

5.

Информация о сетевой маршрутизации полезна для испытателей на проникновение по нескольким причинам. Во-первых, они могут определить, что находится между машиной тестировщика и целевой машиной. Испытатель также может узнать, как работает сеть и как трафик маршрутизируется между целевой машиной и машиной испытателя. Наконец, испытатель может определить, существует ли между целевой и его машиной промежуточный барьер, например брандмауэр или прокси-сервер.

В Kali Linux встроен ряд инструментов, которые позволяют получить информацию о сетевой маршрутизации.

tcptraceroute

Инструмент *tcptraceroute* в дистрибутивах Linux является дополнением к команде *traceroute*. Стандартная команда *traceroute* отправляет целевой машине или UDP, или эхо-пакет ICMP (Internet Control Message Protocol — протокол межсетевых управляющих сообщений) со временем жизни (Time to Live, TTL), равным единице. Значение TTL увеличивается на единицу для каждого хоста до тех пор, пока пакет не достигнет целевой машины. Основное различие между командой *traceroute* и инструментом *tcptraceroute* в том, что последний для целевой машины использует пакет TCP SYN.

Главное преимущество использования *tcptraceroute* состоит в том, что мы можем на пути от машины тестировщика к целевой машине встретить брандмауэр. Брандмауэры часто настраиваются для фильтрации трафика ICMP и UDP, связанного с командой *traceroute*. В этом случае информация о трассировке будет искажена. Использование инструмента *tcptraceroute* позволяет установить TCP-соединение на определенном порте, через который брандмауэр позволит вам пройти, тем самым показав на пути сетевой маршрутизации брандмауэр.

Инструмент *tcptraceroute* использует трехстороннее установление связи TCP, чтобы определить, есть ли доступ через межсетевой экран. Если порт открыт, вы получите пакет SYN/ACK. Если порт закрыт, вы получите пакет RST.

Для запуска *tcptraceroute* в командной строке следует ввести такую команду:

```
# tcptraceroute
```

С этой командой связано несколько функций.

Самая простая функция — выполнение команды в домене. Чтобы продемонстрировать ее, добавьте к команде *traceroute* домен *example.com*:

```
# traceroute www.example.com
```

Отредактированный ответ выглядит следующим образом:

```
traceroute to www.example.com (192.168.10.100), 30 hops max, 40 byte packets
 1 192.168.1.1 (192.168.1.1) 8.382 ms 12.681 ms 24.169 ms
 2 1.static.192.168.xx.xx.isp (192.168.2.1) 47.276 ms 61.215 ms 61.057 ms
 3 * * *
```

```

4 74.subnet192.168.xx.xx.isp (192.168.4.1) 68.794 ms 76.895 ms 94.154 ms
5 isp2 (192.168.5.1) 122.919 ms 124.968 ms 132.380 ms
...
15 * * *
...
30 * * *
```

Как вы можете видеть, в ответе есть несколько строк, информация в которых закрыта звездочками `***`. Если мы посмотрим на выходные данные, то увидим, что по запросу 15 нет никакой информации. Это признак того, что между машиной испытателя и целевой машиной (в нашем случае это домен `example.com`) находится устройство, фильтрующее запросы.

Теперь с помощью команды `tcptraceroute` попробуем обойти эту фильтрацию. Зная, что домен `example.com` находится на веб-сервере, мы воспользуемся командой, чтобы пройти через TCP-порт 80, который является портом HTTP. Введите в командную строку следующее:

```
# tcptraceroute www.example.com
```

На выходе вы получите:

```

Selected device eth0, address 192.168.1.107, port 41884 for outgoing packets
Tracing the path to www.example.com (192.168.10.100) on TCP port 80 (www),
  30 hops max
  1 192.168.1.1 55.332 ms 6.087 ms 3.256 ms
  2 1.static.192.168.xx.xx.isp (192.168.2.1) 66.497 ms 50.436 ms 85.326 ms
  3 * * *
  4 74.subnet192.168.xx.xx.isp (192.168.4.1) 56.252 ms 28.041 ms 34.607 ms
  5 isp2 (192.168.5.1) 51.160 ms 54.382 ms 150.168 ms
  6 192.168.6.1 106.216 ms 105.319 ms 130.462 ms
  7 192.168.7.1 140.752 ms 254.555 ms 106.610 ms
  ...
 14 192.168.14.1 453.829 ms 404.907 ms 420.745 ms
 15 192.168.15.1 615.886 ms 474.649 ms 432.609 ms
 16 192.168.16.1 [open] 521.673 ms 474.778 ms 820.607 ms
```

Как можете видеть из выходных данных `tcptraceroute`, запрос достиг целевой системы.

tctrace

Это еще один инструмент, использующий рукопожатие (квитирование) TCP. Как и `tcptraceroute`, `tctrace` отправляет пакет SYN на определенный хост, и, если ответом на запрос мы получаем SYN/ACK, значит, порт открыт. Пакет RST показывает, что данный порт закрыт.

Для запуска `tctrace` используется следующая команда:

```
# tctrace -i<device> -d<targethost>
```

где `-i<device>` — интерфейс целевой машины, а `-d<targethost>` — доменное имя цели.

Для примера мы выполним `tcptrace`, используя домен `www.example.com` как целевой хост:

```
# tcptrace -i eth0 -d www.example.com
```

На выходе мы получим следующие данные:

```
1(1) [172.16.43.1]
2(1) [172.16.44.1]
3(all) Timeout
4(3) [172.16.46.1]
5(1) [172.16.47.1]
6(1) [172.16.48.1]
7(1) []
...
14(1) [172.16.56.1]
15(1) [172.16.57.1]
16(1) [198.148.81.137] (reached; open)
```

Используем поисковик

Kali Linux содержит много инструментов, позволяющих получить подробную информацию об исследуемом объекте. С помощью инструмента автоматического сбора данных мы можем собрать много информации из общедоступных источников и проанализировать ее. Эти инструменты действуют как поисковые системы и для получения информации о домене могут просматривать различные ресурсы, например Google, сайты социальных сетей или электронную почту. Одним из преимуществ использования этих инструментов является то, что они не ищут непосредственно сайты, а задействуют для получения OSINT (Open Source Intelligence) другие поисковые системы. Применение этих инструментов позволит пентестеру ограничить следы проникновения в целевую систему.

Одни из этих инструментов уже встроены в операционную систему Kali Linux, другие требуют дополнительной установки. В следующих разделах мы расскажем о нескольких инструментах, которые помогут вам собрать большое количество информации.

SimplyEmail. Этот инструмент не только собирает адреса электронной почты, но и выискивает в домене текстовые документы Word и электронные таблицы Excel. Кроме того, существует большое количество различных сайтов и поисковых систем, которые можно использовать. Это такие ресурсы, как Reddit, Pastebin и Canary Bin. Немаловажно, что отчеты создаются в удобном формате HTML.



theharvester — это тоже удобный инструмент для агрегирования адресов электронной почты и другой информации, которая может просочиться с целевого компьютера.

SimplyEmail — сценарий, написанный на Python и состоящий из нескольких модулей. Он легко устанавливается на компьютер.

Чтобы установить SimplyEmail, выполните следующие шаги.

1. Зайдите на сайт GitHub по адресу <https://github.com/killswitch-GUI/SimplyEmail>.
2. Введите следующий код:

```
curl -s
https://raw.githubusercontent.com/killswitch-GUI/SimplyEmail/master/setup/
online-setup.sh | bash
```

3. После запуска сценария он будет готов к работе.

Чтобы открыть меню Help (Справка), введите следующую команду:

```
#!/SimplyEmail.py -h
```

В ответ вы получите следующее:

```
Current Version: v1.0 | Website: CyberSyndicates.com
=====
Twitter: @real_slacker007 | Twitter: @Killswitch_gui
=====
[-s] [-v]
```

Сбор электронной почты является важным этапом многих операций, которые выполняет испытатель на проникновение или «Красная команда». Но нам потребовался хоть и простой, но эффективный способ получить результат, сходный с результатами работы Recon-Ng и theharvester (для запуска введите -h).

Дополнительный аргумент	Описание
-all	Для получения сообщений электронной почты используются не API-методы
-e company.com	Задайте адрес электронной почты пользователя, например ale@email.com
-l	Список загруженных модулей
-t	html/flickr/google. Тест отдельного модуля (для листинга)
-s	Этот аргумент позволяет при анализе электронной почты выбрать режим No-Scope
-v	Укажите этот аргумент для подробного вывода модулей

Чтобы начать поиск, введите следующую команду:

```
#!/SimplyEmail -all -e example.com
```

Начнется выполнение сценария. Учтите, если никакой информации нет, в ответе будут ошибки. Это не означает, что вы сделали ошибку. Просто нужная информация отсутствует. Во время работы инструмента на экране вы увидите следующее:

```
[*] Starting: PasteBin Search for Emails
[*] Starting: Google PDF Search for Emails
[*] Starting: Exalead DOCX Search for Emails
[*] Starting: Exalead XLSX Search for Emails
```

```
[*] Starting: HTML Scrape of Taget Website
[*] Starting: Exalead Search for Emails
[*] Starting: Searching PGP
[*] Starting: OnionStagram Search For Instagram Users
[*] HTML Scrape of Taget Website has completed with no Email(s)
[*] Starting: RedditPost Search for Emails
[*] OnionStagram Search For Instagram Users: Gathered 23 Email(s)!
[*] Starting: Ask Search for Emails
```

Когда поиск завершится, вы получите запрос на проверку адресов электронной почты. Эта операция может занять некоторое время. Но в целевой атаке с использованием инструментов социальной инженерии или при получении конфиденциальных данных определенных лиц (фишинге) время, потраченное на проверку адресов электронной почты, будет затрачено не зря. Для запуска проверки адресов электронной почты достаточно нажать клавишу Y. Нажав клавишу N, вы откажетесь от проверки.

```
[*] Email reconnaissance has been completed:
    Email verification will allow you to use common methods
    to attempt to enumerate if the email is valid.
    This grabs the MX records, sorts and attempts to check
    if the SMTP server sends a code other than 250 for known bad addresses
[>] Would you like to verify email(s)?:
```

По окончании проверки наступит следующий этап — создания отчета:

```
[*] Email reconnaissance has been completed:
    File Location: /root/Desktop/SimplyEmail
    Unique Emails Found: 246
    Raw Email File: Email_List.txt
    HTML Email File: Email_List.html
    Domain Performed: example.com
[>] Would you like to launch the HTML report?:
```

Отчет — это HTML-файл, в котором указано, какие типы поиска были применены и какие данные были обнаружены. Если вы хорошо разбираетесь в HTML, вы даже можете поставить на этом отчете свой логотип и включить его в окончательный отчет об исследовании на проникновение.

Взлом базы данных Google (GHDB)

База данных Google Hacking (GHDB) находится по адресу <https://www.exploit-db.com/google-hacking-database/>. Она позволяет пользователям применять индивидуальные расширенные запросы, которые могут выявить исключительную информацию. Такая информация в обычном списке результатов поиска на <https://www.google.com/> не отображается.

GHDB начинал создавать Джонни Лонг (Johnny Long), основатель сообщества Hackers for Charity («Хакеры за благотворительность»). Сейчас GHDB поддерживается Offensive Security, создателями Kali Linux. В GHDB используются запросы

Google Dork или Google Dork Queries (GDQ) — набор запросов для выявления грубейших дыр в безопасности. При формировании запроса можно также указывать операторы типа `allintext`, `site`, `+`, `-`, `*` и др. При правильном формировании запроса `Googledorks` иногда может выдать интересную и даже конфиденциальную информацию, такую как сообщения об ошибках, список уязвимых серверов и сайтов, конфиденциальные файлы и страницы входа. Конечно, большая часть этой информации через *обычный* поиск Google чаще всего недоступна. Поэтому Google можно использовать в качестве инструмента сбора информации и взлома базы данных.

GHDB достаточно прост в применении. Конечно, и здесь есть поле ввода поискового запроса, но, в отличие от обычного поисковика Google, на этом ресурсе пользователь, вместо того чтобы вводить фразы и запросы Google Dork, может искать ответ в различных категориях. Ниже заголовка страницы находятся ссылки, в которых перечислены многие категории с поисковыми запросами, а также ссылки на запросы, ведущие к поиску Google. С помощью этих категорий нужную информацию легко найдет даже начинающий пользователь.

В качестве примера мы, чтобы выбрать уязвимые серверы из списка категорий, просто ввели `apache` в поле поиска и нажали кнопку Search (Поиск) (рис. 4.6).

The screenshot shows the Exploit Database interface. At the top, there is a navigation menu with a spider logo and the text 'EXPLOIT DATABASE'. On the right, there are icons for GitHub, a user profile, a search icon, and a 'GET CERTIFIED' button. Below the navigation is the 'Google Hacking Database' header with 'Filters' and 'Reset All' buttons. A search bar contains the text 'apache' and a 'Quick Search' button. Below the search bar is a table of results with the following columns: Date Added, Dork, Category, and Author.

Date Added	Dork	Category	Author
2018-06-22	intitle:"apache tomcat/" "Apache Tomcat examples"	Web Server Detection	KhanhNNVN
2018-05-11	"Powered by Apache Subversion version"	Sensitive Directories	Sang Bui
2018-05-07	intitle:"apache tomcat/" + "Find additional important configuration information in:"	Web Server Detection	ManhNho
2018-05-03	intitle:"Apache2 Debian Default Page: It works"	Web Server Detection	ManhNho
2018-03-07	inurl:"server-status" "Server Version: Apache/" "Server Built: " "Server uptime:" "Total accesses" "CPU Usage:"	Web Server Detection	Aamir Rehman
2017-06-27	intitle:"Index of" "Apache/2.4.7 (Ubuntu) Server"	Web Server Detection	anonymous
2016-02-26	intitle:"Apache Status" intext:"Apache Server Status"	Web Server Detection	anonymous
2016-02-17	intext:Apache/2.2.29 (Unix) mod_ssl/2.2.29 intitle:"Index of /"	Web Server Detection	anonymous
2016-02-02	intitle:"TurnKey LAMP" intext:"turnkey lamp release notes" "Apache PHP information"	Files Containing Juicy Info	anonymous
2015-12-14	inurl:"server-status" intext:"Apache Server Status"	Files Containing Juicy Info	anonymous
2015-11-12	intext:"This is Apache Hadoop release" "Local Logs"	Various Online Devices	anonymous

Рис. 4.6. Категории отсортированы по слову `apache`

Вы можете открыть заинтересовавшую вас ссылку, щелкнув на ней кнопкой мыши. Или скопировать в буфер обмена и вставить в поле поискового запроса Google. Возможно, по этому запросу вы найдете дополнительную информацию.

На рис. 4.7 показаны результаты поиска по введенному поисковому запросу в Google. Обратите внимание, что получено 82 200 результатов, но не все содержат интересную информацию об уязвимых серверах.

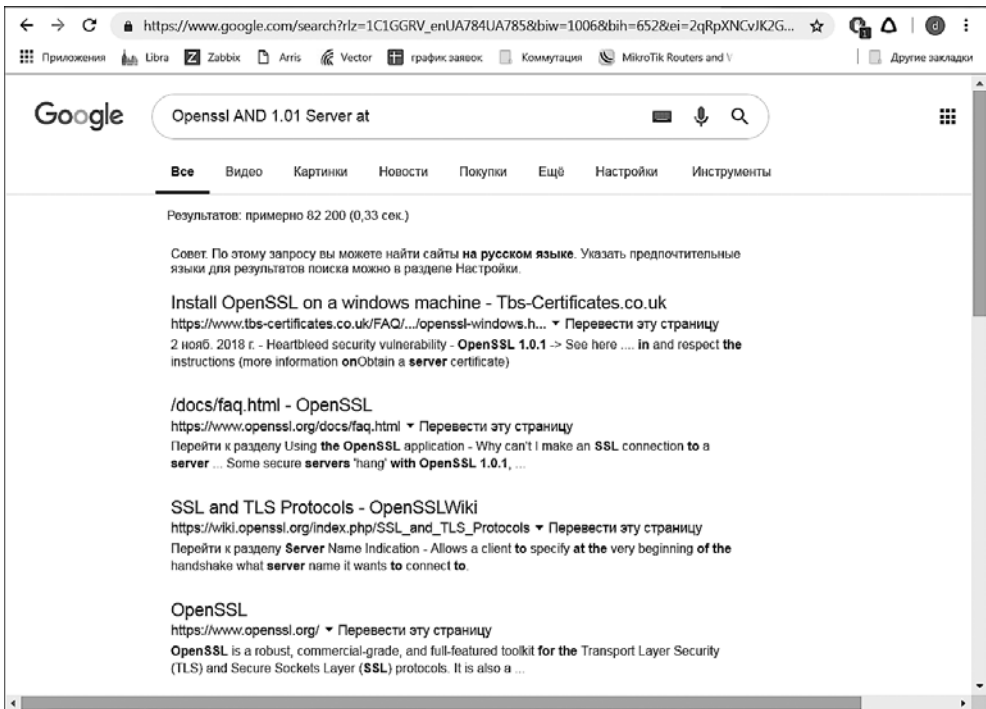


Рис. 4.7. Результаты поискового запроса

В этических и юридических целях вы должны использовать GHDB только для сбора информации.

Metagoofil

Metagoofil — это инструмент, который использует поисковую систему Google для получения метаданных из документов, доступных в целевом домене. В настоящее время поддерживаются следующие типы документов:

- документы Word (.docx, .doc);
- электронные таблицы (.xlsx, .xls, .ods);

- ❑ файлы презентации (.pptx, .ppt, .odp);
- ❑ файлы PDF (.pdf).

Metagoofil выполняет следующие действия.

- ❑ Поиск в целевом домене с помощью Google всех указанных выше типов файлов.
- ❑ Загрузку всех найденных документов и их сохранение на локальном диске.
- ❑ Извлечение метаданных из загруженных документов.
- ❑ Сохранение результата в HTML-файл.

Мы можем обнаружить следующие метаданные.

- ❑ Имя пользователя.
- ❑ Версию программного обеспечения.
- ❑ Имена серверов или компьютеров.

Данную информацию можно использовать позже, на этапе тестирования на проникновение. Metagoofil не входит в стандартный дистрибутив Kali Linux 2.0.

Чтобы установить Metagoofil, выполните следующую команду:

```
# apt-get install metagoofil
```

Когда приложение установится, для запуска введите такую команду:

```
# metagoofil
```

После запуска приложения на экране появятся простые инструкции по использованию и пример. Мы для демонстрации его работы соберем все документы DOC и PDF (-t, .doc, .pdf) из целевого домена (-d hackthissite.org) и сохраним их в каталоге с именем test (-o test). Мы ограничиваем поиск каждого типа файлов 20 файлами (-l 20), а загрузим только пять файлов (-n 5). Созданный отчет сохраним под именем test.html (-f test.html).

Введите следующую команду:

```
# metagoofil -d example.com -l 20 -t doc,pdf -n 5 -f test.html -o test
```

Отредактированный результат ее выполнения выглядит следующим образом:

```
[~] Starting online search...
[~] Searching for doc files, with a limit of 20
    Searching 100 results...
Results: 5 files found
Starting to download 5 of them:
-----
[1/5] /webhp?hl=en [x] Error downloading /webhp?hl=en
[2/5] /intl/en/ads [x] Error downloading /intl/en/ads
[3/5] /services [x] Error downloading /services
[4/5] /intl/en/policies/privacy/
[5/5] /intl/en/policies/terms/
[~] Searching for pdf files, with a limit of 20
Searching 100 results...
```


Results: 25 files found
Starting to download 5 of them:

```
-----  
[1/5] /webhp?hl=en [x] Error downloading /webhp?hl=en  
[2/5] https://mirror.hackthissite.org/hackthiszine/hackthiszine3.pdf  
[3/5] https://mirror.hackthissite.org/hackthiszine/hackthiszine12_print.pdf  
[4/5] https://mirror.hackthissite.org/hackthiszine/hackthiszine12.pdf  
[5/5] https://mirror.hackthissite.org/hackthiszine/hackthiszine4.pdf  
processing
```

[+] List of users found:

```
-----  
emadison
```

[+] List of software found:

```
-----  
Adobe PDF Library 7.0  
Adobe InDesign CS2 (4.0)  
Acrobat Distiller 8.0.0 (Windows)  
PScript5.dll Version 5.2.2  
[+] List of paths and servers found:
```

[+] List of e-mails found:

```
-----  
whooka@gmail.com  
htsdevs@gmail.com  
never@guess  
narc@narc.net  
kfiralfia@hotmail.com  
user@localhost  
user@remotehost.  
user@remotehost.com  
security@lists.  
recipient@provider.com  
subscribe@lists.hackbloc.org  
staff@hackbloc.org  
johndoe@yahoo.com  
staff@hackbloc.org  
johndoe@yahoo.com  
subscribe@lists.hackbloc.org  
htsdevs@gmail.com  
hackbloc@gmail.com  
webmaster@www.ndcp.edu.phpass  
webmaster@www.ndcp.edu.phwebmaster@www.ndcp.edu.ph  
[webmaster@ndcp  
[root@ndcp  
D[root@ndcp  
window...[root@ndcp  
.[root@ndcp  
goods[root@ndcp  
liberation_asusual@yapjames_  
e@yahoo.com.au
```

Из этого кода видно, что из собранных документов мы получаем большое количество информации, например имена пользователей и сведения о пути. Мы можем задействовать полученные имена пользователей для поиска шаблонов в именах и для запуска атаки с применением пароля и грубой силы. Но имейте в виду, что при взломе учетной записи и пароля с помощью грубой силы может появиться риск блокировки учетных записей пользователей. Сведения о пути можно задействовать для определения типа и версии операционной системы, установленной на целевом компьютере. Мы получили всю эту информацию, не заходя на сайт целевого домена.

Metagoofil также способен генерировать информацию в формате HTML-отчета (рис. 4.8).

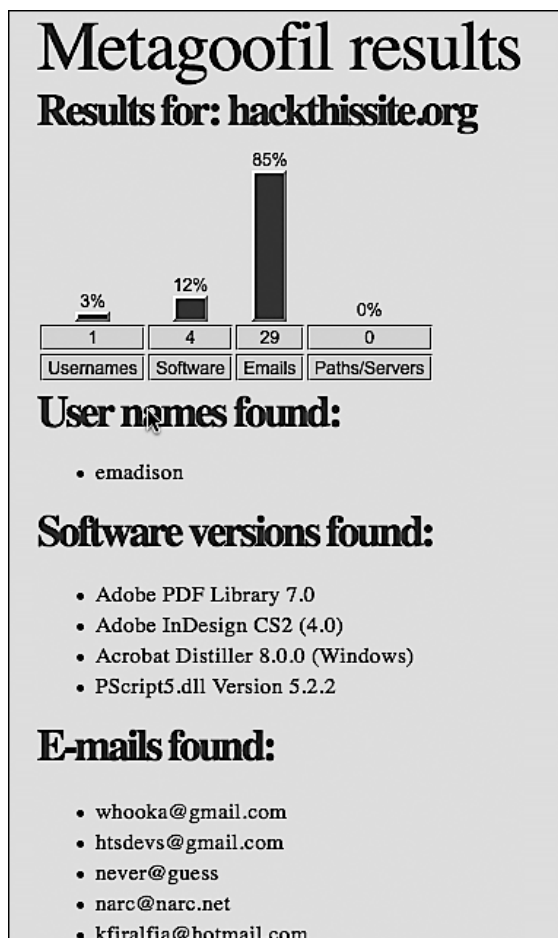


Рис. 4.8. Отчет в формате HTML

В таком отчете мы получаем информацию об именах пользователей, версии программного обеспечения, адресе электронной почты и сведения о сервере из целевого домена.

Автоматизированные инструменты для снятия отпечатков и сбора информации

В этом разделе мы рассмотрим полностью автоматизированные инструменты, в частности два таких, в состав которых входят несколько функций, позволяющих выполнять задачи, которые ранее выполнялись разными инструментами. Они находятся в свободном доступе, и найти их можно на сайте <https://github.com/>. Эти инструменты работают как в Kali Linux 2018.2, так, возможно, и в более ранних версиях.

Devploit

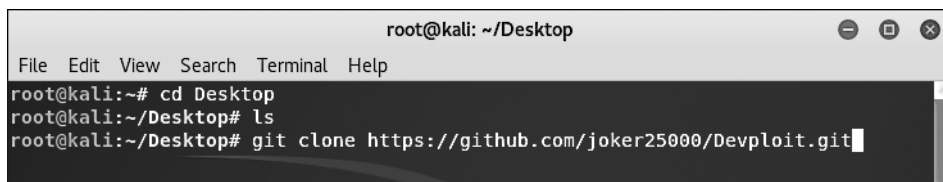
Devploit 3.6, который разработал Joker25000, заявлен как инструмент сбора информации и доступен по адресу <https://github.com/joker25000/Devploit>.

Перед использованием вам следует клонировать Devploit на вашу машину Kali Linux. Только когда будут представлены все опции, вы сможете запустить инструменты выбора. Клонирование выполняется лишь один раз. Далее просто переходите в каталог Deploy.

Откройте новый терминал и, используя команду `cd`, перейдите в каталог, например Desktop. Чтобы просмотреть список с содержимым каталога и убедиться, что вы находитесь там, где нужно, выполните команду `ls`.

Для клонирования Devploit на компьютер используйте команду `git clone` (рис. 4.9):

```
git clone https://github.com/joker25000/Devploit.git
```

A screenshot of a terminal window titled "root@kali: ~/Desktop". The window has a menu bar with "File", "Edit", "View", "Search", "Terminal", and "Help". The terminal shows the following commands and output:

```
root@kali:~# cd Desktop
root@kali:~/Desktop# ls
root@kali:~/Desktop# git clone https://github.com/joker25000/Devploit.git
```

Рис. 4.9. Команда `git clone` введена



При копировании URL-адреса с веб-страницы GitHub проследите, чтобы в конце адреса было обязательно указано расширение `.git`.

Чтобы запустить клонирование (рис. 4.10), нажмите клавишу Enter.

```
root@kali:~/Desktop# git clone https://github.com/joker25000/Devploit.git
Cloning into 'Devploit'...
remote: Counting objects: 262, done.
remote: Total 262 (delta 0), reused 0 (delta 0), pack-reused 262
Receiving objects: 100% (262/262), 280.82 KiB | 39.00 KiB/s, done.
Resolving deltas: 100% (112/112), done.
root@kali:~/Desktop#
```

Рис. 4.10. Клонирование успешно выполнено

После завершения клонирования перейдите в каталог `Deploy`. Его мы создали на Рабочем столе. Для перехода в нужный каталог введите команду `cd Devploit`, а затем для просмотра содержимого каталога воспользуйтесь командой `ls`. Среди других файлов вы должны увидеть `Devploit.py` и `README.me`.

С помощью команды `chmod +x` запустите установку, а затем для старта `Devploit` введите `./install`.



Убедитесь, что предыдущие команды выполняются из каталога `Devploit`.

После установки `Devploit` откройте новый терминал и введите команду `Devploit`, как показано на рис. 4.11.

```
root@kali:~/Desktop/Devploit# chmod +x install
root@kali:~/Desktop/Devploit# ./install

-----
[ ✓ ] Installer The Tool [ ✓ ]
-----
[ ! ] Moving Devploit folder
[ ✓ ] Done
[*] Creating Icons Directory
[*] Creating shortcut command Devploit
-----
[ ✓ ] Devploit Is Installed In Application (information gathering) [ ✓ ]
-----

|Run in Terminal<(Devploit)>|
root@kali:~/Desktop/Devploit#
```

Рис. 4.11. Запуск Devploit

В `Devploit` существует 18 вариантов автоматического сбора информации (рис. 4.12).

```

This Is Simple Script By : Joker-Security
Let's Start --> --> -->

1 } ==> DNS Lookup
2 } ==> Whois Lookup
3 } ==> GeoIP Lookup
4 } ==> Subnet Lookup
5 } ==> Port Scanner
6 } ==> Extract Links
7 } ==> Zone Transfer
8 } ==> HTTP Header
9 } ==> Host Finder
10} ==> IP-Locator
11} ==> Traceroute
12} ==> Robots.txt
13} ==> Host DNS Finder
14} ==> Revrse IP Lookup
15} ==> Collection Email
16} ==> Subdomain Finder
17} ==> Install & Update
18} ==> About Me
00} ==> Exit

Enter 00/18 => => █

```

Рис. 4.12. Варианты автоматического сбора информации

Чтобы выполнить поиск DNS, введите 1, а затем имя домена, например `www.google.com` (рис. 4.13).

```

Enter 00/18 => => 1
Entre Your Domain :www.google.com
:: Truncated, retrying in TCP mode.
www.google.com.      279   IN      A       172.217.6.100
www.google.com.      178   IN      AAAA    2607:f8b0:4009:812::2004

```

Рис. 4.13. Поиск DNS

Чтобы узнать основную географическую информацию о домене или IP, выберите вариант 3 и нажмите `Enter`, а затем введите IP или доменное имя (рис. 4.14). Обязательно ознакомьтесь с остальными доступными опциями.

```

Enter 00/18 => => 3
Enter IP Address : www.google.com
IP Address: 173.194.66.103
Country: US
State: California
City: Mountain View
Latitude: 37.419201
Longitude: -122.057404
Continue/Exit->-> █

```

Рис. 4.14. Получение основной географической информации

RedHawk v2

RedHawk версии 2 — еще один инструмент сбора информации с мощными функциями типа «все в одном». Он применяется для разведки и сбора данных.

Откройте новое окно терминала и перейдите на Рабочий стол (или в каталог по вашему выбору). Клонировать RedHawk v2, введя команду https://github.com/th3j5t4ck3r/RED_HAWK (рис. 4.15).

```
root@kali:~# cd Desktop
root@kali:~/Desktop# git clone https://github.com/Tuhinshubhra/RED_HAWK.git
Cloning into 'RED_HAWK'...
remote: Counting objects: 79, done.
remote: Total 79 (delta 0), reused 0 (delta 0), pack-reused 79
Unpacking objects: 100% (79/79), done.
root@kali:~/Desktop#
```

Рис. 4.15. Клонирование RedHawk v2

Как только все объекты будут распакованы, с помощью команды `cd RED_HAWK` перейдите в каталог RED_HAWK. Используйте команду `ls`, чтобы проверить, что файл `rhawk.php` действительно существует (рис. 4.16).

```
root@kali:~/Desktop# cd RED_HAWK
root@kali:~/Desktop/RED_HAWK# ls
config.php  functions.php  README.md  sqlerrors.ini  version.txt
crawl      LICENSE       rhawk.php  var.php
root@kali:~/Desktop/RED_HAWK#
```

Рис. 4.16. Содержимое каталога RED_HAWK

Для запуска RedHawk выберите тип `php rhawk.php` и нажмите клавишу Enter. Если все было сделано правильно, на экране вы увидите следующую картинку (рис. 4.17).

```

All In One Tool For Information Gathering And Vulnerability Scanning

RED                                Ver 2.0.0
#####  #####  #####  #####
#####  #####  #####  #####
#####  #####  #####  #####
#####  #####  #####  #####
#####  #####  #####  #####
#####  #####  #####  #####
#####  #####  #####  #####
#####  #####  #####  #####
#####  #####  #####  #####
#####  #####  #####  #####

(C) Coded By - R3D#X0R_2H1N A.K.A Tuhinshubhra
[$] Shout Out - You ;)

!!) cURL Module Is Missing! Try 'fix' command OR Install php-curl
!!) DOM Module Is Missing! Try 'fix' command OR Install php-xml

[#] Enter The Website You Want To Scan :

```

Рис. 4.17. Запуск RedHawk

Введите адрес интересующего вас сайта и выберите HTTP или HTTPS. Затем выберите один из доступных вариантов. Например, для поиска Whois введите 1 (рис. 4.18).

```
[#] Enter The Website You Want To Scan : google.com
[#] Enter 1 For HTTP OR Enter 2 For HTTPS: 2

+-----+
+                               +
+                               +
+                               +
+                               +
+-----+
+                               +
+                               +
+                               +
+-----+

Scanning Site : https://google.com

[0] Basic Recon (Site Title, IP Address, CMS, Cloudflare Detection, Robot
nner)
[1] Whois Lookup
[2] Geo-IP Lookup
[3] Grab Banners
[4] DNS Lookup
```

Рис. 4.18. Поиск Whois

Whois-информация для поиска по адресу <https://www.google.com/> отображается следующим образом (рис. 4.19).

```
root@kali: ~/Desktop/RED_HAWK
File Edit View Search Terminal Help
[i] Scanning Site: https://google.com
[s] Scan Type : WHOIS Lookup
[-] Whois Lookup Result:

Domain Name: GOOGLE.COM
Registry Domain ID: 2138514_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2018-02-21T18:36:40Z
Creation Date: 1997-09-15T04:00:00Z
Registry Expiry Date: 2020-09-14T04:00:00Z
Registrar: MarkMonitor Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2083895740
Domain Status: clientDeleteProhibited https://icann.org/epp#cli
d
Domain Status: clientTransferProhibited https://icann.org/epp#c
bited
Domain Status: clientUpdateProhibited https://icann.org/epp#cli
d
Domain Status: serverDeleteProhibited https://icann.org/epp#ser
d
Domain Status: serverTransferProhibited https://icann.org/epp#s
bited
Domain Status: serverUpdateProhibited https://icann.org/epp#ser
d
Name Server: NS1.GOOGLE.COM
Name Server: NS2.GOOGLE.COM
Name Server: NS3.GOOGLE.COM
Name Server: NS4.GOOGLE.COM
```

Рис. 4.19. Найденная Whois информация для адреса <https://www.google.com/>

Результаты опции 3 для <https://www.google.com/> по захвату баннеров будут следующими (рис. 4.20).

```
[i] Scanning Site: https://google.com
[S] Scan Type : Banner Grabbing

HTTP/1.0 301 Moved Permanently
Location: https://www.google.com/
Content-Type: text/html; charset=UTF-8
Date: Thu, 12 Jul 2018 20:35:00 GMT
Expires: Sat, 11 Aug 2018 20:35:00 GMT
Cache-Control: public, max-age=2592000
Server: gws
Content-Length: 220
X-XSS-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
Alt-Svc: quic=":443"; ma=2592000; v="44,43,39,35"
HTTP/1.0 200 OK
Date: Thu, 12 Jul 2018 20:35:00 GMT
Expires: -1
Cache-Control: private, max-age=0
Content-Type: text/html; charset=ISO-8859-1
P3P: CP="This is not a P3P policy! See g.co/p3phelp for more info."
Server: gws
X-XSS-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
Set-Cookie: 1P_JAR=2018-07-12-20; expires=Sat, 11-Aug-2018 20:35:00 GMT;
ain=.google.com
```

Рис. 4.20. Результаты опции 3

Поиск MX (опция 13) для [Google.com](https://www.google.com/) дает следующий результат (рис. 4.21).

```
[#] Choose Any Scan OR Action From The Above List: 13

[+] Scanning Begins ...
[i] Scanning Site: https://google.com
[S] Scan Type : MX Lookup

IP      : 74.125.31.26
HOSTNAME: va-in-f26.1e100.net

[*] Scanning Complete. Press Enter To Continue OR CTRL + C To Stop
```

Рис. 4.21. Результаты обработки опции 13

Пользователю доступно несколько опций, включая А — сканирование всего.

Использование Shodan для поиска подключенных к Интернету устройств

Поисковая система *Shodan* находится по адресу shodan.io. Это не какой-то слабенький поисковик. Shodan с помощью основных и дополнительных строк запросов может обнаруживать подключенные к Интернету уязвимые системы. Веб-сайт

был разработан Джоном Мэзерли (John Matherly) и существует около десяти лет. В настоящее время он стал бесценным инструментом для снятия отпечатков через Интернет. Мы живем в эпоху Интернета вещей (Internet of Things, IoT), и сегодня все больше и больше устройств имеют выход в Сеть. Однако многие из них не защищены должным образом, поэтому становятся уязвимы для хакерских атак и не только.

Shodan сканирует общие порты и выполняет захват баннеров в рамках получения отпечатка, а затем отображает устройства, доступные через Интернет, включая маршрутизаторы и сетевые устройства, веб-камеры и средства наблюдения, дорожные камеры, серверы и системы SCADA и многие другие интересные устройства.

Чтобы получить список открытых портов и сервисов, установленных на устройстве, достаточно в списке результатов щелкнуть кнопкой мыши на отдельном результате. Кроме того, Shodan позволяет создавать отчеты.



Для обеспечения конфиденциальности и по юридическим причинам я решил не использовать скриншоты результатов работы Shodan.

Перед применением Shodan посетите сайт www.shodan.io (рис. 4.22).

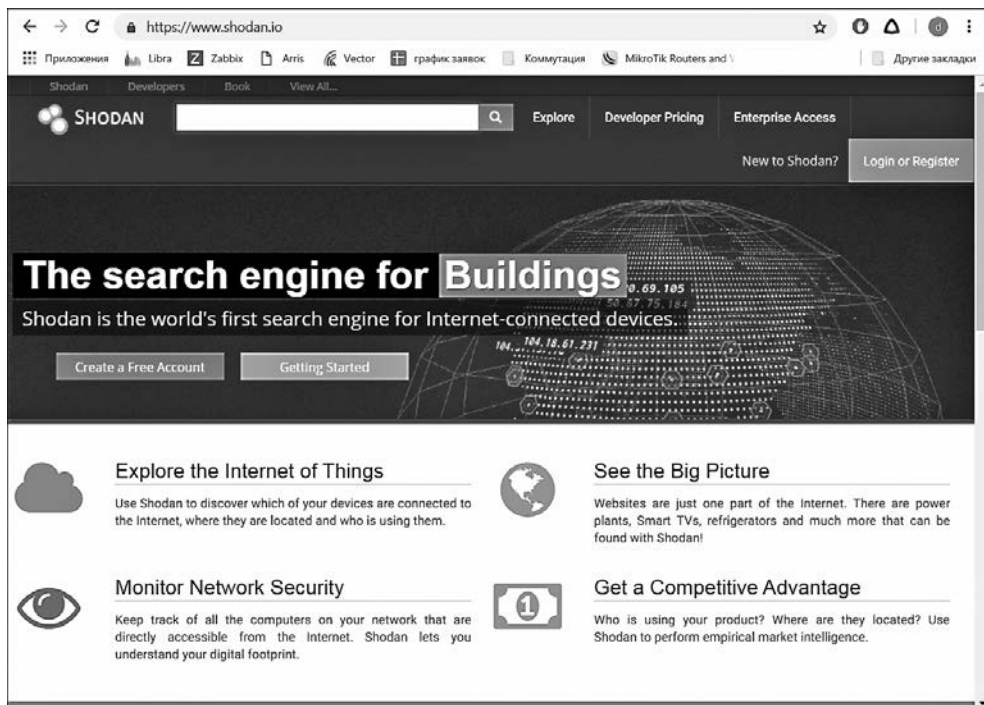


Рис. 4.22. Страница сайта www.shodan.io

Обратите внимание, что этот сервис вы можете использовать бесплатно. Но, если вы не зарегистрируетесь, то будете ограничены одной страницей с результатами. Регистрация бесплатная, она предоставляет доступ к первым двум страницам с ответами на запрос. Чтобы получить доступ ко всем результатам, следует оформить платную подписку.

Поисковые запросы в Shodan. Ниже приведены поисковые запросы, применяемые в Shodan.

- ❑ *Ключевые слова* — наподобие *webcams* (веб-камеры), *CCTV*, *Cisco*, *Fortinet*, *traffic signal* (сигнал светофора), *refrigerator* (холодильник) и др.
- ❑ *Номера портов* — можно указать в соответствии со службами. Например, 3389 (remote desktop) (удаленный Рабочий стол).
- ❑ *Версии ОС* — вместе с кодами стран можно указать операционные системы и версии.
- ❑ Вместе с ключевыми словами и номерами портов также могут быть указаны *названия стран*.
- ❑ Можно использовать *фразы* и комбинированные ключевые слова, включая популярные поисковые фразы, такие как «*пароли по умолчанию*», «*неудачный вход в систему*» и др.

Обратите внимание: в верхней части сайта Shodan правее поля ввода поискового запроса находится кнопка Explore (Исследовать). При ее нажатии можно увидеть список ссылок на различные категории и популярные запросы. Одними из рекомендуемых категорий являются Industrial Control Systems (Промышленные системы управления) и Databases (Базы данных), а на вершине популярности находятся такие запросы, как «веб-камеры», «камеры», Netcam и «пароль по умолчанию».

Щелчок кнопкой мыши на категории Webcams (Веб-камеры) или ввод выражения SQ-WEBCAM даст несколько результатов по веб-камерам, которые расположены в разных странах. Общий поисковый запрос webcamxp также позволит найти камеры, доступные в Интернете. Многие из этих камер управляются дистанционно: можно делать панораму, изменять угол наклона и масштаб.

Убедитесь, что законодательство страны позволяет вам использовать Shodan. Уточните, есть ли юридические ограничения на получение доступа к некоторым устройствам.

Blue-Thunder-IP-локатор

Откройте новый терминал и перейдите в каталог по вашему выбору. Мы для этого примера использовали Рабочий стол.

Создайте клон Blue-Thunder-IP-Locator из GitHub. Для этого используйте команду `git clone https://github.com/th3sha10wbr04rs/Blue-Thunder-IP-Locator-.git` (рис. 4.23).

```
File Edit View Search Terminal Help
root@kali:~# cd Desktop
root@kali:~/Desktop# git clone https://github.com/th3sha10wbr04rs/Blue-Thunder-IP-Locator-.git
Cloning into 'Blue-Thunder-IP-Locator-'...
remote: Counting objects: 42, done.
remote: Total 42 (delta 0), reused 0 (delta 0), pack-reused 42
Unpacking objects: 100% (42/42), done.
framework1:~/Desktop#
```

Рис 4.23. Клонирование Blue-Thunder-IP-Locator

После успешного клонирования измените каталоги на Blue-Thunder-IP-Locator.

Как указано на странице <https://github.com/CreativeBen/Blue-Thunder-IP-Locator->, для установки и обновления библиотек perl следует ввести команду `apt-get install liblocal-lib-perl`.

Если при выполнении предыдущей команды возникла ошибка, введите `Dpkg --configure -a` и повторите предыдущую команду (рис. 4.24).

```
root@kali:~/Desktop/Blue-Thunder-IP-Locator-# apt-get install liblocal-lib-perl
E: dpkg was interrupted, you must manually run 'dpkg --configure -a' to correct the problem.
root@kali:~/Desktop/Blue-Thunder-IP-Locator-# dpkg --configure -a
Setting up libqt5qml5:amd64 (5.10.1-4) ...
Setting up baobab (3.28.0-2) ...
```

Рис. 4.24. Установка библиотек perl

Вам на протяжении всего процесса будут предлагаться различные варианты установки. При появлении таких запросов нажимайте Y.

Далее введите команду `apt-get install libjson-perl` и обновите систему. Для этого введите `apt-get upgrade libjson-perl`.

Кроме того, нужно будет убедиться, что Blue-Thunder имеет соответствующие полномочия. Для этого введите команду `chmod +x blue_thunder.pl` (рис. 4.25).

```
root@kali:~/Desktop/Blue-Thunder-IP-Locator-#
root@kali:~/Desktop/Blue-Thunder-IP-Locator-# chmod +x blue_thunder.pl
root@kali:~/Desktop/Blue-Thunder-IP-Locator-#
```

Рис. 4.25. Настройка Blue-Thunder

Blue-Thunder-IP-Locator требует определенных Perl-зависимостей. Их можно автоматически устанавливать при запуске приложения. Так, библиотека *Ruby-mechanize* предназначена для автоматизации взаимодействия с сайтами.

Перед запуском Blue-Thunder необходимо выполнить перечисленные ниже команды. Все эти команды выполняются из корневого каталога.

Введите `apt-get install libhttp-daemon-ssl perl` (рис. 4.26).

```
root@kali:~# sudo apt-get install libhttp-daemon-ssl perl
Reading package lists... Done
Building dependency tree
Reading state information... Done
```

Рис. 4.26. Установка libhttp-daemon-ssl perl

Возможно, пакет libhttp-daemon-ssl с помощью команды `apt-get install libhttp-daemon-ssl perl` не будет найден. Не переживайте, это в порядке вещей. В этом случае выполните следующую команду (рис. 4.27).

Apt-cache search WWW::Mechanize

```
root@kali:~# apt-cache search WWW::Mechanize
funkload - web testing tool
libhttp-recorder-perl - Perl module to record interaction with websites
```

Рис. 4.27. Поиск пакета libhttp-daemon-ssl perl

Выполните команду `apt-get install libwww-mechanize-perl` (рис. 4.28).

```
root@kali:~# apt-get install libwww-mechanize-perl
Reading package lists... Done
Building dependency tree
Reading state information... Done
```

Рис. 4.28. Установка libwww-mechanize-perl

Теперь, когда все зависимости установлены и/или обновлены, мы можем запустить Blue-Thunder-IP-Locator.

Перейдите в терминале в каталог Blue-Thunder-IP-Locator, введите команду `perl blue_thunder.pl` и нажмите клавишу Enter (рис. 4.29).

```
root@kali:~/Desktop/Blue-Thunder-IP-Locator-# perl blue_thunder.pl
RED_HAWK
```

Рис. 4.29. Запуск perl blue_thunder.pl

Чтобы получить подробные сведения о геолокации, введите команду `perl iplocation.pl`, имя хоста, IP или домена (все команды нужно вводить, находясь в каталоге Blue-Thunder-IP-Locator).

Например, чтобы найти информацию о геолокации Google.com, введите следующий код: `perl bluethunder.pl www.google.com` (рис. 4.30).

Обратите внимание, что в выводе вы найдете название страны, где находится целевой интернет-провайдер, название города и региона, широту и долготу, вре-

менную зону и другие данные. Если ввести предоставленные в отчете координаты (широту и долготу) в поле ввода поискового запроса в «Картах Google», можно на карте увидеть расположение интересующего вас объекта.

```
Ip Geolocation Tool
By: #Ben (TSB)

-----
[!] IP: 216.58.219.110
-----

[+] ORG: AS15169 Google LLC
[+] ISP: Google
[+] Country: United States - US
[+] City: Miami
[+] Region: Florida - FL
[+] Geo: Lat: 25.7617 - Long: -80.1918
[+] Geo: Latitude: 25.7617 - Long: 25.7617
[+] Time: timezone: America/New_York - Long: America/New_York
[+] As number/name: as: AS15169 Google LLC - Long: AS15169 Google LLC
[+] ORG: AS15169 Google LLC
[+] Country code: US
[+] Status: success
```

Рис. 4.30. Сведения о геолокации сайта www.google.com

Резюме

В этой главе мы рассмотрели очень важный этап, выполняемый при испытании на проникновение, — этап сбора информации. Обычно это первый шаг при тестировании на проникновение. На этом этапе следует постараться собрать как можно больше информации о целевой организации. После того как мы познакомимся с полученной на этом этапе информацией, нам будет легче, когда мы начнем атаковать цель. Великий китайский стратег Сунь-цзы очень лаконично изложил общие задачи OSINT и сбора информации: *«Познай себя, познай своего врага, и ты выиграешь сотню битв без потерь»*.

Это высказывание полностью описывает цели и задачи тестирования на проникновение.

В главе мы разобрали несколько инструментов, включенных в Kali Linux, которые можно применять для сбора информации. Мы начали с нескольких общедоступных сайтов, которые можно использовать для сбора информации о целевой организации. Далее было рассказано, как применять инструменты для сбора информации о регистрации домена. Затем мы рассмотрели инструменты, которые можно использовать для получения информации DNS. Позже мы изучили инструменты для сбора информации о маршрутизации. В заключительной части главы были описаны автоматизированные инструменты, в том числе очень мощная поисковая система для хакеров Shodan.

В следующей главе мы обсудим, как обнаружить цель с помощью сканирования, а также как избежать обнаружения.

Вопросы

1. Что означает аббревиатура OSINT?
2. Какие инструменты можно использовать для запроса информации о регистрации домена?
3. Что представляет собой запись A?
4. Какой инструмент использует поисковая система Google для сбора метаданных документов в целевом домене?
5. Какие два автоматизированных инструмента сбора информации мы изучили?
6. Какой инструмент можно применять для поиска информации об устройствах, подключенных к Интернету?

Дополнительные материалы

- ❑ Ресурсы OSINT: <http://osintframework.com/>.
- ❑ Документация и руководство пользователя Maltego: <https://www.paterva.com/web7/docs.php>.
- ❑ Google Cheat Sheet: http://www.googleguide.com/print/adv_op_ref.pdf.
- ❑ Shodan для испытателей на проникновение: <https://www.defcon.org/images/defcon-18/dc-18-presentations/Schearer/DEFCON-18-Schearer-SHODAN.pdf>.