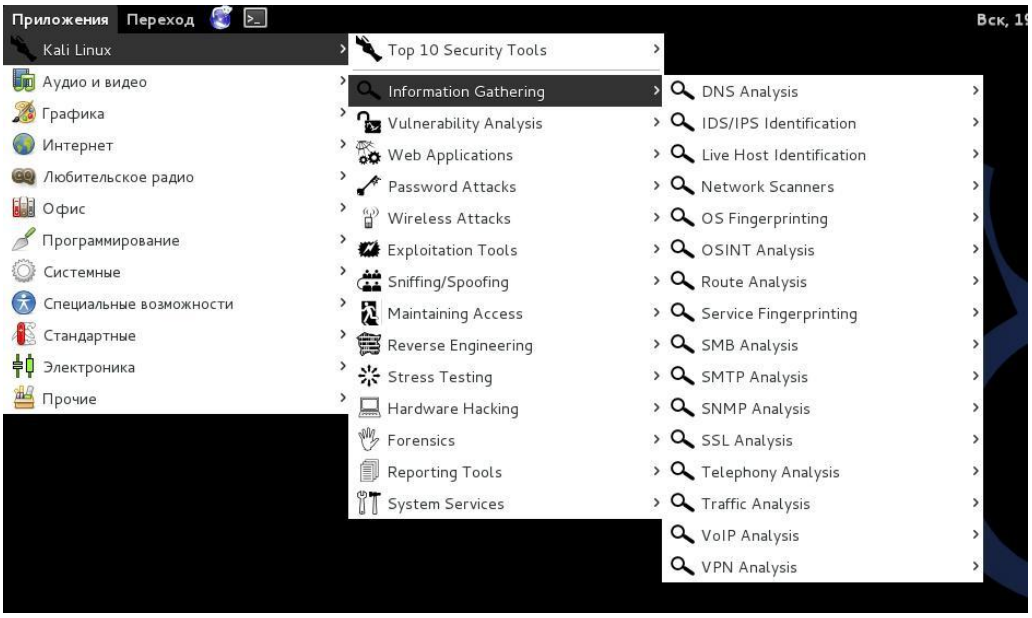
Л8. Процесс выявления и анализа критических недостатков безопасности в Kali Linux

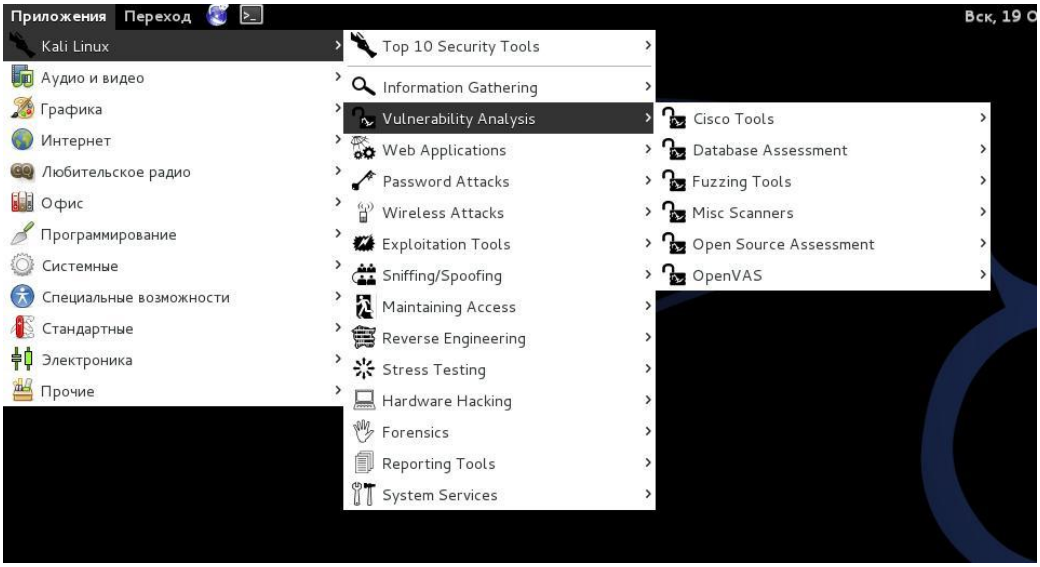
Программ направленных на решение разнообразных задачи в Kali Linux очень много, и хотя они сгруппированы по разделам, глаза всё равно разбегаются, особенно при первом знакомстве.

Information Gathering



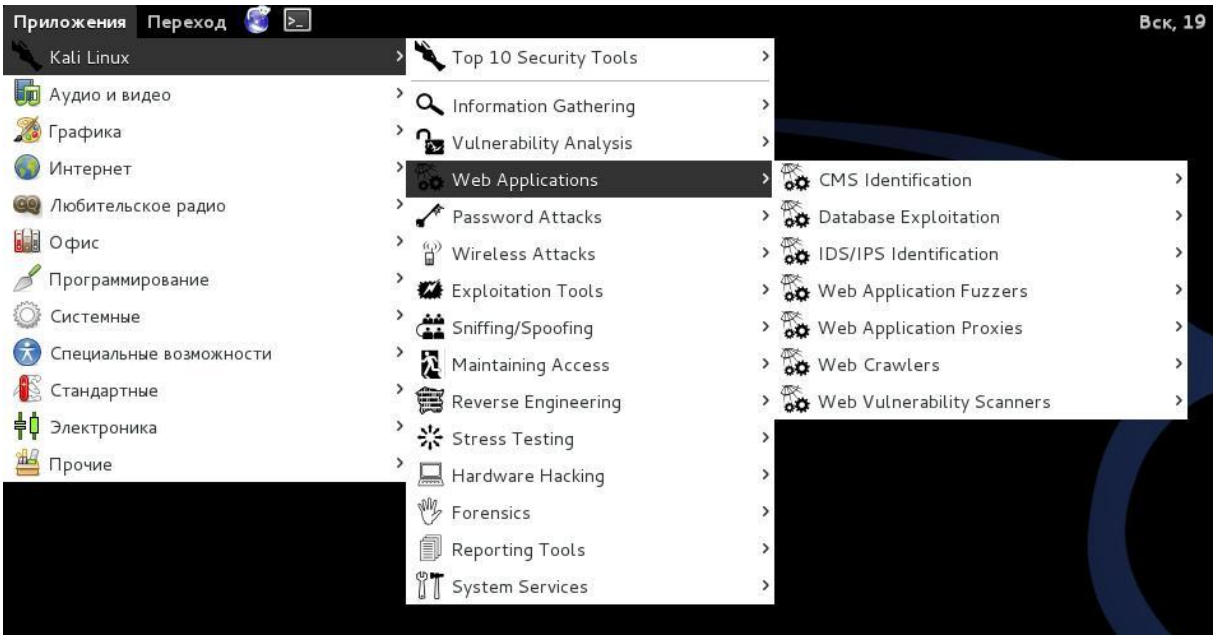
Эти инструменты для разведки используются для сбора данных по целевой сети или устройствам. Инструменты охватывают от идентификаторов устройств до анализа используемых протоколов.

Vulnerability Analysis



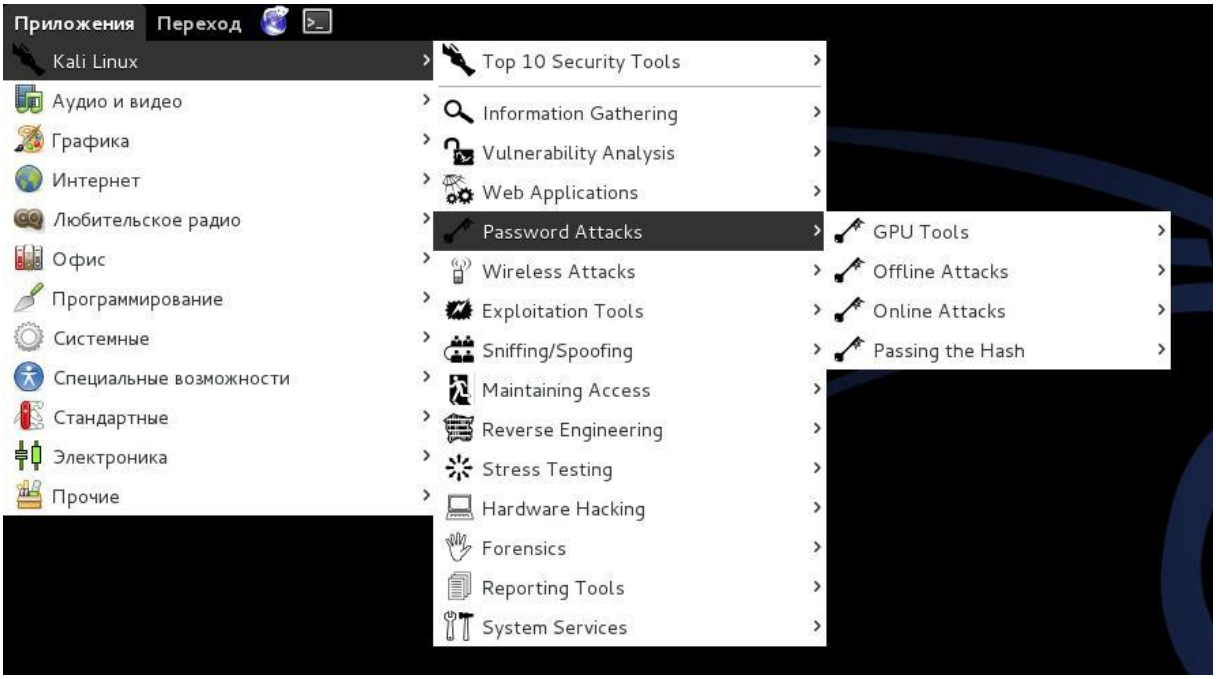
Инструменты из этой секции фокусируются на оценке систем в плане уязвимостей. Обычно, они запускаются в соответствии с информацией, полученной с помощью инструментов для разведки (из раздела Information Gathering).

Web Applications



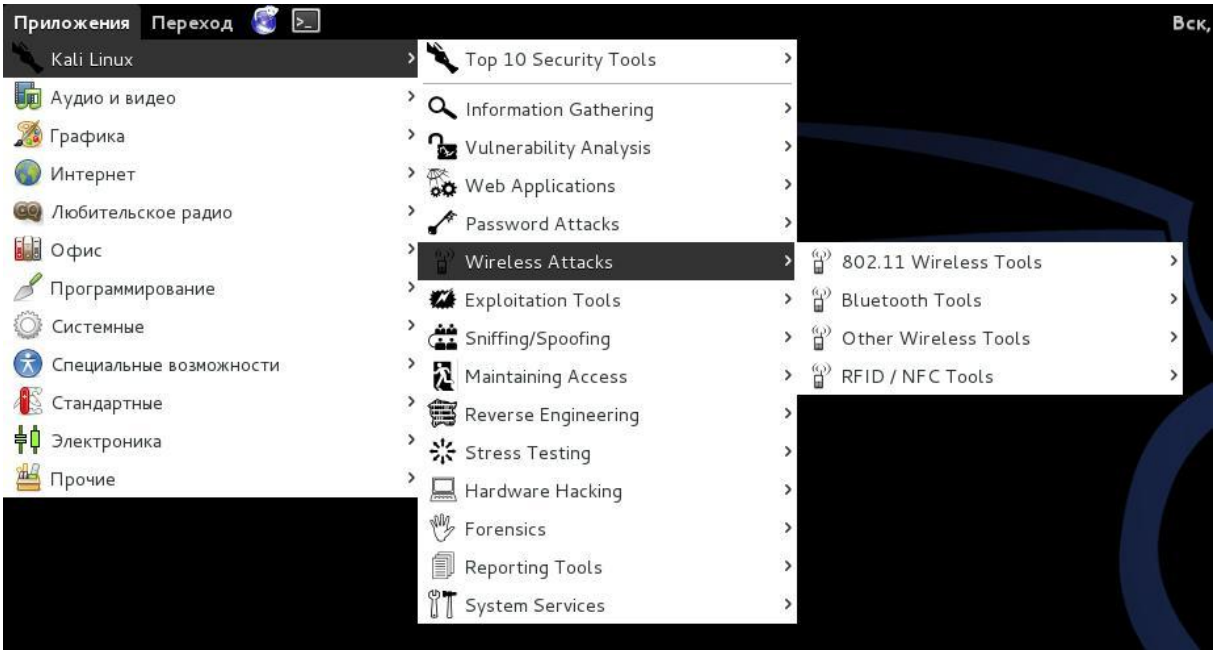
Эти инструменты используются для аудита и эксплуатации уязвимостей в веб-серверах. Многие из инструментов для аудита находятся прямо в этой категории. Как бы там ни было, не все веб-приложения направлены на атаку веб-серверов, некоторые из них просто сетевые инструменты. Например, веб-прокси могут быть найдены в этой секции.

Password Attacks



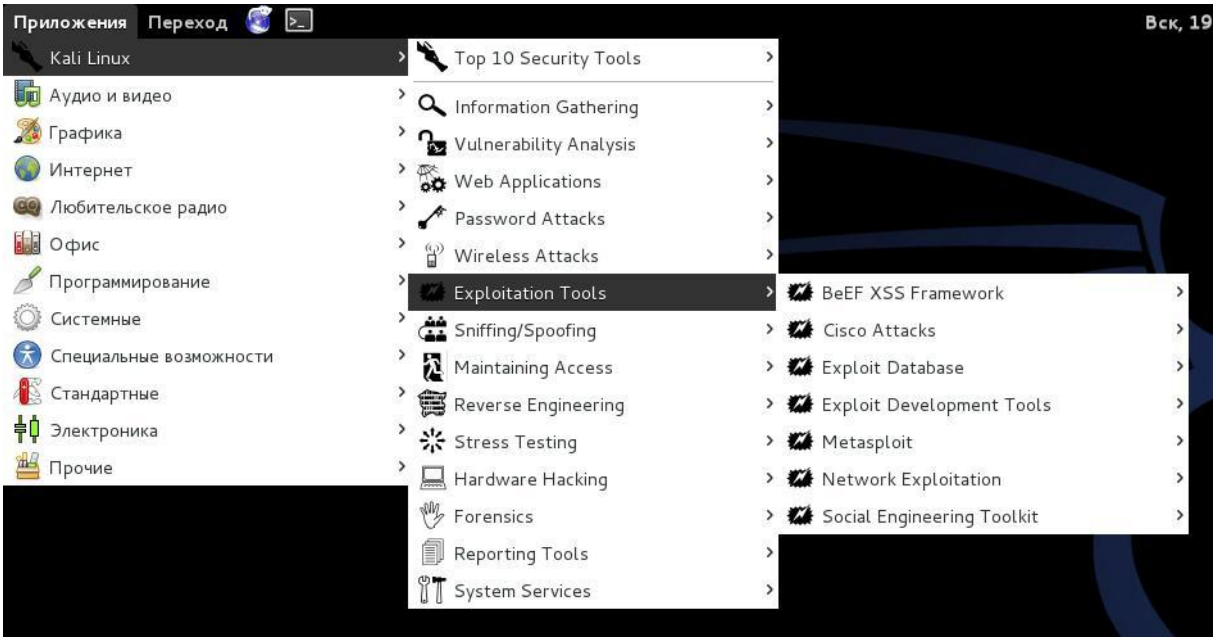
Эта секция инструментов, главным образам имеющих дело с брутфорсингом (перебором всех возможных значений) или вычисления паролей или расшаривания ключей используемых для аутентификации.

Wireless Attacks



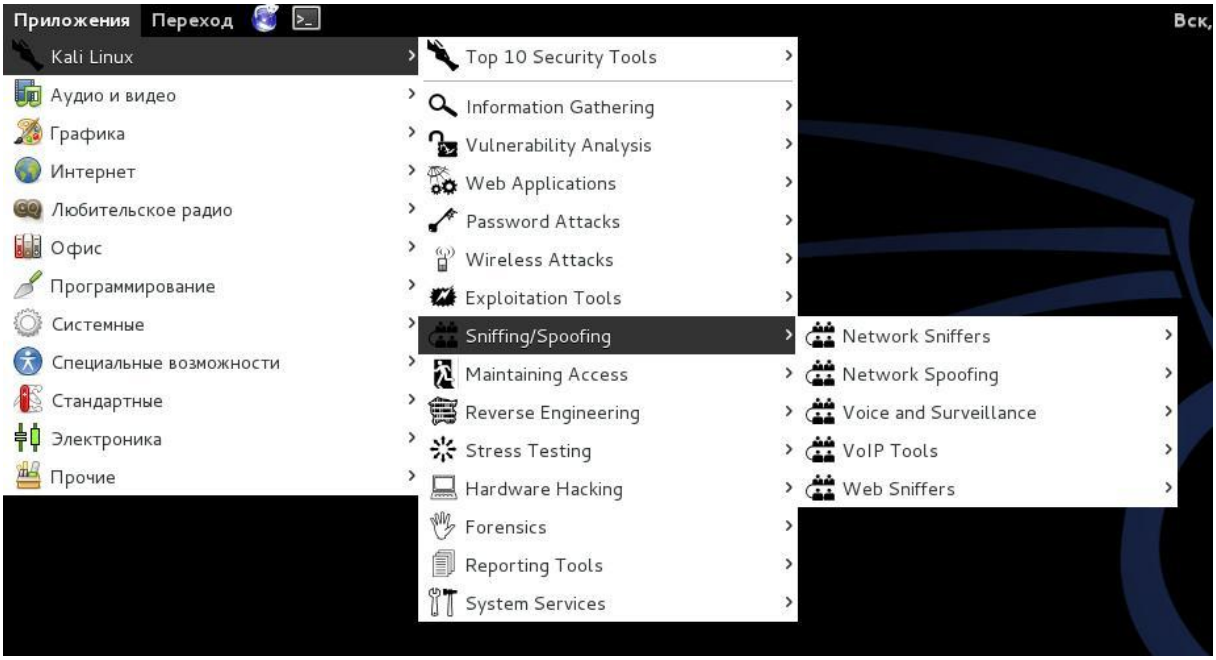
Эти инструменты используются для эксплуатации уязвимостей найденных в беспроводных протоколах. Инструменты 802.11 будут найдены здесь, включая инструменты, такие как aircrack, airmon и инструменты взлома беспроводных паролей. В дополнение, эта секция имеет инструменты связанные также с уязвимостями RFID и Bluetooth. Во многих случаях, инструменты в этой секции нужно использовать с беспроводным адаптером, который может быть настроен Kali в состояние прослушивания.

Exploitation Tools



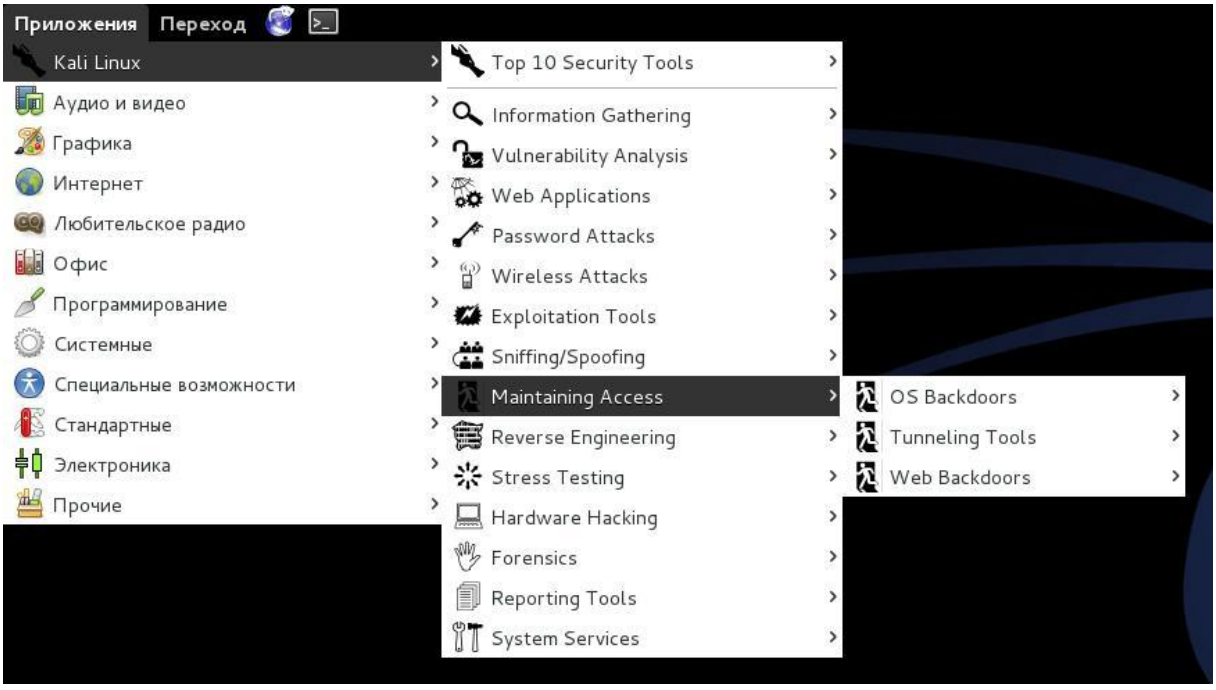
Эти инструменты используются для эксплуатации уязвимостей найденных в системах. Обычно уязвимости идентифицируются во время оценки уязвимостей (Vulnerability Assessment) цели.

Sniffing and Spoofing



Эти инструменты используются для захвата сетевых пакетов, манипуляции с сетевыми пакетами, создания пакетов приложениями и веб подмены (spoofing). Есть также несколько приложений реконструкции VoIP

Maintaining Access

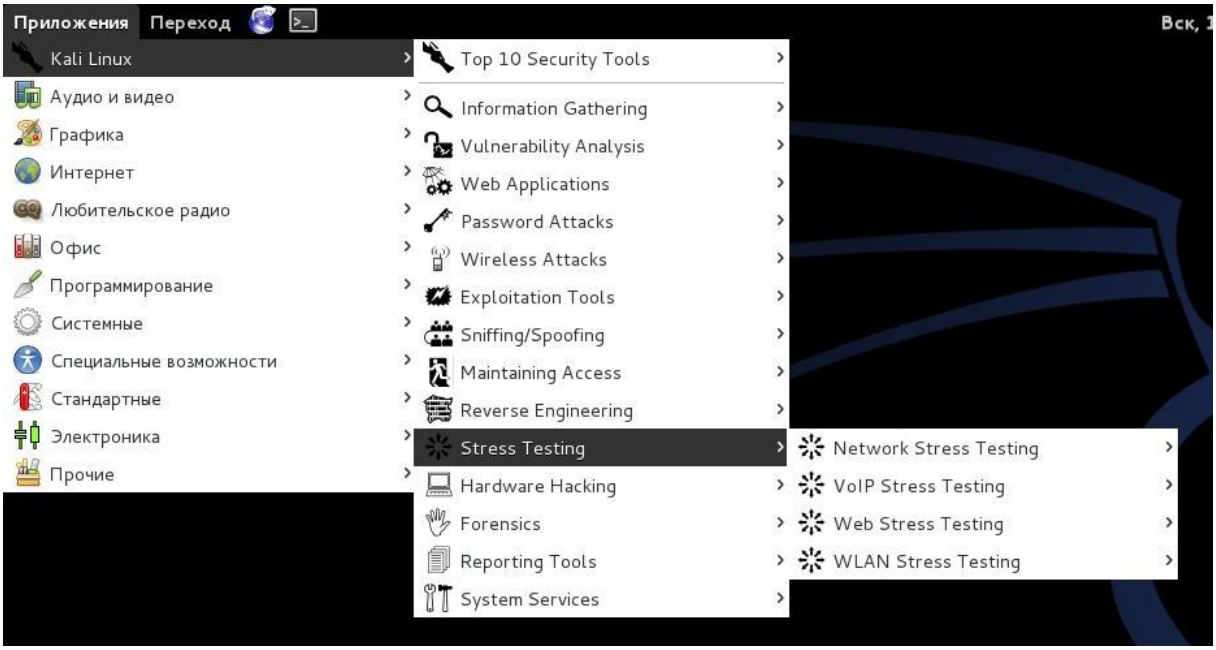


Инструменты поддержки доступа (Maintaining Access) используются как плацдарм и устанавливаются в целевой системе или сети. Обычное дело найти на скомпрометированных системах большое количество бэкдоров и других способов контроля атакующим, чтобы обеспечить альтернативные маршруты на тот случай, если уязвимость, которой воспользовался атакующий, будет найдена или устранена.

Reverse Engineering

Эти инструменты используются для модификации, анализа, отладки (debug) программ. Цель обратной инженерии — это анализ как программа была разработана, следовательно, она может быть скопирована, модифицирована, использована для развития других программ. Обратная инженерия также используется для анализа вредоносного кода, чтобы выяснить, что исполняемый файл делает, или попытаться исследователями найти уязвимости в программном обеспечении.

Stress Testing

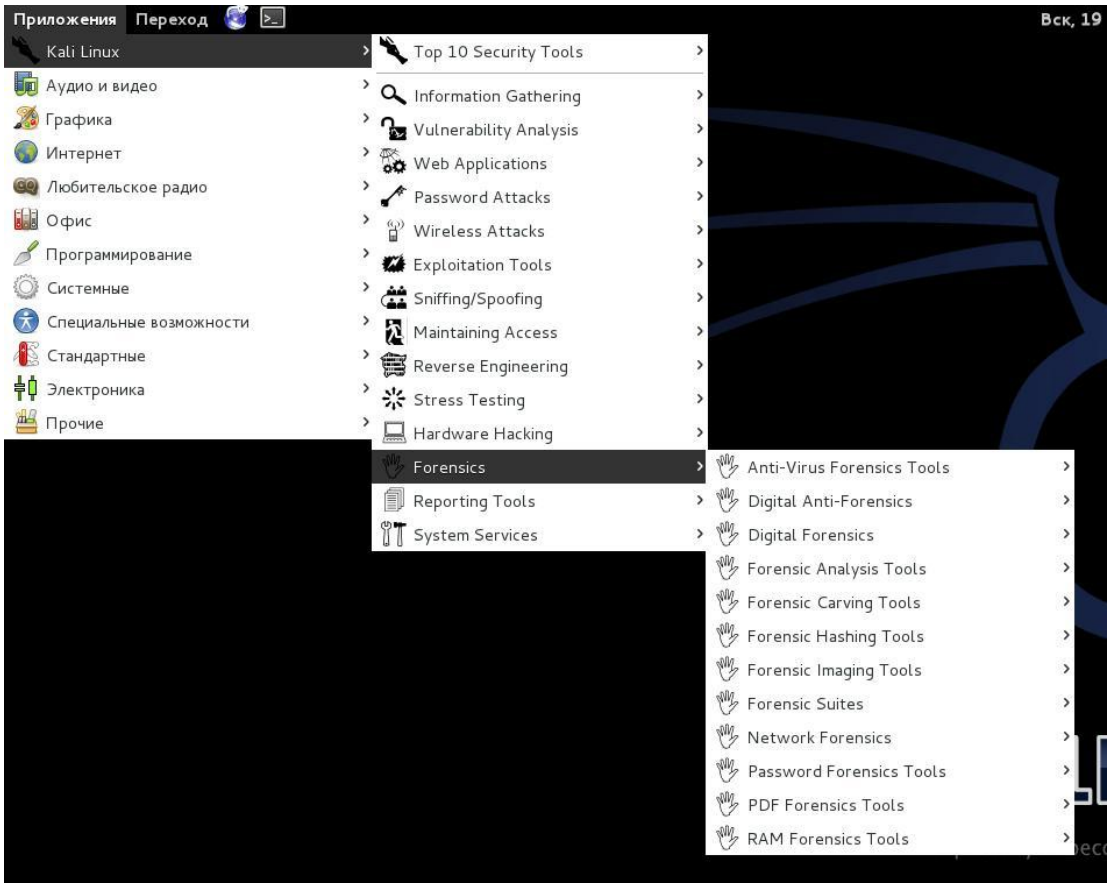


Инструменты для стресс тестинга (Stress Testing) используются для вычисления как много данных система может «переварить». Нежелательные результаты могут быть получены от перегрузки системы, такие как стать причиной открытия всех коммуникационных каналов устройством контроля сети или отключения системы (также известное как атака отказа в обслуживании).

Hardware Hacking

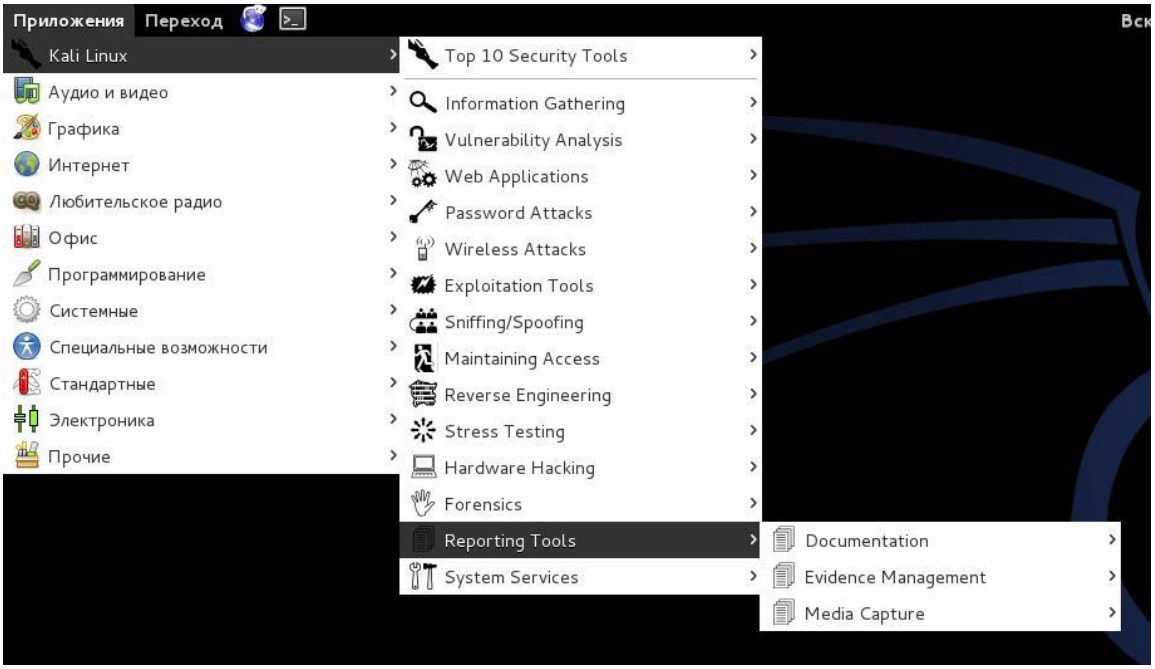
Эта секция содержит инструменты для Android, которые могут быть классифицированы как мобильные и инструменты Android, которые используются для программирования и контроля маленьких электронных устройств

Forensics



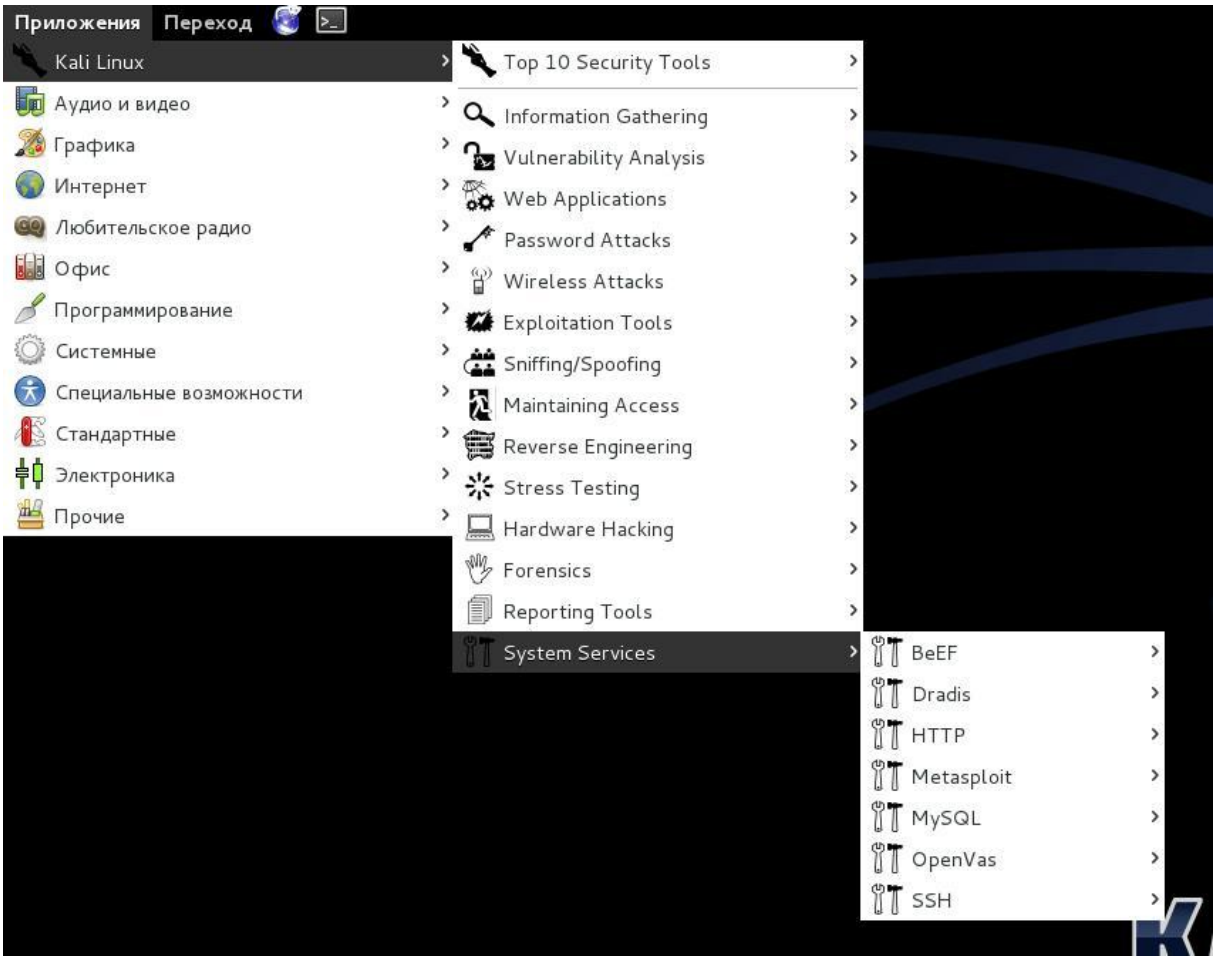
Инструменты криминалистики (Forensics) используются для мониторинга и анализа компьютера, сетевого трафика и приложений.

Reporting Tools



Инструменты для отчётов (Reporting tools) — это методы доставки информации, найденной во время исполнения проникновения.

System Services



Здесь вы можете включить или отключить сервисы Kali. Сервисы сгруппированы в BeEF, Dradis, HTTP, Metasploit, MySQL, и SSH.

В сборку Kali Linux включены также и другие инструменты, например, веб-браузеры, быстрые ссылки на тюнинг сборки Kali Linux, которые можно увидеть в других разделах меню (сеть, инструменты поиска и другие полезные приложения).

Глава 15. Обзор разделов инструментов Kali Linux 1.1.0. Часть 2. Инструменты для сбора информации

Здесь обзор только НЕКОТОРЫХ утилит. На самом деле, программ намного-намного больше. Мы обходим стороной такие вопросы, как использование для сбора информации данных, например, полученных через запросы в Гугл, анализ истории сайта в веб-архивах, анализа доступной информации (объявления о приёме на работу и т. д.), использование базовых утилит для пинга и определение маршрутов. Это всё важно, и это нужно изучать отдельно! Но непосредственно к Kali Linux это не имеет прямого отношения, поэтому данные вопросы пропущены.

1. HTTrack – клонируем веб-сайт

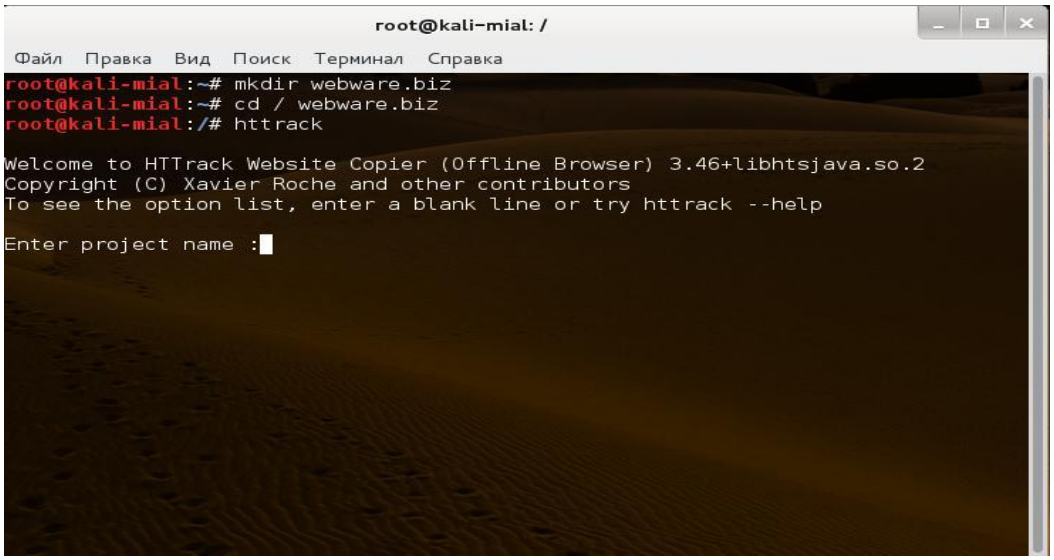
Данная программа сохраняет копию веб-сайта на жёсткий диск. Понятно, что она не сможет скачать скрипты PHP и базы данных. Но анализируя структуру каталогов, размещения страниц и пр. можно сделать определённые выводы, которые будут способствовать разработке стратегии проникновения.

Эта программа установлена не на всех версиях Kali Linux, если у вас её нет, то наберите в командной строке:

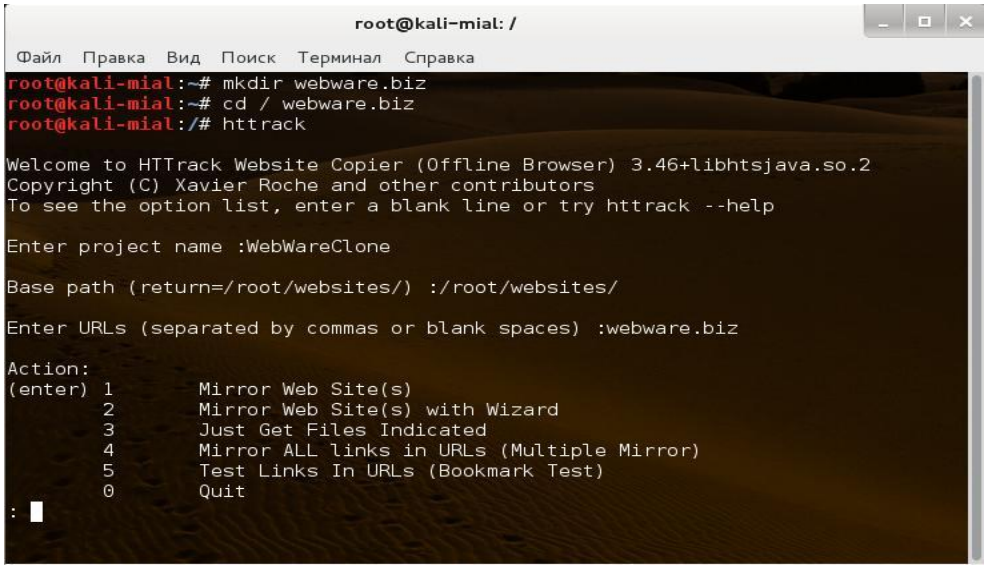
```
1| apt-get install httrack
```

Теперь там же, в терминале, создаём каталог для нашего нового сайта, переходим в этот каталог и запускаем HTTrack:

```
1| mkdir webware.biz
2| cd / webware.biz
3| httrack
```

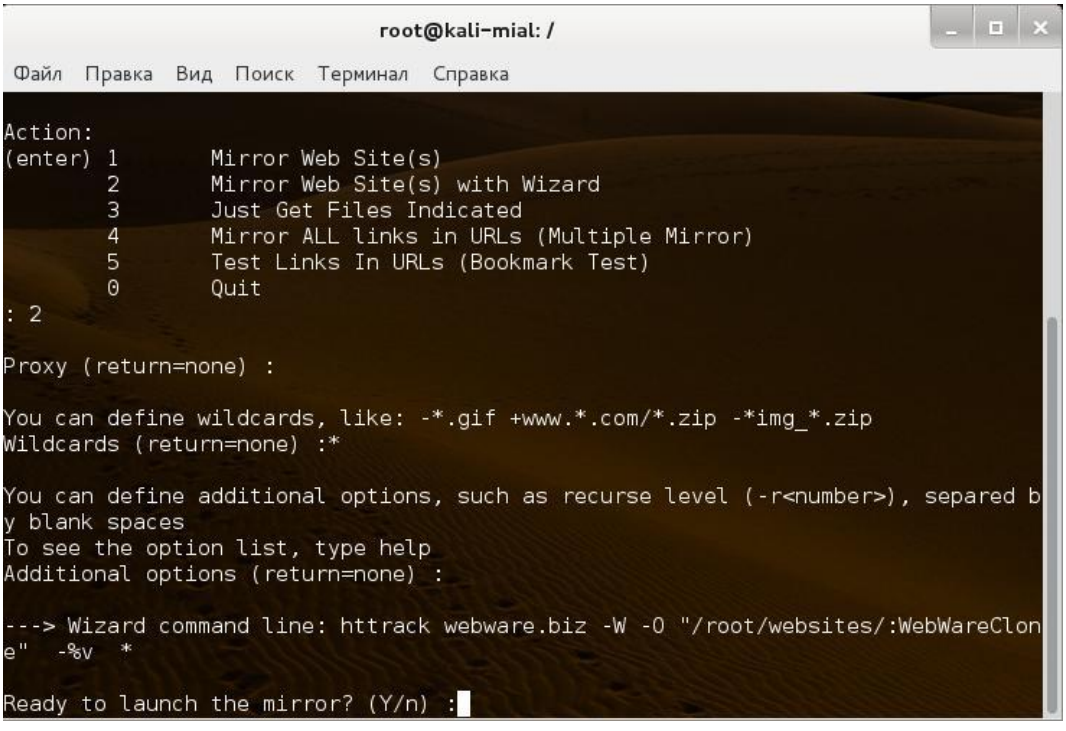


Задаём имя проекта, базовый каталог, вводим URL (адрес сайта) — адрес сайта может быть любым, WebWare.biz взят только для примера, и нам на выбор предоставляется несколько опций:



1|	1. Создать зеркало сайта (сайтов)
2|	2. Создать зеркало сайта (сайтов) с мастером
3|	3. Просто получить указанные файлы
4|	4. Сделать зеркало всех ссылок в URL
5|	5. Протестировать ссылки в URL (Тест закладок)
6|	0. Выход

Самая простая опция — вторая. У нас спрашивают о прокси, Далее спрашивается, какие файлы мы хотим скачать — чтобы скачать всё, поставьте звёздочку (*), мы можем задать дополнительные опции (ключи) — я не стал это делать и, наконец, у нас спрашивают, готовы ли мы начать:

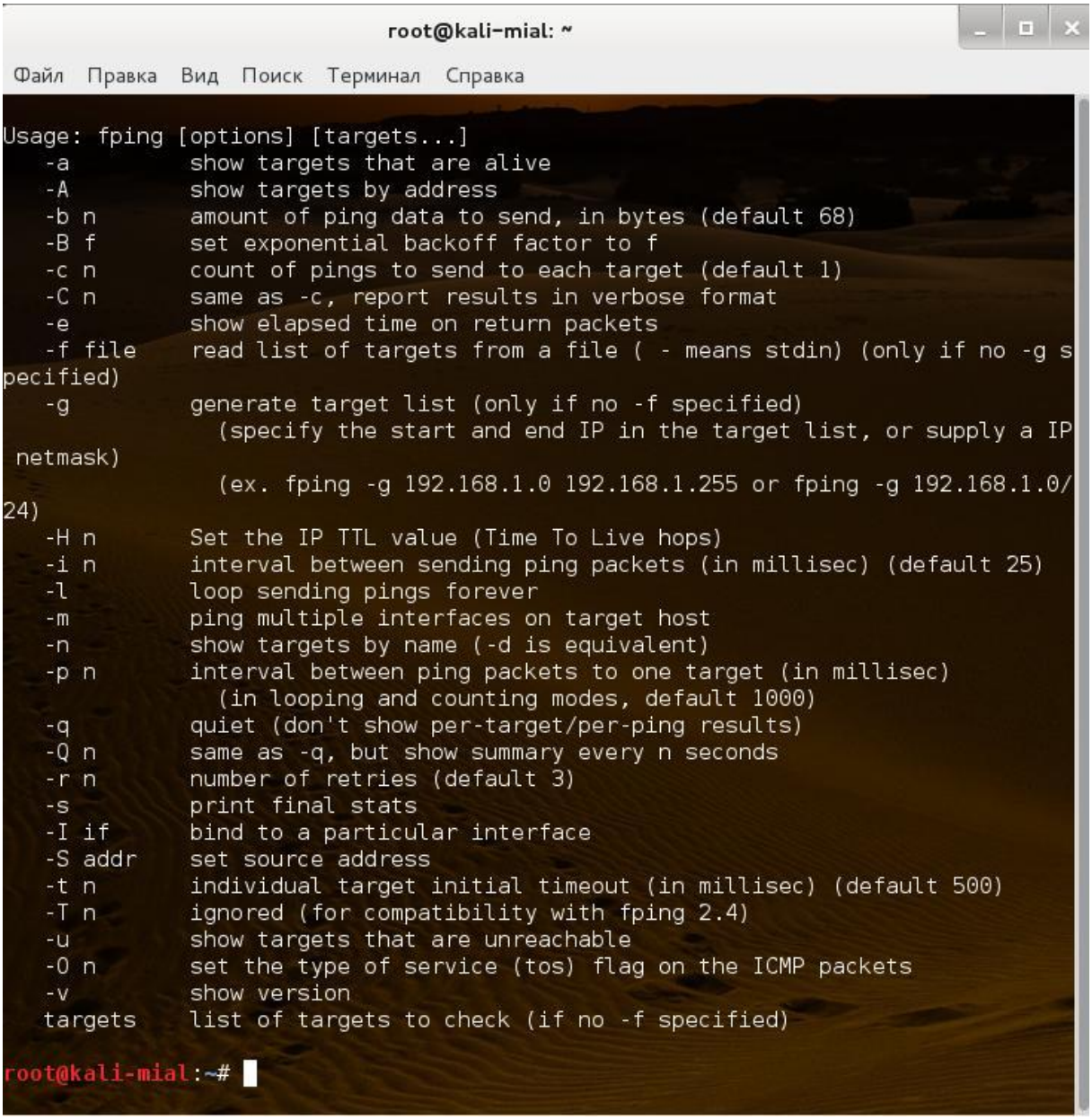


HTTrack начинает свою работу (скриншот логов с сайта):

После окончания клонирования, вы можете подробно изучить структуру каталог, размещения страниц и пр.

2. fping и Nmap — множественный пинг

Про команду ping, уверен, знают все. Её недостаток в том, что она позволяет использовать ICMP для проверки только одного хоста за раз. Команда fping позволит вам сделать пинг множества хостов одной командой. Она также даст вам прочитать файл с множеством хостов или IP адресов и отправит их для использования в эхо запросах пакета ICMP.



1|	fping-asg network/host bits
2|	fping -asg 10.0.1.0/24

Ключ **-a** возвратит результат в виде IP адресов только живых хостов, ключ **-s** отобразит по сканированию, ключ **-g** установит fping в тихих режим, который означает, что программа не позазывает пользователю статус каждого сканирования, только результат, когда сканирование завершено.

Команда **Nmap** делает примерно то же самое.

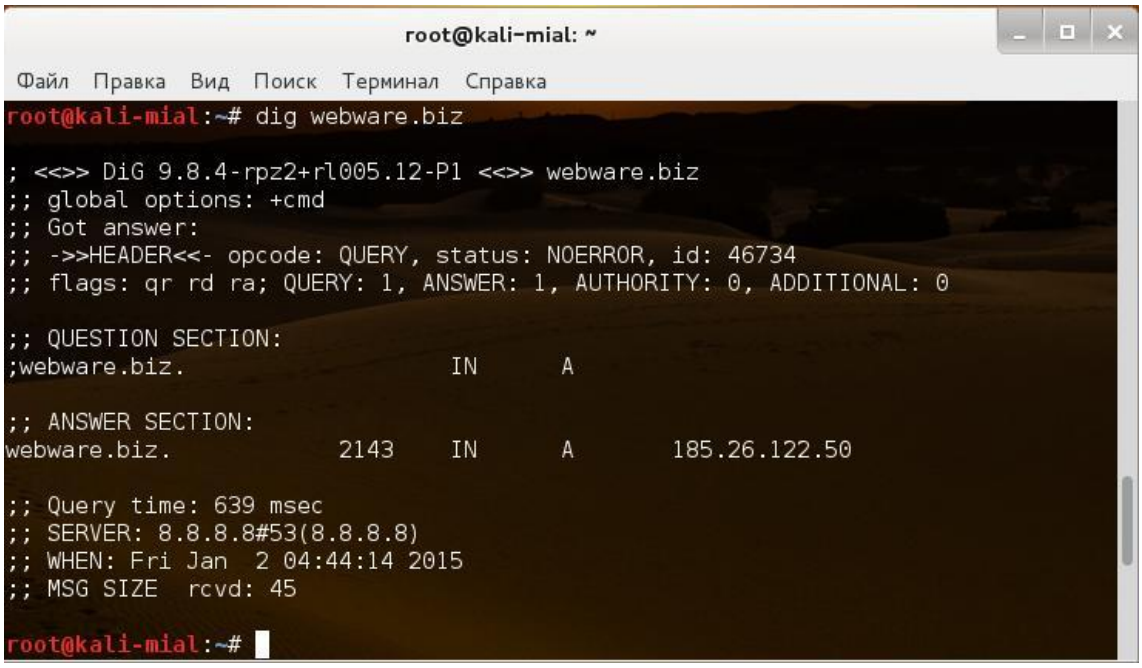
3. Dig — техники разведывания DNS

Используется так:

dig <адрес_сайта>

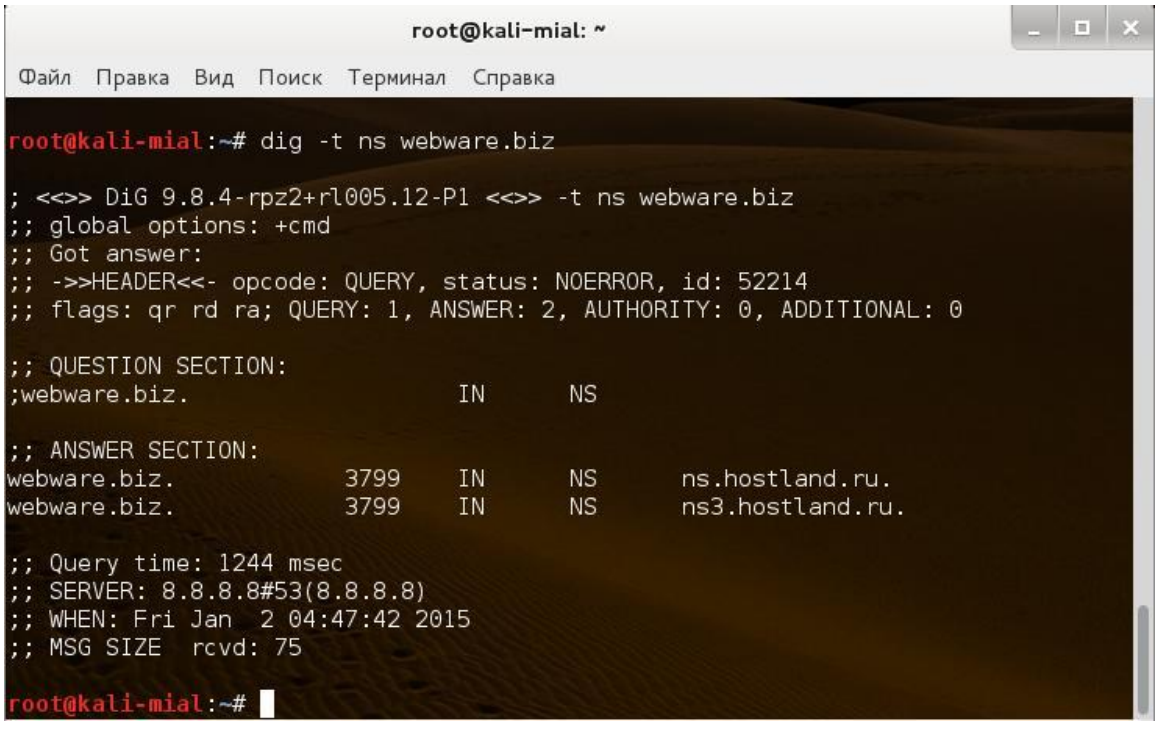
Например:

```
1| dig webware.biz
```



Для поиска авторитетных DNS серверов делаем так (во всех командах WebWare.biz — взят только для примера, заменяйте его на интересующий вас сайт):

```
1| dig -t ns webware.biz
```



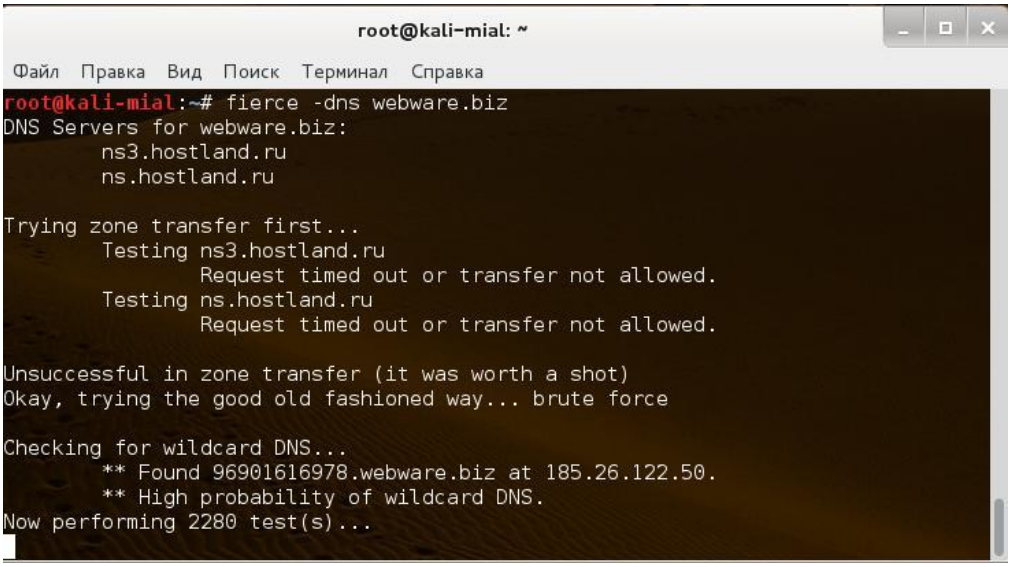
4. Fierce — ищем связанные с сайтом хосты

Этими хостами, например, для сайта WebWare.biz могут быть mail.webware.biz, cloud.webware.biz, th.webware.biz и т.д.

Применяется команда так (адрес сайта поменяйте на свой):

```
1| fierce -dns webware.biz
```

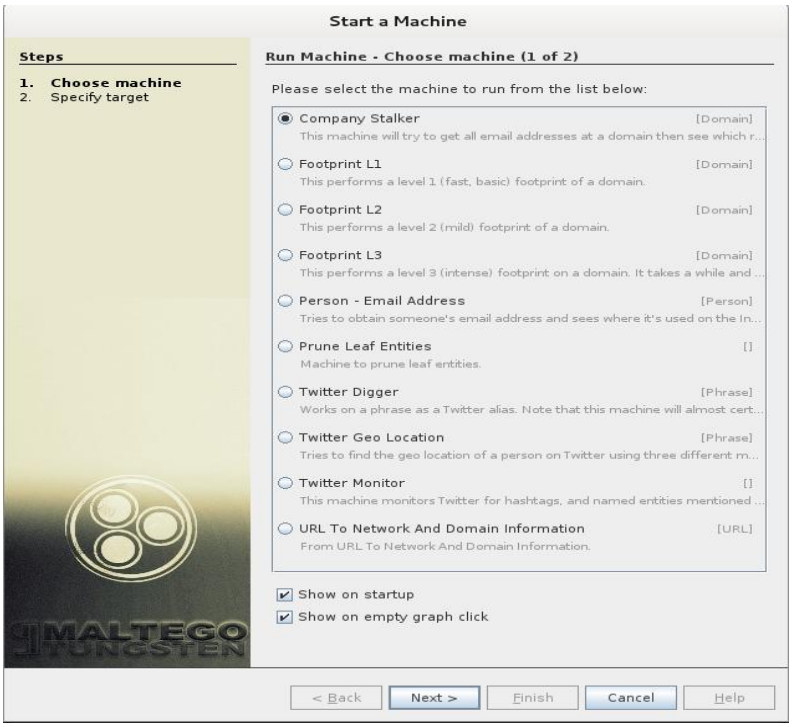
Если zone transfer недоступна, то используется метод перебора.



5. Maltego – графическое отображение собранной информации

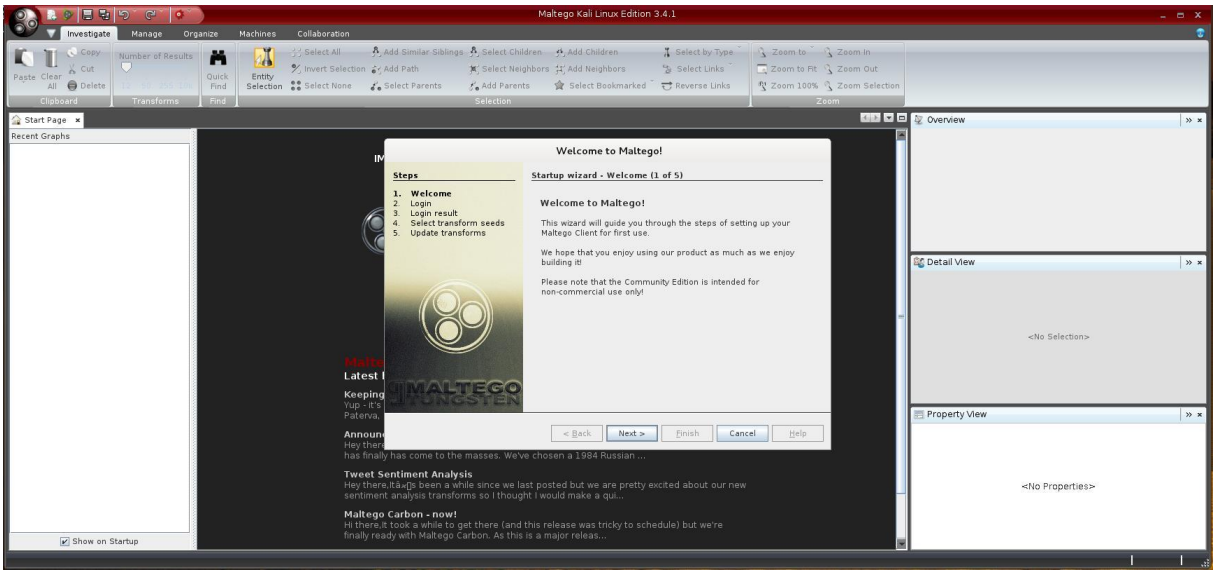
Программа находится в меню: **Information Gathering| DNS Analysis| Maltego**

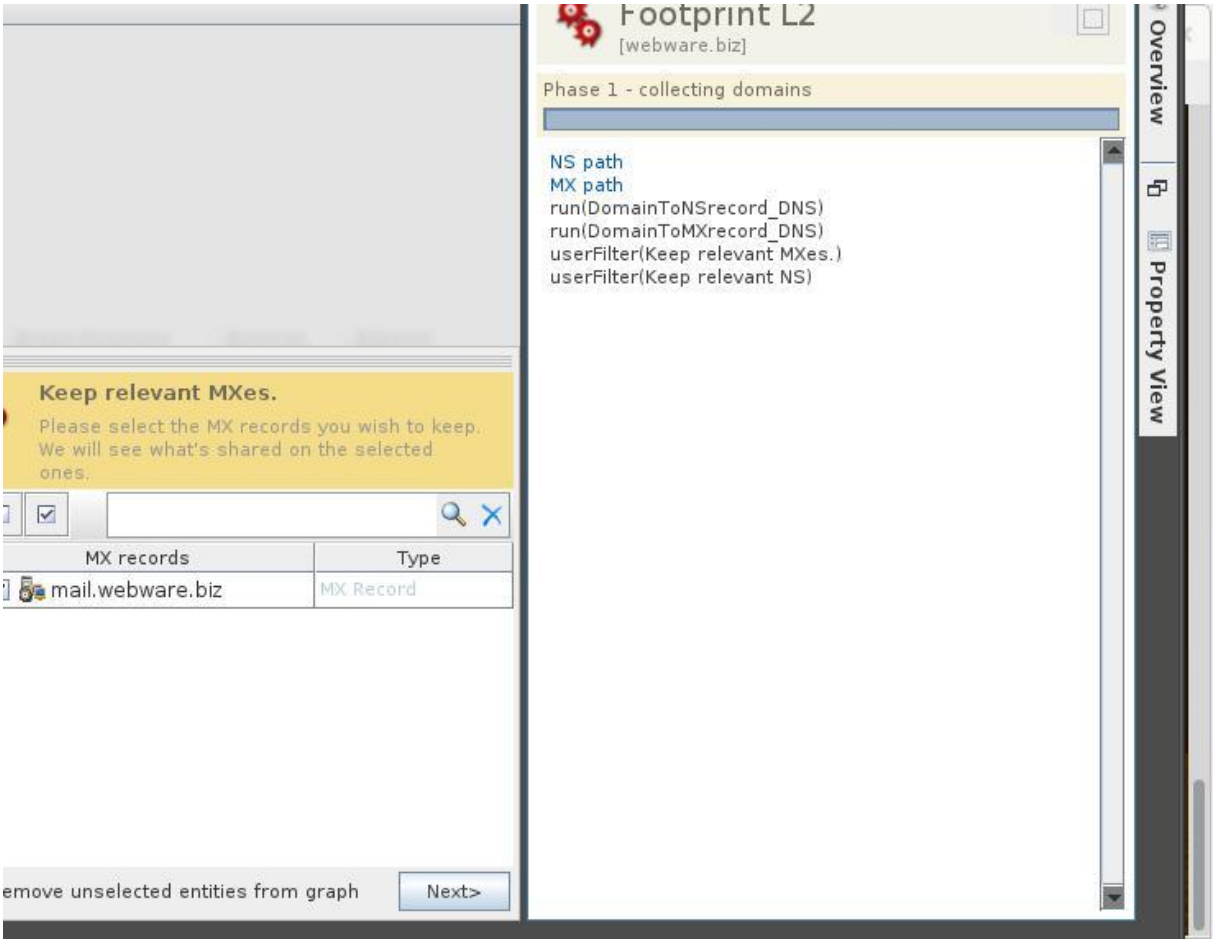
Maltego – это инструмент для сбора информации, встроенный в Kali и разрабатываемый Paterva. Это многоцелевой инструмент для сбора информации, который может собрать информацию из открытых и публичных источников в Интернете. Она может искать данные по сайтам или по адресам электронной почты:

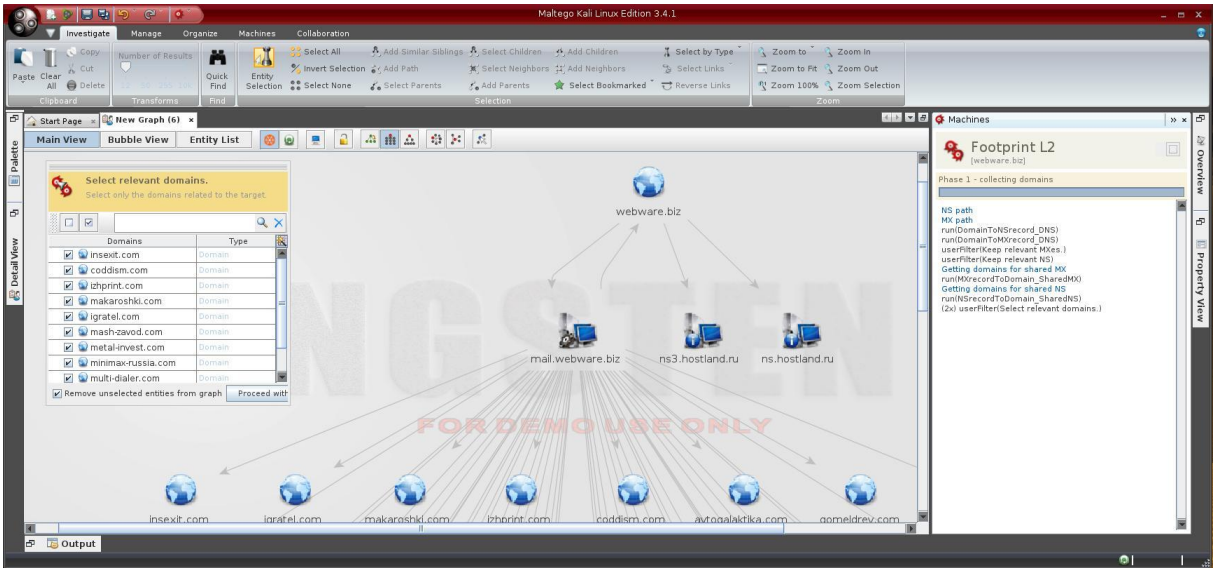


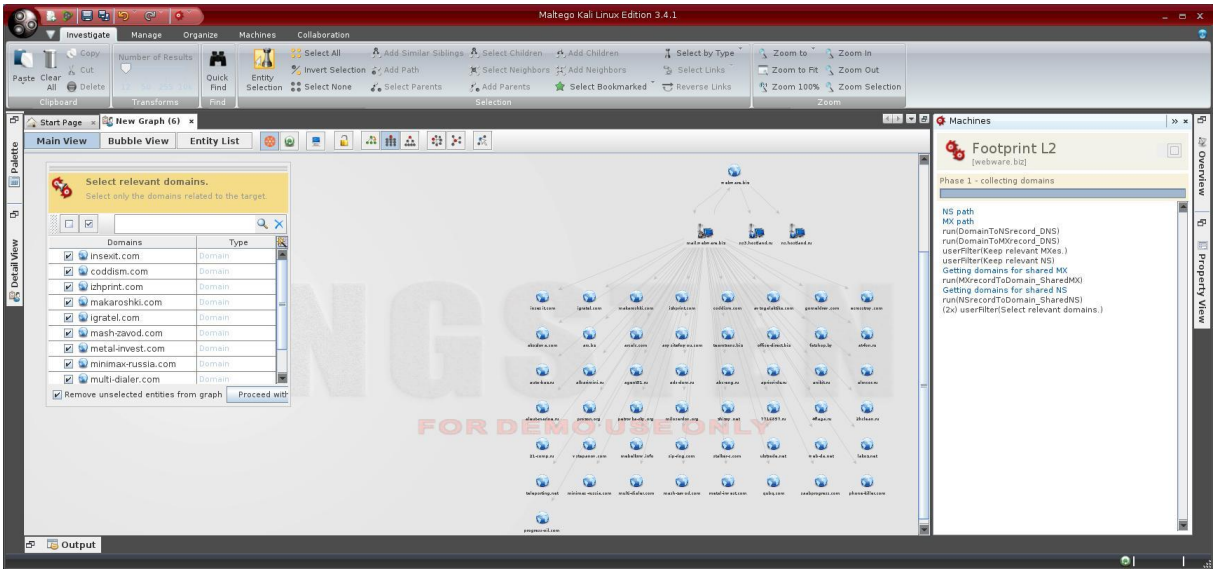
Для того, чтобы использовать программу, необходима обязательная регистрация.

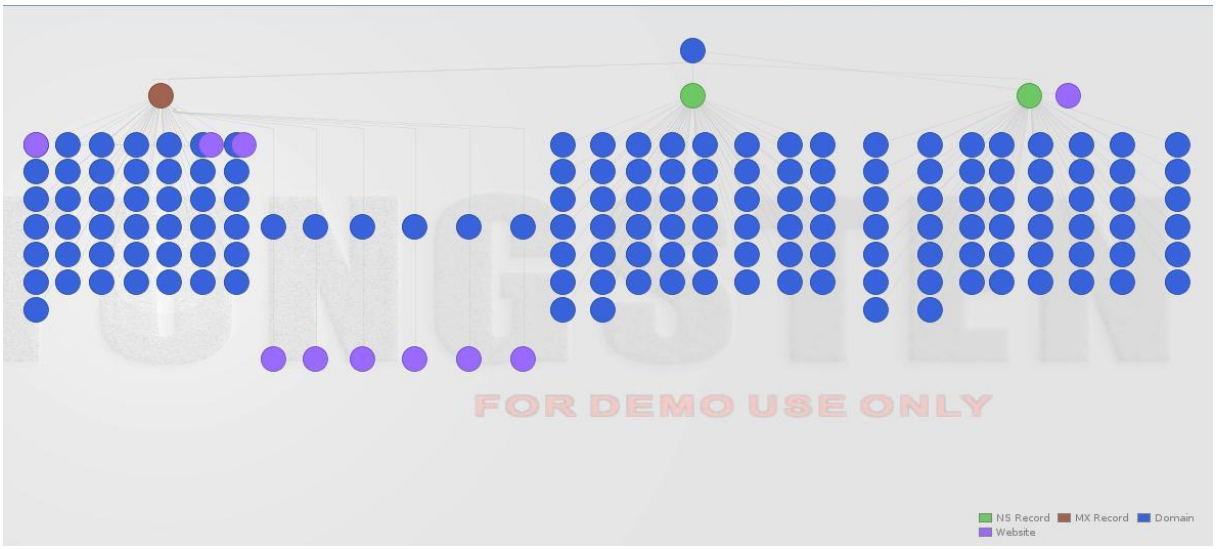
Результаты поиска:




Footprint L2
[webware.biz]
Phase 1 - collecting domains
NS path
MX path
run(DomainToNSrecord_DNS)
run(DomainToMXrecord_DNS)
userFilter(Keep relevant MXes.)
userFilter(Keep relevant NS)
Overview
Property View
Keep relevant MXes.
Please select the MX records you wish to keep. We will see what's shared on the selected ones.
MX records
Type
mail.webware.biz
MX Record
emove unselected entities from graph
Next>


Maltego Kali Linux Edition 3.4.1
Select relevant domains.
webware.biz
mail.webware.biz
ns3.hostland.ru
ns.hostland.ru
Footprint L2
FOR DEMO USE ONLY





6. Nmap — создатель карты сети

Nmap используется для сканирования хостов и служб в сети. Nmap имеет продвинутые функции, которые могут выявить различные приложения, запущенные на системах, также как службы и особенности отпечатков ОС. Это один из наиболее широко используемых сетевых сканеров, он является очень эффективным, но в то же время и очень заметным.

Nmap рекомендуется к применению в специфичных ситуациях, для предотвращения срабатывания механизма защиты.

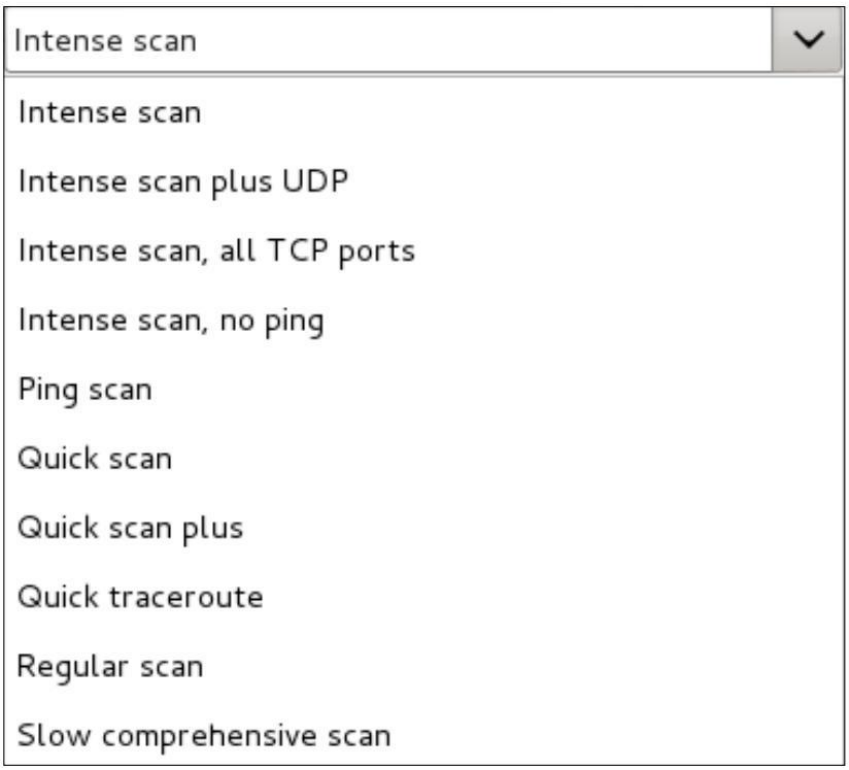
Дополнительно Kali идёт с загруженной **Zenmap**. Zenmap даёт Nmap графический пользовательский интерфейс для выполнения команд.

Zenmap это не только графическая надстройка, программа предлагает и эксклюзивные функции.

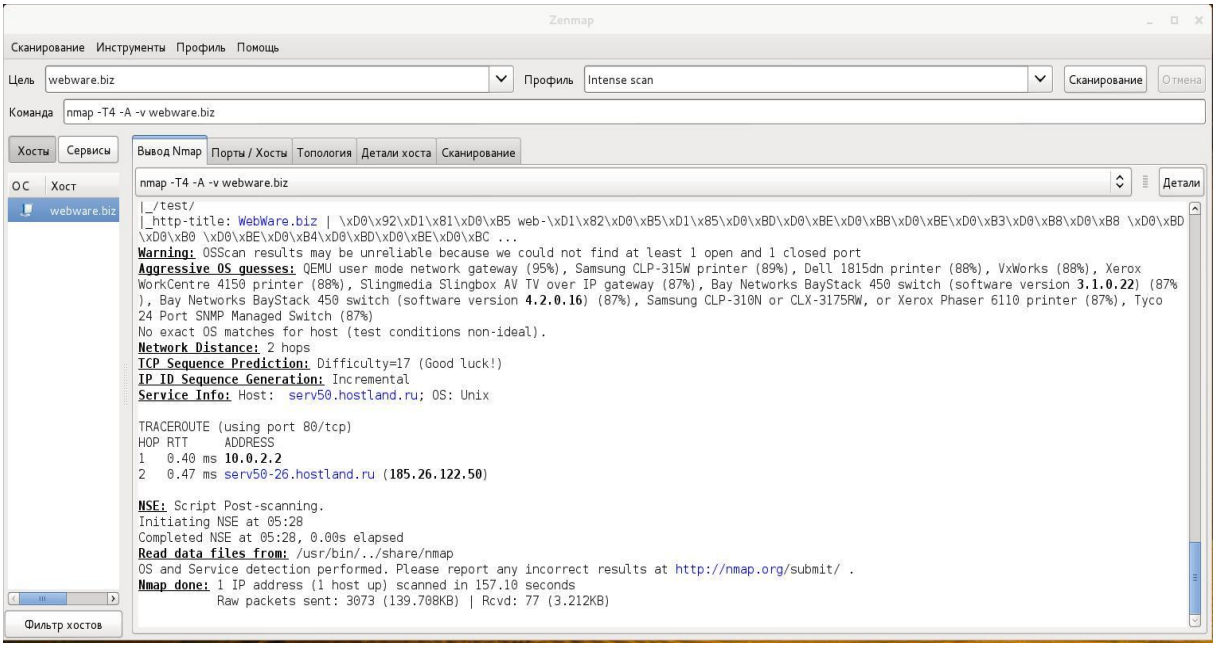
Чтобы запустить Zenmap, идём в меню

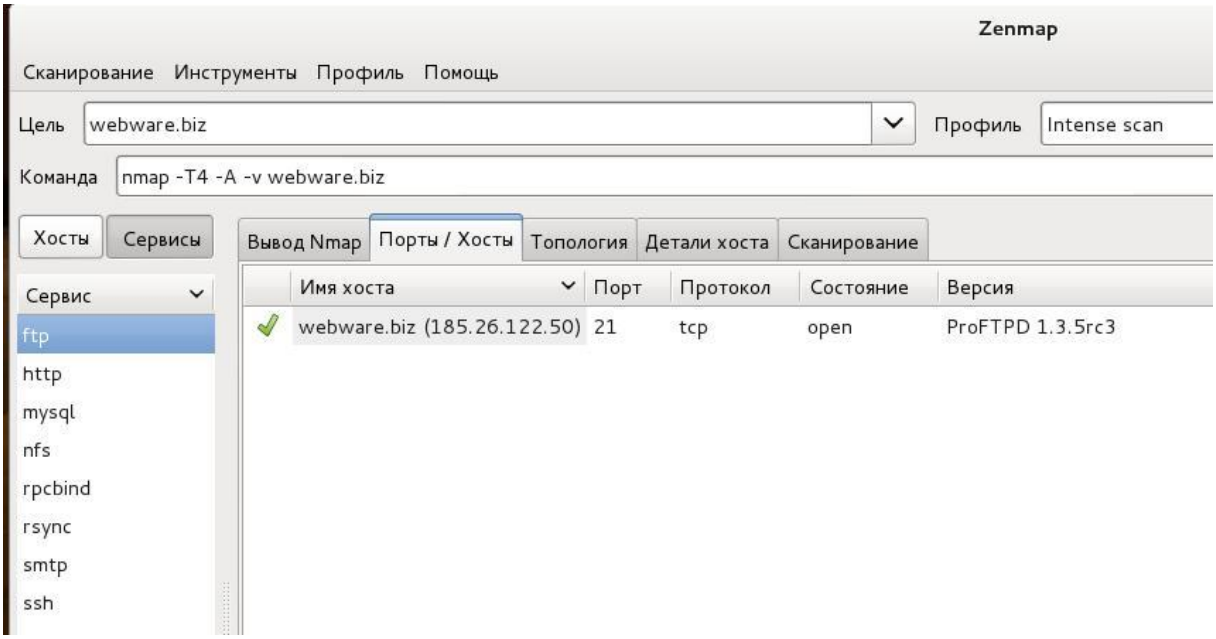
Kali Linux | Information Gathering | Network Scanners | zenmap

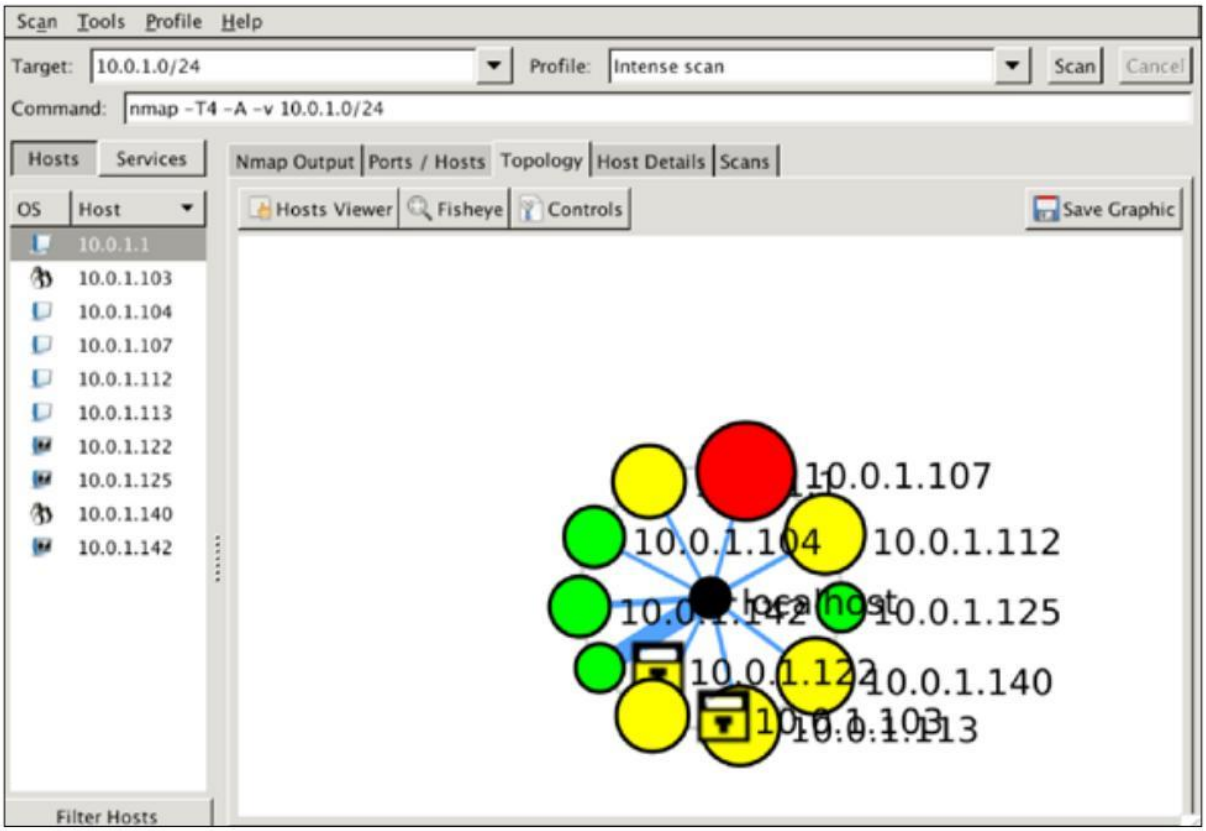
Множество разных вариантов сканирования, можно создавать профили и очень много других полезностей.

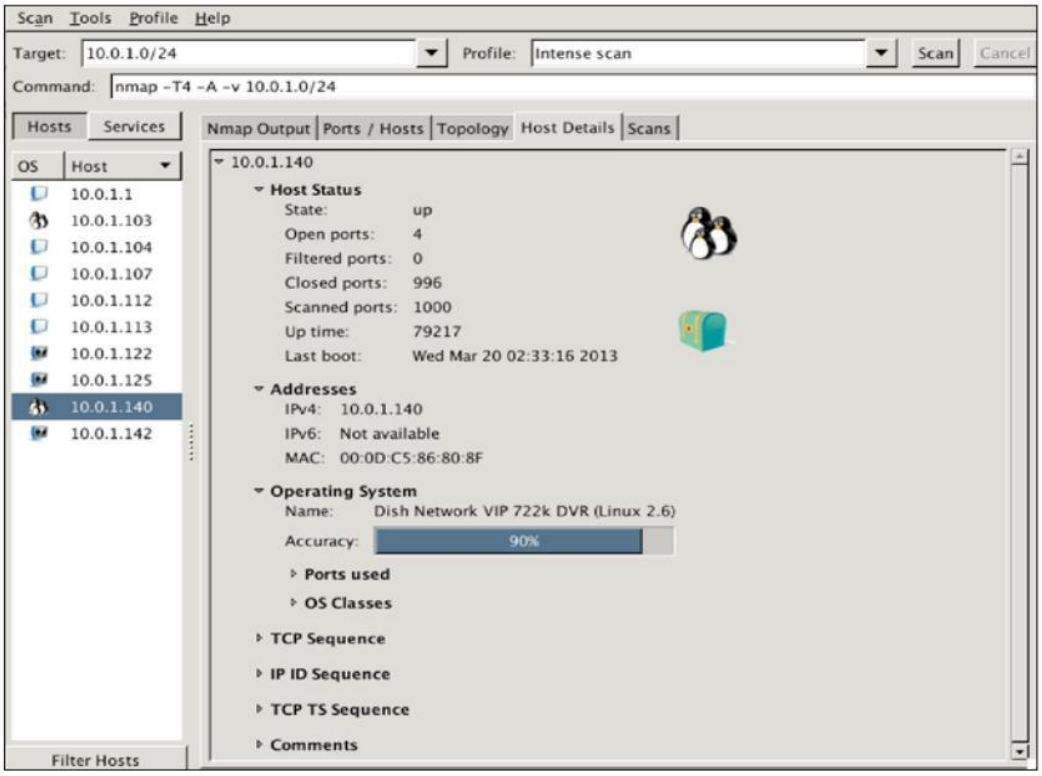


Полученная информация очень обширна и полезна:




Zenmap
Сканирование Инструменты Профиль Помощь
Цель webware.biz
Профиль Intense scan
Команда nmap -T4 -A -v webware.biz
Хосты Сервисы
Вывод Nmap Порты / Хосты Топология Детали хоста Сканирование
Сервис
ftp
http
mysql
nfs
rpcbind
rsync
smtp
ssh
Имя хоста Порт Протокол Состояние Версия
webware.biz (185.26.122.50) 21 tcp open ProFTPD 1.3.5rc3

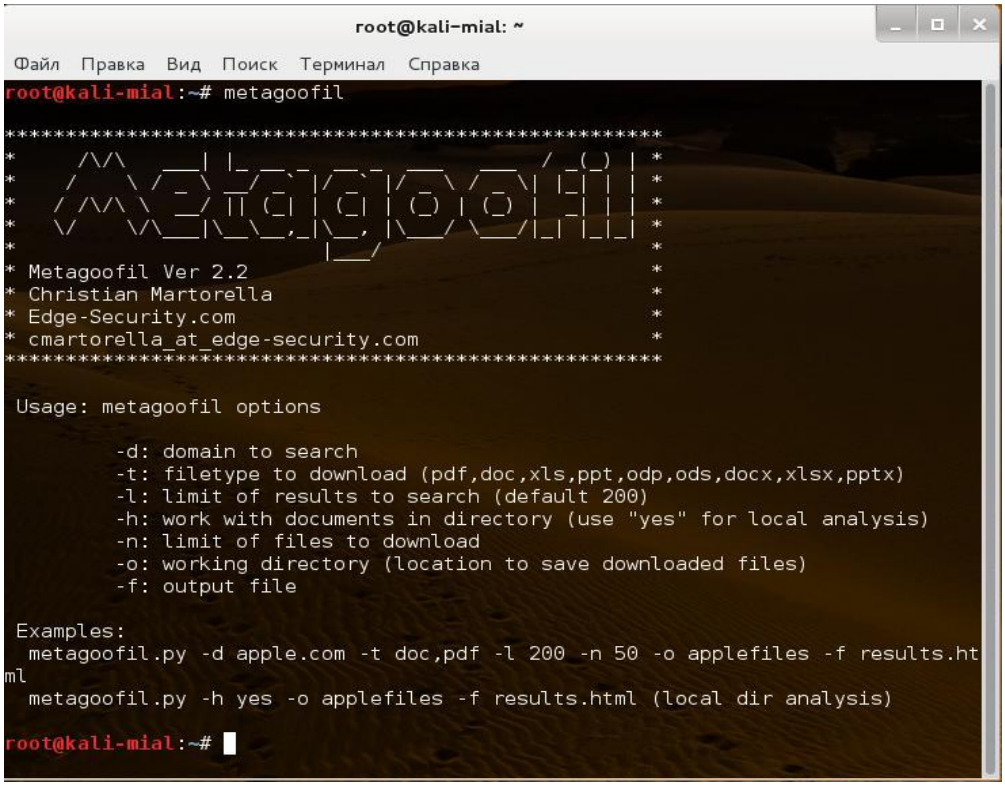

Scan Tools Profile Help
Target: 10.0.1.0/24
Profile: Intense scan
Scan Cancel
Command: nmap -T4 -A -v 10.0.1.0/24
Hosts Services
Nmap Output Ports / Hosts Topology Host Details Scans
OS Host
Hosts Viewer Fisheye Controls
Save Graphic
10.0.1.1
10.0.1.103
10.0.1.104
10.0.1.107
10.0.1.112
10.0.1.113
10.0.1.122
10.0.1.125
10.0.1.140
10.0.1.142
10.0.1.107
10.0.1.104
10.0.1.112
10.0.1.125
10.0.1.140
Filter Hosts



7. Metagoofil — сбор метаданных из файлов с сайта

Не надо недооценивать значение метаданных! Они могут рассказать об именах пользователей, о программах, которые они используют, могут содержать GPS координаты съёмки изображения, об операционных системах пользователей, времени работы над документами и очень-очень многом другом. О том, как удалить метаданные из файла, читайте в статье на нашем братском ресурсе.

При запуске Metagoofil без ключей, она выдаёт подсказки по использованию:



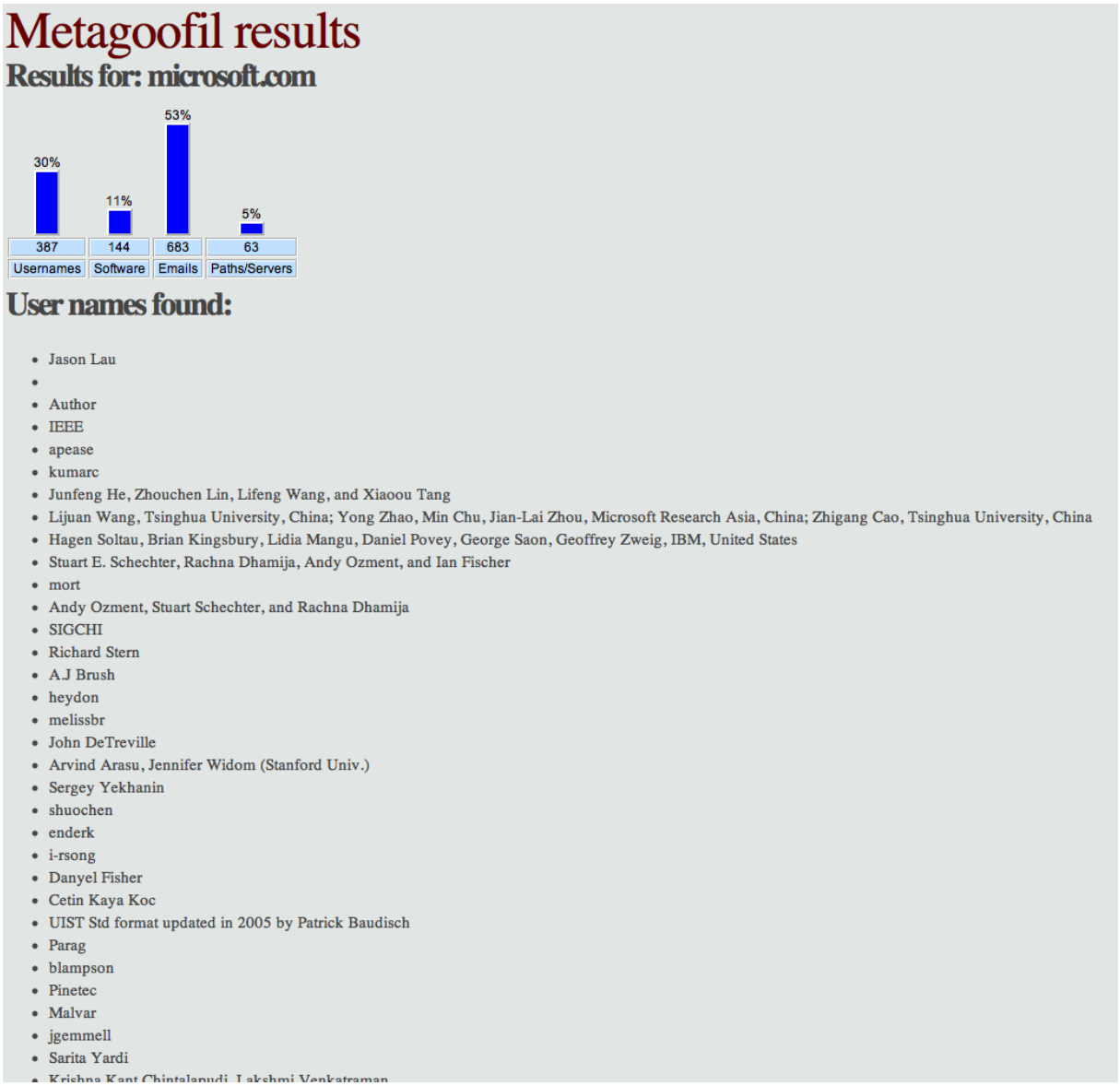
1|	-d	Домен для поиска
2|	-t	Типы файлов для загрузки (pdf,doc,xls,ppt,odp,ods,docx,xlsx,pptx)
3|	-l	Лимит результатов для поиска (по умолчанию 200)
4|	-h	Работать с документами в директории (используйте "yes" для локального анализа)
5|	-n	Лимит файлов для загрузки
6|	-o	Рабочая директория (место для сохранения скаченных файлов)
7|	-f	Файл, в который будут записаны результаты анализа

Пример запуска программы:

```
1| metagoofil -d webware.biz -t doc,pdf -l 200 -n 50 -o applefiles -f results.htm
```

Программа может найти уйму полезной информации: имена пользователей, абсолютные адреса на сервере, имена компьютеров, используемые приложений. Вот примеры отчётов программы.

Список найденных пользователей:



Metagoofil results

Results for: microsoft.com

User names found:

- Jason Lau
-
- Author
- IEEE
- apease
- kumarc
- Junfeng He, Zhouchen Lin, Lifeng Wang, and Xiaoou Tang
- Lijuan Wang, Tsinghua University, China; Yong Zhao, Min Chu, Jian-Lai Zhou, Microsoft Research Asia, China; Zhigang Cao, Tsinghua University, China
- Hagen Soltau, Brian Kingsbury, Lidia Mangu, Daniel Povey, George Saon, Geoffrey Zweig, IBM, United States
- Stuart E. Schechter, Rachna Dhamija, Andy Ozment, and Ian Fischer
- mort
- Andy Ozment, Stuart Schechter, and Rachna Dhamija
- SIGCHI
- Richard Stern
- A.J Brush
- heydon
- melissbr
- John DeTreville
- Arvind Arasu, Jennifer Widom (Stanford Univ.)
- Sergey Yekhanin
- shuochen
- enderk
- i-rsong
- Danyel Fisher
- Cetin Kaya Koc
- UIST Std format updated in 2005 by Patrick Baudisch
- Parag
- blampson
- Pinetec
- Malvar
- jgemmell
- Sarita Yardi
- Krishna Kant Chintalapudi, Lakshmi Venkatraman

Список найденных серверов:

Servers and paths found:

- CEP_Template.dot
- Normal.dot
- CEP_Template
- Normal
- Normal.dotm
- ''
- 'C:\My Documents\DATA\professional support for IT pros mvf.doc'
- 'C:\WINDOWS\TEMP\AutoRecovery save of professional support for IT pros mvf.asd'
- '\\PSSMAX\PUBLIC\ASCENT\Datasheets\professional support for IT pros mvf.doc'
- 'C:\TEMP\AutoRecovery save of professional support for IT pros mvf.asd'
- '\\ordat05\JEFFERSON\MSOFT\PSS\New offerings\Datasheets\professional support for IT pros mvf.doc'
- '\\Pssmax\public\ASCENT\Datasheets\Press Tour\professional support for IT pros mvf.doc'
- 'D:_Support\professional-support-ITpros.doc'
- 'C:\WINNT\Profiles\scottgo\Personal\supportal\portal final\professional-support-ITpros fact.doc'
- 0
- REF_Template.dot
- 'C:\My Documents\DATA\professional support for oems mvf.doc'
- 'C:\WINDOWS\TEMP\AutoRecovery save of professional support for oems mvf.asd'
- 'F:\ASCENT\Datasheets\professional support for oems mvf.doc'
- '\\PSSMAX\PUBLIC\ASCENT\Datasheets\professional support for oems mvf.doc'
- '\\ordat05\JEFFERSON\MSOFT\PSS\New offerings\Datasheets\professional support for oems mvf.doc'
- 'C:\TEMP\AutoRecovery save of professional support for oems mvf.asd'
- '\\Pssmax\public\ASCENT\Datasheets\Press Tour\professional support for oems mvf.doc'
- 'C:\WINNT\Profiles\scottgo\Personal\supportal\portal final\professional-support-for-oems fact.doc'
- spieltr97.dot
- '\\PSSMAX\PUBLIC\ASCENT\Premier - Expertise\Datasheets\premier support for the enterprise - radams 4_20.doc'
- 'F:\ASCENT\Datasheets\premier support for the enterprise - radams 4_20.doc'
- '\\ordat05\JEFFERSON\MSOFT\PSS\New offerings\Datasheets\premier support for the enterprise - radams 4_20.doc'
- '\\Pssmax\public\ASCENT\Datasheets\Press Tour\premier support for the enterprise - radams 4_20.doc'
- '\\Pssmax\public\ASCENT\Datasheets\premier support for the enterprise .doc'
- 'J:\Ascent\Datasheets\premier support for the enterprise .doc'
- '\\pssmax\public\ASCENT\Marketing\Datasheets\premiersupportfortheenterprise.doc'
- 'C:\windows\TEMP\BEL-LUX - English - License 2.0 - v3 - marked.doc'
- 'C:\windows\TEMP\BEL-LUX - English - License 2.0 - v3 - clean.doc'
- '\\PAULIANA\USERS\MKA\Microsoft\MS Eur Localization Guidelines\Campus II\Belgium\BEL-LUX - English - License 2.0 - v3 - marked.doc'
- '\\PAULIANA\USERS\MKA\Microsoft\MS Eur Localization Guidelines\Campus II\Belgium\BEL-LUX - English - License 2.0 - v3 - clean.doc'
- 'C:\windows\TEMP\AutoHerstel-versie van BEL-LUX - English - License 2.asd'
- '\\moliere\LEGAL\SusanSv\EDUCATION\CA & SA 2.0\Localization\Belgium\2. With my changes\BEL&LUX_ENG - School Campus License Agreement.doc'
- '\\moliere\LEGAL\SusanSv\EDUCATION\CA & SA 2.0\FINAL\Belgium\BEL&LUX_ENG - School Campus License Agreement - July 99.doc'

Найденные версии программного обеспечения:

Software versions found:

- þÿMicrosoft® Word 2010
- MiKTeX pdfTeX-1.40.11
- TeX
- pdfeTeX-1.20a
- LaTeX with hyperref package
- Acrobat Distiller 7.0 (Windows)
- Acrobat Distiller Command 3.01 for Solaris 2.3 and later (SPARC)
- IEEE Copyright
- pdfTeX-1.10b
- Acrobat Distiller Command 2.1 for SunOS/Solaris (SPARC)
- GPL Ghostscript 8.15
- dvips(k) 5.92b Copyright 2002 Radical Eye Software
- MiKTeX pdfTeX-1.20a
- Acrobat Distiller 4.05 for Windows
- AFPL GhostScript via GhostWord
- Microsoft Word 11.0
- AFPL Ghostscript 8.51
- dvips(k) 5.95a Copyright 2005 Radical Eye Software
- Acrobat Distiller 3.0 for Windows
- PScript5.dll Version 5.2.2
- pdfTeX-1.40.9
- Acrobat Distiller 6.0 (Windows)
- AFPL Ghostscript 7.04
- dvips(k) 5.86 Copyright 1999 Radical Eye Software
- GNU Ghostscript 6.51
- MiKTeX GPL Ghostscript 8.54
- dvips(k) 5.95b Copyright 2005 Radical Eye Software
- Acrobat Distiller 5.0.5 (Windows)
- dvipdfm 0.13.2c, Copyright © 1998, by Mark A. Wicks
- TeX output 2005.06.06:1620
- MiKTeX pdfTeX-1.40.4
- PDFlib+PDI 5.0.2p1 (COM/Win32)
- Conference Management Services, College Station, TX
- pdfTeX-1.0b-pdfcrypt
- PSNormalizer.framework
- ESP Ghostscript 815.02
- MiKTeX pdfTeX-1.40.10
- PDFlib+PDI 6.0.1p1 (COM/Win32)

Итак, мой список инструментов для сбора информации получился всего на семь пунктов. Те, кто заходил в раздел **Information Gathering**, знают, что там несколько десятков программ. Я рассмотрел самые, на мой взгляд, интересные.

Глава 16. Лучшие хакерские программы

Хакерские инструменты: список инструментов по безопасности для тестирования и демонстрации слабостей в защите приложений и сетей, эти инструменты предназначены для профессионалов по информационной безопасности.

Источник: https://n0where.net/best-hacking-tools/

Пароли	
Cain & Abel	Cain & Abel — это инструмент по восстановлению пароля для операционной системы Microsoft. Этот инструмент позволяет восстановить пароли различного рода посредством прослушивания сети.
CacheDump	CacheDump, лицензирована под GPL, демонстрирует, как восстановить информацию из записей кэша: имя пользователя и MSCASH.
John the Ripper	John the Ripper быстрый взломщик паролей, в настоящее время доступен на разного рода Unix (официально поддерживаются 11 не считая различных архитектур), Windows, DOS, BeOS и OpenVMS.
FSCrack	GUI (графический интерфейс) для John the Ripper. FSCrack — это "морда" для John the Ripper (JtR), т.е. графический интерфейс (GUI) для доступа к большинству функциям JtR.
Hydra	Очень быстрый взломщик входа по сети, программа поддерживает множество различных служб. Одна из самых больших дыр в безопасности — это пароли, об этом говорят все исследования по безопасности паролей.
keimpx	keimpx инструмент с открытым исходным кодом, выпущен под модифицированной версией лицензии Apache License 1.1. Он может быть использован для быстрой проверки полезности учётных данных по сети через SMB.
Medusa	Medusa предназначена для скоростного, массово параллельного, модульного брут-форса входа. Цель — поддерживать все службы, которые позволяют удалённую аутентификацию.
Ncrack	Ncrack — это высокоскоростной инструмент взлома паролей аутентификации. Он был создан в помощь компания по обеспечению безопасности их сетей посредством активного тестирования всех их хостов и сетевых устройств на предмет выявления слабых паролей.
Ophcrack	Ophcrack — это взломщик паролей Windows, основанный на радужных таблицах. Это очень эффективная реализация радужных таблиц, осуществлённая изобретателем данного метода.

RainbowCrack	RainbowCrack — это много целевая реализация теории радужных таблиц Philippe Oechslin. Про радужные таблицы в Википедии.
phrasen|drescher	phrasen|drescher (p|d) — это модульный и мульти процессный обходчик паролей для их взлома. Он поставляется с рядом плагинов, а простые API позволяют простую разработку новых плагинов.
LCP	Главная цель программы LCP — это аудит и восстановление пользовательского пароля в Windows NT/2000/XP/2003.
Crunch	Crunch — это генератор списка слов, в котором вы можете задать набор стандартных символов или любых других символов по своему желанию. crunch сгенерирует все возможные комбинации и пермутации.
Fcrackzip	Обычно, программы появляются исходя из потребностей. Ситуация с fcrackzip не исключение. Я не особо использую формат zip, но недавно мне понадобился взломщик паролей. Fcrackzip — это программа для взлома паролей zip.
Enumiax	EnumIAX — это инструмент для брут-форса имени пользователя протокола Inter Asterisk Exchange версии 2 (IAX2). enumIAX может работать в двух различных режимах: последовательное предположение имени пользователя или атака по словарю.
Wyd	wyd.pl был рождён из следующих двух ситуации: 1. Необходимо выполнить тест на проникновение, а дефолтный список слов не содержит валидного пароля. 2. Во время судебно-медицинской экспертизы при расследовании преступлений файл должен быть открыт без знания пароля.
Bruter	Bruter — это параллельный брутфорсер сетевого входа для Win32. Цель этого инструмента — продемонстрировать важность выбора сильного пароля. Цель Bruter — это поддержка различных служб, которые позволяют удалённую аутентификацию.
The ssh bruteforcer	Инструмент для выполнения атаки по словарю на SSH серверы. Это простой инструмент, вы задаёте целевой сервер, целевой аккаунт, список слов, порт и ждёте.
Lodowep	Lodowep — это инструмент для анализа стойкости пароля аккаунта в веб-серверной системе Lotus Domino. Инструмент поддерживает как сессионную, так и базовую аутентификацию.

SSHatter	SSHatter использует техники брут-форса для определения, как зайти на сервер SSH. Она тщательно пробует каждую комбинации из списка имён пользователей и паролей для определения верной комбинации.

Сканирование	
Amap	Amap — это инструмент сканирования следующего поколения, который идентифицирует приложения и службы, даже если они не прослушивают порт по умолчанию. Это достигается установлением фиктивной связи и анализом ответа.
Dr.Morena	Dr.Morena — это инструмент для подтверждения настройки правил в файерволе. Настройка файервола выполняется комбинированием более чем одного правила.
Firewalk	Firewalk является инструментом для активно разведки сети, он пытается определить, какой уровень (слой) четвёртого протокола пройдёт на заданный IP устройства перенаправления. Firewalk работает отправляя пакеты TCP или UDP с TTL на единицу больше, чем целевой шлюз.
Netcat	Netcat — это особенная утилита, которая читает и пишет данные в сетевые соединения, используя протокол TCP/IP. Она создана как надёжный "фоновый" инструмент, который может быть использован напрямую или с лёгкостью задействован другой программой.
Ike Scan	Ike-scan — это инструмент командной строки, который использует протокол IKE для обнаружения, снятия отпечатков пальцев и тестирования серверов IPSec VPN. Он доступен для Linux, Unix, MacOS и Windows под лицензией GPL.
Nmap	Nmap (‘Network Mapper’ — "сетевой картограф") — это бесплатная утилита с открытым исходным кодов для исследования сетей или для аудита безопасности. Она создавалась для быстрого сканирования огромных сетей, но также прекрасно работает и в отношении единичных хостов.
Zenmap	Zenmap — это официальная графическая оболочка (GUI) для Nmap Security Scanner. Она мультиплатформенная (Linux, Windows, Mac OS X, BSD и т.д.).

Onesixtyone	onesixtyone это сканер SNMP, который использует технику развёртки для достижения высокой производительности. Он может просканировать всю сеть класса B за 13 минут.
SuperScan 4	Мощный сканер портов TCP, пингер, резолвер. SuperScan 4 — это обновление SuperScan — крайне популярного сканера портов под Windows SuperScan
Autoscan	AutoScan-Network — это сканер сети (обнаружение и управление приложениями). Для сканирования вашей сети не требуется настройка. Главная цель — вывести список подключённого оборудования в вашей сети.
Knocker	Knocker — это простой и лёгкий в использовании сканер безопасности портов TCP, написан на C, анализирует все службы, запущенные на этих портах.
Nsat	NSAT — это надёжный сканер, который предназначен для различного рода широких сканирований, сохраняя стабильность на протяжении дней. Сканирование на нескольких пользовательских машинах (локальное незаметное низкоприоритетные опции сканирования).
OutputPBNJ	PBNJ — это набор инструментов для мониторинга изменений в сети в течение долгового времени. Он выполняет это посредством проверки целевых машин на изменения. Собираемая информация включает подробности о запущенных службах на них, а также состояние служб.
ScanPBNJ	ScanPBNJ выполняет сканирование Nmap, а затем сохраняет результаты в базе данных. ScanPBNJ сохраняет информацию о просканированных машинах. ScanPBNJ сохраняет IP адреса, операционные системы, имена хостов и бит localhost.
glypeahead	По умолчанию, Glype proxy script имеет несколько ограничений на какие хосты/порты он может иметь доступ. В дополнение, proxy script нормально отображает сообщения об ошибках, связанные с cURL.
Unicornscan	Unicornscan — это новый движок сбора и корреляции информации, созданный для сообществ по тестированию и исследованию безопасности.

TCP Fast Scan	Очень-очень быстрый сканер tcp портов под Linux. Работает очень быстро. Может одновременно сканировать множество хостов / портов + диапазонов
Multi Threaded TCP Port Scanner 3.0	Этот инструмент может быть использован для сканирования портов конкретного IP. Он также может описать каждый порт стандартным именем (известных и зарегистрированных портов).
MingSweeper	MingSweeper — это инструмент разведки сети, предназначенный для облегчения высокоскоростного выявления узлов и их идентификации в большом адресном пространстве.
Umap(UPNP Map)	Umap (UPNP Map) пытается сканировать открытые порты TCP на хостах за включённым UPNP Internet Gateway Device(IGD) NAT.
SendIP	SendIP имеет огромное количество опций командной строки чтобы указать содержимое каждого заголовка NTP, BGP, RIP, RIPng, TCP, UDP, ICMP или сырых IPv4 и IPv6 пакетов. Программа также позволяет добавлять в пакеты любые данные.
PortSentry	Инструменты Sentry обеспечивают безопасность служб на уровне хоста для платформ Unix. PortSentry, Logcheck/LogSentry и HostSentry защищают от сканирования портов, автоматизируют аудит файлов журналов и выявляют продолжительную подозрительную активность логина.
CurrPorts	CurrPorts отобразить список открытых в данный момент портов TCP/IP и UDP на вашем ПК. Также для каждого открытого порта в построенном списке будет отображена информация о процессе, который открыл этот порт.
Nscan	Сам по себе NScan — это сканер портов, который использует метод connect() для составления списка открытых портов хоста. Отличие от большинства других сканеров портов — это гибкость и скорость.
NetworkActiv Scan	NetworkActiv Port Scanner — это инструмент исследования и администрирования сети, который позволяет сканировать и исследования внутренние LAN и внешние WAN.
Blues Port Scanner	Хороший сканер портов — просто один из базовых инструментов каждого, кто-то всерьёз интересуется интернет-штучками. BluesPortScan — это, я думаю, самый быстрый сканер для 32-битных Windows, из тех, которые могут быть найдены в сети.

ZMap	ZMap сканер с открытым исходным кодом, который даёт возможность исследователям просканировать сети размером с весь Интернет. На единственной машине с хорошим каналом ZMap выполнить полное сканирование всех адресов IPv4 в течение 45 минут, упираясь в теоретический придел гигабитных Ethernet.
subdomain-bruteforcer	Subdomain-bruteforcer — это многопоточный инструмент написанной на Python для перечисления субдоменов из файла словаря. Особенно полезен для поиска админок ил и других хитроумных веб-практик.
ircsnapshot	Ircsnapshot — это бот, написанный на Python, которые подсоединяется к серверу чтобы извлечь пользовательские хостмаски, имена и принадлежность каналов; также используется для создания карты на основе наскрёбанных данных. Полезен для разведки на IRC сервере полном подозрительных ботов. Поддерживает SOCKS и TOR.

Сниффинг	
Wireshark	Wireshark используется сетевыми специалистами по всему миру для решения проблем, анализа, разработки программного обеспечения и протоколов, а также в образовании.
Chaosreader	Бесплатный инструмент для отслеживания TCP/UDP/... сессий и извлечения данных приложений из "подсмотренных" или сдампленных (tcpdump) логов. Это "всеядная" программа, она извлекает сессии telnet, FTP файлы, HTTP передачи (HTML, GIF, JPEG, ...), SMTP письма, ... из захваченных данных внутри сетевого трафика.
dsniff	dsniff — это коллекция инструментов для сетевого аудита и тестирования на проникновение. dsniff, filesnarf, mailsnarf, msgsnarf, urlsnarf, и webspy пассивно следят за сетью в поисках интересной информации.
Ettercap	Ettercap — это инструмент для атаки человек-по-середине в LAN. Её особенностями являются сниффинг живых соединений, фильтрация контента на лету и многие другие интересные трюки.
NetworkMiner	NetworkMiner это инструмент для криминалистического анализа сети (Network Forensic Analysis Tool — NFAT) под Windows. NetworkMiner может быть использован как пассивный сетевой сниффер/перехватчик пакетов для определения операционных систем, сессий, имён хостов,

	открытых портов и т.д.
RawCap	RawCap — это бесплатная программа командной строки, сетевой сниффер под Windows, который использует сырые сокеты.
Spike proxy	Не все приложения делаются одинаково, и, следовательно, многие должны анализироваться индивидуально. SPIKE Proxy — это инструмент профессионального уровня для поиска уязвимостей уровня приложений в веб-приложениях.
Tcpdump	Tcpdump выводит заголовки пакетов на сетевом интерфейсе, которые соответствуют логическому выражению.
Tcpreplay	Tcpreplay это набор инструментов под лицензией BSD написанных Aaron Turner для операционных систем UNIX (и Win32 под Cygwin), которые дают вам возможность использовать ранее захваченный трафик в формате libpcap для тестирования различных сетевых устройств.
Pirni Sniffer	Pirni — это первый в мире нативный (родной) сетевой сниффер для iPhone. Wi-FI iPhone'a имеет некоторые большие недостатки в аппаратном обеспечении, которые препятствуют должным образом перевести устройство в режим promiscious.
Ufasoft Snif	Ufasoft Snif — это сетевой сниффер, предназначенный для захвата и анализа покетов проходящих через сеть. Используя драйвер пакетов, он запрашивает все пакеты в сети, в которой находится драйвер сетевой карты (даже если пакеты не адресованы этому компьютеру).

Перечисление	
dnsenum	Цель Dnsenum — собрать так много информации о домене, как это возможно.
DumpSec	SomarSoft's DumpSec — это программа аудита безопасности для Microsoft Windows NT/XP/200x.
LDAP Browser	LDAP Browser — это главный клиент директорий LDAP в стиле Explorer, доступный для платформ Win32.
NBTEnum	NetBIOS Enumeration Utility (NBTEnum) — это утилита под Windows, которая может быть использована для перечисления информации NetBIOS от одного хоста или диапазонов хостов.

nbtscan	Этот инструмент может сканировать на открытые NETBIOS имена серверов в локальной или удалённой TCP/IP сети, а это является первым шагов для поиска открытых общих ресурсов.
wmi client	Это реализация клиента DCOM/WMI, основанная на источниках Samba4. Программа использует механизмы RPC/DCOM для взаимодействия со службами WMI на машинах Windows 2000/XP/2003.
Dnsmap	Dnsmap, в первую очередь, предназначен для использования пентестерами во время фазы сбора информации при оценке безопасности инфраструктуры.
Dnsrecon	Одной из лучших функций этого инструмента, дающей прекрасные результаты, является перечисление служебных записей SRV.
Dnstracer	Dnstracer определяет, откуда заданный сервер доменных имён (DNS) получает свою информацию и следует по цепочке DNS серверов приходя к тому серверу, которые является первоначальным источником данных.

Сетевые инструменты	
fragroute	fragroute перехватывает, модифицирует и перезаписывает исходящий трафик, предназначенный для указанного хоста.
hping	hping — ассемблер/анализатор командный строки ориентированный на TCP/IP пакеты.
Scapy	Scapy — это мощная интерактивная программа манипуляции пакетами. Она способна подделывать или декодировать пакеты многих протоколов, отправлять их по проводу, захватывать их, проверять на соответствие запросы и ответы и многое другое.
Stunnel	Программа stunnel предназначена для работы обёрткой шифрования SSL между удалённым клиентом и локальным (запускаемые inetd) или удалённым сервером.
tcptraceroute	tcptraceroute это использующая TCP пакеты реализация трассировки. Обычно используют traceroute(8), отсылающую либо UDP, либо ICMP ECHO пакеты с TTL один и увеличением TTL вплоть до достижения пункта назначения.

tracetcp	tracetcp — трассирующая утилита командной строки под WIN32, которая использует пакеты TCP SYN, а не ICMP/UDP пакеты, которые обычно используются для этого в других реализациях, что приводит к обходу шлюзов, блокирующих традиционные пакеты трассировки.
Yersinia	Yersinia — сетевой инструмент, созданный для получения преимущества из некоторых слабостей различных сетевых протоколов. Программа анализирует и тестирует развёрнутые сети и системы.
Nemesis	Nemesis — это утилита командной строки под UNIX подобные и Windows системы для создания и инжекта пакетов. Nemesis хорошо подойдёт для тестирования систем обнаружения вторжений в сеть (Network Intrusion Detection Systems), файерволов, IP стеков и множества других задач. Будучи утилитой командной строки, Nemesis великолепно подходит для автоматизации и скриптинга.

Беспроводные	
Aircrack-ng	Aircrack — программа по взлому ключей 802.11 WEP и WPA-PSK, она может восстановить ключи, когда достаточно захвачено пакетов с данными.
Kismet	Kismet это детектор беспроводных сетей 802.11 layer2, сниффер система выявления вторжения. Kismet будет работать с любыми беспроводными картами, которые поддерживают режим сырого мониторинга (raw monitoring — rfmon) и может снифить трафик 802.11b, 802.11a и 802.11g.
NetStumbler	NetStumbler поставляет инструменты, которые помогут вам обнаружить стандарты 802.11 a/b/g WLAN. Хотя вардрайвинг является главным главным использованием этой программы, она также может быть использована для верификации сетевых настроек.
AirGrab WiFi Radar	AirGrab WiFi Radar — это инструмент для отображения информации о базовых станциях Apple Airport и других WiFi (802.11b/g/n) беспроводных точек доступа.
AirMobile agent	Клиентское приложение загружается на ваш PDA или мобильный телефон Windows где оно будет работать в тихом режиме в фоне. Если приложение находит мошенническую точку доступа, то она будет исследовать ТД на предмет является ли она прямой угрозой для вашей сети.
AirRadar 2	AirRadar позволяет вам сканировать на наличие открытых сетей и помечает их как избранные или фильтрует их. Просматривайте детальную сетевую информацию, график уровня сигнала сети и

	автоматически подключайтесь к открытым точка в радиусе доступности.
iStumbler	iStumbler — это лидирующий инструмент по обнаружению беспроводных сетей для Mac OS X, он имеет плагины для нахождения сетей AirPort, Bluetooth устройств, служб Bonjour и информацию по расположению с вашим Mac.
KisMAC	KisMAC — это приложение с открытым исходным кодом, бесплатное, которое является сниффером/сканером для Mac OS X. У него есть преимущества по сравнению с MacStumbler / iStumbler / NetStumbler в том, что оно использует режим наблюдения и пассивное сканирование.
WirelessMon	WirelessMon — это программный инструмент, который позволяет пользователям мониторить статус беспроводного WiFi адаптера(ов) и собирать информацию о близлежащих беспроводных точках доступа и хот-спотах в реальном времени.
Vistumbler	Vistumbler это сканер беспроводных сетей, написан на AutoIT для Vista, Windows 7, and Windows 8. WiFiDB — это база данных, написанная на PHP и хранящаяся в файлах Vistumbler VS1. Хранит треки о всех точках доступа с GPS, картах в kml, графиках сигнала, статистики и прочем.
WaveStumbler	WaveStumbler — это консольный составитель карт сетей, основанных на 802.11 под Linux. Он рапортует о базовой информации ТД, такой как канал, WEP, ESSID, MAC и т.д.
Xirrus Wi-Fi Inspector	Xirrus Wi-Fi Inspector — это мощный инструмент для управления и решения проблем с Wi-Fi в компьютерах с Windows XP SP2 и более поздних, Vista, или 7. Создан для тестирования характеристик целостности и производительности вашего Wi-Fi соединения.
AirMagnet VoFi Analyzer	AirMagnet VoFi Analyzer — единственное в индустрии решение для разрешения проблем голос-через-WLAN в полевых условиях. VoFi Analyzer обеспечивает полный анализ зашифрованного WLAN трафика, оценивает все звонки с точки зрения качества звонка и активно идентифицирует проблемы всех видов, включая проблемы с телефоном, проблемы с роумингом, проблемы с QoS и RF. *Программа платная — это похоже на рекламную вставку — оставлю из уважения к труду авторов подборки.*

Airpwn	Airpwn — это фреймворк для 802.11 (беспроводных) инжектов пакетов. Airpwn прослушивает входящие беспроводные пакеты и если дата соответствует заданному в файлах настройки образцу, в пользовательское содержимое вставляется “spoofed” от беспроводной точки доступа. С точки зрения беспроводного клиента, airpwn становится сервером.
WifiScanner	WifiScanner — это инструмент, который был создан для обнаружения беспроводных узлов (например, точек доступа и беспроводных клиентов. Он распространяется по лицензии GPL. Он работает с картами CISCO® card и prism картой с драйвером hostap или драйвером wlan-ng, prism54g, Hermes/Orinoco, Atheros, Centrino, … Встроена система IDS для выявления аномалий вроде узурпации MAC.

Bluetooth	
Haraldscan	Сканер Bluetooth под Linux и Mac OS X. Harald Scan способен выявить мажорные и минорные классы устройств, а также попытке резолвить MAC адрес устройства для большинства известных вендоров Bluetooth MAC.
FTS4BT	FTS4BT — передовой анализатор протокола Bluetooth. Разработчики и инженеры по тестированию полагаются на FTS4BT когда проходят цикл разработки, отладки, тестирования, верификации и квалификации.
BlueScanner	BlueScanner — это bash скрипт, который реализует сканер Bluetooth устройств. Этот инструмент создан для извлечения всей возможной информации из Bluetooth устройства без необходимости сопряжения.
Blooover II	Blooover II — это инструмент для аудита, основан на Java (J2ME). Он существует в виде версии Blooover II для аудита мобильных J2ME и в издании для производителей. Простая утилита для тестирования уязвимостей.
BTScanner	BTScanner для XP — это инструмент аудита окружения Bluetooth под Microsoft Windows XP, реализация использует библиотеки bluecove (открытую реализацию JSR-82 Bluetooth API для Java).
BlueSpam	BlueSpam ищет всевозможные устройства bluetooth и отправляет на них файл (спамет их) если они поддерживают OBEX. По умолчанию будет отправлен маленький текст. Для настройки сообщения, которое должно

	быть отправлено, вам нужен наладонник с картой SD/MMC card, там вы создаёте директорию /PALM/programs/BlueSpam/Send/ и кладёте туда файл (будут работать файлы любого типа .jpg всегда клёво) который вам хотелось бы отправить.
BTCrawler	Приложение используется для поиска Bluetooth устройств и обеспечиваемых ими служб. Запустите на устройстве с поддержкой J2ME, MIDP 2.0 и JSR082 (Java API для Bluetooth)
Bluediving	Bluediving — это набор для тестирования на проникновение Bluetooth. Он реализует атаки вроде Bluebug, BlueSnarf, BlueSnarf++, BlueSmack, имеет аткие особенности как спуфинг адреса Bluetooth, шел AT и сокета RFCOMM и реализация инструментов вроде carwhisperer, bss, генератор пакетов L2CAP, сбрасыватель соединений L2CAP, сканер RFCOMM и режим сканирования greenplaque scanning mode (используя более чем одно hci устройство).
Bluesnarfer	Bluesnarfer крадёт информацию из беспроводных устройств через Bluetooth соединение. Связь может быть между мобильными телефонами, PDA или компьютерами. Вы можете иметь доступ к календарю, списку контактов, почтовым и текстовым сообщениям.

Веб сканеры	
Arachni	Arachni — это полностью автоматизированная система, которая в полную силу проверяет ваш веб-сайт "на вшивость". Как только сканирование запущено, это приложение больше не будет беспокоить вас, вмешательство пользователя больше не требуется.
Burp Suite	Burp Suite — это интегрированная платформа для выполнения тестирования безопасности веб-приложений.
CAL9000	CAL9000 — это коллекция инструментов тестирования безопасности веб-приложений, дополненная функциями установки веб-прокси и автоматических сканеров. CAL9000 даёт вам гибкость и функциональность, которая вам нужна для более эффективных усилий при ручном тестировании.
CAT	CAT создан для удовлетворения потребностей при ручном тестировании на проникновение веб-приложений для более комплексных, требовательных задач в тестировании приложений.

CookieDigger	CookieDigger помогает выявить слабое создание куки и небезопасные реализации управление сессиями в веб-приложениях. Этот инструмент работает собирая и анализируя кукиз, которые генерируются веб-приложением для множества пользователей.
DIRB	DIRB — это сканер веб контента. Он ищет существующие (и/или скрытые) веб объекты. В основе его работы лежит поиск по словарю, он формирует запросы к веб-серверу и анализирует ответ.
Fiddler	Fiddler — это отладочный веб-прокси, который записывает весь трафик HTTP(S) между вашим компьютером и Интернетом. Fiddler позволяет вам инспектировать весь HTTP(S) трафик, устанавливать точки прерывания и "играться" с входящими и исходящими данными.
Gamja	Gamja будет искать слабые точки — XSS(межсайтовый скриптинг) и SQL-инъекции — а также ошибки валидации URL параметра. Кто может знать, какой параметр является слабым параметром? Gamja будет полезной в поиске уязвимостей [XSS, ошибок валидации, SQL-инжектов].
Grendel-Scan	Инструмент для автоматического сканирования безопасности веб-приложений. Также присутствует много функция для ручного тестирования на проникновение.
HTTrack	HTTrack — это бесплатная и простая в использовании утилита оффлайн браузера. Она позволяет вам загружать сайт из Всемирной Сети на локальный диск, создавать рекурсивную структуру каталогов, получать HTML, картинки и другие файлы с сервера на ваш компьютер.
LiLith	LiLith — это инструмент, написанный на Perl для аудита веб-приложений. Этот инструмент анализирует веб-страницы в поиска тэга <form>, который обычно перенаправляет на динамичные страницы, на которых можно искать SQL-инъекции и другие слабости.
Nikto2	Nikto — это сканер веб-серверов с открытым исходным кодом (GPL), он выполняет полное тестирование веб-серверов по множеству параметров, включая более 6500 потенциально опасных файлов/CGI.
Paros	Программа под названием ‘Paros’ для людей, которые нуждаются в безопасности их веб-приложений. Она бесплатная и полностью написана на Java.
Powerfuzzer	Powerfuzzer — это высоко автоматизированный и полностью настраиваемый веб-фаззлер (основанный на HTTP протоколе фаззлер

	приложений), он основан на многих других доступных фаззлеров с открытым исходным кодом и информации, собранной из ряда источников безопасности и веб-сайтов.
ProxyScan.pl	proxyScan.pl — это инструмент безопасного тестирования на проникновение для сканирования хостов и портов через веб прокси сервер. Особенности включают различные HTTP методы, такие как GET, CONNECT, HEAD, а также диапазоны хостов и портов.
Ratproxy	Полуавтоматический, в значительное мере пассивный инструмент аудита безопасности веб-приложений, оптимизирован на точное и чувствительное выявление и автоматическую аннотацию потенциальных проблем и связанных с безопасностью образцов построения, основанных на наблюдении существующего, генерируемого пользователем трафика в комплексной среде web 2.0.
ScanEx	Это простая утилита, которая запускается против целевого сайта и ищет внешние ссылки и вредоносные кроссдоменные инжекты. Т.е. она выявляет сайты, которые уязвимы к XSS и в которых уже подложен инжект.
Scrawlr	Scrawlr, создана HP Web Security Research Group совместно MSRC, если сказать коротко, это SQL-инжектор и кролер. Scrawlr обойдёт весь веб-сайт в это же время анализируя параметры каждой веб-страницы на уязвимость SQL Injection.
Springenwerk	Springenwerk — это бесплатный сканер безопасности кроссайтового скриптинга (XSS), написанный на Python.
Sqlmap	sqlmap — это инструмент с открытым исходным кодом для тестирования на проникновение, который автоматизирует процесс выявления и эксплуатирования бреши SQL-инъекций, при этом она позволяет получить все данные с сервера базы данных.
Sqlsus	sqlsus — инструмент с открытым исходным кодом для MySQL-инъекций и захвата, написан на Perl.
THCSSLCheck	Инструмент Windows, который проверяет удалённый ssl стек на поддерживаемые шифры и версию.
w3af	w3af — это фреймворк атаки и аудита веб-приложений. Цель проекта — создать фреймворк для помощи в обеспечении безопасности ваших веб-приложений, путём поиска и эксплуатирования уязвимостей веб-

	приложений.
Wapiti	Wapiti позволяет вам проводить аудит безопасности веб-приложений. Он выполняет сканирование "чёрный ящик" (без доступа к исходному коду), т.е. он не изучает исходный код приложения, а работает с уже развернутыми сайтами, он ищет в них скрипты и формы, в которые можно было бы повставлять данные.
Webfuzzer	Webfuzzer — это инструмент, который может быть полезен как тестерам на проникновение, так и веб-мастерам. Как характеризует сам автор своё детище "это сканер веб уязвимостей бедного человека".
WebGoat	WebGoat содержит намеренно небезопасные веб-приложения J2EE, поддерживаемые OWASP, они предназначены быть уроками по безопасности веб-приложений.
Websecurify	Websecurify Suite — это решение по безопасности веб-приложений, предназначенных для запуска исключительно из вашего веб-браузера.
WebSlayer	WebSlayer — это инструмент предназначенный для брут-форсинга веб-приложений, он может использоваться для нахождения источников, на которые не ведут ссылки (каталоги, сервлеты, скрипты и т.д.), брутфорсятся GET и POST параметры, брутфорсяться параметры форм (пользователь/пароль), фаззлинг и т.д. Этот инструмент имеет генератор запросов и прост и эффективен для анализа.
WhatWeb	WhatWeb идентифицирует веб-сайты. Его цель — ответить на вопрос, “Что это за веб-сайта?”. WhatWeb распознаёт веб-технологии, включая системы управления содержимым (CMS), платформы для блоггинга, статистику/анализ пакетов, JavaScript библиотеки, веб-сервера и встроенные устройства.
Wikto	Wikto — это Nikto для Windows – но с парочкой модных функций, включая проверку кода на ошибки логики Fuzzy, фоновый майнер, поиск каталогов с использованием Google и мониторинг запросов/ответов HTTP в реальном времени.
WSDigger	WSDigger — это бесплатный с открытым исходным кодом инструмент, созданный в McAfee Foundstone для автоматической проверки веб-служб по принципу "чёрного ящика" (без доступа к исходному коду) — фактически, для тестирования на проникновение. WSDigger — это более чем инструмент, это фреймворк для тестирования веб-служб.

XSSploit	XSSploit — это мультиплатформенный сканер и эксплуататор межсайтового скриптинга, он написан на Python. Он был создан для помощи в поиске и использовании XSS уязвимостей в миссиях тестирования на проникновение.
Fireforce	Fireforce это расширение для Firefox, созданное для выполнения брут-форс атак на GET и POST формы. Fireforce может использовать словари или генерировать пароли, основываясь на разных наборах символов.
Netsparker	Netsparker — это сканер безопасности веб-приложений с поддержкой как выявления так и эксплуатации уязвимостей. Его цель — работать без ложных срабатываний, сообщать только о реальных уязвимостях после успешного их эксплуатирования или после проверки их другими способами.
Havij	Havij — это автоматизированный инструмент по SQL-инжектам, которые помогает тестерам на проникновение находить и эксплуатировать SQL-инъекции в веб-странице.

Уязвимости в базах данных	
Berkeley DB	Oracle Berkeley DB — это семья открытых, встраиваемых баз данных, которые позволяют разработчикам инкорпорировать в их приложения быстрые, масштабируемые, транзакционные базы данных с промышленным уровнем надёжности и доступности.
Database browser	Database browser — это универсальный редактор таблиц. Это простой в использовании инструмент, который позволяет пользователям подключаться к любой базе данных и бродить по ней или изменять данные, запускать sql скрипты, экспортировать и печатать данные.
Db2utils	db2utils — эта маленькая коллекция утилит db2. В данный момент она включает три различные утилиты: db2disco, db2fakesrv и db2getprofile.
Oracle Auditing Tools	Oracle Auditing Tools — это набор инструментов, которые могут быть использованы для аудита безопасности внутри сервера базы данных Oracle.
Oscanner	Oscanner — это оценочный фреймворк Oracle, разработанный на

	Java. Он имеет основанную на плагинах архитектуру и поставляется с парой плагинов.
SQL Auditing Tools	SQLAT — это набор инструментов, которые могут быть полезны при пентестинге MS SQL сервера. Эти инструменты всё ещё в разработке, но уже достаточно стабильны. Эти инструменты выполняют атаки по словарю, загружают файлы, читают регистр и дампят SAM.
THC-ORACLE	THC представляет крипто документ по анализу механизма аутентификации, используемом в базах данных Oracle. THC дальнейшие релизы практических инструментов для захвата и взлома паролей от баз данных Oracle за секунды.
thc-orakelcrackert11g	OrakelCrackert это взломщик хешей паролей от баз данных Oracle 11g, используя слабости в стратегии хранения паролей Oracle. С Oracle 11g были представлены чувствительные к регистру хеши SHA1.
DBPwAudit	DBPwAudit — это Java инструмент, который позволяет выполнять различный онлайн аудиты качества паролей для нескольких движков баз данных. Дизайн приложения позволяет легко добавлять дополнительные драйвера баз данных простым копированием новых JDBC драйверов в директорию jdbc.
MYSQLAudit	Скрипт наPython для базового аудита распространённых ошибок конфигурации в MySQL.
sqlininja	sqlininja эксплуатирует веб-приложения, которые используют Microsoft SQL Server в качестве фоновой базы данных. Она фокусируется на получении работающего шелла на удалённом хосте. sqlninja не ставит на первое место поиск SQL-иъекций, но автоматизирует процесс эксплуатации, как только она была найдена.
GreenSql	GreenSQL это файервол с открытым исходным кодом для баз данных, используемый для защиты от атак SQL-инъекции. GreenSQL работает как прокси и имеет встроенную поддержку для MySQL и PostgreSQL.

Сканеры уязвимостей	

Metasploit Framework	The Metasploit Framework — это продвинутая платформа с открытым исходным кодом для разработки, тестирования и эксплуатирования кода.
OpenVAS	OpenVAS — это фреймворк нескольких служб и инструментов, предлагающих всестороннее и мощное решение по управлению сканированием уязвимостей.
Nessus	Nessus выявляет, сканирует и профилирует многочисленные устройства и источники для увеличения безопасности и соответствия в вашей сети.
Porkbind	Porkbind — это многопоточный сканер серверов имён, который может рекурсивно делать запросы на сервера имён поддоменов для строк версий (например, сервера имён sub.host.dom, затем сервера имён host.dom).
Canvas	Immunity CANVAS от Immunity делает доступными сотни эксплойтов, систему автоматического эксплуатирования и всесторонний, надёжный фреймворк по разработке эксплойтов для тестерировщиков на проникновение и профессионалов по безопасности по всему миру.
Social-EngineerToolkit (SET)	Social-Engineer Toolkit (SET) создан для продвинутых атак на "человеческий фактор". SET был выпущен вместе с запуском http://www.social-engineer.org и быстро стал стандартным инструментом в арсенале пентестеров.
Acunetix	Acunetix web vulnerability scanner — это инструмент созданный для выявления дыр в безопасности в ваших веб-приложениях, которые при атаке, вероятно, станут слабым звеном, через которые будет получен незаконный доступ к вашей системе и данным. Он ищет множество уязвимостей, включая SQL-инъекции, межсайтовый скриптинг и слабые пароли.
RIPS	RIPS — это инструмент, написанный на PHP, для поиска уязвимостей в PHP приложениях используя статический анализ кода.
Rapid7 NeXpose	Rapid7 NeXpose — это сканер уязвимостей, цель которого поддержать полный жизненный цикл управления уязвимостями, включая обнаружение, выявление, верификацию, классификацию риска, анализ влияния, описание и смягчение. Он интегрирован с Rapid7 от Metasploit для исследования уязвимостей.

VulnDetector	VulnDetector — это проект нацеленный на сканирование веб-сайта и выявление различных связанных с веб уязвимостью безопасности в веб-сайте. В настоящее время VulnDetector может выявить такие уязвимости как межсайтовый скриптинг (XSS) и SQL-инъекции (SQLI) в веб-скриптах, но не имеет простого в работе интерфейса.
Damn Small SQLi Scanner	DSSS поддерживает blind/error SQLi тесты, сканирование в одну глубину и продвинутое сравнение различных атрибутов, чтобы отличить слепые ответы (заголовки, статусные коды HTTP, отфильтрованного только по длине текста и нечёткое сравнение самого контента). Если вы удовлетворены результатами сканирования коммерческих инструментов, то я уверен, что вы будете ещё более удовлетворены этим инструментом.
CAT.NET	CAT.NET — это анализатор исполнимого кода, который помогает выявить распространённые варианты определённых преобладающих уязвимостей, которые могут привести к атакам общего вектора, таким как межсайтовый скриптинг (XSS), SQL-инжекты и XPath инжекты.
Peach Fuzzer	Peach — это SmartFuzzer, который может и составлять запросы как генерацией, так и перестановкой. Peach требует создание файлов PeachPit, которые определяют структуру, тип информации и отношения для данных.
GFI LanGuard	GFI LanGuard — это сканер безопасности сети и уязвимостей, созданный для помощи в управлениями патчами, сетью и аудита программного обеспечения и оценки уязвимостей. Цена зависит от количества IP адресов для сканирования. Есть бесплатная пробная версия для сканирования до 5 IP адресов.
MBSA	Microsoft Baseline Security Analyzer (MBSA) — это простой в использовании инструмент, предназначенный для IT профессионалов, который помогает малым и средним бизнесам определять их состояние безопасности в соответствии с рекомендациями по безопасности Microsoft и предлагает конкретные рекомендации по итогу проверки.

Уязвимые приложения	
Damn Vulnerable	Damn Vulnerable Web App (DVWA) это веб-приложение на

Web Application (DVWA)	PHP/MySQL, которое чертовски уязвимое. Главная его цель — это помощь профессионалам по безопасности для тестирования их способностей и инструментов не нарушая закон, помочь веб-разработчиком лучше понимать процессы безопасности веб-приложений и помочь учителям/студентам научить/изучить безопасности веб-приложений в обстановке класса.
Damn Vulnerable Linux	Damn Vulnerable Linux (DVL) — этот дистрибутив Linux всем хорош, не так ли? Его разработчики потратили часы, начиняя его сломанным, плохо сконфигурированным, устаревшим и уязвимым программным обеспечением, что делает его уязвимым для атак. DVL не создан для запуска на вашем компьютере — это инструмент для студентов изучающих безопасность.
Metasploitable	Metasploitable — это традиционная уязвимая виртуальная машина Linux. Эта VM может быть использована для проведения тренингов по безопасности, тестировании инструментов по безопасности и практике в тестировании популярных техник по проникновению.
Kioptrix	Этот образ Kioptrix VM является лёгкой задачей. Цель игры — получить доступ рута любыми возможными способами, кроме реального взлома сервера VM или игрока). Цель этой игры — научить основным инструментам и техникам в оценке уязвимостей и их эксплуатации.
HoneyDrive	HoneyDrive — это виртуальное устройство (OVA) с установленной Xubuntu Desktop 12.04 32-битной версией. Оно содержит различные пакеты такого программного обеспечения как "приманки" — honeypot. Это Kippo SSH honeypot, Dionaea malware honeypot, Honeyd low-interaction honeypot, Glastopf web honeypot вместе с Wordpot, Thug honeyclient и другие.
Badstore	Badstore.net предназначен для того, чтобы вы понимали, как хакеры охотятся на уязвимости веб-приложений и чтобы вы понимали как уменьшить вашу подверженность.
OWASP Insecure Web App Project	InsecureWebApp — это веб-приложение, которое включает приложения с распространёнными уязвимостями. Это цель для автоматического и ручного тестирования на проникновения, анализа исходного кода, оценки уязвимостей и моделирования угроз.
VulnApp	VulnApp — это ASP.net приложение под лицензией BSD,

	реализующее самые распространённые приложения, с которыми мы сталкиваемся в обстоятельствах проведения своих тестов на проникновение.
OWASP Vicnum	Vicnum это проект OWASP, состоящий из уязвимых веб-приложений, основанных на играх, обычно использующих для убийства времени. Эти приложения демонстрируют популярные проблемы веб-безопасности, такие как межсайтовый скриптинг, sql инжекты и проблемы с манипуляцией сессиями.
OWASP Broken Web Applications Project	The Broken Web Applications (BWA) Project производит виртуальную машину с запущенными различными приложениями с известными уязвимостями.
LAMPSecurity	Тренинг LAMPSecurity — это серия образов виртуальных машин вместе с дополнительной документацией, предназначенной для обучения безопасность Linux, Apache, PHP, MySQL.
Virtual Hacking Lab	Зеркало намеренно небезопасных приложений и старого программного обеспечения с известными уязвимостями. Используется концептов / тренингам по безопасности / в целях обучения. Доступен как в образах виртуальных машин или как live iso или в по отдельности.
WAVSEP	The Web Application Vulnerability Scanner Evaluation Project — это уязвимое веб-приложение, разработанное чтобы помочь оценить особенности, качество и точность сканеров уязвимостей веб-приложений. Эта оценочная платформа содержит набор уникальных уязвимых веб-страниц, которые могут использоваться для тестирования различных свойств сканеров веб-приложений.
Moth	Moth — это образ VMware с настроенными уявзимыми веб-приложениями и скриптами, которые вы можете использовать для тестирования сканеров безопасности веб-приложений, тестировать инструменты статичного анализа кода (SCA), давая вводный курс в безопасность веб-приложений.
SecuriBench	Stanford SecuriBench — это набор реальных рабочих программ для использования в качестве испытательного полигона для статических и динамических инструментов безопасности. Выпуск .91a фокусируется на веб-приложениях написанных на Java.
NETinVM	NETinVM это единичный образ для виртуальной машины VMware

	или VirtualBox, который содержит готовую для запуска серию виртуальных машин User-mode Linux (UML) (Linux пользовательского режима), которые, когда запущены, соответствуют целой компьютерной сети внутри виртуальной машины VMware или VirtualBox.
Dojo	Web Security Dojo — это настроенная автономная обучающая среда по безопасности веб-приложений. Для загрузки доступны версии под VirtualBox и VMware. Dojo — это проект с открытым исходным кодом, цель которого — быть обучающей средой, которую можно использовать как платформу для тестирования на проникновение, поскольку в неё уже включены уязвимые службы и приложения.

Live CD	
BackTrack	BackTrack — это основанный на Linux арсенал для тестирования на проникновение, которые помогает профессионалам в безопасности в их оценке, находясь в их чисто родной среде, выделенной для хакинга. В настоящее время дистрибутив переименован в Kali Linux.
Kali Linux	Kali Linux (ранее известный как BackTrack) — это основанный на Debian дистрибутив с коллекцией инструментов по безопасности и криминалистике. Его особенностями являются своевременные обновления безопасности, поддержка архитектуры ARM, выбор из четырёх популярных окружений рабочего стола и лёгкое обновление до новых версий дистрибутивов.
BackBox	BackBox — это дистрибутив Linux, основанный на Ubuntu. Он был создан для осуществления тестов на проникновение и оценки безопасности. Создан быть быстрым, простым в использовании и обеспечивать минимальное, но полное окружение рабочего стола; благодаря его собственным репозиториям программного обеспечения, всегда остаётся обновлённым до последних стабильных версий большинства наиболее используемых и хорошо известных инструментов для этического хакинга.
Samurai	The Samurai Web Testing Framework — это live окружение linux, которое было настроено для функционирования в качестве окружения для пентестинга. CD содержит лучшие опен сорсные и бесплатные инструменты, которые фокусируются на тестировании и атаке веб-сайтов.

Katana	Katana — это портативный мультизагрузочный набор по безопасности, который собрал вместе много современных дистрибутивов по безопасности и портативных приложений для запуска на одной флешке. Он включает дистрибутивы, которые сфокусированы на пентестинге, аудите, криминалистическом исследовании, восстановлении системы, анализе сети и удалении зловредных программ. Katana также поставляется с более чем 100 портативными приложениями Windows; такими как Wireshark, Metasploit, NMAP, Cain & Abel и многими другими.
blackbuntu	Дистрибутив для тестирования на проникновение, основан на Ubuntu 10.10, который специально был создан для тренировки студентов и практикантов по информационной безопасности.
Bugtraq	Bugtraq — это дистрибутив, основанный на ядре 2.6.38, имеет широкий спектр инструментов для проникновения и криминалистики. Bugtraq можно установить с Live DVD или USB диска, этот дистрибутив собран из последних пакетов, настроен, ядро обновлено и пропатчено для лучшей производительности и распознавания различного железа, включены патчи для беспроводных инжектов, которые другие дистрибутивы не распознают.
Network Security Toolkit (NST)	Загрузочный ISO live CD/DVD (NST Live) основан на Fedora. Этот набор инструментов был создан для обеспечения простого доступа к самым качественным приложениями по безопасности сети с открытым исходным кодом и должен запускаться на большинстве x86/x86_64 платформ.
Pentoo	Pentoo — это LiveCD дистрибутив для тестирования на проникновение на основе Gentoo.Его особенности — множество инструментов для аудита и тестирования сетей, от сканирования и выявления до эксплуатирования уязвимостей.
BlackArch	BlackArch дистрибутив основанный на Arch.Там более 600 инструментов в репозитории пакетов BlackArch. The BlackArch live ISO поставляется с множеством менеджеров окон, включая dwm, Awesome, Fluxbox, Openbox, wmii, i3 и Spectrwm. Репозиторий пакетов BlackArch совместим с существующими установками Arch.

Глава 17. База данных эксплойтов от Offensive Security (создателей Kali Linux)

Git репозиторий Базы данных эксплойтов и searchsploit: сходства и различия

База данных эксплойтов (The Exploit Database) — это архив публичных эксплойтов и соответствующего уязвимого программного обеспечения, она создаётся и поддерживается для тестировщиков на проникновение и исследователей уязвимостей. Её цель — это создание и обслуживание самой полной коллекции эксплойтов, собранных от прямых подписок, списков почтовых рассылок и других публичных источников. Эксплойты представленных в свободном доступе в базе данных с удобной навигацией. База данных эксплойтов — это в большей степени хранилище эксплойтов и рабочих моделей, чем советы, что делает её ценным ресурсом для тех, кому нужны рабочие данные прямо сейчас. Говоря простым языком, большая часть содержащегося в базе — это рабочие эксплойты.

Репозиторий обновляется ежедневно — по мере того, как становятся известными новые эксплойты. Дополнительно обратите внимание на Базу данных эксплойтов бинарных файлов (Exploit Database Binary Exploits). В этом месте собраны скомпилированные и готовые файлы тех эксплойтов, которые нужно компилировать или которые нужно создавать особым образом. В Kali Linux эти бинарники отсутствуют. Если вы нашли эксплойт, который нужно компилировать, то смотрите имя файла, например это 31583.txt. Отбрасываем расширение и ищем по названию 31583 в базе данных бинарников. Находим там файл 31583.docx — это не бинарник, это уже рабочий концепт. Кроме собственно бинарников, там присутствуют особым образом сделанные картинки, базы данных, я видел аудио файл, ну и, конечно, много исполнимых файлов. Думаю, причиной, по которым эти файлы не попали в Kali является то, что многие из этих файлов определяются антивирусными программами как вирусы.

Об Exploit Database Binary Exploits как-то не очень много говорят — я узнал о ней совсем недавно, чисто случайно. Её также можно клонировать себе в систему и искать ещё и по ней.

К репозиторию также прилагается утилипа **searchsploit**, которая позволяет производить поиск по базе по одному или по нескольким словам.

Итого, у нас имеется 3 очень похожих ресурса:

- Git репозиторий Базы данных эксплойтов
- Программа searchsploit в Kali Linux
- Веб-сайт https://www.exploit-db.com/

Программа searchsploit в Kali Linux отличается от Git репозитория тем, что:

- её база обновляется не каждый день
- отсутствуют некоторые ключи, которые есть в утилите из Git репозитория (-u, -t, -w, —colour, —id)
- разное количество файлов в базах

Веб-сайт www.exploit-db.com — это что-то вроде графического интерфейса для всего этого богатства. Веб-сайт мне нравится тем, что показывает последние поступления. Если нужен какой-то свежак, то за ним нужно идти именно сюда.

Установка searchsploit

На Kali Базу данных эксплойтов смысла устанавливать нет, там практически то же самое в searchsploit.

Кстати, если вы собираетесь пользоваться searchsploit (хоть в Kali, хоть в другом дистрибутиве), то посмотрите статью «Metasploit Exploitation Framework и searchsploit — как искать и как использовать эксплойты». Там есть полезные советы, которые не попали в эту заметку.

Итак, я буду устанавливать searchsploit (Базу данных эксплойтов) на Linux Mint (аналогично для Ubuntu и Debian).

Для сторонних программ я создал в пользовательском каталоге директорию opt:

```
1| mkdir opt
```

Переходим туда:

```
1| cd opt
```

Если у вас ещё нет git, то установите его:

```
1| sudo apt-get install git
```

Клонируем репозиторий:

```
1| git clone https://github.com/offensive-security/exploit-database.git
```

Поиск по Базе данных эксплойтов

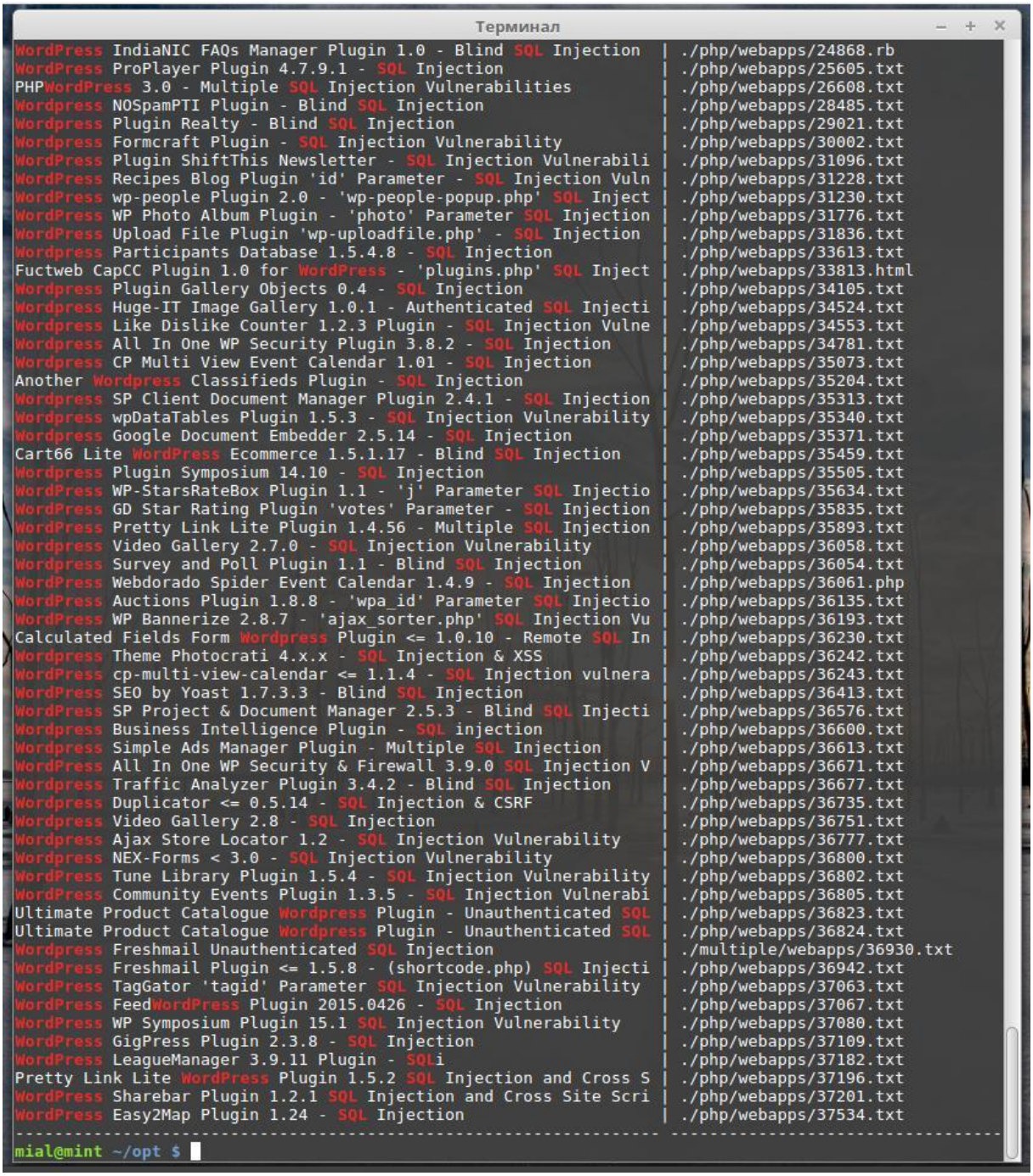
Запускать searchsploit из любого места так:

```
1| ~/opt/exploit-database/searchsploit
```

Пример поиска:

```
1| ~/opt/exploit-database/searchsploit wordpress sql
```

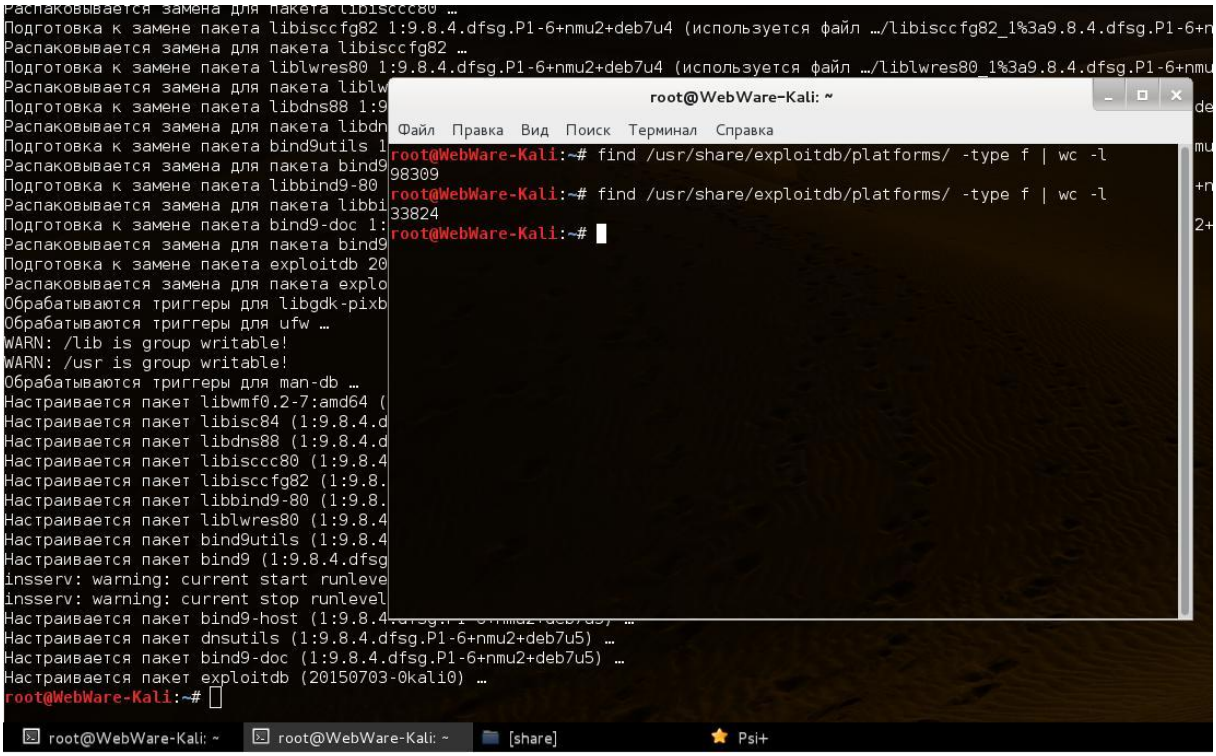
Т.е. я ищу по ключевым словам wordpress и sql:



Мне стало интересно, одинаковое ли количество файлов в установленной Базе данных эксплойтов и в базе searchsploit, которая в Kali (благо, в Kali как раз сегодня обновилась exploitdb):

1|	mial@mint ~/opt $ find /home/mial/opt/exploit-database/platforms/ -type f | wc -l 33888
2|	root@WebWare-Kali:~# find /usr/share/exploitdb/platforms/ -type f | wc -l 98309
3|	root@WebWare-Kali:~# find /usr/share/exploitdb/platforms/ -type f | wc -l 33824

Команду выполнял 2 раза — до принятия сегодняшних обновок и сразу же после их принятия:



Ничего себе обновились — минус 65 тысяч файлов! Наверное, какие-нибудь дубли или что-то подобное.

Не забывайте время от времени обновлять :

```
1| ~/opt/exploit-database/searchsploit -u
```