультет.
Михайлов Сергей Юрьевич
Mihailov Sergey Yurevich
Студент Омского государственного технического университета, радиотехнический факультет.
Пепеляев Алексей Вениаминович
Pepelyev Alexey Veniaminovich
Доцент Омского государственного технического университета.

УДК 004.7

АНАЛИЗ СЕТЕВОГО ТРАФИКА КОРПОРАТИВНОЙ СЕТИ ПОСРЕДСТВОМ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ WIRESHARK

ANALYSIS OF THE NETWORK TRAFFIC OF CORPORATE NETWORK THROUGH WIRESHARK SOFTWARE

Аннотация: в работе рассмотрены анализаторы сетевых протоколов, способы перехвата сетевого трафика; продемонстрировано практическое применение программного инструмента Wireshark, выявлены его преимущества и недостатки.

Annotation: the work examines network protocol analyzers, methods of intercepting network traffic; demonstrated the practical application of the software tool Wireshark, revealed its advantages and disadvantages.

Ключевые слова: сетевой протокол, снифер, анализатор, Wireshark, сетевой трафик, перехват трафика.

Keywords: network protocol, sniffer, analyzer, Wireshark, network traffic, traffic interception.

Анализатор сетевых протоколов – программное обеспечение, предназначенное для перехвата данных, а также их непосредственного анализа по тому или иному фильтру. В большинстве анализаторов также присутствует функция фильтрации пакетов.

Способы перехвата трафика:

- обычное «прослушивание» сетевого интерфейса;
- подключение снифера в разрыв канала;
- ответвление (программное или аппаратное) трафика и направление его копии на снифер;
- анализ побочных электромагнитных излучений и восстановление таким образом прослушиваемого трафика;
- атака на канальном (MAC-spoofing) или сетевом уровне (IP-spoofing), приводящая к перенаправлению трафика жертвы или всего трафика сегмента на снифер с последующим возвращением трафика в надлежащий адрес.

Анализ прошедшего через снифер трафика: по мере движения потоков данных по сети анализатор перехватывает каждый протокольный блок данных (PDU), после чего расшифровывает или анализирует его содержание. Снифер может анализировать только то, что проходит через его сетевую карту.

Примеры сниферов:

CommView – присутствует возможность установки своих правил на сбор трафика. Также можно, например, перехватывать входящие пакеты, а остальные игнорировать.

SpyNet – служит для перехвата и декодирования сетевых пакетов.

Analyzer – требует установку специального драйвера. Присутствует возможность просмотра информации о сетевой карте. Служит прекрасным инструментом для работы с локальной сетью.

Wireshark — инструмент для захвата и анализа сетевого трафика. Работает с подавляющим большинством известных протоколов, имеет понятный, логичный графический интерфейс и мощнейшую систему фильтров.

Возможности Wireshark:

- Работает на большинстве современных ОС.
- Перехват трафика сетевого интерфейса в режиме реального времени .
- Множество протокольных декодировщиков.
- Сохранение и открытие ранее сохраненного сетевого трафика.
- Импорт и экспорт файлов из других пакетных анализаторов.
- Фильтрация пакетов по множеству критерий.
- Поиск пакетов по множеству критерий.
- Подсветка пакетов разных протоколов.
- Создание статистики.

Перехват пакетов: для старта программы и перехвата данных нажмите кнопку «Interface List» (Список интерфейсов), которая помогает вывести весь список сетевых адаптеров для перехвата трафика.

В открывшемся окне «Capture Interface» (Перехват интерфейсов) программы Wireshark установите флажок рядом с интерфейсом, подключенным к локальной сети, и нажмите кнопку «Start», чтобы начать перехват данных. ***Фильтры пакетов:*** фильтрация пакетов применяется для выборки необходимых пакетов данных из общего потока трафика. Например, существует фильтрация по протоколам и IP-адресам.

Перехват ICMP-пакетов (ping)

На рисунке 1 отображено использование утилиты ping. В качестве аргумента функции выступает веб-ресурс Yandex.

```
MacBook-Pro-Aleksandr:~ Alx.Krw$ ping ya.ru
PING ya.ru (87.250.250.242): 56 data bytes
64 bytes from 87.250.250.242: icmp_seq=0 ttl=57 time=43.643 ms
64 bytes from 87.250.250.242: icmp_seq=1 ttl=57 time=43.860 ms
64 bytes from 87.250.250.242: icmp_seq=2 ttl=57 time=44.043 ms
64 bytes from 87.250.250.242: icmp_seq=3 ttl=57 time=43.869 ms
64 bytes from 87.250.250.242: icmp_seq=4 ttl=57 time=43.899 ms
64 bytes from 87.250.250.242: icmp_seq=5 ttl=57 time=43.766 ms
64 bytes from 87.250.250.242: icmp_seq=6 ttl=57 time=43.010 ms
```

Рис. 1. Иллюстрация работы утилиты ping

Параллельно запускаем Wireshark, выбираем соответствующий сетевой интерфейс и запускаем процедуру сбора сетевых пакетов. Для отображения пакетов, относящихся к утилите ping, необходимо отфильтровать собранный трафик по протоколу ICMP. Результат приведен на рисунке 2.

▸	5 0.433583	172.31.3.21	87.250.250.242	ICMP	98 Echo (ping) request	id=0x7415, se
	6 0.477242	87.250.250.242	172.31.3.21	ICMP	98 Echo (ping) reply	id=0x7415, se
	13 1.433736	172.31.3.21	87.250.250.242	ICMP	98 Echo (ping) request	id=0x7415, se
	16 1.476584	87.250.250.242	172.31.3.21	ICMP	98 Echo (ping) reply	id=0x7415, se

Рис. 2. Фильтрация пакетов по ICMP протоколу

Удаленное SSH-подключение к серверу

На рисунке 3 отображены сведения удаленного подключения к серверу посредством протокола SSH.

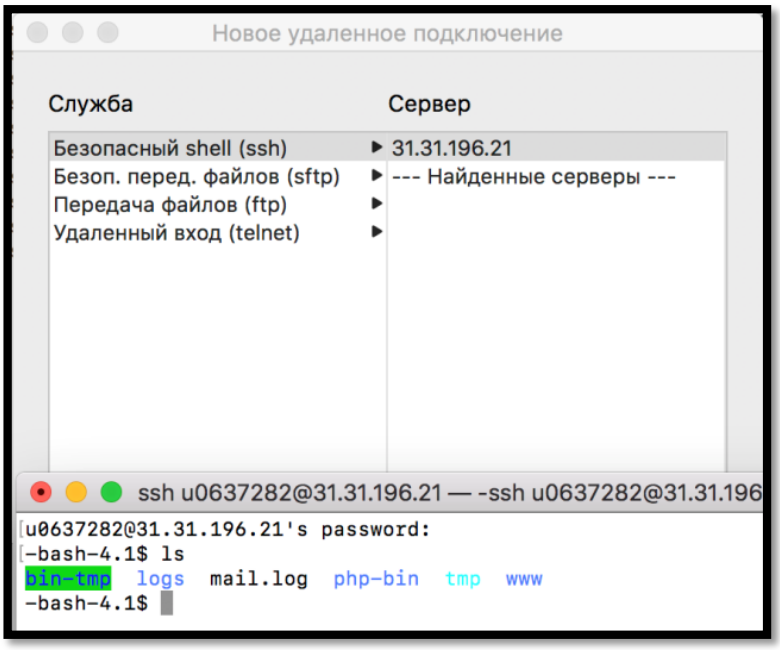

Рис. 3. SSH-подключение

На рисунке 4 выполнена фильтрация трафика по протоколу SSH.

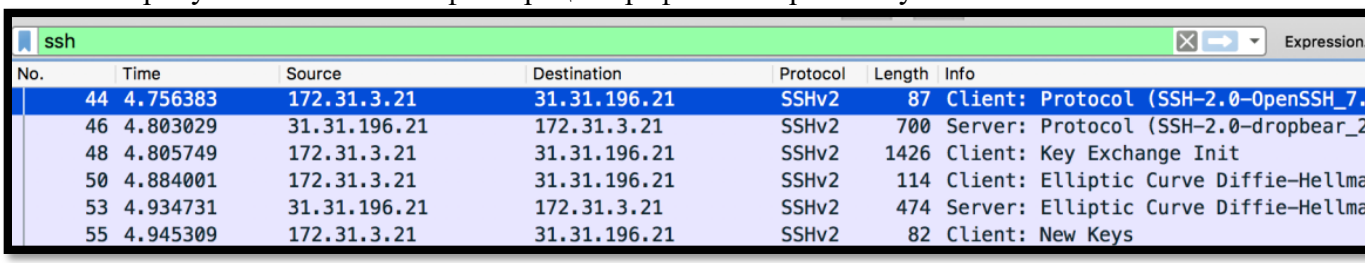

Рис. 4. Фильтрация пакетов по протоколу SSH

В данном случае пароль восстановить из пакетов, к сожалению, не удастся, так как при SSH-подключении используется шифрование.

FTP-подключение

На рисунке 5 приведена информация о FTP-подключении к удаленному серверу. В данном случае для инициализации подключения используется интегрированное программное обеспечение FileZilla.

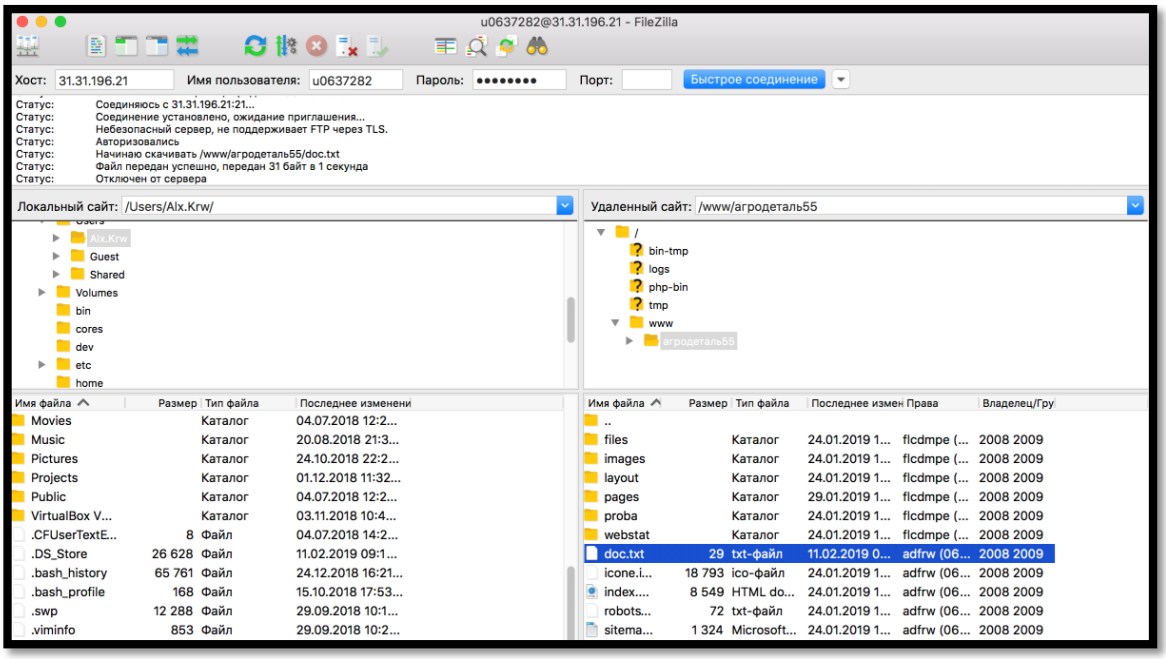

Рис. 5. FTP-подключение

На рисунке 6 приведена фильтрация перехваченных сетевых пакетов по протоколу FTP.

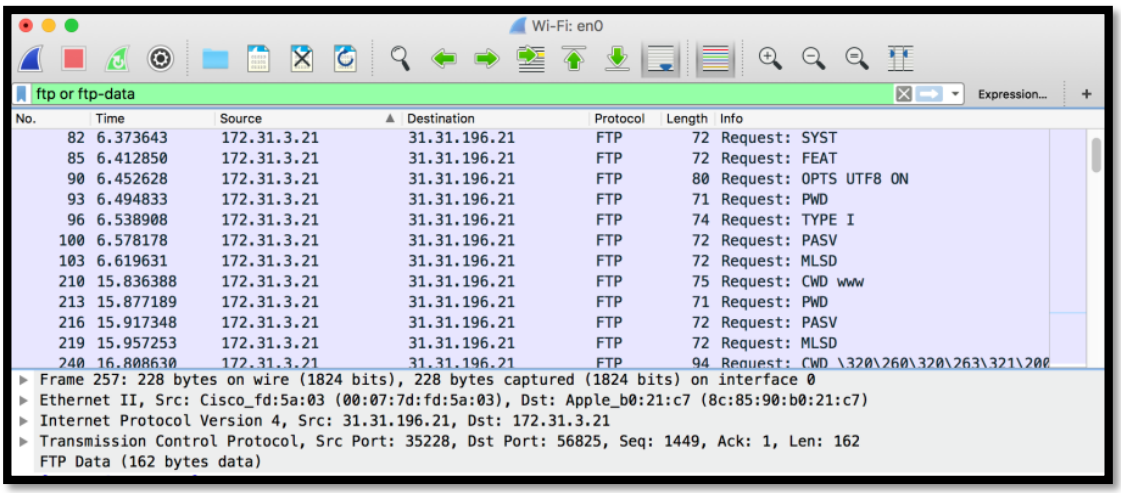

Рис. 6. Фильтрация пакетов по протоколу FTP

На рисунке 7 один из FTP-пакетов разобран более подробно. Видно, что выполнялась передача текстового файла, содержимое которого «Hello world!».

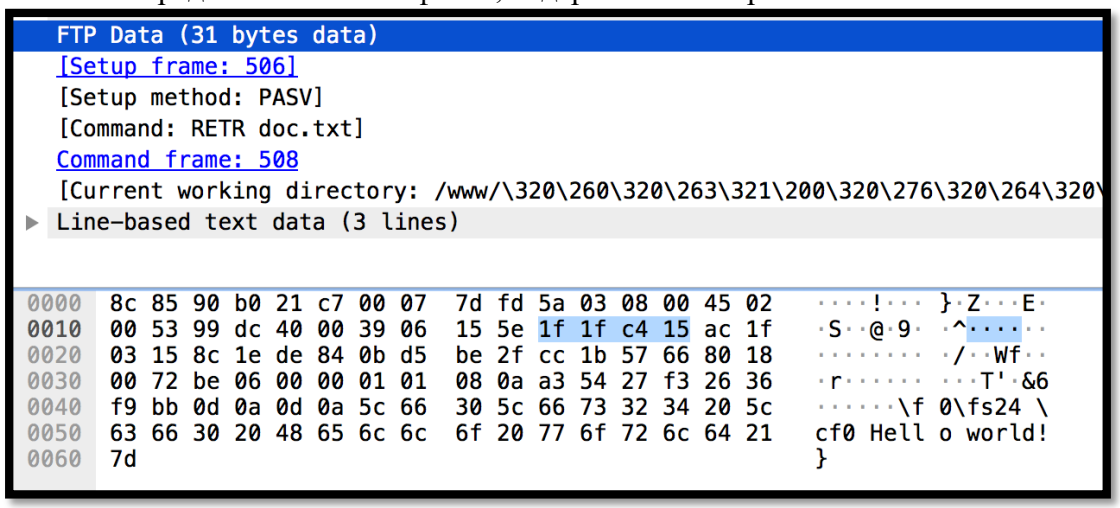

Рис. 7. Содержимое скачиваемого файла

На рисунке 8 отображено визуальное отображение статистических данных: количество перехватываемых пакетов в секунду на протяжении некоторого промежутка времени.

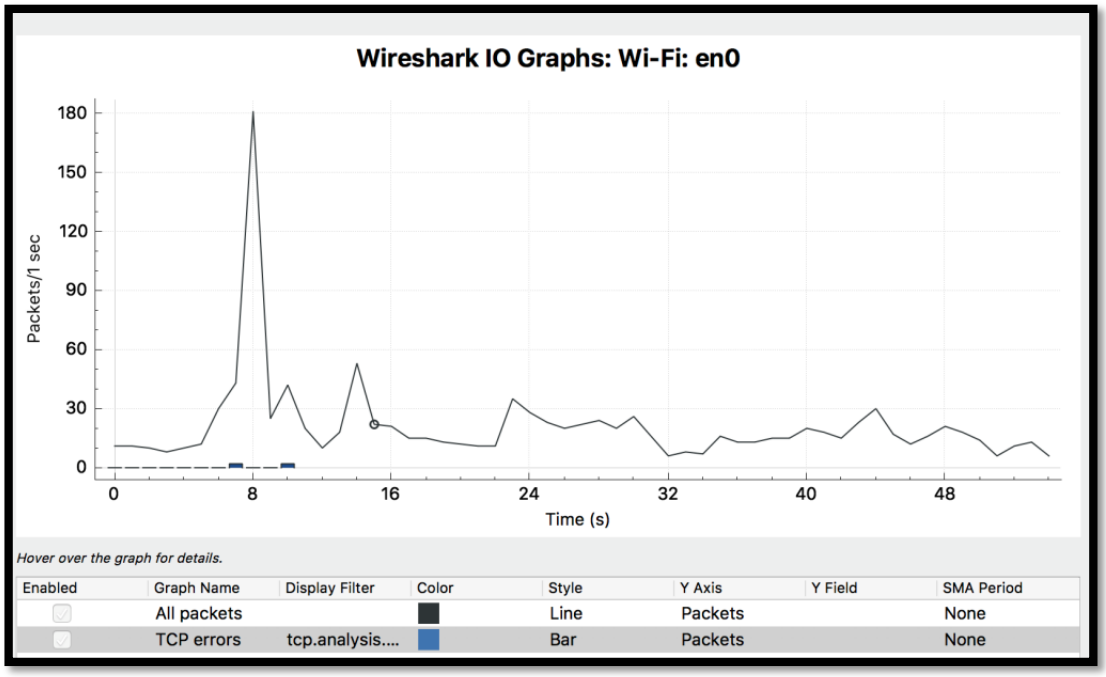

Рис. 8. Статистика Wireshark

Таким образом, в ходе данной работы были рассмотрены:

1. Определение анализатора сетевых протоколов.
2. Способы перехвата сетевого трафика.
3. Примеры существующих на рынке сниферов.
4. Возможности Wireshakr.
5. Перехват ICMP-пакетов.
6. Выполнение SSH-подключения к удаленному серверу.
7. Выполнение FTP-подключения к удаленному серверу.
8. Анализ сетевых пакетов анализируемых протоколов: ICMP, SSH, FTP.
9. Визуальное отображение статистических данных программы Wireshark.

Библиографический список:

1. Маркин Ю. В., Санаров А. С. Обзор современных инструментов анализа сетевого трафика. http://www.ispras.ru/preprints/docs/prep_27_2014.pdf, дата обращения 10.03.2019.

2. Wireshark Trace Files. Режим доступа: http://www.wiresharkbook.com/studyguide_supplements/9781893939943_traces.zip, дата обращения 11.03.2019.

3. Wireshark. Режим доступа: http://www.wireshark.org/ , дата обращения 11.03.2019.