Халявный соседский вайфай — Lurkmore

В эту статью нужно добавить как можно больше методов взлома вайфая для тех, кто не умеет кодить на ляпукс.

Также сюда можно добавить интересные факты, картинки и прочие кошерные вещи.

«NechtoIzPodvala: клиент: «неделю назад моя сеть переименовалась в „халявный интернет“, а скорость упала в 3 раза. Что это значит, какие-то проблемы с роутером?» »

— суть явления

Халявный соседский вайфай (сокращенно *ХСВ*) — расово верный способ попадания в интернеты. В густонаселённых районах дефолт-сити встречается чуть чаще, чем всегда.

Как искать?

«xxx: сосед сука до сих пор не оплатил свой незапароленный вай-фай. а ведь пора бы — второе число уж настало… »

— 411634

Для обнаружения используется ноутбук с установленным NetStumbler. Особой крутостью считается использование ноутбука с внешней wi-fi картой и антенной, изготовленной из пустой банки Pringles, которая ВНЕЗАПНО даёт невероятное усиление сигнала, вплоть до сотен метров прямой видимости.

Для кого-то не особо сильной проблемой считается шифрование трафика и пароль, который в простых случаях подбирается за пару часов, а то и за секунды. Если особо повезёт — трафик шифрован безблагодатной WEP, которая ломается на раз винрарными программками вроде aircrack-ng. «Безопасность» WEP характеризуется следующей фразой одного анонимного эксперта: «Использование WEP — это, практически, приглашение в сеть».

Также доставляет шпиёнская программа airodump-ng из того же комплекта aircrack-ng, которая позволяет подсматривать пароли от страничек Вконтакте всякого быдла, пользующегося открытым ХСВ, и не только ХСВ, а к вайфаю от полосатиков это тоже относится, там шифрование можно сделать (помимо airodump'а надо анализатор поставить, типа Wireshark). Это же относится и к шифрованному трафику, который можно расшифровать, если знаешь пароль. А на телефоне с ведром для этого можно воспользоваться программкой dSploit (А лучше cSploit. В нее даже Metasploit запилен). Кулхацкеры не дремлют!

В настоящее время взлом запароленных сетей с целью получения халявного вайфая всё ещё возможен. WEP был повсеместно вытеснен очень надёжным WPA2, но место дырки унаследовала надстройка WPS, которая легко ломается брутфорсом за одну ночь и сливает после этого пароль. Защита одна — отключение WPS на корню.

FON

Умные люди не в нашей стране придумали полулегальный (ввиду необходимости получать лицензию для предоставление каналов связи) способ распространения интернетов в больших городах. Реализация в этой стране тупа, чуть более, чем полностью (с недавних пор ещё и МТС присоединился).

Стандартные места появления ХСВ

- Подоконник (шанс словить что-то с улицы необычайно высок)
- Туалет
- Стена, ведущая в квартиру высокотехнологичных, но тупых соседей (такие, обычно, всегда тупые). Не забудьте попрыгать с ноутбуком — эта стена может оказаться потолком.

Карманные устройства

С появлением различных мобильников, смартфонов, коммуникаторов, нетбуков, psp, айподов, фотокамер и прочей портативной хуйни со встроенным вайфаем, способ становится всё более и более популярным.

Яркий тому пример — Гуглофоны. В андроид-маркете лежат в свободном доступе программы для взлома wep-сетей, например Penetrate, Router Keygen. Скачиваем, запускаем, качаем доп. таблицы и… ну ты понел. Они сами все сделают, а тебе остается уникальное право выбора сети, которую захочешь сломать. К сожалению, эти программы работают только на роутерах Thomson, а наша страна, конечно же, пользуется только роутерами D-Link, TP-Link, ZyXEL и Eltex.

Однако есть ещё вариант с запуском aircrack-ng непосредственно на смартфоне. Вопрос только в Wi-Fi чипе устройства: в большинстве смартфонов Android используются одни и те же от Broadcom — это bcm4325, bcm4329 или bcm4330, которые работают нестандартным образом, не давая переводить Wi-Fi модуль в режим монитора, необходимый aircrack-ng. Но и тут для некоторых топовых смартов есть решение.

Гопстоп-телеком

Можно воровать инет у гопников, слушающих музыку на [b] лавке у подъезда. Для этого своё устройство (мобилу или bluetooth-адаптер) нужно назвать «Vvedite1234» или аналогично. Потом добавить в спаренные устройства любое найденное из окна (устройства у гопников на лавке видны даже с 9-го этажа). Естественно, тупые вводят на запрос кода эти самые «1234». Дальше сами.

Хотя, если вы альтруист, то лучше воздержитесь. Гопота имеет обыкновение юзать не 3G, а GPRS, что влетает ей в копеечку. Вас, конечно, поймать будет сложновато, но вот денег уйдёт достаточно, чтобы она вышла на охоту за мобилкой. Частое использование немного (на жалкие 3000$) снижает стоимость вашей типичной хаты.

ХСВ от самого оператора

Hacking Wi-Fi in Backtrack using aircrack-ng
Сабж в Backtrack

ВНЕЗАПНО полосатики первыми в этой стране решили давать интернет по вайфайке на халяву. Акция действует на большей части территории Default city. Но интернеты даются не просто так, а за просмотр двухминутной рекламы. Причем страничка с рекламой снабжена счетчиком времени, который останавливается в случае сворачивания странички. Но это легко обойти с помощью православного браузера Опера:

1. Ждем немного времени (сервер тоже проверяет время, и если открыть перенаправление раньше двух минут, он пошлет вас). Страничку можно сворачивать.
2. Открываем исходный код страницы.
3. Уменьшаем значение 1000 в строке setTimeout(\'asd_tick()\',1000) в 10 раз.
4. Нажимаем «сохранить изменения». Любуемся на счетчик.
5. ???
6. PROFIT!

Есть и более простой способ для нубов: сворачиваем страницу, ждем 2 минуты и меняем в адресной строке play на redir. Но вид люто, бешено отматывающегося счетчика доставляет.

Доступ дается только на 15 минут, потом описанные действия надо повторять.

Скорость соединения — говно, иногда ниже EDGE. Но большим вином является то, что у оператора остается только MAC-адрес пользователя! Нигде регистрироваться и сообщать свои данные не надо. Можно сменить свой MAC-адрес и выкладывать картинки с ЦП и делать другие нехорошие дела (это относится не только к данному способу, а ко всей технологии ХСВ вообще). Лучше при этом менять свое местоположение, так как можно определить положение передатчика при помощи направленных антенн. Так что пативены все равно могут приехать к тебе, Анонимус[1]!

Аттракцион невиданной щедрости все ещё работает, особенно на территории сети Макдональдс, без рекламы, но с ограничением 15Мб в те же 15 минут.

Конец сказки

Согласно постановлению российского правительства №758 от 31.07.2015, раздача халявного вайфая запрещена, ибо пользователи никак не идентифицируются, и могут невозбранно написать нехорошего про великую державу и старика Кабаева. И если на момент выхода закона большинство обладателей роутеров никак не отреагировало, то ныне встретить открытую сеть практически невозможно. Ибо никто не хочет отвечать за экстремизьмь, запощенный со своего IP хуй знает кем.

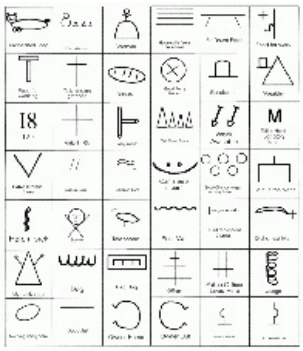
А у них?

У буржуев всё, конечно же, абсолютно так же. В пиндоссии, чуть более чем всегда, на роутерах оставляют дефолт-пароль и логин вроде ~~123456789~~ admin/admin, чем собственно и пользуются все, кому не лень. А шифрование? Какое шифрование? Пиндос покупает роутер в магазине, вставляет его в розетку и включает в него проводок с интернетом. В итоге 90% населённых пунктов СШАшки покрыты сетью Wi-Fi с

названием linksys[2].

В Германии дела обстоят несколько иначе. Пользователю чаще всего прямо на дом доставляется провайдерский маршрутер с включенным по дефолту шифрованием и рандомным числовым паролем, напечатанным на наклейке снизу роутера. В деревнях (хотя у русского человека язык не повернется называть деревней то, что больше похоже на элитный коттеджный поселок с улицами покрытыми брусчаткой и парой-тройкой гипермаркетов) наиболее популярен ADSL, поэтому подключение интернета сводится к вводу логина/пароля в модем, правильному подключению проводов с непривычными штекерами и звонку провайдеру. Так что большая часть даже небольших населенных пунктов покрыта шифрованными сетями со словом Fritz в SSID, причем так густо, что крайне трудно найти такой закоулок, где ловит менее двух сетей одновременно.

Warchalking (или *вардрайвинг*) — так называется метод воровства этого вашего интернета посредством Wi-Fi. Слово образовано от двух английских слов: *war* — война и *chalk* — мел. Почему тут употребляются именно эти слова, вы поймёте после прочтения нижеследующего текста.



Классическая схема символов, употребляемых поциентами

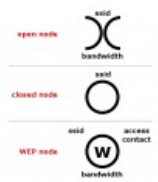
Немного истории

Ещё в древние времена, в Англии, местные расовые нищеброды часто помечали дома специальными символами, которые рисовали мелом или кусочком угля. Данные символы служили меткой тех домов, где могли накормить или предоставить ночлег. Существовали и предупреждающие символы. Например, на домах ментов и проч. Со временем, конечно, данный язык меток постепенно вымирал и мог бы и совсем исчезнуть, кабы не обрёл своё второе рождение после изобретения беспроводного доступа к сети Интернет (здесь: Wi-Fi).

Современное использование

Теперь мел стали использовать для пометки мест халявного доступа к сетке. Обычно рисуют специальный символ, пароль на доступ в сеть и пропускную способность канала. А выполняют рисунки всё те же нищеброды, что и прежде, только более технологичные. Также, есть экземпляры, которые вмуровывают в стену флешки и винты — just for lulz.

Пруфпики



Краткий инструктаж по употребляемым современным символам.

Среди варчокеров встречаются и яблочники.

Очередной поциент пометил ареал своего обитания.

Ссылки

- Тот самый NetStumbler
- Знакомимся с технологией Wi-Fi
- Wi-Фу: Боевые приемы взлома и защиты беспроводных сетей — архив, зеркало.
- Wi-Fi: Все, что Вы хотели знать, но боялись спросить — книжка, зеркало.
- Wi-Fi: Беспроводная сеть — книжка, зеркало
- aircrack-ng
- Простая инструкция к aircrack-ng
- Всё о вардрайвинге
- Для жителей ДС скоро будет 3,5 млн. легко взламываемых вайфай-точек.
- ZOMG TEH DRAMA из Е-бурга.

Примечания

1. ↑ Не совсем так. Смотреть тут и тут

2. ↑ В этой же стране первенство держит слово «dlink» с той же парой admin:admin

Интернет
Интернеты 127.0.0.1 ADSL Bitcoin CMS DDoS Frequently asked questions GPON I2P Internet White Knight IPv6 IRC MediaGet Miranda NO CARRIER QIP Ru@razlogoff.org SEO Skype Tor TOS Via WAP Ёбаное BT Админ Акадо Американские интернеты Анонимус Аська Бан Бесплатный хостинг картинок Блог Блогосфера Бот Ботнет Браузерка Бугагашечки Бурление говн Вап-чаты Веб 1.0 Веб 2.0 Вики Виртуал Вордфильтр Голосование ногами Гостевуха Диалап Дом.ру Домашняя страница Дорвей Единый реестр запрещённых сайтов Жаббер Заповеди интернета Заработок в интернете Идентификация пользователей в интернете Известные интернет-флешмобы Имиджборд Инвайт Интернет-магазин Интернет-сервисы Искра Кик Кириллические домены Кликбейт Коммент Комьюнити Лесенка Лог Локалка Макхост Мем Микроблог Мобильный интернет Модератор Некропост Ник Оптимизатор Ответы Офлайн Оффтопик Письма счастья Подкаст Поисковая бомба Покровитель интернетов Пост Правила интернетов Предыдущий оратор Премодерация Пруфлинк Рерайтинг Ростелеком Сабж Сетевые онанисты Симпафка Синдром вахтёра Ситилайн Скайнет Скриншот Смайл Социальная сеть