cyber-punk (twitter.com/cyberpunkych)

Боевой смартфон

РУБРИКА MOBILE
ЗАПУСКАЕМ В СЛЕДУЮЩЕМ НОМЕРЕ

HOWTO: КАК ИЗ ДЕВАЙСА НА IOS/ANDROID СДЕЛАТЬ ХАКЕРСКИЙ ИНСТРУМЕНТ

«Смартфон с хакерскими утилитами? Нет такого», — еще недавно сказали бы мы тебе. Запустить привычные инструменты для реализации атак можно было разве что на каком-нибудь Maemo. Теперь же многие инструменты портировали под iOS и Android, а некоторые хак-тулзы были специально написаны для мобильного окружения. Может ли смартфон заменить ноутбук в тестах на проникновение? Мы решили проверить.

ANDROID

Android — популярная платформа не только для простых смертных, но и для правильных людей. Количество полезных][-утилит здесь просто зашкаливает. За это можно сказать спасибо UNIX-корням системы, значительно упростившим портирование многих инструментов на Android. Увы, некоторые из них Google не пускает в Play Store, так что придется ставить соответствующие APK вручную. Также для некоторых утилит нужен максимальный доступ к системе (например, файрволу iptables), поэтому следует заранее позаботиться о root-доступе. Для каждого производителя здесь используется собственная технология, но найти необходимую инструкцию достаточно просто. Неплохой набор HOWTO собрал ресурс LifeHacker (bit.ly/eWgDlu). Однако если какой-то модели тут найти не удалось, на помощь всегда приходит форум XDA-Developers (www.xda-developers.com), на котором можно найти различную информацию фактически по любой модели Android-телефона. Так или иначе, часть из ниже описанных утилит заработают и без root-доступа.

МЕНЕДЖЕР ПАКЕТОВ

BotBrew
bit.ly/Jc0J6N

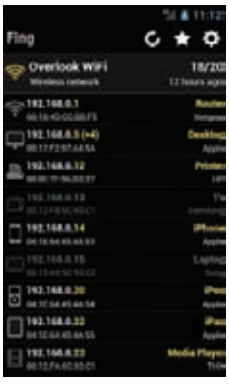
Начнем обзор с необычного менеджера пакетов. Разработчики называют его «утилитами для суперпользователей», и это недалеко от правды. После установки BotBrew ты получаешь репозиторий, откуда можешь загрузить огромное количество скомпилированных под Android привычных инструментов. Среди них: интерпретаторы Python и Ruby для запуска многочисленных инструментов, которые на них написаны, сниффер tcpdump и сканер Nmap для анализа сети, Git и Subversion для работы с системами контроля версий и многое другое.

СЕТЕВЫЕ СКАНЕРЫ

PIPS
bit.ly/OEV0h9

Незаметный смартфон, который в отличие от ноутбука легко помещается в карман и никогда не вызывает подозрений, может быть полезен для исследования сети. Выше мы уже сказали, как можно установить Nmap, но есть еще один вариант. PIPS — это специально адаптированный под Android, хотя и неофициальный порт сканера Nmap. А значит, ты сможешь быстро найти активные устройства в сети, определить их ОС с помощью опций по fingerprinting'у, провести сканирование портов — короче говоря, сделать все, на что способен Nmap.

Fing
bit.ly/zb3hfX

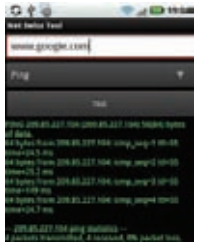


С использованием Nmap'а, несмотря на всю его мощь, есть две проблемы. Во-первых, параметры для сканирования передаются через ключи для запуска, которые надо не только знать, но еще и суметь ввести с неудобной мобильной клавиатуры. А во-вторых, результаты сканирования в консольном выводе не такие наглядные, как того хотелось бы. Этих недостатков лишен сканнер Fing, который очень быстро сканирует сеть, делает fingerprinting, после чего в понятной форме выводит список всех доступных устройств, разделяя их по типам (роутер, десктоп, iPhone и так далее). При этом по каждому хосту можно быстро посмотреть список открытых портов. Причем прямо отсюда можно подключиться, скажем, к FTP, используя установленный в системе FTP-клиент, — очень удобно.

NetAudit
bit.ly/P4imcZ

Когда речь идет об анализе конкретного хоста, незаменимой может оказаться утилита NetAudit. Она работает на любом Android-устройстве (даже нерутованном) и позволяет не только быстро определить устройства в сети, но и исследовать их с помощью большой fingerprinting-базы для определения операционной системы, а также CMS-систем, используемых на веб-сервере. Сейчас в базе более 3000 цифровых отпечатков.

Net Tools
bit.ly/TBqMNu



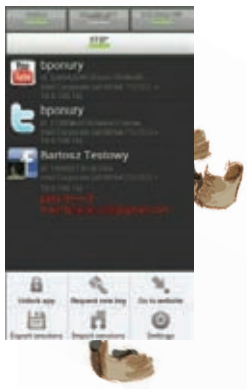
Если же нужно, напротив, работать на уровне ниже и тщательно исследовать работу сети, то здесь не обойтись без Net Tools. Это незаменимый в работе системного администратора набор утилит, позволяющий полностью продиагностировать работу сети, к которой подключено устройство. Пакет содержит более 15 различного рода программ, таких как ping, traceroute, arp, dns, netstat, route.

МАНИПУЛЯЦИИ С ТРАФИКОМ

Shark for Root
bit.ly/wpexhA

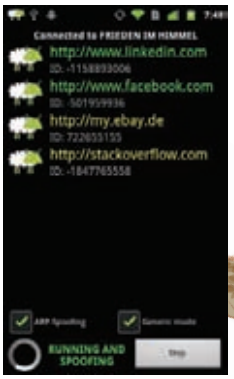
Основанный на tcpdump сниффер честно логирует в pcap-файл все данные, которые далее можно изучить с помощью привычных утилит вроде Wireshark или Network Miner. Так как никакие возможности для MITM-атак в нем не реализованы, это скорее инструмент для анализа своего трафика. К примеру, это отличный способ изучить то, что передают программы, установленные на твой девайс из сомнительных репозиториев.

FaceNiff
bit.ly/eTaedh



Если говорить о боевых приложениях для Android, то одним из самых нашумевших является FaceNiff, реализующий перехват и внедрение в перехваченные веб-сессии. Скачав APK-пакет с программой, можно практически на любом Android-смартфоне запустить этот хек-инструмент и, подключившись к беспроводной сети, перехватывать аккаунты самых разных сервисов: Facebook, Twitter, «ВКонтакте» и так далее — всего более десяти. Угон сессии осуществляется средствами применения атаки ARP spoofing, но атака возможна только на незащищенных соединениях (вклиниваться в SSL-трафик FaceNiff не умеет). Чтобы сдержать поток скриптокидисов, автор ограничил максимальное число сессий тремя.

DroidSheep
bit.ly/qnfJPr



Если создатель FaceNiff хочет за использование денежку, то DroidSheep — это полностью бесплатный инструмент с тем же функционалом. Правда, на официальном сайте ты не найдешь дистрибутива (это связано с суровыми законами Германии по части security-утилит), но его без проблем можно найти в Сети. Основная задача утилиты — перехват пользовательских веб-сессий популярных социальных сетей, реализованный с помощью все того же ARP Spoofing'а. А вот с безопасными подключениями беда: как и FaceNiff, DroidSheep наотрез отказывается работать с HTTPS-протоколом.

Network Spoofer
bit.ly/No4urr

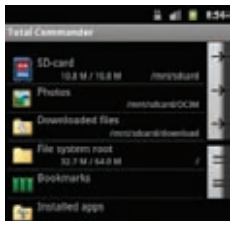
Эта утилита также демонстрирует небезопасность открытых беспроводных сетей, но несколько в другой плоскости. Она не перехватывает пользовательские сессии, но позволяет с помощью спуфинг-атаки пропускать HTTP-трафик через себя, выполняя с ним заданные манипуляции. Начиная от обычных шалостей (заменить все картинки на сайте троллфейсами, перевернуть все изображения или, скажем, подменив выдачу Google) и заканчивая фишинговыми атаками, когда пользователю подсовываются фейковые страницы таких популярных сервисов, как facebook.com, linkedin.com, vkontakte.ru и многих других.

Anti (Android Network Toolkit by zImperium LTD)
bit.ly/LWWqvG

Если спросить, какая хак-утилита для Android наиболее мощная, то у Anti, пожалуй, конкурентов нет. Это настоящий хакерский комбайн. Основная задача программы — сканирование сетевого периметра. Далее в бой вступают различные модули, с помощью которых реализован целый арсенал: это и прослушка трафика, и выполнение MITM-атак, и эксплуатация найденных уязвимостей. Правда, есть и свои минусы. Первое, что бросается в глаза, — эксплуатация уязвимостей производится лишь с центрального сервера программы, который находится в интернете, вследствие чего о целях, не имеющих внешнего IP-адреса, можно забыть.

ТУННЕЛИРОВАНИЕ ТРАФИКА

Total Commander
bit.ly/07SaMk

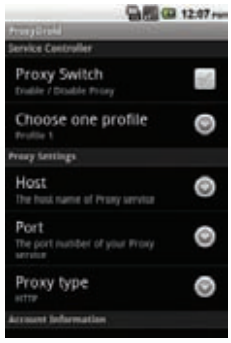


Хорошо известный файловый менеджер теперь и на смартфонах! Как и в настольной версии, тут предусмотрена система плагинов для подключения к различным сетевым директориям, а также канонический двухпанельный режим — особенно удобно на планшетах.

SSH Tunnel
bit.ly/xEiurW

Хорошо, но как обеспечить безопасность своих данных, которые передаются в открытой беспроводной сети? Помимо VPN, который Android поддерживает из коробки, можно поднять SSH-туннель. Для этого есть замечательная утилита SSH Tunnel, которая позволяет завернуть через удаленный SSH-сервер трафик выбранных приложений или всей системы в целом.

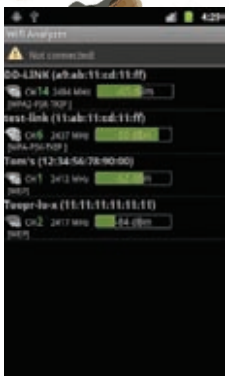
ProxyDroid
bit.ly/HpTI5c



Часто бывает необходимо пустить трафик через прокси или сокс, и в этом случае выручит ProxyDroid. Все просто: выбираешь, трафик каких приложений нужно туннелировать, и указываешь прокси (поддерживаются HTTP/HTTPS/SOCKS4/SOCKS5). Если требуется авторизация, то ProxyDroid это также поддерживает. К слову, конфигурацию можно забиндить на определенную беспроводную сеть, сделав разные настройки для каждой из них.

БЕСПРОВОДНЫЕ СЕТИ

Wifi Analyzer
bit.ly/y7P0Q0



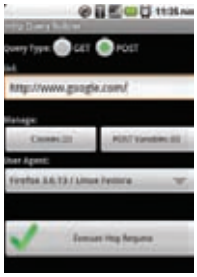
Встроенный менеджер беспроводных сетей не отличается информативностью. Если нужно быстро получить полную картину о находящихся рядом точках доступа, то утилита Wifi Analyzer — отличный выбор. Она не только покажет все находящиеся рядом точки доступа, но и отобразит канал, на котором они работают, их MAC-адрес и, что важнее всего, используемый тип шифрования (увидев заветные буквы «WEP», можно считать, что доступ в защищенную сеть обеспечен). Помимо этого, утилита идеально подойдет, если нужно найти, где физически находится нужная точка доступа, благодаря наглядному индикатору уровня сигнала.

WiFiKill
bit.ly/rf2Hyq

Эта утилита, как заявляет ее разработчик, может быть полезна, когда беспроводная сеть под завязку забита клиентами, а именно в этот момент нужен хороший коннект и стабильная связь. WiFiKill позволяет отключить клиентов от интернета как выборочно, так и по определенному критерию (к примеру, возможно постебаться над всеми яблочниками). Программа всего-навсего выполняет атаку ARP spoofing и перенаправляет всех клиентов на самих себя. Этот алгоритм до глупости просто реализован на базе iptables. Такая вот панель управления для беспроводных сетей фастфуда :).

АУДИТ ВЕБ-ПРИЛОЖЕНИЙ

HTTP Query Builder
bit.ly/RNzgiF



Манипулировать HTTP-запросами с компьютера — плевое дело, для этого есть огромное количество утилит и плагинов для браузеров. В случае со смартфоном все немного сложнее. Отправить кастомный HTTP-запрос с нужными тебе параметрами, например нужной cookie или измененным User-Agent, поможет HTTP Query Builder. Результат выполнения запроса будет отображен в стандартном браузере.

Router Brute Force ADS 2
bit.ly/PawVKA

Если сайт защищен паролем с помощью Basic Access Authentication, то проверить его надежность можно с помощью утилиты Router Brute Force ADS 2. Изначально утилита создавалась для брутфорса паролей на админки роутера, но понятно, что она может быть использована и против любого другого ресурса с аналогичной защитой. Утилита работает, но явно сыровата. К примеру, разработчиком не предусмотрен грубый перебор, а возможен только брутфорс по словарю.

AnDOSid
bit.ly/P4iYiL

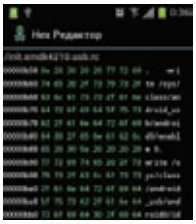
Наверняка ты слышал о такой программе вывода из строя веб-серверов, как Slowloris. Принцип ее действия — создать и удерживать максимальное количество подключений с удаленным веб-сервером, таким образом не давая подключиться к нему новым клиентам. Так вот, AnDOSid — аналог Slowloris прямо в Android-девайсе! Грустно, но двухсот подключений зачастую достаточно, чтобы обеспечить нестабильную работу каждому четвертому веб-сайту на Apache.

РАЗНЫЕ ПОЛЕЗНОСТИ

Encode
bit.ly/PiKVp4

При работе с многими веб-приложениями и анализе их логики достаточно часто встречаются данные, передаваемые в закодированном виде, а именно Base64. Encode поможет тебе раскодировать эти данные и посмотреть, что же именно в них хранится. Возможно, подставив кавычку, закодировав их обратно в Base64 и подставив в URL исследуемого сайта, ты получишь заветную ошибку выполнения запроса к базе данных.

HexEditor
bit.ly/N43hJd



Если нужен шестнадцатеричный редактор, то для Android он тоже есть. С помощью HexEditor ты сможешь редактировать любые файлы, в том числе и системные, если повысишь программе права до суперпользователя. Отличная замена стандартному редактору текстов, позволяющая с легкостью найти нужный фрагмент текста и изменить его.

УДАЛЕННЫЙ ДОСТУП

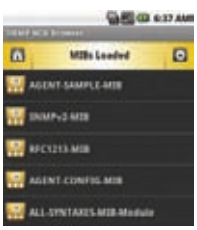
ConnectBot
bit.ly/JaVdQM

Получив доступ к удаленному хосту, нужно иметь возможность им воспользоваться. А для этого нужны клиенты. Начнем с SSH, где стандартом де-факто уже является ConnectBot. Помимо удобного интерфейса, предоставляет возможность организации защищенных туннелей через SSH-подключения.

PocketCloud Remote RDP/VNC
bit.ly/HsRzDE

Полезная программа, позволяющая подключаться к удаленному рабочему столу через сервисы RDP или VNC. Очень радует, что это два клиента в одном, нет необходимости использовать разные тулзы для RDP и VNC.

SNMP MIB Browser
bit.ly/QwL2PN



Специально написанный для Android браузер MIB, с помощью которого можно управлять сетевыми устройствами по протоколу SNMP. Сможет пригодиться для развития вектора атаки на различные маршрутизаторы, ведь стандартные community string (проще говоря, пароль для доступа) для управления через SNMP еще никто не отменял.

IOS

Не менее популярна среди разработчиков security-утилит платформа iOS. Но если в случае с Android права root'а были нужны только для некоторых приложений, то на устройствах от Apple джейлбрейк обязателен почти всегда. К счастью, даже для последней прошивки iДевайсов (5.1.1) уже есть тулза для джейлбрейка. Вместе с полным доступом ты еще получаешь и альтернативный менеджер приложений Cydia, в котором уже собраны многие утилиты.

РАБОТА С СИСТЕМОЙ

MobileTerminal

code.google.com/p/mobileterminal

Первое, с чего хочется начать, — это установка терминала. По понятным причинам в стандартной поставке мобильной ОС его нет, но он нам понадобится, чтобы запускать консольные утилиты, о которых мы далее будем говорить. Лучшей реализацией эмулятора терминала является MobileTerminal — он поддерживает сразу несколько терминалов, жесты для управления (например, для передачи <Ctrl + C>) и вообще впечатляет своей продуманностью.

iSSH

bit.ly/5muhyY

Еще один, более сложный вариант получить доступ к консоли устройства — установить на нем OpenSSH (это делается через Cydia) и локально подключаться к нему через SSH-клиент. Если использовать правильный клиент вроде iSSH, в котором изумительно реализовано управление с сенсорного экрана,— то ты из одного места сможешь работать с локальной консолью и удаленными хостами.

ПЕРЕХВАТ ДАННЫХ

Pirni & Pirni Pro

code.google.com/p/n1mda-dev

Теперь, когда доступ к консоли есть, можно попробовать утилиты. Начнем с Pirni, первого полноценнного сниффера для iOS. Конструктивно ограниченный модуль Wi-Fi, встроенный в iУстройства, невозможно перевести в promiscious-режим, необходимый для нормального перехвата данных. Так что для сниффинга используется классический ARP-спуфинг, с помощью которого весь трафик пропускается через само устройство. Стандартная версия утилиты запускается из консоли, однако есть более продвинутая версия — Pirni Pro, которая может похвастаться графическим интерфейсом. Причем она умеет на лету парсить HTTP-трафик и даже автоматически вытаскивать оттуда интересные данные (к примеру, логины-пароли), используя для этого регулярные выражения, которые задаются в настройках.

Intercepter-NG (console edition)

sniff.su

Небезызвестный сниффер Intercepter-NG с недавнего времени имеет консольную версию, которая работает на iOS и Android. В ней уже реализован граббинг паролей, передаваемых по самым разным протоколам, перехват сообщений мессенджеров, а также воскрешение файлов из трафика. При этом доступны функции сканирования сети и качественный ARP Poison. Для работы необходимо предварительно установить через Cydia пакет libpcap. Вся инструкция по запуску сводится к установке правильных прав: chmod +x intercepter_ios. Далее, если запустить сниффер без параметров, появится понятный интерактивный интерфейс.

Ettercap-NG

https://github.com/TheWorm/Ettercap-NG

Трудно поверить, но этот сложнейший инструмент для реализации MITM-атак все-таки портировали под iOS. После колоссальной работы получилось сделать полноценный мобильный порт. Чтобы избавить себя от танцев с бубном вокруг зависимостей во время самостоятельной компиляции, лучше установить уже собранный пакет, используя Cydia, предварительно добавив в качестве источника данных theworm.altervista.org/cydia. В комплекте идет и утилита etterlog, которая помогает извлечь из собранного дампа трафика различного рода полезную информацию (к примеру, аккаунты к FTP).

АНАЛИЗ БЕСПРОВОДНЫХ СЕТЕЙ

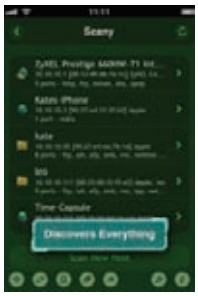
WiFi Analyzer

sites.google.com/site/iphonewifianalyzer

В старых версиях iOS умельцы запускали aircrack и могли ломать WEP-ключ, но мы проверили: на новых устройствах программа не работает. Поэтому для исследования Wi-Fi нам придется довольствоваться только Wi-Fi-сканерами. WiFi Analyzer анализирует и отображает информацию обо всех доступных 802.11 сетях вокруг, включая информацию о SSID, каналах, вендорах, MAC-адресах и типах шифрования. С такой программой легко найти физическое местоположение точки, если ты вдруг его забыл, и, например, посмотреть написанный WPS PIN, необходимый для подключения.

СЕТЕВЫЕ СКАНЕРЫ

Scany
bit.ly/QPHXVx



Какой программой пользуется любой пентестер в любой точке планеты независимо от целей и задач? Сетевым сканером. И в случае с iOS это, скорее всего, будет мощнейший тулкит Scany. Благодаря набору встроенных утилит можно быстро получить подробную картину о сетевых устройствах и, к примеру, открытых портах. Помимо этого пакет включает в себя утилиты тестирования сети, такие как ping, traceroute, nslookup.

Fing
bit.ly/PqNOV3

Впрочем, многие отдают предпочтение Fing'у. Сканер имеет достаточно простой и ограниченный функционал, но его вполне хватит для первого знакомства с сетью, скажем, кафетерия :). В результатах отображается информация о доступных сервисах на удаленных машинах, MAC-адреса и имена хостов, подключенных к сканируемой сети.

Nikto
cirt.net/nikto2

Казалось бы, про Nikto все забыли, но почему? Ведь этот веб-сканер уязвимостей, написанный на скрипт-языке (а именно на Perl), ты легко сможешь установить через Cydia. А это значит, что ты без особого труда сможешь запустить его на своем джейлбрейкнутом устройстве из терминала. Nikto с радостью предоставит тебе дополнительную информацию по испытуемому веб-ресурсу. К тому же ты своими руками можешь добавить в его базу данных знаний собственные сигнатуры для поиска.

УДАЛЕННОЕ УПРАВЛЕНИЕ

SNMP Scan
bit.ly/UJKDbm

Многие сетевые устройства (в том числе дорогие роутеры) управляются по протоколу SNMP. Эта утилита позволяет просканировать подсети на наличие доступных сервисов SNMP с заранее известным значением community string (проще говоря, стандартными паролями). Заметим, что поиск сервисов SNMP со стандартными community string (public/private) в попытке получить доступ к управлению устройствами — неотъемлемая часть любого теста на проникновение наряду с идентификацией самого периметра и выявлением сервисов.

iTap mobile RDP / iTap mobile VNC
bit.ly/OpK1sI

Две утилиты от одного производителя предназначены для подключения к удаленному рабочему столу по протоколам RDP и VNC. Подобных утилит в App Store много, но именно эти особенно удобны в использовании.

ВОССТАНОВЛЕНИЕ ПАРОЛЕЙ

Hydra
bit.ly/UEKK7X

Легендарная программа, помогающая «вспомнить» пароль миллионам хакеров по всему миру, была портирована под iOS. Теперь прямо с iPhone'а возможен перебор паролей к таким сервисам, как HTTP, FTP, Telnet, SSH, SMB, VNC, SMTP, POP3 и многим другим. Правда, для более эффективной атаки лучше запастись хорошими словарями для брутфорса.

PassMule
bit.ly/PbFZkh

Всем не понаслышке известна такая уязвимость, как использование стандартных паролей. PassMule представляет собой своего рода справочник, в котором собраны всевозможные стандартные логины и пароли для сетевых устройств. Они удобно разложены по названиям вендоров, продуктам и моделям, так что найти нужный не составит труда.

ЭКСПЛУАТАЦИЯ УЯЗВИМОСТЕЙ

METASPLOIT
www.metasploit.com

Сложно представить себе более хакерскую утилиту, нежели Metasploit, — и именно она завершает наш сегодняшний обзор. Metasploit — это пакет разнообразных инструментов, основная задача которого заключается в эксплуатации уязвимостей в программном обеспечении. Представь: около 1000 надежных, проверенных и необходимых в повседневной жизни пентестера эксплойтов — прямо на смартфоне! С помощью такого инструмента реально можно обосноваться в любой сети. Metasploit позволяет не только эксплуатировать бреши в серверных приложениях — доступны также инструменты для атак на клиентские приложения (например, через модуль Browser Autopwn, когда в трафик клиентов вставляется боевая нагрузка). Мобильной версии тулкита не существует, однако на Apple-устройство можно установить стандартный пакет, воспользовавшись подробной инструкцией (bit.ly/metasploit_ios).