Санкт-Петербургский государственный политехнический университет

Институт компьютерных наук и кибербезопасности

Высшая школа компьютерных технологий и информационных систем

**Отчет по лабораторной работе №6**

**по курсу «Технологии компьютерный сетей»**

«Wireshark: 802.11»

**Работу выполнил студент группы №5130901/10203:**

Алексеев Лев Сергеевич

Подпись:

**Работу принял преподаватель:**

Богач Наталья Владимировна

Подпись:

Санкт-Петербург

2024

**Wireshark: 802.11**

В данной лабораторной работе мы исследуем протокол беспроводных сетей 802.11. До настоящего момента во всех лабораторных работах Wireshark мы захватывали только кадры, передаваемые по проводному Ethernet-подключению. В этой же работе, так как 802.11 ― это протокол уровня беспроводного канала связи, мы будем захватывать кадры «из воздуха». К сожалению, драйверы многих устройств 802.11 NIC не имеют инструментов для захвата/копирования полученных кадров 802.11 для дальнейшего использования с программным обеспечением Wireshark. Поэтому в данной работе мы возьмем для анализа трассировочную таблицу заранее захваченного кадра и предположим, что при ответе на вопросы к данной работе, вы будете пользоваться именно этой таблицей.

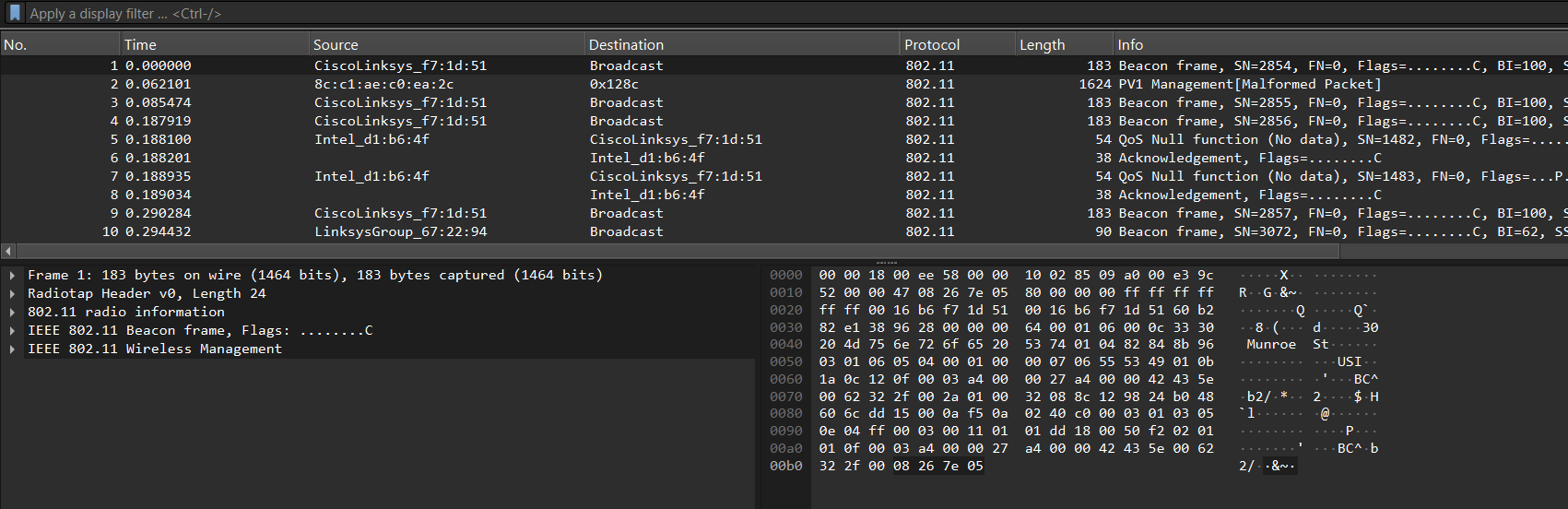
****

Рис. 1. Окно программы Wireshark после открытия файла Wireshark\_802\_11.pcap.

1. Назовите идентификаторы SSID двух точек доступа, согласно таблице трассировки транслирующих наибольшее количество сигнальных кадров.

Идентификаторы SSID двух точек доступа, транслирующих наибольшее количество сигнальных кадров «30 Munroe St» и «linksys\_ses\_24086».

1. Какова величина временных интервалов между трансляциями сигнальных кадров точки доступа linksys\_ses\_24086? 30 Munroe St? (Подсказка: значение длительности временного интервала содержится в самом сигнальном кадре).

Согласно кадру управления беспроводной локальной сетью 802.11 сигнальный промежуток обеих точек доступа составляет 0,1024 с.

1. Каков (в шестнадцатеричной нотации) исходящий МАС-адрес (адрес отправителя данных) сигнального кадра ТД 30 Munroe St? Вспомните по рис. 6.13, что в кадре 802.11 используются три типа адреса: исходящий, адрес назначения и BSS. С детальным обсуждением структуры кадра 802.11 можно ознакомиться в разделе 7 стандартизирующего документа IEEE 802.11 (см. выше).

Исходящий МАС-адрес сигнального кадра «30 Munroe St» 00:16:b6:f7:1d:51.

1. Каков (в шестнадцатеричной нотации) МАС-адрес назначения (адрес получателя данных) сигнального кадра ТД 30 Munroe St?

МАС-адрес назначения адрес получателя данных сигнального кадра ТД «30 Munroe St» ff:ff:ff:ff:ff:ff, т.е. это не что иное, как широковещательный адрес Ethernet.

1. Каков (в шестнадцатеричной нотации) МАС-адрес BSS сигнального кадра ТД 30 Munroe St?

МАС-адрес BSS ID сигнального кадра ТД «30 Munroe St» 00:16:b6:f7:1d:51.

1. Сигнальные кадры точки доступа 30 Munroe St сообщают, что данная точка доступа может поддерживать четыре скорости передачи данных и восемь дополнительных «расширенных поддерживаемых скоростей». Что это за скорости?

Поддерживаемые скорости: 1,0, 2,0, 5,5 и 11,0 Мбит/с. Расширенные скорости 6,0, 9,0, 12,0, 18,0, 24,0 36,0 48,0 и 54,0 Мбит/с.

1. Найдите кадр 802.11, содержащий сегмент SYN TCP для первой сессии ТСР (которая загружает файл alice.txt). Какие значения содержат три поля МАС-адреса в кадре 802.11? Который из МАС-адресов данного кадра соответствует беспроводному хосту (дайте МАС-адрес хоста в шестнадцатеричном представлении)? Точке доступа? Маршрутизатору первого транзитного участка? Каков IP-адрес беспроводного хоста, выполняющего отправку сегмента ТСР? Каков IP-адрес назначения? Соответствует ли IP-адрес назначения хосту, точке доступа, маршрутизатору первого транзитного участка или какому-либо другому устройству, подключенному к сети? Объясните.

Время отправки TCP SYN соответствует временной отметке трассировочной таблицы t=24,811093 с. МАС-адрес хоста, отправляющего TCP SYN 00:13:02:d1:b6:4f. МАС-адрес получателя, коим является маршрутизатор первого транзитного участка и к которому подключен хост 00:16: b6:f7:1d:51. IP- адрес хоста, отправляющего ТСР SYN 128.199.245.12, что соответствует адресу сервера gaia.cs.umass.edu.

1. Найдите кадр 802.11, содержащий сегмент SYNACK для данной сессии ТСР. Какие значения содержат три поля МАС-адреса в кадре 802.11? Который из МАС-адресов данного кадра соответствует беспроводному хосту? Точке доступа? Маршрутизатору первого транзитного участка? Соответствует ли указанный в кадре МАС-адрес отправителя IP-адресу устройства, отправившего сегмент ТСР, инкапсулированный в данной дейтаграмме? (Подсказка: повторно изучите рис. 5.19 в книге, если вы не уверены, как следует отвечать на данный вопрос, либо на соответствующую часть предыдущего вопроса. Понимание этого момента крайне важно.

Время получения ТСР SYNACK соответствует временной отметке трассировочной таблицы t=24,827751 с. МАС-адрес отправителя кадра 802.11, содержащего сегмент ТСР SYNACK 00:16:b6:f4:eb:a8, что соответствует адресу маршрутизатора первого транзитного участка, к которому подключен хост. МАС-адрес получателя, коим является сам хост, 91:2a:b0:49:b6:4f. МАС-адрес BSS 00:16:b6:f7:1d:51. IP-адрес сервера, отправляющего TCP SYNACK 128.199.245.12.

1. Согласно таблице трассировки, какие два действия выполняет (в том смысле, какие кадры отправляет) хост сразу после отметки времени t=49 для завершения установленной на момент начала трассировки ассоциации с точкой доступа 30 Munroe St? (Подсказка: одно из действий находится на уровне IP, второе ― на уровне 802.11). Прочитав спецификацию стандарта 802.11, ожидали ли вы увидеть на данном этапе какой-либо кадр, который отсутствует в данной таблице трассировки?

В момент времени t=49,583615 на DHCP-сервер (чей IP-адрес 192.168.1.1) покидаемой хостом сети осуществляется отправка запроса на высвобождение DHCP. В момент времени t=49,609617 хост отправляет кадр DEAUTHENTICATION (Тип кадра = 00 [Управление], тип подкадра = 12 [Отмена аутентификации]).

1. Изучите файл трассировки и найдите кадры AUTENTICATION, отправляемые хостом точке доступа и наоборот. Сколько кадров AUTENTICATION было отправлено беспроводным хостом точке доступа linksys\_ses\_24086, имеющей МАС-адрес Cisco\_Li\_f5:ba:bb, начиная примерно с временной отметки t=49?

Первая отправка кадра AUTENTICATION от хоста точке доступа была осуществлена в момент времени t=49,638857.

1. Намеревается ли хост произвести аутентификацию по введенному ключу или желает, чтобы аутентификация была открытой?

Хост запрашивает открытую аутентификацию (указав Алгоритм Аутентификации: Открытая Система).

1. Присутствует ли вы в трассировочной таблице ответ AUTENTICATION от ТД linksys\_ses\_24086?

Я не могу найти никакого ответа, посланного точкой доступа. Возможная причина этому заключается в том, что данная ТД настроена требовать ключ безопасности от хостов, пытающихся произвести подключение, поэтому, скорее всего, ТД просто игнорирует (то есть не отвечает на) требования открытого доступа.

1. Теперь давайте подумаем, что происходит как только хост прекращает попытки ассоциации с точкой доступа linksys\_ses\_24086 и теперь пытается подключиться к ТД 30 Munroe St. Найдите кадры AUTENTICATION отправленные хостом точке доступа и наоборот. В какой момент времени регистрируется кадр AUTENTICATION, отправленный хостом на ТД 30 Munroe St, и в какой момент времени зарегистрирован ответ AUTENTICATION от этой ТД хосту? (Примечание, для отображения на экране только кадров AUTENTICATION, присутствующих в трассировочной таблице и относящихся к интересующему нас беспроводному хосту, вы можете воспользоваться следующим выражением фильтрации: wlan.fc.subtype == 1 and wlan.fc.type==0 and wlan.addr == IntelCor\_d1:b6:4f).

В момент времени t=63,168087 зарегистрирован кадр AUTENTICATION, отправленный c адреса 00:13:02:d1:b6:4f (беспроводной хост) на адрес 00:16:b7:f7:1d:51 (BSS). В момент времени t=63.169071 зарегистрирована отправка кадра AUTHENTICATION в обратном направлении: от BSS беспроводному хосту.

1. Для ассоциации хоста с точкой доступа используется кадр запроса ассоциации (ASSOCIATE REQUEST), отправляемый хостом точке доступа и соответствующий ему кадр ответа на запрос об ассоциации (ASSOCIATE RESPONSE), направляемый точкой доступа хосту. В какой момент времени регистрируется кадр ASSOCIATE REQUEST, отправленный хостом на ТД 30 Munroe St? Когда был отправлен соответствующий кадр ASSOCIATE REPLY? (Примечание, для отображения на экране только кадров ASSOCIATE REQUEST и ASSOCIATE RESPONSE, присутствующих в трассировочной таблице, вы можете воспользоваться следующим выражением фильтрации: wlan.fc.subtype < 2 and wlan.fc.type==0 and wlan.addr == IntelCor\_d1:b6:4f).

В момент времени t=63,169910 зарегистрирована отправка кадра ASSOCIATE REQUEST с адреса 00:13:02:d1:b6:4f (беспроводной хост) на адрес 00:16:b7:f7:1d:51 (BSS). В момент времени t=63.192101 зарегистрирована отправка кадра AUTHENTICATION в обратном направлении: от BSS беспроводному хосту.

1. Какие скорости передачи данных намеревается использовать хост? Точка доступа? Для ответа на эти вопросы вам потребуется рассмотреть поля параметров кадров управления беспроводной локальной сетью 802.11.

Согласно информации, распространяемой в кадре ASSOCIATE REQUEST поддерживаемые скорости передачи данных 1, 2, 5,5, 11, 6, 9, 12, 18, 24, 32, 48 и 54 Мбит/с. Информация о тех же скоростях передается в кадре ASSOCIATE RESPONSE.

1. Каковы адреса BSS ID MAC отправителя и получателя, указанные в этих кадрах? Какова цель отправки кадров двух вышеупомянутых типов? (Для ответа на последний вопрос вам потребуется углубиться в чтении рекомендуемых ранее в тексте лабораторной работы онлайн источников).

В момент времени t=2.297613 зарегистрирована отправка пробного запроса PROBE REQUEST с исходящим адресом 00:12:1f:57:13, адресом назначения ff:ff:ff:ff:ff:ff и идентификатором BSSID ff:ff:ff:ff:ff:ff. В момент времени t=2.300697 зарегистрирована отправка пробного запроса PROBE RESPONSE с исходящим адресом 00:16:b6:f7:1d:51, адресом назначения и идентификатором BSSID 00:16:b6:f7:1d:51. Кадр пробного запроса PROBE REQUEST используется хостом при применении методики активного сканирования с целью обнаружения точек доступа. Кадр пробного ответа PROBE RESPONSE отправляется точкой доступа хосту, пославшему пробный запрос