Атака беспроводных пакетных радиосетей

Введение

Когда вы работаете в Интернете через беспроводную сеть, то всегда есть риск потерять свои учетные данные, заполняя их при регистрации или авторизации на закрытом сайте. Эти данные можно легко перехватить, так как чаще всего они передаются в сети в незашифрованном виде. Если для соединения используется протокол HTTP, данные передаются в явном виде и все что остается сделать для получения вашего пароля – это просто найти его в перехваченных пакетах. В статье мы рассмотрим программы-анализаторы, которые могут быть использованы для получения учетных данных при работе с беспроводными сетями. Но для начала будет приведена небольшая классификация беспроводных сетей и видов атак на эти сети.

Виды беспроводных сетей

Доступ к беспроводной широкополосной радиосети может быть обеспечен через: WLAN (Wireless Local Area Network), WMAN (Wireless Metropolitan Area Network) и WWAN (Wireless Wide Area Network).

Сеть, построенная по схеме WLAN, состоит из беспроводного клиента (абонента) и точки доступа. Точка доступа может быть подключена непосредственно к Интернету, либо другой сетевой инфраструктуре. В качестве среды передачи используется ISM радиодиапазон 2.4 и 5 ГГц. Принципы шифрования сетей WLAN описывается в наборе стандартов Wi-Fi 802.11. Ряд различных протоколов, определенных в этом семействе стандартов имеет различные рабочие частоты и различную максимальную пропускную способность. Краткий обзор стандартов приведен в таблице ниже:

Стандарт	Год выпуска	Скорость Мбит/сек	Частота, ГГц
802.11a	1999	54	5
802.11b	1999	11	2.4
802.11g	2003	54	2.4
802.11n	2009	600	2.4, 5
802.11ac	2011	6700	5

Несмотря на то, что стандарт 11a занимает первое место в приведенной таблице, первым на свет появился 802.11b и стал широко распространенным стандартом беспроводных сетей, а уже затем появились 11a, 11g и т.д. Дело в том, что работа над 11a началась раньше, и параллельно велась работа с 11b, который имел счастье быть законченным быстрее.

Сети WMAN – это одна из форм беспроводной сети, которая имеет зону охвата "размера города". Типичным представителем таких сетей является WiMAX (IEEE 802.16), который представляет собой беспроводной цифровой стандарт связи, имеющий высокую надежность, скорость передачи данных и эффективность. Сети, построенные на базе WiMAX, могут обеспечить радиус покрытия территории до 50 км.

Здесь стоит отметить, что понятие радиуса покрытия той или иной беспроводной технологии вещь очень относительная и спорная. Здесь скорее речь идет о том, каких масштабов целесообразно строить сеть определенной технологии. Если ~~упороться~~ очень постараться, то на 50 км можно развернуть сеть и на базе Wi-Fi, вот только эффективна ли будет эта сеть? Так что подобная классификация относительна, но не лишена здравого смысла. Двигаемся дальше.

Сети WWAN призваны охватывать гораздо более широкую область, нежели Wi-Fi или WiMAX, с охватом на межнациональной или даже глобальной основе. Обеспечить нас беспроводными глобальными сетями с большой дальностью позволяют сотовые сети, такие как GPRS, HSPA, UMTS и конечно же в перспективе глобальное покрытие LTE.

Визуально представить описанную классификацию поможет диаграмма, приведенная на рисунке 1 ниже:

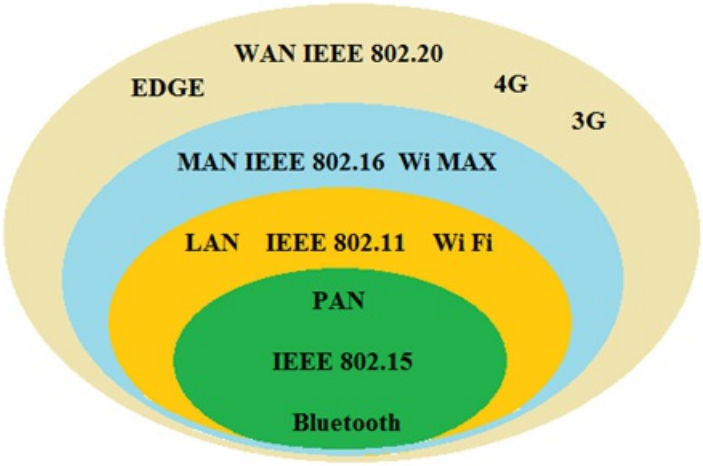

Рисунок 1 – Классификация беспроводных сетей по радиусу действия

Нами не были рассмотрены сети PAN (Persanal Area Network) персональные сети, имеющие малые радиусы действия (до 10 метров) и построенные на таких технологиях как Bluetooth и ZigBee. Опустим их рассмотрение, так как в большинстве своем проблемы безопасности в таких сетях не стоят так остро, как в выше рассмотренных сетях.

Классификация атак на беспроводные Wi-Fi сети

С классификацией самих беспроводных сетей определились, теперь же определимся с классификацией атак на эти сети. Ниже будут даны только общие описания используемых атак без подробного описания их реализации. О реализации некоторых из них поговорим ниже.

Вредоносные соединения (англоязычный термин – Malicious Associations) – это такой вид атаки, при которой беспроводное устройство злоумышленника подключается к сети вместо "законного пользователя". С использованием компьютерных программ злоумышленник заставил думать точку доступа, что его устройство является компьютером авторизованного пользователя. Для подобной атаки хакеру достаточно узнать связку логин-пароль для доступа в сеть. После того как доступ был получен злоумышленник может получить пароли, запускать атаки на сеть или размножать троянов. Так как беспроводные сети работают на 2 и 3 уровнях модели OSI, то никакие VPN здесь не помогут и подобный вид атаки может быть очень опасным и оказать катастрофические последствия на работу сети. UML-модель данной атаки показана на рисунке 2.

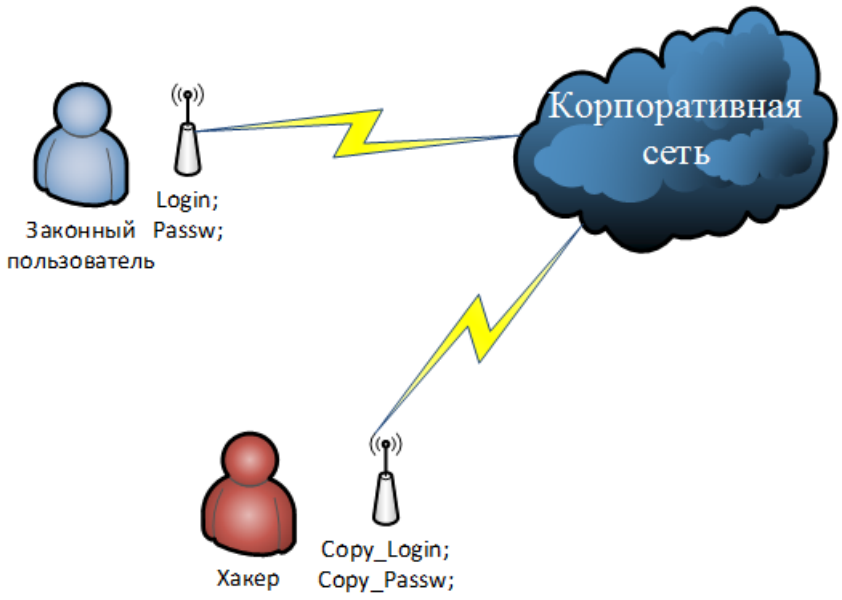

Рисунок 2 – Модель атаки Malicious Associations

Подмена MAC-адреса (MAC Spoofing) – злоумышленник прослушивает сетевой трафик и идентифицирует MAC-адрес компьютера, имеющего права на работу в сети. Большинство беспроводных сетей используют фильтрацию MAC-адреса, чтобы разрешить доступ только авторизованным сетевым устройствам с конкретным MAC-ID. В 802.11 есть существенный косяк,

связанный с тем, что MAC-адреса передаются в заголовках пакетов в незашифрованном виде. Никакого специального оборудования для его обнаружения не требуется, достаточно любого ПО-анализатора, способного показать структуру пакета, рисунок 3.

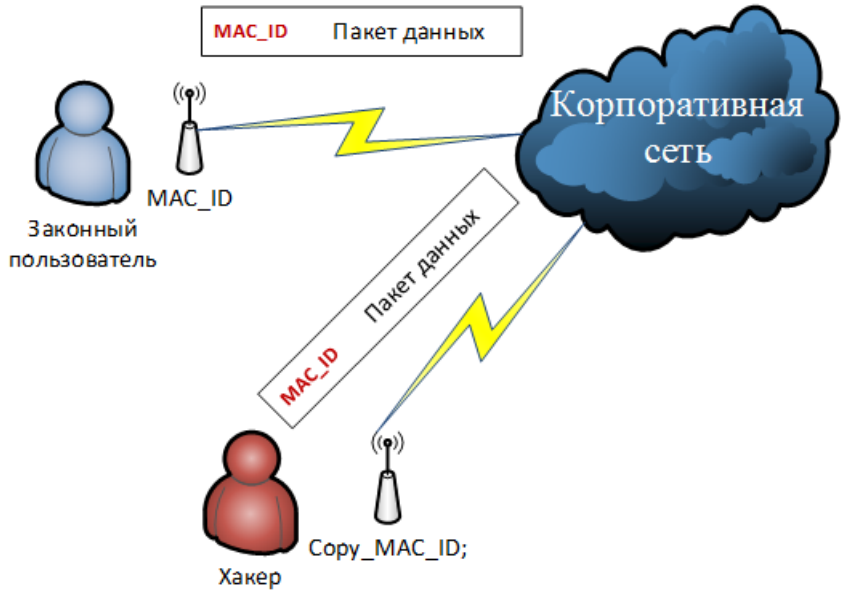

Рисунок 3 – Модель атаки MAC Spoofing

Man-In-The-Middle – ~~мужик по середине~~ атака посредника. Модель атаки выглядит следующим образом: атакующий находится между легитным абонентом и точкой доступа. Злоумышленник подключается к точке доступа и производит подмену сообщений, которыми обмениваются абоненты с точкой доступа. Конечно же, абонент не знает о существовании "посредника". Взломщик, подключившись к каналу связи, может осуществлять вмешательство в протокол передачи сообщений, удаляя или искажая в нем информацию, рисунок 4.

Рисунок 4 – Man-In-The-Middle

Network Injection – позволяет злоумышленникам использовать точки доступа, которые передают нефильтрованный сетевой трафик, такой как Spanning Tree, OSPF, RIP, HSRP. Злоумышленник может вводить фиктивные команды конфигурации сети, которые могут повлиять на маршрутизаторы, коммутаторы и хабы. В результате действия хакера целая сеть может потребовать перезагрузки или даже перепрошивки большого количества устройств.

Caffe Latte. Оригинальное название атаки, применяемое в англоязычной литературе. Называется она так, потому что получение пароля от беспроводной сети можно обеспечить менее чем за 6 минут. В общем, пока готовится кофе. :) Данная атака позволяет получить WEP ключ прямо из операционной системы клиента, при этом взломщику даже не обязательно находится в зоне обслуживания беспроводной точки доступа. Если кратко, то делается это путем захвата пакета ARP от клиента, производятся небольшие манипуляции с содержимым пакеты и впоследствии его отправка обратно клиенту. Применяется в сочетании с вышеописанным методом.

Denial-of-Service, или DoS атака. Дословно переводится как "Отказ в обслуживании", происходит тогда, когда злоумышленник постоянно посылает точке доступа различные запросы, такие как запрос соединения, сообщения о себе и другие команды. В результаты от огромного количества сообщений точка доступа может быть отключена на какое-то время. После возвращения точки доступа в эфир, между всеми устройствами, которые она раньше обслуживала, будет проходить процедура "рукопожатия" с обменом ключей для установления соединения. Злоумышленник может перехватить пакеты рукопожатия и получить несанкционированный доступ к системе.

Перечисленный список атак является лишь верхушкой айсберга по сравнению с тем огромным количеством разновидностей атак, которые в настоящее время возможны в сети.

Симуляция атаки на конкретную Wi-Fi сеть

В этом разделе будет построена беспроводная сеть и смоделирована ее атака. Цель данного эксперимента заключается в том, чтобы, во-первых, продемонстрировать возможность взлома беспроводной сети с помощью программного обеспечения, находящего на просторах Интернета в свободном доступе, а, во-вторых, показать, что в результате этой атаки в принципе может быть получена важная и конфиденциальная информацию о пользователях.

Модель атаки: мы находимся в кафе, где можно получить ~~халявный~~ бесплатный доступ к Wi-Fi. Предположим, что в данной задаче проблема получения пароля перед нами не стоит, так как пароль для доступа в сеть можно получить у официанта, либо у любого сотрудника заведения. Нам интересна возможность получения конфиденциальной информации, такой как логин-пароль от социальных сетей, либо почтовых ящиков.

В эксперименте используются персональные устройства пользователей под управлением различным операционных систем и ноутбука. Мониторинг сети производится с ноутбука под управлением ОС Windows 10 с использованием программных пакетов: Cain & Abel и Wireshark.

В рассматриваемых моделях атак учувствовали респонденты, предупрежденные об эксперименте и о том, что на них тестируется возможность получения конфиденциальных данных. Рассмотрим алгоритмы атак с описанием используемого программного обеспечения.

Cain & Abel – это инструмент подбора и восстановления пароля для операционных систем Microsoft. Программа позволяет определять пароли прослушиванием сетевого трафика, а также с использованием большого количество словарей, встроенного криптоанализатора, возможна даже запись разговора по VoIP. Программа может подбирать пароли для доступных беспроводных сетей, расшифровывать кэшированные пароли и производить анализ протоколов маршрутизации.

Ниже будет приведен принцип использования ПО C&A для атаки беспроводной сети по алгоритму Man-In-The-Middle совместно в Caffe Latte.

Скачать программу можно на следующем сайте: oxid.it. Установка и запуск программы происходит стандартно, как и любое другое приложение для Windows. После запуска программы, выглядеть она должна так, как показано на рисунке ниже:

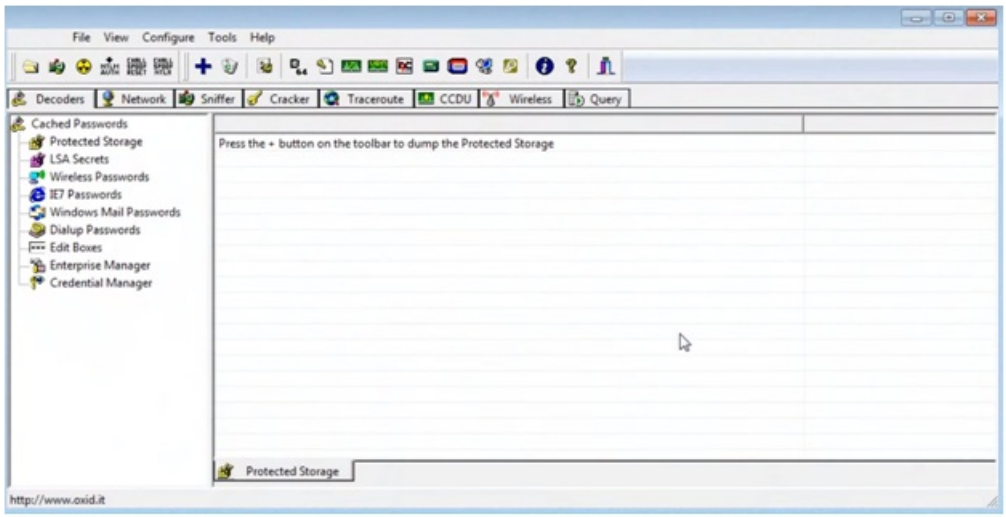

Рисунок 5 – Внешний вид запущенной программы Cain & Abel

Перед началом работы нужно убедиться, что в настройках выбрано правильное сетевое устройство, через которое будет производиться мониторинг сети. Это актуально в том случае, если на вашей рабочей станции их больше одного. Делается это из меню Configure в верхнем меню программы, рисунок 6.

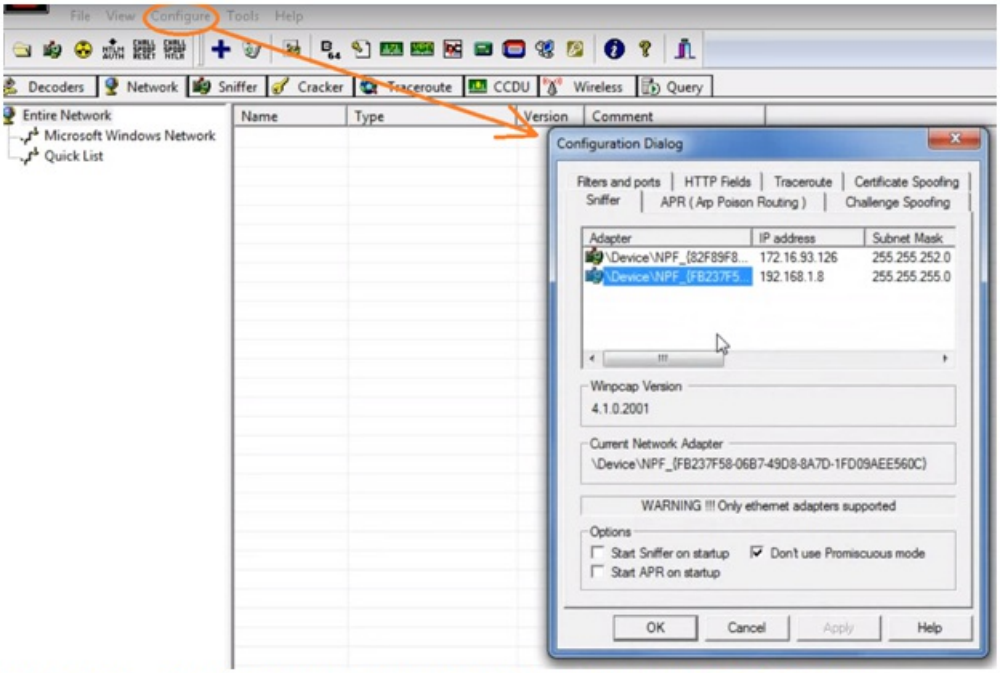

Рисунок 6 – Выбор сетевого интерфейса в программе Cain & Abel

Первым делом необходимо определить соседние устройства, которые функционируют с вами в одной локальной сети. Для этого переходим последовательно по закладкам, изображенным на рисунке 7. 1 – Sniffer; 2 – Start/Stop Sniffer (активируем сниффер-бота); 3 – выбираем диапазон мак-адресов, сканирование которых предполагается. В данном случае нас интересуют все устройства, доступные в нашей подсети, поэтому выбираем "All hosts in my subnet" – ok.

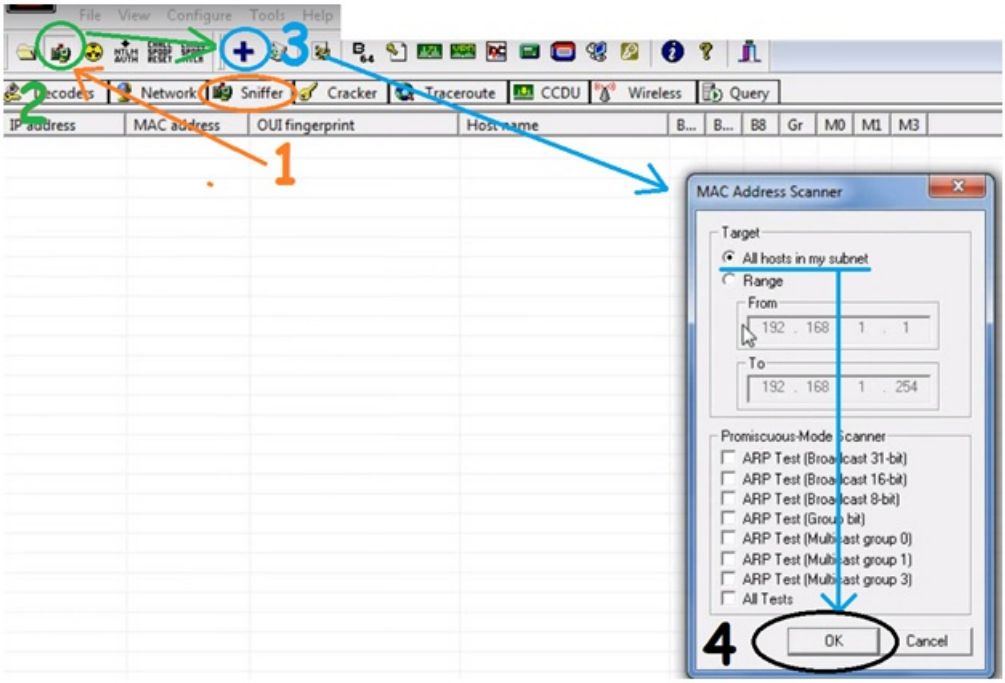

Рисунок 7 – Запуск сниффера в ПО Cain & Abel

На рисунке 8 показан результат работы запущенного бота. Можно увидеть, что в локальной сети найдено 4 устройства.

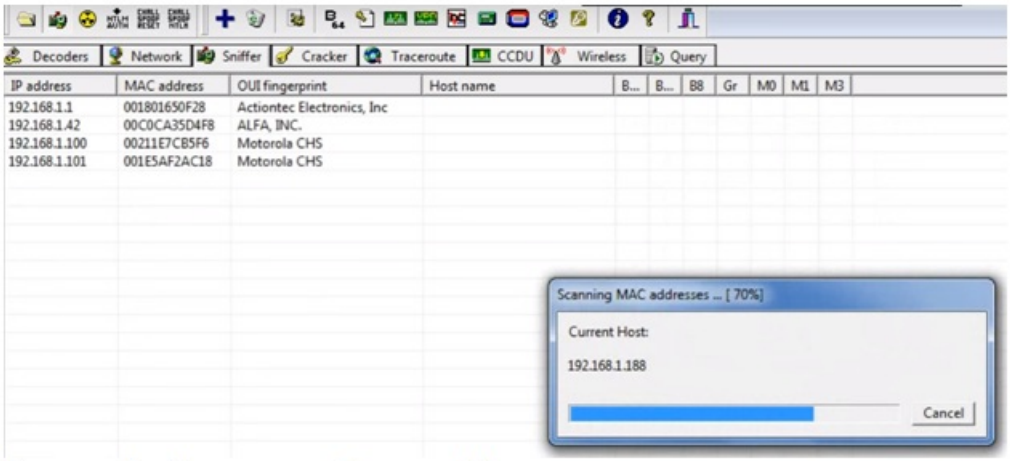

Рисунок 8 – Результат работы сниффера

Применительно к данной сети модель атаки будет выглядеть следующим образом: атакующий (в данном случае наш компьютер) становится посредником между хостом 1 и точкой выхода в глобальную сеть Интернет. Хост 1 думает, что атакующая машина является роутером, а роутер думает, что атакующий является хостом 1. Таким образом, атакующий становится транзитным звеном, через который проходит весь трафик, рисунок 9.

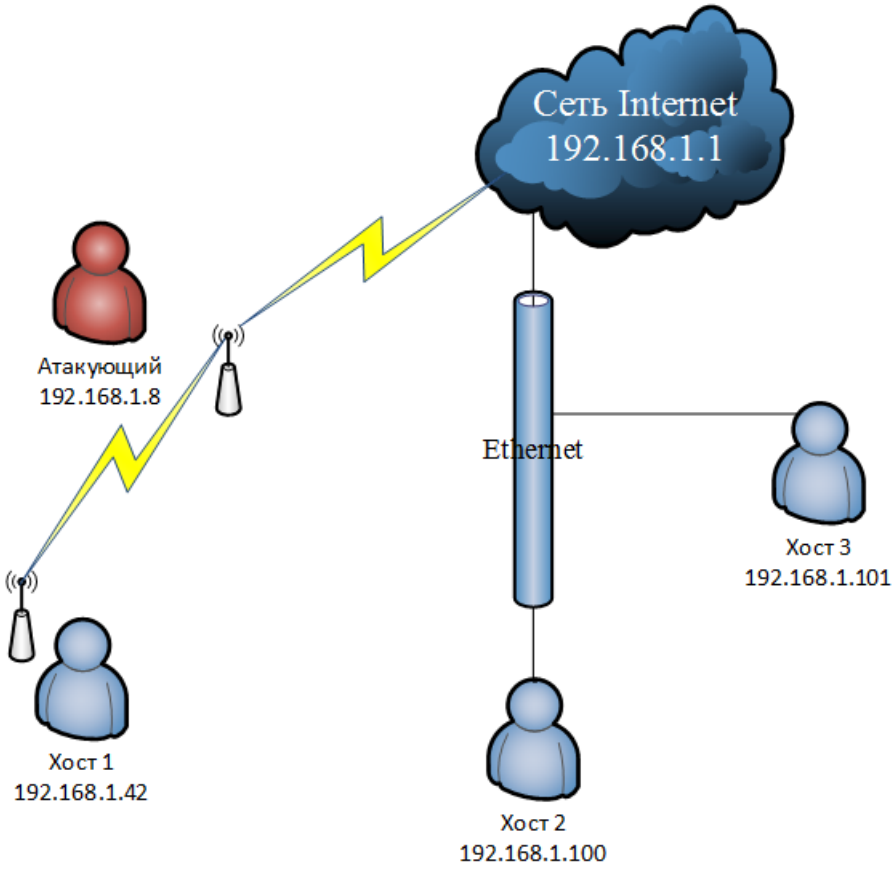

Рисунок 9 – Модель атаки на беспроводную сеть

На следующем шаге, в программе нужно настроить данную модель. Один из вариантов – это использовать "зараженные" ARP пакеты. О работе и назначении протокола ARP можно почитать в специальной литературе, здесь же мы опустим принцип его работы, отметим лишь суть: когда хост 1 пошлет широковещательный запрос для определения мак-адреса получателя, наша машина "представится" этим получателем, хоть таковым и не является. С этого момента хост 1 будет посылать через нас все свои пакеты.

Для модификации протоколов ARP переходим по вкладкам: 1–2–3–4. На 3 шаге выбирается конфигурация нашего сетевого интерфейса, а на 4 – атакуемого, рисунок 10.

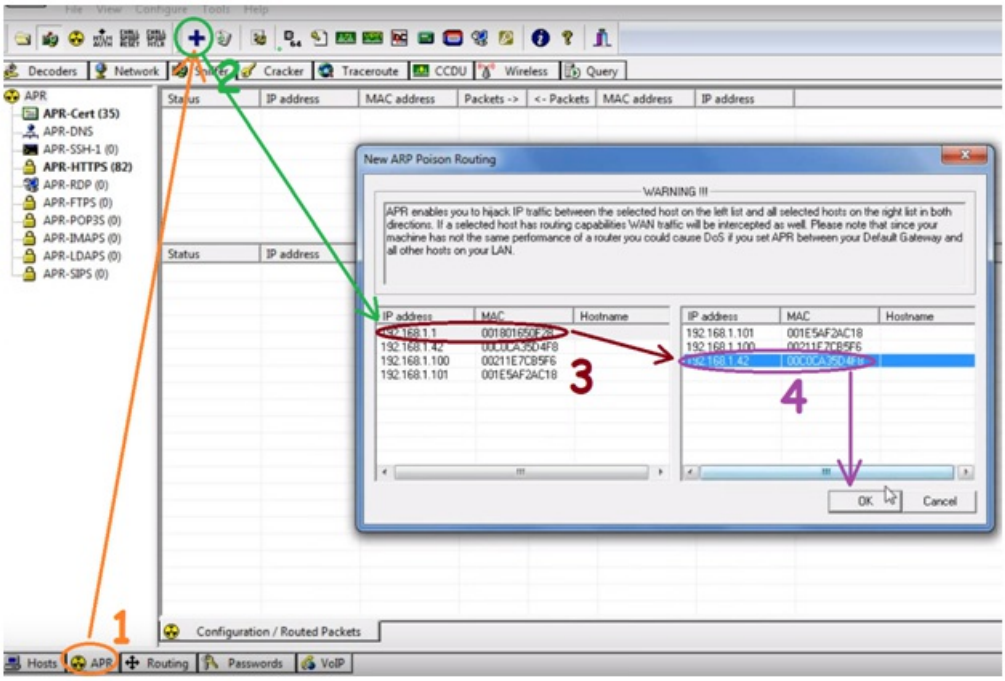

Рисунок 10 – Модификация протокола ARP

Если все выполнено правильно, должна появиться запись, изображенная на рисунке 11. Жмем Start/stop APR, после чего статус записи меняется с Idle на Poisoning.

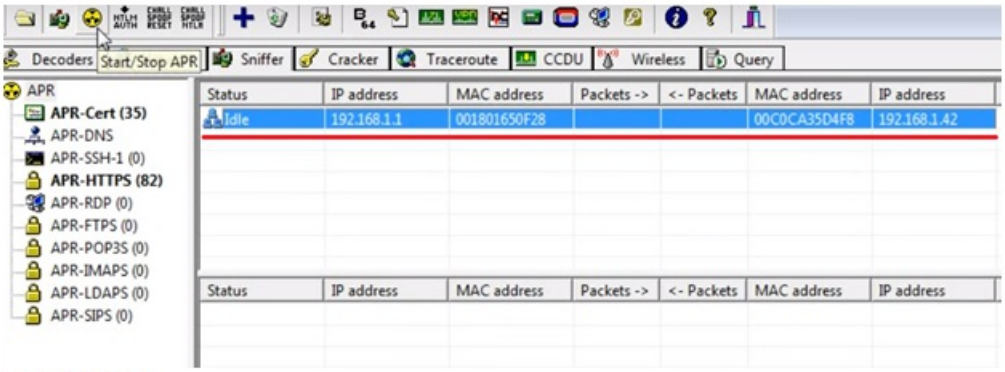

Рисунок 11

После этого, все сетевые операции, произведенные пользователем на прослушиваемом компьютере, будут отображаться в программном пакете в нижней части программы. При этом слева будет показано количество перехваченных пакетов различных сетевых протоколов: SSH, HTTPS, FTP. Например, на рисунке 12 показано, что количество HTTPS пакетов –128 штук.

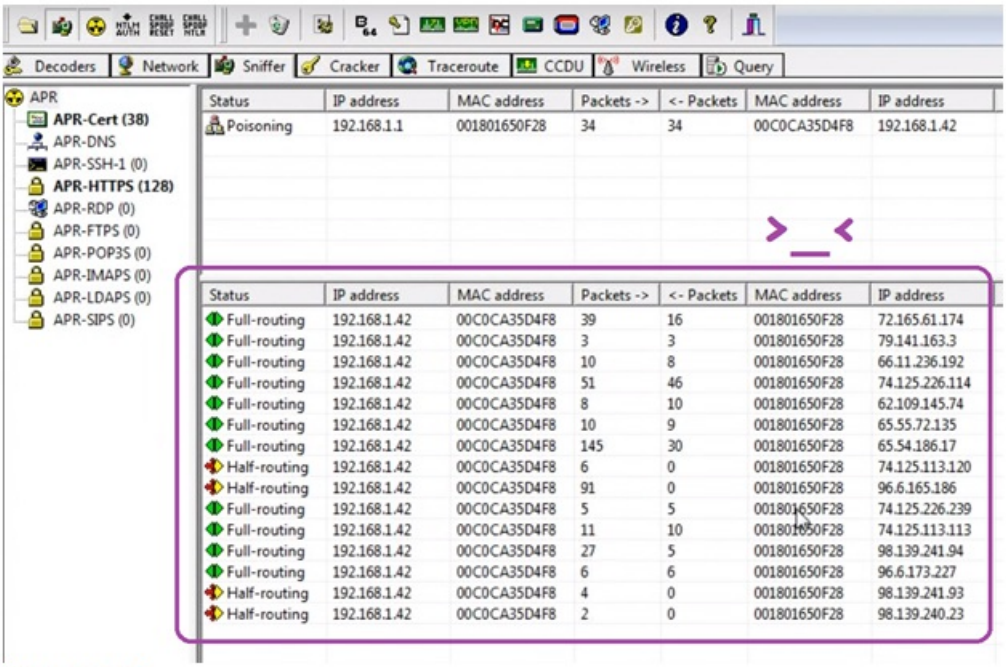

Рисунок 12

В программе имеется отдельная вкладка Password, которая позволяет просмотреть сразу все пакеты, которые содержали пароли, рисунок 13. Таким образом, это лишает необходимости просматривать содержимое всех полученных HTTP пакетов на предмет содержания в них связки логин-пароль.

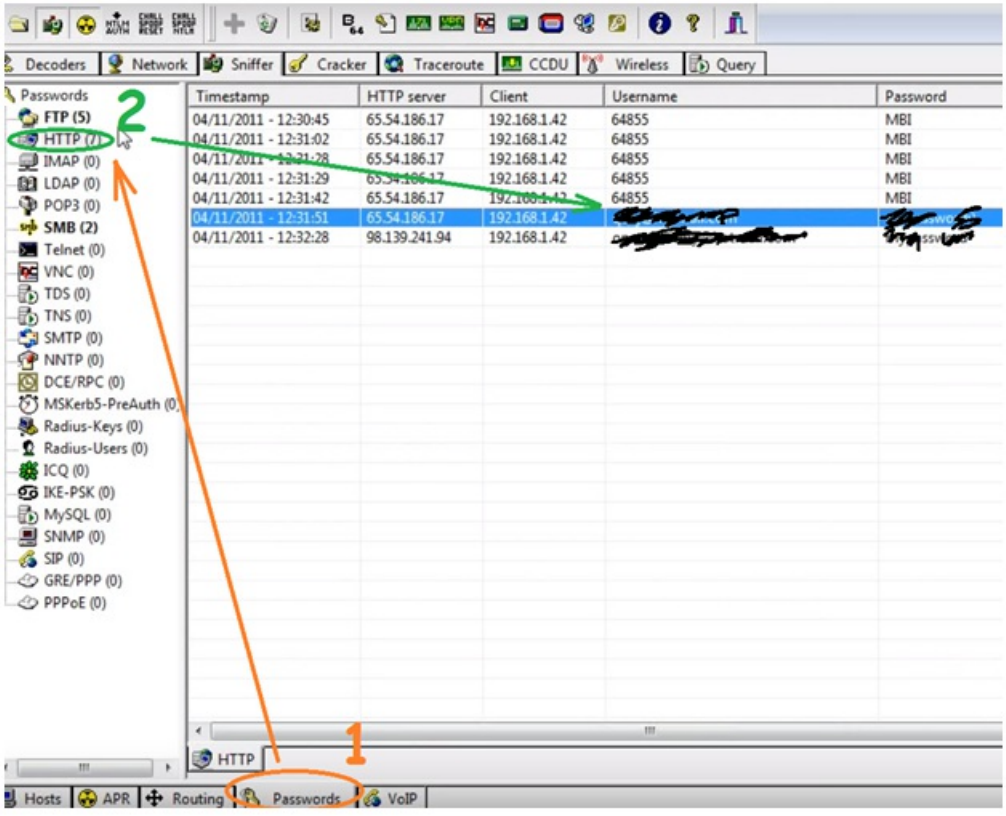

Рисунок 13

Таким нехитрым способом могут быть получены учетные данные пользователей с помощью рассмотренной программы. Перейдем к рассмотрению следующей программы.

Wireshark – это анализатор сетевых протоколов, который позволяет в интерактивном режиме просматривать трафик, проходящий по компьютерным сетям. Программа очень популярна среди системных администраторов, и, скорее всего, каждый специалист, чья работа связана с эксплуатацией компьютерных сетей хотя бы раз в ней работал. Инструмент очень функциональный и включает в себя возможность тестирования сотен протокол: Ethernet, 802.11, HDLC, ATM, Bluetooth,

USB, Token Ring. Программа умеет расшифровывать многие протоколы, включая IPsec, Kerberos, SNMP, SSL/TLS, WEP, WPA и WPA2.

При подключении к сети по тому же сценарию, что и выше, программа позволяет перехватывать пакеты. Так же, как и в предыдущей программе, сначала выбираем сетевой интерфейс и жмем кнопку начала мониторинга трафика, рисунок 14.

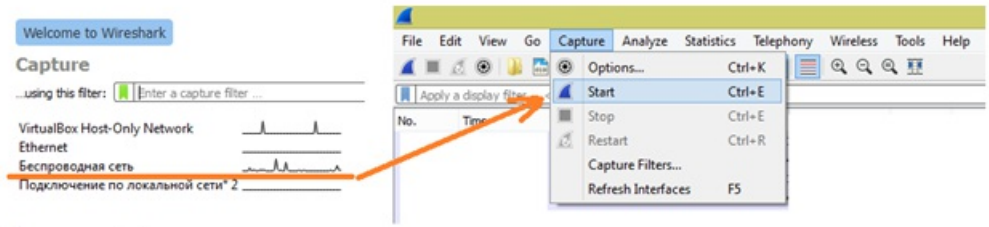

Рисунок 14

Достаточно пользователю открыть страницу браузера, как в Wireshark"е начнет появляться большое количество перехваченных пакетов. Для получения конфиденциальных данных злоумышленника, конечно же, интересуют только определенные типы пакетов, содержащие так называемые POST данные. Этот тип данных появляется при заполнении формы авторизации в браузере. Для отображения подобных пакетов в поле Filet программы Wireshark нужно ввести команду http.request.method == "POST". И если такой тип данных был перехвачен, то программа тут же отобразит эти пакеты, рисунок 15.

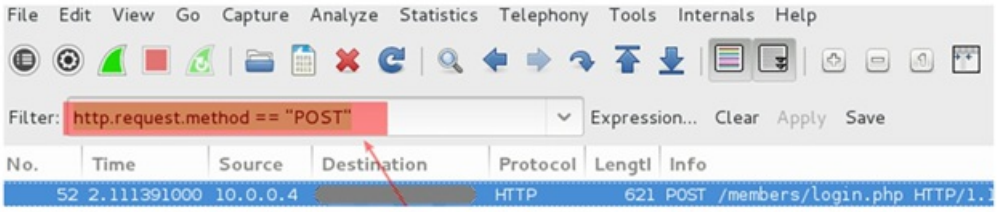

Рисунок 15

Нажав ПКМ на выбранный пакет и перейдя по вкладкам Follow – TCP Stream можно отобразить содержимое пакета, в котором просматриваются поля password и user, рисунок 16.

Date: Mon, 10 Nov 2014 23:52:21 GMT

Server: Apache/2.2.15 (CentOS)

X-Powered-By: PHP/5.3.3

P3P: CP="NOI ADM DEV PSAi COM NAV OUR OTRo STP IND DEM"

Set-Cookie: non=non; expires=Thu, 07-Nov-2024 23:52:21 GMT; path=/

Set-Cookie: password=[redacted] expires=Thu, 07-Nov-2024 23:52:21 GMT; path=/

Set-Cookie: scifuser=[redacted] expires=Thu, 07-Nov-2024 23:52:21 GMT; path=/

Location: loggedin.php

Content-Length: 0

Connection: close

Content-Type: text/html; charset=UTF-8

Рисунок 16

Вероятнее всего, эти поля будут зашифрованы, если пакет прилетел из Facebook, Vkontakte и других прошаренных сервером. Поэтому для расшифровки пароля придется использовать ресурс http://www.onlinehashcrack.com/hash-identification.php#res, либо утилиту hashcat.

К слову сказать, с помощью Wireshark может быть осуществлён перехват пароля WPA2 в сети Wi-Fi.

Для этого, правда, нужно перехватить пакеты "рукопожатия" между абонентом и точкой доступа. Тут два варианта: либо дождаться, когда это рукопожатие произойдет само собой, что, конечно же, может быть значительно долго, но как показывает практика в среднем – чуть больше 20-ти часов. Либо использовать второй вариант – организация DoS атаки на точку доступа. В этом случае точка доступа уйдет в перезагрузку на какое-то время, а после включения будет инициировать подключение к тем абонентам, с которыми потеряла связь.

Заключение и выводы

Все чаще на улицах, магазинах и в офисах можно встретить заманчивые надписи Free Wi-Fi, но не стоит вестись на халяву, забыв о безопасности. Атаки типа Man-In-The-Middle, Café Latte, Denial-of-Service не являются редкостью, и как было показано в материалах данной статьи легко реализуются с помощью бесплатного программного обеспечения, в пару кликов устанавливаемого на самую популярную в мире операционную систему семейства Windows. Тем не менее, можно сформулировать несколько общих правил безопасности, соблюдение которых может в значительной мере обезопасить вашу работу в сети:

1. Отключайте автоматическое подключение к доступным Wi-Fi сетям;
2. Избегайте подключения к точкам доступа с отключенным шифрованием передаваемых данных;
3. Предпочтительнее всего для серфинга в Интернете использовать точки доступа с включенным WPA/WPA2 шифрованием. На сегодняшний день это самый надежный тип кодирования данных в Wi-Fi;
4. В общественных сетях Wi-Fi лучше вообще избежать осуществление финансовых операций покупки в интернет-магазинах, проверку электронной почты и т.д. То есть не посещать все те ресурсы, где требуется аутентификация;
5. Лучше вообще выключать адаптер Wi-Fi на телефоне, или ноутбуке, если не требуется подключение к сети.