

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное
учреждение высшего образования
Дальневосточный федеральный университет

ШКОЛА ЕСТЕСТВЕННЫХ НАУК

Кафедра информационной безопасности

О Т Ч Е Т

о прохождении учебной (ознакомительной) практики

Выполнили студенты гр.
С8118-10.05.01ммзи

Ковальчук Е.Е.
Данилов Д.М.
Горынин О.Р.

(подпись)

Отчет защищен с оценкой

Руководитель практики
Старший преподаватель кафедры
информационной безопасности ШЕН

С.С. Зотов

С.С. Зотов

(подпись)

(И.О. Фамилия)

« 31 » _____ июля 2021 г.

(подпись)

(И.О. Фамилия)

Регистрационный № _____

« 31 » _____ июля 2021 г.

Практика пройдена в срок

с « 19 » _____ июля 2021 г.

по « 31 » _____ июля 2021 г.

на предприятии

Кафедра информационной
безопасности ШЕН ДВФУ

(подпись)

Е.В. Третьяк

(И.О. Фамилия)

г. Владивосток
2020

Оглавление	
Задание на практику	3
Введение	4
Протоколы защиты Wi-Fi сетей	5
Почему Linux, а не Windows	7
Утилиты	8
Кrack-что это такое?	20
Вывод:	21
Список используемых литературы и источников	22

Задание на практику

- Рассмотреть наиболее актуальные способы взлома Wi-Fi сетей
- Показать часть утилит, используемых для «хакинга» на Linux
- Узнать способы защиты Wi-Fi сетей
- Объяснить, почему Linux, а не Windows
- На основании проведенного исследования подвести выводы

Введение

В наше время стремительно развиваются беспроводные технологии в области информатизации, так как не всегда удобен, а иногда даже не возможен монтаж проводных линий связи. Но насколько безопасна передача информации по такому виду связи, какие способы хищения и защиты существуют на сегодняшний день, всё это весьма актуально на сегодняшний день. В данной работе проведён анализ беспроводных сетей Wi-Fi открытого и закрытого типа. Показаны, какие факторы влияют на надёжность передаваемой информации в открытой сети. Описаны технологии сетей закрытого типа, как правило, использующие шифрование для защиты пакетов данных в канале передачи информации. Рассмотрим одну из актуальных уязвимостей обхода защитного рубежа точки доступа и успешного произведения атаки типа «человек посередине» - KRACK.

Протоколы защиты Wi-Fi сетей

С развитием беспроводных технологий, наиболее востребованным способом доступа в глобальную сеть интернет и к локальным вычислительным сетям является технология Wi-Fi. Её использование, начинается с появлением ноутбуков, персональных компьютеров, мобильных устройств и заканчивается «умной» бытовой техникой. Данный вид связи значительно упростил доступ к сети пользователям и открыл возможности, недоступные при использовании проводных видов связи, однако не каждый знает, сколько опасности поджидает каждого пользователя при неграмотной настройки использовании Wi-Fi.

Беспроводные сети Wi-Fi делятся на два типа — открытые и закрытые.

Сети открытого типа (OPEN), как правило, не используют защиту для подключения к самому устройству или, используют удалённую защиту доступа к сети, когда аутентификация пользователя происходит не на самом устройстве, а на удалённом сервере. Однако ни один из вышенаписанных способов не защищает пользователей, подключённых к самой Wi-Fi сети от атак типа MITM (человек посередине), это когда вся информация в сети проходит через злоумышленника, что негативно сказывается на надёжности передаваемой информации в открытой сети. Такой вид сети не рекомендуется для использования с точки зрения защиты информации, когда есть необходимость использования данного вида сети для передачи конфиденциальной информации, то рекомендуется использовать VPN (виртуальная частная сеть) для защиты самого канала передачи данных, а также использовать HTTPS (расширенный протокол HTTP использующий шифрование SSL для скрытия запросов от клиента к серверу). Эта технология позволяет просмотреть передаваемые пакеты данных при их перехвате, что повышает надёжность передачи информации в сети Wi-Fi.

Другой вид беспроводной сети — сети закрытого типа, как правило, используют шифрование для защиты пакетов данных в канале передачи информации. Для них используются наиболее популярные технологии защиты такие, как: Wired Equivalent Privacy (WEP — устаревшая технология для обеспечения безопасности беспроводной Wi-Fi сети), Wi-Fi Protected Access (WPA и WPA2 — представляет собой обновлённую технологию защиту устройств беспроводной связи, и Wi-Fi Protected Setup/Quick Security Setup (WPS/QSS — защищённая установка, использующаяся в WPA/WPA2). Надо отметить, что у сети закрытого типа тоже есть уязвимости, но при правильной конфигурации, риски можно минимизировать.

Технология WEP одна из самых первых технологий защиты. В настоящее время крайне ненадёжная и не рекомендуется для использования. Проблема

в том, что поток данных шифруется временным ключом, часть которого есть в каждом пакете. Следовательно, если перехватить необходимое число пакетов, появляется возможность получить ключ любой длины. Защита данной технологии нецелесообразна, так как время перехвата ключа зависит от объёма передаваемой информации по беспроводной сети, чем её больше передаётся, тем быстрее у злоумышленника появляется возможность перехвата ключа.

Технология WPA, которая является суммой протоколов EAP, MIC, TKIP, 802.1X позволяющая её использовать в коммерческом секторе. В отличие от WEP в WPA восстановление основного ключа невозможно, но есть способ узнать ключ, который необходим для проверки целостности, а также ключевой поток данных. Чтобы реализовать такой атаки злоумышленнику необходимо знать MAC адрес клиента, подключённого к Wi-Fi сети, для дальнейшей кражи этого адреса и подмены на своём устройстве, в уязвимой сети Wi-Fi должна быть поддержка WMM и QoS и смена временного ключа не ниже 3600 секунд. Самая простая защита от данного вида уязвимости, просто уменьшить значения временного ключа, что даст гарантию от второго вида взлома — это стандартный брутфорс, то есть, подбор всех возможных комбинаций обычным перебором. Защита от данного метода взлома, ежемесячная смена пароля.

Технология WPA2 дополненная версия технологии WPA. В ней устранена уязвимость с хищением и подменой ключевого потока, так же добавлен новый протокол AES/CCMP с совершенно новым алгоритмом шифрования основанном на AES256 с дополнительной защитой и проверкой на целостность. Данную технологию, возможно, взломать только с помощью брутфорса, защита от которого является ежемесячная смена ключа. WPA2 на сегодняшний день является самым надёжным способом защиты беспроводных сетей Wi-Fi.

Протокол WPS/QSS разработан для создания защищённой WPA2 сети, а так же простому подключению к ней. В данном протоколе предусмотрено подключение по восьми значному PIN-коду. Уязвимость данного протокола заключается в следующем. Так как в PIN-коде используется восемь цифр — подбор PIN-кода составляет 108 вариантов. Последняя цифра является контрольной суммой, которая высчитывается по семи первым цифрам — следовательно, подбор PIN-кода составляет 107. Однако в самом протоколе изначально есть уязвимость, которая позволяет разделить PIN-код на две части, 4 и 3, которые подбираются отдельно друг от друга в таком случае подбор PIN-кода 104 и 103 составляет 11000 комбинаций. Данный протокол крайне уязвим, так как после получения PIN-кода, отсылается информация о ключе WPA2 клиенту, делавшему запрос на подключение, который

впоследствии может быть использован. Однозначного решения проблемы нет, наиболее эффективно, использовать таймер «охлаждения» после неправильного ввода пароля. Рекомендуется отключать данный протокол в настройках сети, для предотвращения кражи ключа WPA2 и несанкционированного подключения к беспроводной сети.

Существует вид атаки под названием «злой двойник», который используется в многолюдных местах. Суть атаки заключается в копирование имени SSID беспроводной сети, и на основании его создаётся поддельная беспроводная сеть с более сильным сигналом излучения, чем у настоящей беспроводной сети. Для уменьшения риска от данной атаки, рекомендуется уменьшить время смены частоты радиоканалов, а также использовать шифрование при передаче данных. Таким образом, на основе проведенного анализа популярных технологий защиты беспроводной сети Wi-Fi, на сегодняшний день наиболее оптимальная технология защиты — это WPA2, внутри которой используется шифрование канала передачи данных. Это позволит пользователям беспроводной сети Wi-Fi защититься от взлома злоумышленников.

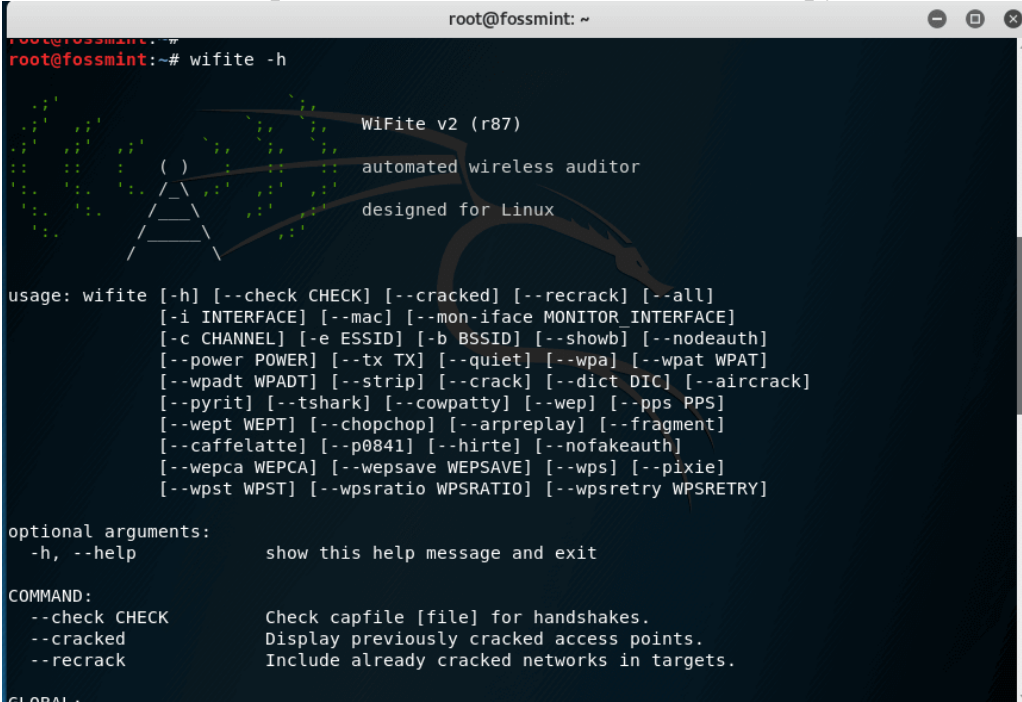
Почему Linux, а не Windows

Какая операционная система лучше подходит для хакинга..Несмотря на то что некоторые операции можно проводить из-под Windows и Mac OS , почти весь инструментарий разработан специально для Linux .Приложения для Linux , которые были разработаны под Linux , а затем перенесены на Windows, могут терять некоторые возможности. Вдобавок, некоторые опции, которые встроены в Linux , недоступны в Windows . По этой причине инструменты хакеров в большинстве случаев разработаны только для Linux .

Утилиты

1. Wifite2

Wifite2 – утилита для аудита Wi-Fi сетей с открытыми исходниками, разработанная на Python для идеальной работы с пентестерскими дистрибутивами. Утилита отлично справляется со снятием маскировки и взломом скрытых точек доступа, взломом слабых паролей WEP с использованием ряда методов хакинга и многим другим.



```
root@fossmint: ~
root@fossmint:~# wifite -h

WiFi v2 (r87)
automated wireless auditor
designed for Linux

usage: wifite [-h] [--check CHECK] [--cracked] [--recreate] [--all]
             [-i INTERFACE] [--mac] [--mon-iface MONITOR_INTERFACE]
             [-c CHANNEL] [-e ESSID] [-b BSSID] [--showb] [--nodeauth]
             [--power POWER] [--tx TX] [--quiet] [--wpa] [--wpa2 WPAT]
             [--wpa2t WPADT] [--strip] [--crack] [--dict DIC] [--aircrack]
             [--pyrit] [--tshark] [--cowpatty] [--wep] [--pps PPS]
             [--wep2t WEPT] [--chopchop] [--arp2p] [--fragment]
             [--caffelatte] [--p0841] [--h1rte] [--nofakeauth]
             [--wepca WEP2A] [--wep2t WEPT] [--wps] [--pixie]
             [--wps2t WPST] [--wpsratio WPSRATIO] [--wpsretry WPSRETRY]

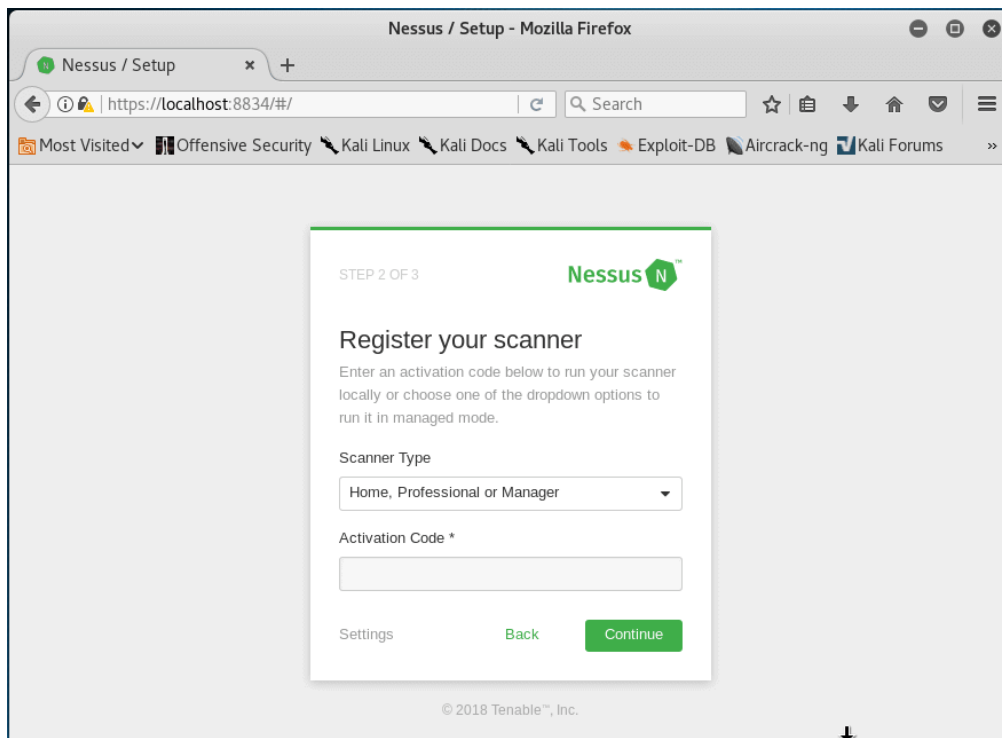
optional arguments:
  -h, --help            show this help message and exit

COMMAND:
  --check CHECK          Check capfile [file] for handshakes.
  --cracked              Display previously cracked access points.
  --recreate             Include already cracked networks in targets.
```

Инструмент аудита беспроводных сетей Wifite

2. Nessus

Nessus – средство удалённого сканирования, которое подходит для проверки компьютеров на наличие уязвимостей. Сканер не делает активной блокировки любых уязвимостей на вашем компьютере, но быстро обнаруживает их благодаря запуску больше 1200 проверок уязвимостей и выдаёт предупреждения о необходимости конкретных исправлений безопасности.



Сканер уязвимостей Nessus

3. Aircrack-ng

Aircrack-ng - инструмент для хакинга беспроводных паролей WEP, WAP и WPA2.

Он перехватывает пакеты из сети, выполняет анализ с помощью восстановленных паролей. У него консольный интерфейс. В дополнение к этому Aircrack-ng использует стандартную FMS-атаку (атаку Фларера-Мантина-Шамира) вместе с несколькими оптимизациями, такими как атаки Ког и PTW, чтобы ускорить процесс, который быстрее WEP.

```

root@fossmint: ~
root@fossmint:~# aircrack-ng

Aircrack-ng 1.2 rc4 - (C) 2006-2015 Thomas d'Otreppe
http://www.aircrack-ng.org

usage: aircrack-ng [options] <.cap / .ivs file(s)>

Common options:

-a <amode> : force attack mode (1/WEP, 2/WPA-PSK)
-e <essid> : target selection: network identifier
-b <bssid> : target selection: access point's MAC
-p <nbcpu> : # of CPU to use (default: all CPUs)
-q        : enable quiet mode (no status output)
-C <macs> : merge the given APs to a virtual one
-l <file>  : write key to file

Static WEP cracking options:

-c        : search alpha-numeric characters only
-t        : search binary coded decimal chr only
-h        : search the numeric key for Fritz!BOX
-d <mask> : use masking of the key (A1:XX:CF:YY)
-m <maddr> : MAC address to filter usable packets
-n <nbits> : WEP key length : 64/128/152/256/512
-i <index> : WEP key index (1 to 4), default: any
-f <fudge> : bruteforce fudge factor, default: 2
-k <korek> : disable one attack method (1 to 17)
-x or -x0 : disable bruteforce for last keybytes
-x1       : last keybyte bruteforcing (default)
-x2       : enable last 2 keybytes bruteforcing
  
```

Сетевая безопасность Wi-Fi в Aircrack-ng

4. Netcat

Netcat, – сетевая утилита, с помощью которой вы используете протоколы TCP/IP для чтения и записи данных через сетевые подключения. Применяется для создания любого типа соединения, а также для исследования и отладки сетей с помощью режима туннелирования, сканирования портов и других фиш.

```
root@fossmint: ~  
root@fossmint:~#  
root@fossmint:~# nc -h  
[v1.10-41.1]  
connect to somewhere: nc [-options] hostname port[s] [ports] ...  
listen for inbound: nc -l -p port [-options] [hostname] [port]  
options:  
-c shell commands as '-e'; use /bin/sh to exec [dangerous!!]  
-e filename program to exec after connect [dangerous!!]  
-b allow broadcasts  
-g gateway source-routing hop point[s], up to 8  
-G num source-routing pointer: 4, 8, 12, ...  
-h this cruft  
-i secs delay interval for lines sent, ports scanned  
-k set keepalive option on socket  
-l listen mode, for inbound connects  
-n numeric-only IP addresses, no DNS  
-o file hex dump of traffic  
-p port local port number  
-r randomize local and remote ports  
-q secs quit after EOF on stdin and delay of secs  
-s addr local source address  
-T tos set Type Of Service  
-t answer TELNET negotiation  
-u UDP mode  
-v verbose [use twice to be more verbose]  
-w secs timeout for connects and final net reads  
-C Send CRLF as line-ending  
-z zero-I/O mode [used for scanning]  
port numbers can be individual or ranges: lo-hi [inclusive];  
hyphens in port names must be backslash escaped (e.g. 'ftp\data').  
root@fossmint:~#
```

Инструмент сетевого анализа Netcat

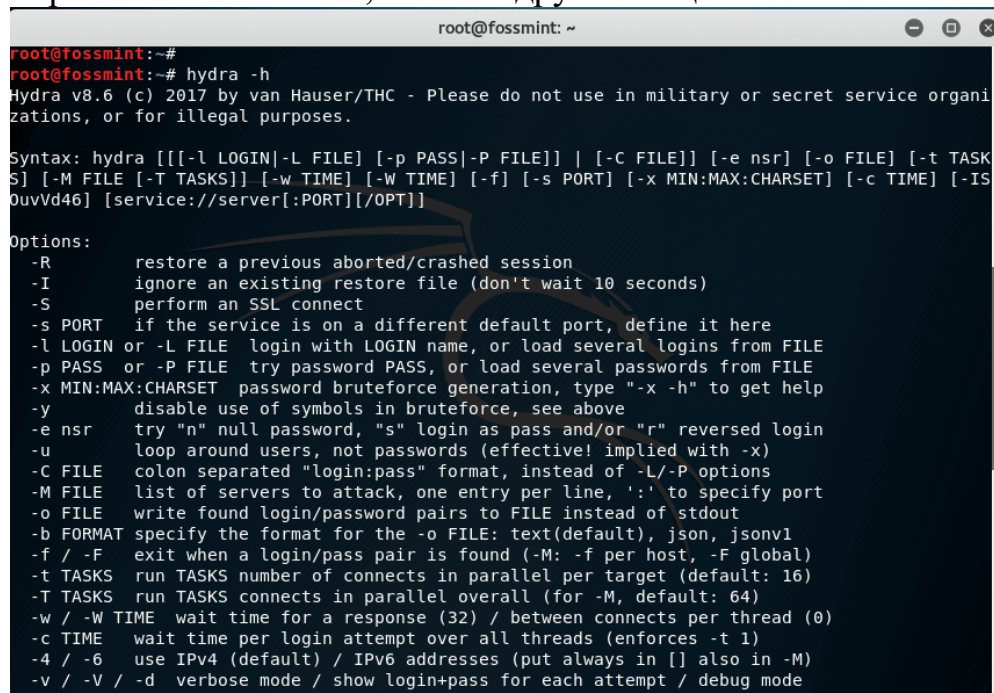
5. Yersinia

Yersinia сетевая утилита, которая разработана для использования уязвимых сетевых протоколов под видом безопасной сетевой системы анализа и тестирования.

```
root@fossmint: ~  
root@fossmint:~# yersinia -h  
Yersinia...  
The Black Death for nowadays networks  
by Slay & tomac  
http://www.yersinia.net  
yersinia@yersinia.net  
Prune your MSTP, RSTP, STP trees!!!!  
Usage: yersinia [-hVGIID] [-l logfile] [-c confille] protocol [protocol_options]  
-V Program version.  
-h This help screen.  
-G Graphical mode (GTK).  
-I Interactive mode (ncurses).  
-D Daemon mode.  
-d Debug.  
-l logfile Select logfile.  
-c confille Select config file.  
protocol One of the following: cdp, dhcp, dot1q, dot1x, dtp, hsrp, isl, mpls, stp, vtp.
```

6. THC Hydra

THC Hydra использует атаку грубым методом для хакинга практически любой удалённой службы аутентификации. Поддерживает скоростные переборы по словарю для 50+ протоколов, включая Telnet, HTTPS и FTP. Используется это средство для взлома веб-сканеров, беспроводных сетей, обработчиков пакетов, Gmail и других вещей.



```
root@fossmint: ~
root@fossmint:~# hydra -h
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Syntax: hydra [[[-l LOGIN|-L FILE] [-p PASS|-P FILE]] | [-C FILE]] [-e nsr] [-o FILE] [-t TASKS] [-M FILE] [-T TASKS]] [-w TIME] [-W TIME] [-f] [-s PORT] [-x MIN:MAX:CHARSET] [-c TIME] [-IS ouVvD46] [service://server[:PORT][:OPT]]

Options:
-R      restore a previous aborted/crashed session
-I      ignore an existing restore file (don't wait 10 seconds)
-S      perform an SSL connect
-s PORT if the service is on a different default port, define it here
-l LOGIN or -L FILE login with LOGIN name, or load several logins from FILE
-p PASS or -P FILE try password PASS, or load several passwords from FILE
-x MIN:MAX:CHARSET password brute-force generation, type "-x -h" to get help
-y      disable use of symbols in brute-force, see above
-e nsr   try "n" null password, "s" login as pass and/or "r" reversed login
-u      loop around users, not passwords (effective! implied with -x)
-C FILE  colon separated "login:pass" format, instead of -L/-P options
-M FILE  list of servers to attack, one entry per line, ':' to specify port
-o FILE  write found login/password pairs to FILE instead of stdout
-b FORMAT specify the format for the -o FILE: text(default), json, jsonv1
-f / -F  exit when a login/pass pair is found (-M: -f per host, -F global)
-t TASKS run TASKS number of connects in parallel per target (default: 16)
-T TASKS run TASKS connects in parallel overall (for -M, default: 64)
-w / -W TIME wait time for a response (32) / between connects per thread (0)
-c TIME  wait time per login attempt over all threads (enforces -t 1)
-4 / -6  use IPv4 (default) / IPv6 addresses (put always in [] also in -M)
-v / -V / -d verbose mode / show login+pass for each attempt / debug mode
```

Hydra – взломщик логинов

7. Pixiewps

Pixiewps – написанный на C оффлайн-инструмент атак методом «грубой силы», который используется для программных реализаций с маленькой или отсутствующей энтропией(неопределенностью).

```
root@fossmint: ~
root@fossmint:~#
root@fossmint:~# pixiewps -h

Pixiewps 1.4 WPS pixie-dust attack tool
Copyright (c) 2015-2017, wiire <wi7ire@gmail.com>

Usage: pixiewps <arguments>

Required arguments:

-e, --pke      : Enrollee public key
-r, --pkr      : Registrar public key
-s, --e-hash1  : Enrollee hash-1
-z, --e-hash2  : Enrollee hash-2
-a, --authkey  : Authentication session key
-n, --e-nonce  : Enrollee nonce

Optional arguments:

-m, --r-nonce  : Registrar nonce
-b, --e-bssid  : Enrollee BSSID
-v, --verbosity : Verbosity level 1-3, 1 is quietest [3]
-o, --output   : Write output to file
-j, --jobs     : Number of parallel threads to use [Auto]

-h           : Display this usage screen
--help      : Verbose help and more usage examples
-V, --version : Display version

--mode N[,... N] : Mode selection, comma separated [Auto]
--start [mm/]yyyy : Starting date (only mode 3) [+1 day]
```

Брутфорс-инструмент для оффлайн-режима Pixiewps

8. Metasploit Framework

Metasploit Framework – платформа с открытым исходным кодом, с помощью которой эксперты по безопасности проверяют уязвимости, а также делают оценку безопасности, чтобы повысить осведомлённость в этой области.

```
root@fossmint: ~
root@fossmint:~# msfconsole -h
Usage: msfconsole [options]

Common options
-E, --environment ENVIRONMENT The Rails environment. Will use RAILS_ENV environment variable if that is set. Defaults to production if neither option not RAILS_ENV environment variable is set.

Database options
-M, --migration-path DIRECTORY Specify a directory containing additional DB migrations
-n, --no-database              Disable database support
-y, --yaml PATH                Specify a YAML file containing database settings

Framework options
-c FILE                        Load the specified configuration file
-v, --version                  Show version

Module options
--defer-module-loads           Defer module loading unless explicitly asked.
-m, --module-path DIRECTORY   An additional module path

Console options:
-a, --ask                      Ask before exiting Metasploit or accept 'exit -y'
-H, --history-file FILE        Save command history to the specified file
-L, --real-readline            Use the system Readline library instead of RbReadline
-o, --output FILE              Output to the specified file
-p, --plugin PLUGIN            Load a plugin on startup
-q, --quiet                    Do not print the banner on startup
-r, --resource FILE            Execute the specified resource file (- for stdin)
-X, --execute-command COMMAND Execute the specified string as console commands (use ; for
```

Инструмент для пентеста Metasploit Framework

9. Nikto2

Nikto2 – опенсорс веб-сканер для исчерпывающего и скоростного тестирования объектов в интернете. Это достигается путём поиска больше 6500 потенциально опасных файлов, устаревших программных версий, уязвимых конфигураций серверов и проблем в этой сфере.

```
root@fossmint: ~  
root@fossmint:~#  
root@fossmint:~# nikto -h  
Option host requires an argument  
  
-config+      Use this config file  
-Display+    Turn on/off display outputs  
-dbcheck     check database and other key files for syntax errors  
-Format+     save file (-o) format  
-Help        Extended help information  
-host+       target host  
-id+         Host authentication to use, format is id:pass or id:pass:realm  
-list-plugins List all available plugins  
-output+     Write output to this file  
-noSSL       Disables using SSL  
-no404       Disables 404 checks  
-Plugins+    List of plugins to run (default: ALL)  
-port+       Port to use (default 80)  
-root+       Prepend root value to all requests, format is /directory  
-ssl         Force ssl mode on port  
-Tuning+     Scan tuning  
-timeout+    Timeout for requests (default 10 seconds)  
-update      Update databases and plugins from CIRT.net  
-Version     Print plugin and database versions  
-vhost+      Virtual host (for Host header)  
+ requires a value  
  
Note: This is the short help output. Use -H for full help text.  
root@fossmint:~#
```

Сканер веб-серверов Nikto

10. Nmap (Network Mapper)

Network Mapper – опенсорсная утилита, предназначенная для разнообразного настраиваемого сканирования IP-сетей с любым количеством объектов, определения состояния объектов сканируемой сети.

```

root@fossmint:~#
root@fossmint:~# nmap -h
Nmap 7.60 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}

TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file

HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PY/PP[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host

SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  -sI <zombie host[:probeport]>: Idle scan
  -sY/sZ: SCTP INIT/COOKIE=ECHO scans
  -sO: IP protocol scan
  -b <FTP relay host>: FTP bounce scan

```

Инструмент Nmap для обнаружения сетей и аудита безопасности

11. Maltego

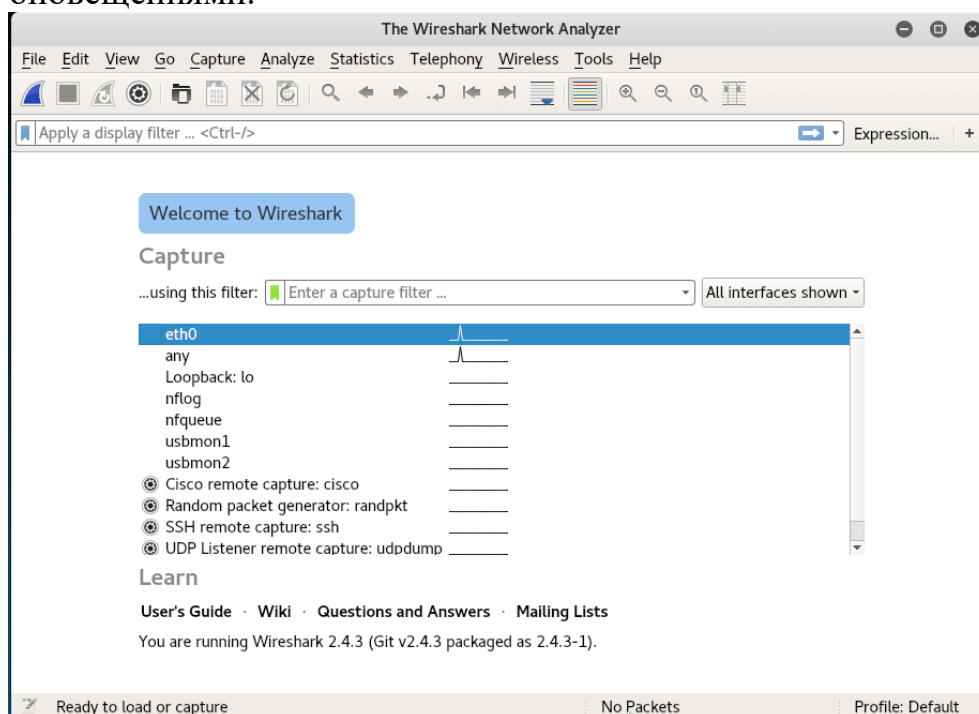
Maltego – авторское программное обеспечение, широко используется для опенсорсной компьютерно-технической экспертизы и разведки. Эта утилита анализа связей с графическим интерфейсом представляет интеллектуальный анализ данных в режиме реального времени, а также иллюстрированные наборы информации с использованием графов на основе узлов и соединений нескольких порядков.



Разведывательный инструмент Maltego

12. Wireshark

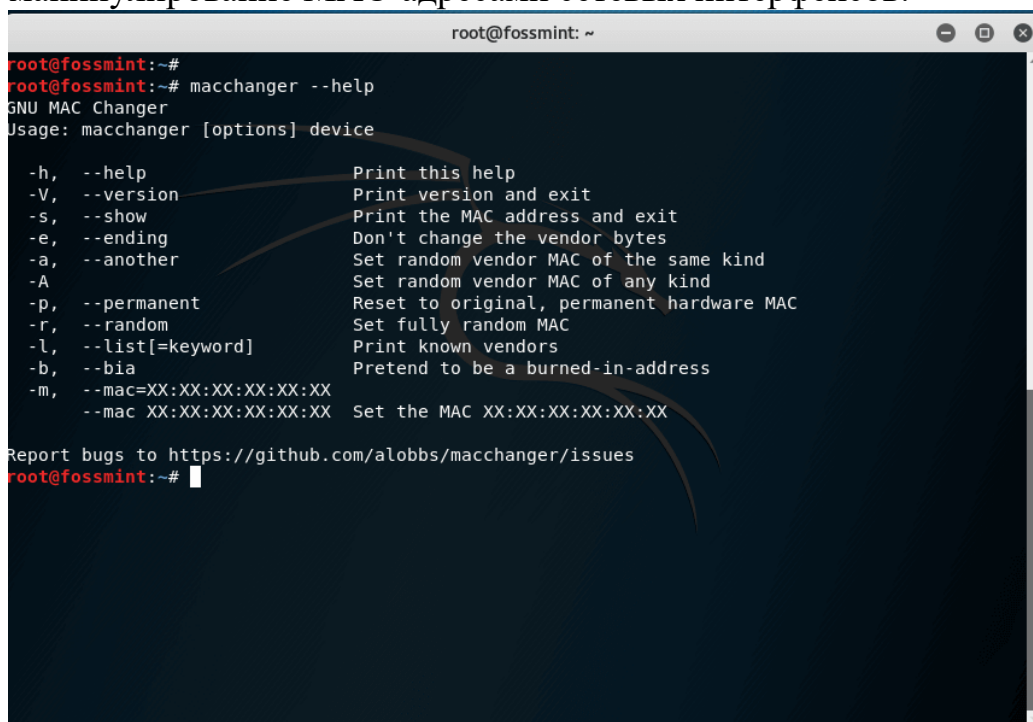
Wireshark – открытый анализатор пакетов. С его помощью просматривается действия в сети на микроскопическом уровне в сочетании с доступом к файлам pcap, настраиваемыми отчётами, расширенными триггерами и оповещениями.



Анализатор трафика сетей Wireshark

13. GNU MAC Changer

GNU MAC Changer – сетевая утилита, которая облегчает и ускоряет манипулирование MAC-адресами сетевых интерфейсов.



GNU MAC Changer

14. John the Ripper (Джон-потрошитель)

John the Ripper – используется в сообществе для оценки безопасности информационных систем или сетей средствами моделирования атаки злоумышленника

```

root@fossmint: ~
root@fossmint:~# john
Created directory: /root/.john
John the Ripper password cracker, version 1.8.0.6-jumbo-1-bleeding [linux-x86-64-avx]
Copyright (c) 1996-2015 by Solar Designer and others
Homepage: http://www.openwall.com/john/

Usage: john [OPTIONS] [PASSWORD-FILES]
--single[=SECTION]           "single crack" mode
--wordlist[=FILE] --stdin    wordlist mode, read words from FILE or stdin
--pipe                       like --stdin, but bulk reads, and allows rules
--loopback[=FILE]           like --wordlist, but fetch words from a .pot file
--dupe-suppression           suppress all dupes in wordlist (and force preload)
--prince[=FILE]             PRINCE mode, read words from FILE
--encoding=NAME              input encoding (eg. UTF-8, ISO-8859-1). See also
                             doc/ENCODING and --list=hidden-options.
--rules[=SECTION]           enable word mangling rules for wordlist modes
--incremental[=MODE]        "incremental" mode [using section MODE]
--mask=MASK                  mask mode using MASK
--markov[=OPTIONS]          "Markov" mode (see doc/MARKOV)
--external=MODE              external mode or word filter
--stdout[=LENGTH]           just output candidate passwords [cut at LENGTH]
--restore[=NAME]            restore an interrupted session [called NAME]
--session=NAME              give a new session the NAME
--status[=NAME]             print status of a session [called NAME]
--make-charset=FILE         make a charset file. It will be overwritten
--show[=LEFT]               show cracked passwords [if =LEFT, then uncracked]
--test[=TIME]               run tests and benchmarks for TIME seconds each
--users[=:]LOGIN|UID[,...]  [do not] load this (these) user(s) only
--groups[=:]GID[,...]      load users [not] of this (these) group(s) only
--shells[=:]SHELL[,...]    load users with[out] this (these) shell(s) only

```

Взломщик паролей John The Ripper

15. Kismet Wireless

Kismet Wireless – система обнаружения вторжений, сетевой детектор и анализатор паролей.


```
root@fossmint: ~
root@fossmint:~# kismet_server -h
Usage: kismet_server [OPTION]
Nearly all of these options are run-time overrides for values in the
kismet.conf configuration file. Permanent changes should be made to
the configuration file.
*** Generic Options ***
-v, --version                Show version
-f, --config-file <file>    Use alternate configuration file
--no-line-wrap              Turn off linewrapping of output
                           (for grep, speed, etc)
-s, --silent                Turn off stdout output after setup phase
--daemonize                Spawn detached in the background
--no-plugins               Do not load plugins
--no-root                  Do not start the kismet_capture binary
                           when not running as root. For no-priv
                           remote capture ONLY.

*** Kismet Client/Server Options ***
-l, --server-listen         Override Kismet server listen options

*** Kismet Remote Drone Options ***
--drone-listen             Override Kismet drone listen options

*** Dump/Logging Options ***
-T, --log-types <types>    Override activated log types
-t, --log-title <title>    Override default log title
-p, --log-prefix <prefix>  Directory to store log files
-n, --no-logging           Disable logging entirely

*** Packet Capture Source Options ***
-c <capture-source>       Specify a new packet capture source
```

Wi-Fi-детектор Kismet

16. Snort

Snort - это система предотвращения вторжений (IPS) с открытым исходным кодом. Snort IPS использует ряд правил, которые помогают определить вредоносную сетевую активность, и использует эти правила для поиска пакетов, которые соответствуют им, и генерирует предупреждения для пользователей.

```
root@fossmint: ~
root@fossmint:~# snort -h
snort: option requires an argument -- 'h'

    _ _ _
   / _ _\~
  (o"  )~
   ' _ _'

-*> Snort! <*-
Version 2.9.7.0 GRE (Build 149)
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using libpcap version 1.8.1
Using PCRE version: 8.39 2016-06-14
Using ZLIB version: 1.2.8

USAGE: snort [-options] <filter options>
Options:
-A          Set alert mode: fast, full, console, test or none (alert file alerts only)
            "unsock" enables UNIX socket logging (experimental).
-b          Log packets in tcpdump format (much faster!)
-B <mask>   Obfuscated IP addresses in alerts and packet dumps using CIDR mask
-c <rules>  Use Rules File <rules>
-C          Print out payloads with character data only (no hex)
-d          Dump the Application Layer
-D          Run Snort in background (daemon) mode
-e          Display the second layer header info
-f          Turn off fflush() calls after binary log writes
-F <bpf>    Read BPF filters from file <bpf>
-g <gname>  Run snort gid as <gname> group (or gid) after initialization
-G <oxid>   Log Identifier (to uniquely id events for multiple snorts)
-h <hn>     Set home network = <hn>
            (for use with -l or -B, does NOT change $HOME_NET in IDS mode)
-H          Make hash tables deterministic.
```

Средство предотвращения сетевых вторжений Snort

17. Hashcat

Hashcat - инструмент для восстановления паролей. Он используется для подбора паролей на основе хэша, генерируя комбинации для атаки методом перебора

```
root@fossmint: ~/Downloads
root@fossmint:~/Downloads# hashcat --help
hashcat - advanced password recovery

Usage: hashcat [options]... hash[hashfile|hccapxfile [dictionary|mask|directory]]...

- [ Options ] -

Options Short / Long      | Type | Description
-----
-m, --hash-type           | Num  | Hash-type, see references below
-m 1000
-a, --attack-mode         | Num  | Attack-mode, see references below
-a 3
-V, --version             |      | Print version
-h, --help                |      | Print help
--quiet                  |      | Suppress output
--hex-charset            |      | Assume charset is given in hex
--hex-salt               |      | Assume salt is given in hex
--hex-wordlist            |      | Assume words in wordlist are given in hex
--force                  |      | Ignore warnings
--status                 |      | Enable automatic update of the status screen
--status-timer           | Num  | Sets seconds between status screen updates to X
--status-timer=1
--machine-readable       |      | Display the status view in a machine-readable format
--keep-guessing          |      | Keep guessing the hash after it has been cracked
--loopback               |      | Add new plains to induct directory
--weak-hash-threshold    | Num  | Threshold X when to stop checking for weak hashes
```

Средство восстановления паролей Hashcat

18. Fern Wifi Cracker

Fern Wifi Cracker – инструмент защиты в сетях Wi-Fi с графическим пользовательским интерфейсом, написанный на Python и предназначенный для аудита уязвимостей сети. Используется для взлома и восстановления ключей WEP/WPA/WPS, а также для атак на Ethernet-сети.



Fern Wifi Cracker

19. Burp Suite Scanner

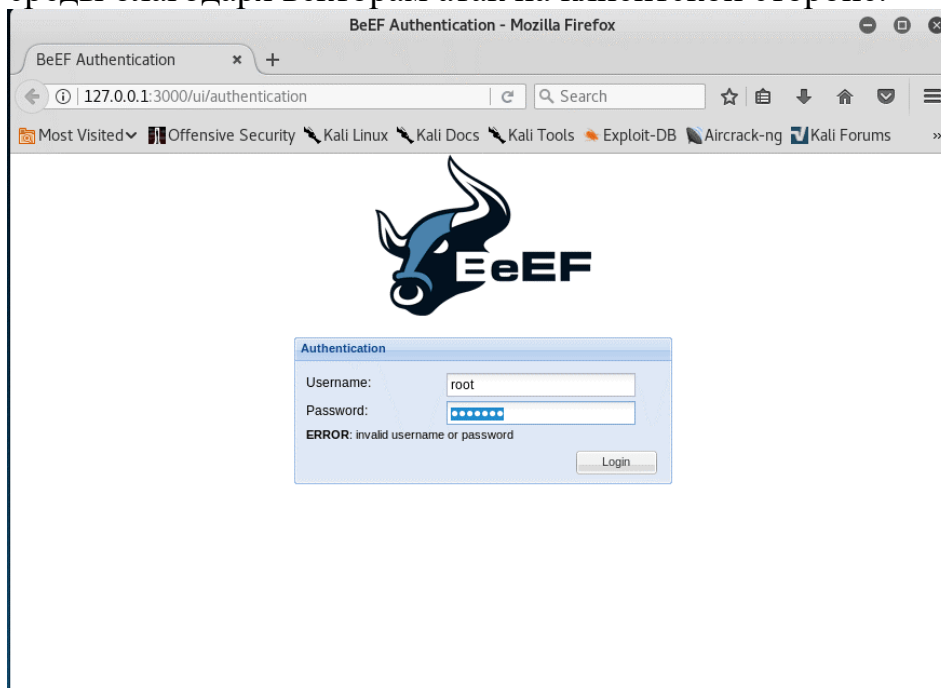
Burp Suite Scanner – профессиональная интегрированная графическая платформа для тестирования уязвимостей в веб-приложениях.



Сканер уязвимостей Burp Security

20. BeEF (Browser Exploitation Framework)

BeEF, – инструмент проникновения, который фокусируется на уязвимостях браузера. С помощью него выполняется оценка уровня безопасности целевой среды благодаря векторам атак на клиентской стороне.



Кrack-что это такое?

Специалисты по информационной безопасности обнаружили критическую уязвимость в самом популярном протоколе защиты WI-FI WPA2 и дали название KRACK. Эта уязвимость позволяет атакующим обходить защитный рубеж точки доступа и успешно проводить атаки типа «человек посередине» которые характеризуются возможностью прослушивания трафика пользователя.

Технология беспроводного подключения к точке доступа устроена таким образом, что в момент подключения пользователем осуществляется четырехэлементный хэндшейк, который подтверждает, что клиент и точка доступа обладают корректными учетными данными. А также «хэндшейк» согласовывает свежий ключ шифрования, предназначенный для защиты трафика.

Злоумышленник, используя уязвимость, принуждает участников реинсталлировать ключи шифрования. Это приводит к тому, что злоумышленник, успешно совершив атаку, может беспрепятственно прослушивать трафик и манипулировать им по собственному усмотрению. Проблема усугубляется тем, что данной уязвимости подвержены практически все устройства, подключенные к Wi-Fi сети вне зависимости от типа устройства, операционной системы и марки производителя.

Чтобы обезопасить от данной уязвимости необходимо соблюдать несколько базовых правил:

- Использовать защищенное соединение HTTPS. Это не панацея, потому что сбросить HTTPS-соединение злоумышленнику не составит особого труда. Поэтому следует обращать внимание и на зеленую иконку замка в адресной строке браузера. Ее наличие означает, что подключение защищено;
- Использование VPN-соединения позволит создать еще один рубеж защиты. Трафик в этом случае передается не напрямую, а через защищённый канал;
- Следить за обновлениями ПО как на устройстве пользователя, так и на самих точках доступа. Многие производители оборудования уже исправили данную уязвимость.

Из-за того, что рассматриваемой атаке подвержены практически все устройства, подключенные к Wi-Fi-сети, проблема имеет массовый характер и может коснуться практически любого пользователя. Ни одна система защиты не способна обеспечить твердую уверенность в том, что уязвимость не будет использована. Приведенные рекомендации позволяют до минимума снизить риск проведения такой атаки и обезопасить данные пользователей.

Вывод:

Выполняя данную научную работу, мы исследовали протоколы защиты сетей Wi-Fi, ознакомились с их актуальностью и уязвимостями, выдвинули пути временного решения некоторых проблем. Узнали дополнительные утилиты для работы со взломами на Linux-оидных системах и определили, почему на Linux работать удобней, чем на Windows. Ознакомились с одной из самых актуальных и сложно-решаемых атак Krack. И выяснили, что вид устройства или системы никак не влияет на защиту устройства от атак.

Список используемых литературы и источников

- <https://www.elibrary.ru/>
- [Варлатая, С. К. Анализ методов защиты беспроводной сети Wi-Fi от известных способов взлома злоумышленником // Молодой ученый. — 2015. — № 1 \(81\). — С. 36-37. — URL: https://moluch.ru/archive/81/](#)
- <https://www.phdays.com/ru/>
- <https://www.elibrary.ru/item.asp?id=36712221>
- <https://www.elibrary.ru/item.asp?id=42765753>
- <https://www.kaspersky.ru/blog/krackattack/19022/>
- <https://www.youtube.com/watch?v=Oh4WURZoR98>
- https://elibrary.ru/download/elibrary_30719199_38478982.pdf