Лучшие инструменты пен-тестера: беспроводные сети

xakep.ru/2009/09/10/49438/

Содержание статьи

У каждого из команды][— свои предпочтения по части софта и утилит для пентеста. Посовещавшись, выяснилось, что выбор так разниться, что можно составить настоящий джентльменский набор из проверенных программ. На том и решили. Чтобы не делать сборную солянку, весь список мы разбили на темы и в этот раз коснемся утилит для вардрайвинга и пентеста беспроводных сетей. Пользуйся на здоровье.

Netstumbler

Сайт: www.stumbler.net

Определенно один из самых известных и лучших инструментов для вардрайвинга. У стемблера всего одна задача — обнаружить в эфире точки доступа, считать SSID и записать полученную информацию в логфайл вместе с координатами, если к программе подключен приемник GPS. После удачного вардрайвинга, информацию о найденных AP-шках месте с данными о месторасположениями можно экспортировать в log-файл, преобразовать его с помощью многочисленных конверторов в понятный Google'у формат KML и за пару секунд отобразить все точки доступа на карте с помощью Google Maps или декстопной программы Google Earth.

Для поиска живых точек доступа **Netstumbler** использует приемы активного сканирования, т.е. не просто прослушивает эфир, но и каждую секунду отправляет специальные фреймы. Надо сказать, что специфические LC/SNAP-фреймы, сгенерированные стемблером, легко распознаются современными IDS-системами. К тому же активное сканирование не поможет тебе в поиске спрятанных (hidden) точек доступа, впрочем сама подборка информации не фонтан. Например, **Netstumbler** может распознать лишь факт использования шифрования сети, не уточняя какой именно механизм используется. Вдобавок, программа наотрез отказывается работать под Vista'ой и вряд ли когда-нибудь это делать захочет. В результате, получаем отличную программу, если нужно просканировать эфир на наличие точек доступа и записать их координаты, но только под виндой и без надежды получить какую-либо еще ценную информацию.

Vistumbler

Сайт: www.vistumbler.net

Ну хорошо, а как быть если на ноуте/нетбуке стоит Vista или Win7? По правде говоря, возможность активного сканирования точек доступа есть в самой системе. Это делается с помощью консольной утилиты netsh:

```
netsh wlan show networks
mode=bssid
```

Однако умелец Andrew Calcutt быстро сварганил GUI-интерфейс, в котором вывод

команды приводится в опрятный вид и объединяется с информации расположении обнаруженных AP-шек, считывая ее с текущими координатами GPS. Под никсами, кстати, существуют аналогичные утилиты, которые парсят вывод команды iwlist.

Забавно, что **Vistumbler** написан с помощью тулзы для автоматизации различных действий AutoIt (подробнее о ней можешь прочитать в статье "Пусть он все сделает сам!" в #107][),
позволяющая разработать приложения даже тем людям, которые о программировании толком никогда и не слышали. При этом **Vistumbler** не просто работает, а работает отменно, отображая помимо уровня сигнала MAC-адрес вендора, используемую систему шифрования, и прочие параметры. Данные о расположении найденных точек можно "на лету" экспортировать в KML формат и в реальном времени отслеживать их появления на карте через Google Earth. Для вардрайверов полезной также окажется функция, с помощью которой уровень сигнала обозначается с помощью различных звуковых файлов. Справедливости ради, стоит сказать, что в **Netstumbler**‘е также можно было провернуть подобный трюк, но лишь при помощи внешних скриптов.

inSSIDer

Сайт:
www.metageek.net/products/inssider

Расстроенный тем фактом, что **Netstumbler** не развивался несколько лет и не работает Вистой и даже 64-битной XP, Charles Putney решил написать свою собственную утилиту для поиска Wi-fi сетей, после чего опубликовал исходники на известном портале The Code Project. Идею подхватил Norman Rasmussen, после чего на свет появилась новая версия **inSSIDer**‘а, построенная на базе Native Wi-Fi API. Инсайдер подобно **Netstumbler** использует активные методы сканирования, а всю найденную о точках доступа информацию отображает в табличке, сдабривая данные красивыми графиками уровня сигнала. Тулза очень простая — ничего лишнего, но я нередко использую именно ее для поиска Wi-Fi спотов и определения используемой ими защиты.

Kismet

Сайт:
www.kismetwireless.net

А это уже полноценное никсовое приложение для поиска беспроводных сетей, снифинга, и даже обнаружения вторжений. **Kismet** кардинально отличается от **Netstumbler** и подобных ему тулз тем, что для определения беспроводных сетей применяет пассивное сканирование (ничего не вещая в эфир). Причем используемые методики позволяют определить некоторую информацию о клиентах, подключенных в сети, а также найти скрытые (non-beaconing) сети, правда, только в том случае если в них есть некоторая активность. **Kismet** автоматическим может определить используемые диапазоны IP адресов, перехватывая TCP, UDP, ARP и DHCP пакеты, дампить трафик в формат для Wireshark/TCPDump, и даже определять примерное расстояние до точки доступа (работа с GPS, разумеется, поддерживается).

Примечательно, что после более чем 5 лет разработки, создатели вот-вот порадуют нас совершенно новым релизом. В частности, в конце мая вышла Kismet-2009-05-RC1, в которой был кардинально переработан интерфейс (по-прежнему используется ncurse), переделаны конфигурационные файлы, добавлены новые опции для фильтрации данных и новая система предупреждений, оптимизирована загрузка процессора, проработана система плагинов. Что касается порта для винды, то он есть, но реализован компанией CACE и, увы, работает только со специальными Wi-Fi адаптерами Cace AirPcap.

Aircrack-ng

Сайт: aircrack-ng.org

Aircrack-ng — полноценный программный комплекс для взлома 802.11 WEP (Wired Equivalent Privacy) Encryption и WPA/WPA2-PSK ключей для WiFi-сетей. Сам набор состоит из нескольких утилит и включает airodump (снифер для сетей 802.11), aireplay (тулза для инжекции Wi-Fi фреймов), aircrack (взлом WEP и брутфорс WPA-PSK), а также airdecap (декодирование перехваченных WEP/WPA файлов). В общем случае для взлома WEP необходимо определенное количество перехваченных пакетов: как только будет захвачено нужное количество фреймов, aircrack-ng будет готова провести статическую атаку на WEP-ключ. Сейчас **Aircrack-ng** поддерживает три способа для "восстановления" ключа:

- первый метод через PTW атаку: основное преимущество заключается в небольшом количестве перехваченных пакетов, необходимых для взлома WEP-ключа. Но метод работает только с arp-пакетами, и это, естественно, большой недостаток;
- второй вариант — через FMS / KoreK атаки. Метод включает в себя различные статические воздействия (FMS, KoreK, Brute force) для поиска WEP ключа и требует больше пакетов, чем в случае PTW атаки;
- третий вариант – это подбор с использованием словаря (word list), используется, в основном, для взлома WPA/WPA2 ключей.

Полноценная версия **Aircrack-ng** существует только для Linux, хотя на официальном сайте доступна "недоверсия" для ивнды. Разработчики честно предупреждают, что для ее работы нужно самому доработать DLL конкретно для своего Wi-Fi адаптера.

Technitium

Сайт: www.technitium.com

Что удивительно, но фильтрация по MAC-адресам по-прежнему остается достаточно часто используемой защитой. Впрочем, огранить доступ от случайных зевак она действительно сможет, а от вардрайверов… ну, пускай ребята балуются :). Подключиться к таким AP в этом случае могут только клиенты, которые занесены в список доверенных машин. Обойти же подобную защиту проще простого — нужно лишь сменить MAC-адрес своего беспроводного адаптера на доверенный. Подходящий MAC легко определить все той же утилитой Airodump, перехватив пару пакетов. Изменить MAC-адрес под никсами поможет утилита macchanger. Что касается винды, то и тут

существует немало программ, в том числе платная SMAC и бесплатная **Technitium**. Обе требуют лишь выбрать сетевой адаптер и указать для него желаемый MAC-адрес. Убедись в том, что адрес успешно сменился (команда ipconfig /all в консоле) и попробуй установить соединение. К сожалению, с первого раза ты можешь легко обломаться, поскольку авторизированный клиент может быть уже подключен к сети. Выселить его оттуда поможет все та же программа Void1 и деаутентифакционные пакеты.

void11

Сайт:

wirelessdefence.org/Contents/Void11Main.htm

Void11 используется для деаутентификации беспроводных клиентов от точки доступа, или, проще говоря, для принудительно отключения клиентов от точки доступа. После такого отключения беспроводной клиент будет автоматически пытаться подключиться к точке доступа (повторить ассоциацию). А при каждом повторном подключении будет создаваться трафик, который нужен для подбора ключа. К тому же, можно отключить клиента, занять его MAC-адрес и таким образом обойти фильтрацию по MAC-адресам. К сожалению, средства Windows это не позволяют, зато подобный фокус легко реализуем под никсами с помощью этой утилиты:

```
void11_penetration -s КЛИЕНТСКИЙ_MAC -B MAC_ТОЧКИ_ДОСТУПА -D
wlan0
```

Asleap

Сайт:
www.willhackforsushi.com/Asleap.html

Если в ходе сканирования, твой стамблер в колонке Vendor (производитель оборудования) покажет слово CISCO, не лишнем будет вспомнить о протоколе авторизации LEAP (Lightweight Extensible Authentication Protocol), разработанный как раз-таки циско. Проверить догадки об используемом в сети протоколе может помочь снифер, который должен показать пакеты REQUEST, EAP-CISCO Wireless (LEAP). Главная особенность LEAP состоит в том, что для авторизации нужен не только пароль, но и имя пользователя! По умолчанию в Windows этот протокол не поддерживается, поэтому для работы потребуется установить специальный клиент — Aironet Client Utilities. А есть ли смысл его устанавливать? Конечно! Несмотря на продуманность протокола, даже в нем обнаружили уязвимости, позволяющие легко подобрать пароль с помощью перехваченных пакетов LEAP-авторизации. Первым это пронюхал Joshua Wright — разработчик утилиты **ASLEAP**. Эта утилита перехватывает сетевые пакеты при повторном коннекте клиента, после чего брутит пароли для идентификации. Утилита работает нативно под Linux'ом, однако на официальном сайте есть версия программы и под винду (правда, не самого последнего билда)

WifiZoo

Раз воспользовавшись утилитой **WifiZoo**, понимаешь, насколько просто перехватывается различная информация в открытых Wi-Fi сетях. Сама задача утилиты — пассивно собирать различную информацию из сети. Написанная на Python'е (в основе лежит, кстати говоря, лежит программа Scapy), тулза позволяет извлечь из эфира массу полезной для вардрайвера инфы и представить ее в виде красивых графиков. Это не только данные о точках доступа (SSID), но и информация об использующих их клиентах (с указанием адресов отправки и назначения), а также (и это самое вкусное) самая разная инфа, передаваемая в открытом виде по сети: пароли для незащищенных протоколов (pop3/ftp/telnet), почтовый трафик, http кукисы и данные для авторизации, и т.д.

Единственный недостаток **WifiZoo** заключается в отсутствии режима Channel hopping, в результате прога может прослушивать беспроводной интерфейс, но не может прыгать с канала на канал. Этот недостаток с лихвой компенсируется предварительно запущенным **Kismet**'ом. Перехваченные данные утилита бережливо складывает в папку logs/, указывая в названии файлов источник данных (ssids.log, cookies.log, httpauth.log и т.д.). А для большего удобства в комплекте идет GUI-интерфейс, реализованный в виде веб-сервера, который по умолчанию поднимается на 127.0.0.1:8000.

CommView for WiFi

Сайт:
www.tamos.ru/products/commwifi/

Специальная версия известного виндового снифера **CommView**, созданная для захвата и анализа сетевых пакетов в беспроводных сетях 802.11a/b/g/n. Утилита получает информацию от беспроводного сетевого адаптера и сразу декодирует анализируемые данные, отображая их в удобном для переваривания виде. В случае необходимости, пакеты можно дешифровать с использованием пользовательских ключей WEP или WPA-PSK и декодировать вплоть до самого низкого уровня с полным анализом распространенных протоколов (сейчас поддерживается более 70). Более того — можно полностью воссоздать TCP-сессию, и посмотреть, к примеру, HTTP-трафик со всеми запросами и соответственно интересной инфой, вроде данных для авторизации. Весь перехваченный трафик может быть сохранен в файл для последующего анализа. Что особенно радует — так это гибкая система фильтров, которая позволяет отбрасывать ненужные пакеты и перехватывать только то, что нужно. А настраиваемые предупреждения позволяют сообщать пользователю о важных событиях, таких как подозрительные пакеты, высокая загрузка сети или неизвестные адреса. Словом, отличная программа для винды за исключением одного момента — она платная.

Wireless Security Auditor

Сайт: www.elcomsoft.ru

Еще одна платная, но очень любопытная разработка. **Wireless Security**

Auditor позволяет проверить надежность (да, теперь это так называется! WPA/WPA2, но используя современные методики для вычислений с помощью графических процессоров. В дополнение к режиму, когда восстановление производится средствами только центрального процессора, **WSA** использует технологию, которая в процессе восстановления ключа задействует графические акселераторы. Тут надо сказать, что сама программа не перехватывает трафик из беспроводной сети, а имеет дело только дампом сетевых сообщений (поддерживаются форматы TCPDUMP, CommView, PSPR), т.е. работает в связке со снифером. Важно, что для ускорения вычислений подойдет вовсе не любая карта, а только топовые модели ускорителей: NVIDIA (GeForce 8, 9, 200 и выше) или ATI (RADEON HD 3000 Series и выше). EWSA поддерживает атаки по словарю и поддерживает режима мутации пароля (например, слово password заменяет на p@ssword и т.д.)

WirelessKeyView

Сайт:
www.nirsoft.net/utils/wireless_key.html

Уже сам не раз сталкивался с ситуацией, когда тупо забываешь ключ от собственной точки доступа. Кажется, это была строчка из Лермонтова? Черт, или Пушкина? Не помню. Моментально освежить память помогает утилита **WirelessKeyView**, которая вытаскивает из реестра сохраненные в системе WEP/WPA ключи. Приятно, что **WirelessKeyView** работает как сервисом Wireless Zero Configuration в WinXP, так и WLAN AutoConfig, которым пользуются юзеры Висты.