Л34. Сбор информации о целевой организации.

Одним из ключевых терминов, связанных со сбором информации, является *разведка по открытым источникам — Open Source Intelligence (OSINT)*. Военные и разведывательные организации делят свои разведывательные источники на различные типы. Настоящий шпионаж, предполагающий взаимодействие агентов, часто называют агентурной деятельностью — *Human Intelligence (HUMINT)*. Захват радиосигнала с целью взлома шифра называется радиоразведкой — *Signals Intelligence (SIGINT)*. Но испытатель на проникновение вряд ли воспользуется одним из перечисленных методов OSINT. OSINT — это информация, полученная из источников, не защищенных средствами контроля безопасности. Эти средства контроля должны препятствовать утечке информации. Нередко это сведения из публичных записей или информация, которой целевые организации обмениваются при своей повседневной деятельности.

Для поиска и получения этой, безусловно, полезной информации испытателю на проникновение потребуются специальные знания и инструменты. Продолжительность этапа сбора в значительной степени зависит от уже полученных данных. Кроме того, показывая пути утечки информации, мы можем понять, какие действия следует предпринять для повышения безопасности. В этой главе мы разберем, сколько информации может получить человек, знающий, что и где искать.

Использование общих ресурсов

В Интернете существует несколько общедоступных ресурсов, которые можно применять для сбора информации о целевом домене. Преимущество использования этих ресурсов заключается в том, что сетевой трафик не отправляется непосредственно в целевой домен, поэтому в журнал событий целевого домена такие действия не записываются.

Ниже вы найдете перечень ресурсов, которые можно использовать для сбора такой информации.

URL-адрес ресурса	**Описание**
http://www.archive.org	Здесь хранятся архивы сайтов
http://www.domaintools.com/	Содержит сведения о доменных именах
http://www.alexa.com/	На этом ресурсе содержится база данных о сайтах

Продолжение ⇩

(Продолжение)

URL-адрес ресурса	Описание
http://serversniff.net/	Это бесплатный «швейцарский армейский нож» для сетей, проверки серверов и маршрутизации
http://centralops.net/	Здесь вы найдете бесплатные сетевые утилиты, такие как domain, email, browser, ping, traceroute и Whois
http://www.robtex.com	На данном ресурсе вы можете найти информацию о домене и сети
http://www.pipl.com/	Здесь вы можете попробовать найти в Интернете людей по их имени и фамилии, городу, штату и стране
http://wink.com/	Данная бесплатная поисковая система позволяет находить людей по имени, номеру телефона, адресу электронной почты, сайту, фотографии и т. д.
http://www.isearch.com/	Бесплатная поисковая система, позволяющая найти людей по имени, номеру телефона и адресу электронной почты
http://www.tineye.com	TinEye — поисковая система обратного изображения. Мы можем использовать TinEye, чтобы узнать, откуда взялось изображение, как оно применяется, существуют ли его модифицированные версии, или найти версии с более высоким разрешением
http://www.sec.gov/edgar.shtml	Данный сайт может быть использован для поиска информации о публичных компаниях в комиссии по ценным бумагам и биржам

Чтобы использовать эти ресурсы, требуется только подключение к Интернету и браузер, который есть в каждой операционной системе. Поэтому мы и предлагаем вам, прежде чем воспользоваться инструментами, встроенными в Kali Linux, поработать с этими публичными ресурсами.

Чтобы защитить домен от злоупотреблений, мы изменили доменное имя, которое было использовано в наших примерах. Мы будем указывать несколько доменных имен, таких как example.com от IANA и адрес бесплатного хакерского сайта https://www.hackthissite.org/.

Запрос сведений о регистрации домена

После того как вы узнаете целевое доменное имя, вам нужно запросить базу данных Whois и найти информацию об этом домене. База данных Whois предоставит информацию о DNS-сервере и контактную информацию домена. Whois — это протокол для поиска регистраций в Интернете, баз данных зарегистрированных доменных имен, IP-адресов и автономных систем. Данный протокол указан в RFC 3912 (https://www.ietf.org/rfc/rfc3912.txt).

По умолчанию Kali Linux уже поставляется с Whois-клиентом. Чтобы получить Whois-информацию о домене, просто введите следующую команду:

```
# whois example.com
```

Ниже приводится ответ Whois на введенную команду:

```
Domain Name: EXAMPLE.COM
    Registrar: RESERVED-INTERNET ASSIGNED NUMBERS AUTHORITY
Sponsoring Registrar IANA ID: 376
    Whois Server: whois.iana.org
    Referral URL: http://res-dom.iana.org
    Name Server: A.IANA-SERVERS.NET
    Name Server: B.IANA-SERVERS.NET
    Updated Date: 14-aug-2015
    Creation Date: 14-aug-1995
    Expiration Date: 13-aug-2016
>>> Last update of whois database: Wed, 03 Feb 2016 01:29:37 GMT <<<
```

Из представленного Whois ответа мы можем получить информацию о DNS-сервере и контактном лице домена. Она будет полезна на последующих этапах тестирования на проникновение.

Помимо использования клиента Whois из командной строки, информация также может быть собрана с помощью следующих сайтов:

- www.whois.net;
- www.internic.net/whois.html.

Для соответствующего домена можно также перейти к регистратору доменов верхнего уровня:

- Америка: www.arin.net/whois/;
- Европа: www.db.ripe.net/whois;
- Азиатско-Тихоокеанский регион: www.apnic.net/apnic-info/whois_search2.

Внимание: для применения домена верхнего уровня регистратором whois домен должен быть зарегистрирован через собственную систему. Например, при использовании WHOIS ARIN поиск будет выполняться только в базе данных WHOIS ARIN. Базы данных Whois RIPE и APNIC использованы не будут.

После получения информации из базы Whois нам следует собрать информацию о DNS-записях целевого домена.

Анализ записей DNS

Целью использования средств категории записи DNS является сбор информации о DNS-серверах и соответствующих записях целевого домена.

Далее приведены некоторые общие типы записей DNS.

Например, при тестировании на проникновение клиент может попросить вас узнать все хосты и IP-адреса, доступные для их домена. Единственная информация,

которой вы располагаете, — это доменное имя организации. Мы рассмотрим несколько общих инструментов, которые в такой ситуации могут вам помочь.

Тип записи	Описание
SOA	Начало записи полномочий
NS	Запись имени сервера
A	Запись адреса IPv4
MX	Запись обмена почтой
PTR	Запись указателей
AAAA	Запись адреса IPv6
CNAME	Аббревиатура канонического имени. Используется в качестве псевдонима для другого канонического доменного имени

Получение имени хоста

После того как мы получим информацию о DNS-сервере, необходимо узнать IP-адрес хоста. Можно использовать следующие средства командной строки для поиска IP-адреса хоста с DNS-сервера:

```
# host hackthissite.org
```

По умолчанию команда `host` будет искать записи A, AAAA и MX домена. Чтобы запросить отдельную запись, добавьте параметр `-a`:

```
# host -a hackthissite.org
Trying "hackthissite.org"
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 32115
;; flags: qr rd ra; QUERY: 1, ANSWER: 12, AUTHORITY: 0, ADDITIONAL: 0
;; QUESTION SECTION:
;hackthissite.org. IN ANY
;; ANSWER SECTION:
hackthissite.org. 5 IN A 198.148.81.135
hackthissite.org. 5 IN A 198.148.81.139
hackthissite.org. 5 IN A 198.148.81.137
hackthissite.org. 5 IN A 198.148.81.136
hackthissite.org. 5 IN A 198.148.81.138
hackthissite.org. 5 IN NS ns1.hackthissite.org.
hackthissite.org. 5 IN NS c.ns.buddyns.com.
hackthissite.org. 5 IN NS f.ns.buddyns.com.
hackthissite.org. 5 IN NS e.ns.buddyns.com.
hackthissite.org. 5 IN NS ns2.hackthissite.org.
hackthissite.org. 5 IN NS b.ns.buddyns.com.
hackthissite.org. 5 IN NS d.ns.buddyns.com.
Received 244 bytes from 172.16.43.2#53 in 34 ms
```

Команда host, запрашивая DNS-серверы, перечисленные в файле /etc/resolv.conf вашей системы Kali Linux, ищет эти записи. Если вы хотите использовать другие DNS-серверы, просто укажите адрес нужного сервера в качестве последнего параметра командной строки.

Если для команды host в качестве параметра вы укажете имя домена, будет вызван метод прямого просмотра. Если же в качестве параметра для команды host зададите IP-адрес, будет применен метод обратного просмотра.

Попробуйте с помощью IP-адреса применить метод обратного просмотра:

```
host 23.23.144.81
```

Какую информацию вы получите с помощью этой команды?

Команду host также можно использовать для передачи зоны DNS. С помощью этого механизма мы можем собирать информацию о хостах, доступных в домене.

Передача зоны DNS — это механизм, используемый для репликации базы данных DNS с главного DNS-сервера на другой DNS-сервер, обычно называемый подчиненным. Без этого механизма администраторы должны обновлять каждый DNS-сервер отдельно. Запрос на передачу зоны DNS должен быть выдан полномочному DNS-серверу домена.

В настоящее время очень редко можно найти DNS-сервер, который в ответ на запрос передачи произвольной зоны позволяет передачу зоны DNS. Это объясняется характером той информации, которая может быть собрана в процессе передачи зоны DNS.

Если вы нашли DNS-сервер, передающий зоны без ограничения, значит, он настроен неправильно.

dig: техники разведывания DNS

Для опроса DNS вы, кроме команды host, можете использовать dig. По сравнению с командой host у dig есть некоторые преимущества: эксплуатационная гибкость и понятные результаты на выходе. С помощью команды dig вы можете попросить систему обработать список поисковых запросов из файла.

Опросим с помощью dig домен http://hackthissite.org. Если команде dig, кроме имени домена, больше не предоставлять никаких параметров, мы получим только запись A домена. Чтобы запросить любой другой тип записи DNS, следует сообщить дополнительные параметры:

```
# dig hackthissite.org
; <<>> DiG 9.9.5-9+deb8u5-Debian <<>> hackthissite.org
;; global options: +cmd
;; Got answer:
```

```
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 44321
;; flags: qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; MBZ: 0005 , udp: 4096
;; QUESTION SECTION:
;hackthissite.org. IN A
;; ANSWER SECTION:
hackthissite.org.   5  IN  A  198.148.81.139
hackthissite.org.   5  IN  A  198.148.81.137
hackthissite.org.   5  IN  A  198.148.81.138
hackthissite.org.   5  IN  A  198.148.81.135
hackthissite.org.   5  IN  A  198.148.81.136
;; Query time: 80 msec
;; SERVER: 172.16.43.2#53(172.16.43.2)
;; WHEN: Tue Feb 02 18:16:06 PST 2016
;; MSG SIZE rcvd: 125
```

Из результата видно, что выходные данные `dig` теперь возвращают DNS-записи A.

DMitry: магический инструмент для сбора информации

Deepmagic Information Gathering Tool (DMitry) — инструмент для сбора информации «все в одном». Его можно использовать для сбора следующей информации:

- записи протокола Whois (получение регистрационных данных о владельцах доменных имен) с применением IP-адреса или доменного имени;
- сведений о хосте от https://www.netcraft.com/;
- данных о поддоменах в целевом домене;
- адресов электронной почты целевого домена.

Кроме того, сканируя порты, мы получим списки открытых, фильтрованных и закрытых портов целевого компьютера.

Конечно, всю эту информацию можно получить с помощью разных других инструментов Kali Linux. Но гораздо удобнее использовать для этих целей один инструмент.

Поскольку в DMitry предусмотрено больше возможностей анализа DNS, нам кажется, что этот инструмент больше подходит для классификации зоны DNS, а не для анализа маршрута.

Чтобы получить доступ к DMitry из меню Kali Linux, перейдите в раздел Applications ▸ Information Gathering ▸ dmitry (Приложения ▸ Сбор информации ▸ dmitry) или введите в командную строку следующую команду:

```
# dmitry
```

Для примера выполним с целевым хостом следующие действия.

1. Выполним поиск Whois.
2. Получим информацию от https://www.netcraft.com/.
3. Выполним поиск всех возможных поддоменов.
4. Проведем поиск всех возможных адресов электронной почты.

Для выполнения указанных действий выполните следующую команду:

```
# dmitry -iwnse hackthissite.org
```

Далее приведен сокращенный результат ее выполнения:

```
Deepmagic Information Gathering Tool
"There be some deep magic going on"
HostIP:198.148.81.138
HostName:hackthissite.org
Gathered Inet-whois information for 198.148.81.138
---------------------------------
inetnum:        198.147.161.0 - 198.148.176.255
netname:        NON-RIPE-NCC-MANAGED-ADDRESS-BLOCK
descr:          IPv4 address block not managed by the RIPE NCC
remarks:        http://www.iana.org/assignments/ipv4-recovered-address-
                space/ipv4-recovered-address-space.xhtml
remarks:
remarks:        ----------------------------------------------------
country:        EU # Country is really world wide
admin-c:        IANA1-RIPE
tech-c:         IANA1-RIPE
status:         ALLOCATED UNSPECIFIED
mnt-by:         RIPE-NCC-HM-MNT
mnt-lower:      RIPE-NCC-HM-MNT
mnt-routes:     RIPE-NCC-RPSL-MNT
created:        2011-07-11T12:36:59Z
last-modified:  2015-10-29T15:18:41Z
source:         RIPE
role:           Internet Assigned Numbers Authority
address:        see http://www.iana.org.
admin-c:        IANA1-RIPE
tech-c:         IANA1-RIPE
nic-hdl:        IANA1-RIPE
remarks:        For more information on IANA services
remarks:        go to IANA web site at http://www.iana.org.
mnt-by:         RIPE-NCC-MNT
created:        1970-01-01T00:00:00Z
last-modified:  2001-09-22T09:31:27Z
source:         RIPE # Filtered
% This query was served by the RIPE Database Query Service version 1.85.1 (DB-2)
```

Мы также можем использовать команду `dmitry` для простого сканирования портов. Для этого введите следующее:

```
# dmitry -p hackthissite.org -f -b
```

Результат выполнения команды выглядит таким образом:

```
Deepmagic Information Gathering Tool
"There be some deep magic going on"
HostIP:198.148.81.135
HostName:hackthissite.org
Gathered TCP Port information for 198.148.81.135
---------------------------------
Port     State
...
14/tcp   filtered
15/tcp   filtered
16/tcp   filtered
17/tcp   filtered
18/tcp   filtered
19/tcp   filtered
20/tcp   filtered
21/tcp   filtered
22/tcp   open
>> SSH-2.0-OpenSSH_5.8p1_hpn13v10 FreeBSD-20110102
23/tcp   filtered
24/tcp   filtered
25/tcp   filtered
26/tcp   filtered
...
79/tcp   filtered
80/tcp   open
Portscan Finished: Scanned 150 ports, 69 ports were in state closed
All scans completed, exiting
```

С помощью предыдущей команды мы обнаружили, что целевой хост использует программное обеспечение для фильтрации пакетов. Открыт только порт 22, к которому можно подключиться через SSH, и порт 80, обычно предназначенный для веб-сервера. Данная информация представляет интерес, так как указан тип установки SSH. Можно продолжить исследование уязвимостей, установив OpenSSH.

Maltego: графическое отображение собранной информации

Maltego — приложение с открытым кодом, которое предназначено для разведки и криминалистики. Оно позволяет добывать, собирать и систематизировать информацию. Maltego собирает информацию из открытых источников. После того как информация будет собрана, Maltego поможет определить ключевые связи между

данными и отобразить их в графическом виде. Такое отображение информации облегчит ее восприятие.

Maltego позволяет получить следующую информацию об инфраструктуре Интернета:

- имя домена;
- имя DNS;
- Whois-информацию;
- сетевые блоки;
- IP-адрес.

Maltego также можно использовать для сбора такой информации о людях, как:

- компании и организации, адреса электронной почты, связанные с конкретным человеком;
- сайты, социальные сети, связанные с данной персоной;
- социальные сети, связанные с человеком;
- номера телефонов;
- информация в социальных сетях.

По умолчанию Kali Linux поставляется с Maltego 3.6.1. Ниже перечислены ограничения доступной версии:

- нельзя использовать в коммерческих целях;
- максимум 12 результатов на преобразование;
- обязательная регистрация на сайте;
- действие ключа API ограничено несколькими днями;
- работает на более медленном сервере, доступном всем пользователям сообщества;
- общение между клиентом и сервером не шифруется;
- не обновляется до следующей версии;
- отсутствует поддержка конечных пользователей;
- нет обновлений преобразований на серверной стороне.

В Maltego доступно более 70 преобразований. Слово «преобразование» (transform) относится к фазе сбора информации Maltego. Одно преобразование означает, что Maltego выполнит только один этап сбора информации.

Чтобы получить доступ к Maltego из меню Kali Linux, выберите из основного меню пункты Application ▸ Information Gathering ▸ Maltego (Приложения ▸ Сбор информации ▸ Maltego). Maltego можно запустить, введя в командную строку терминала команду:

```
# maltego
```

После запуска программы вы увидите экран приветствия Maltego. Через несколько секунд появится следующий мастер запуска, который поможет вам настроить клиент Maltego. Для продолжения настройки нажмите кнопку Next (Далее). Появится следующее окно, в котором необходимо создать учетную запись и получить данные для входа.

После входа в систему введите свои личные данные (имя и адрес электронной почты). Затем необходимо выбрать источник преобразования (рис. 4.1).

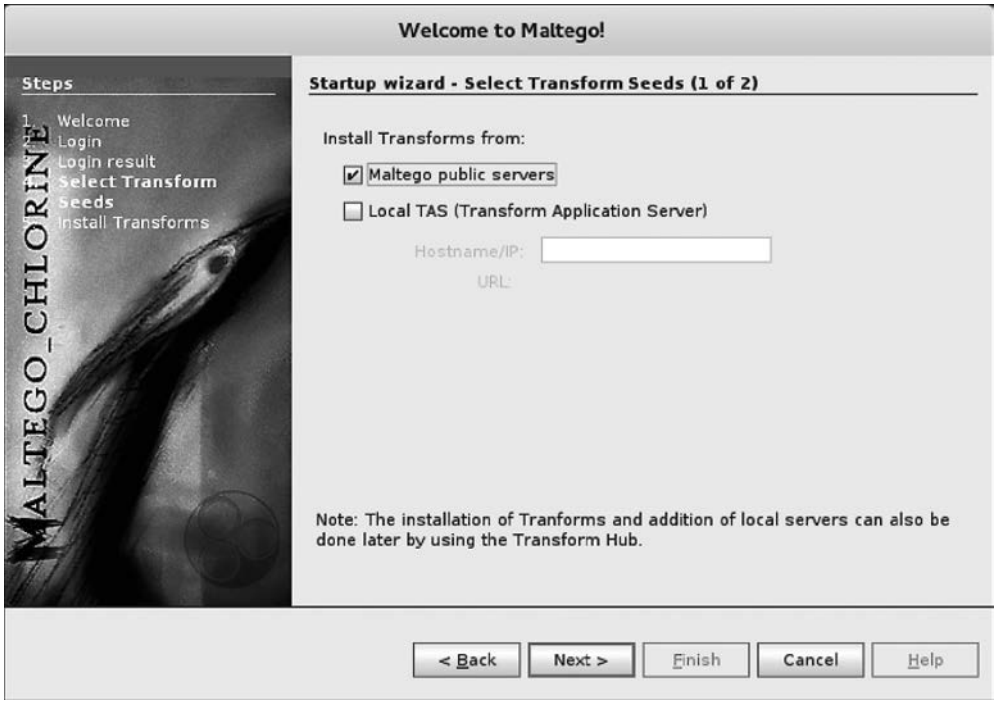

Рис. 4.1. Выбор источника преобразования

Клиентское приложение Maltego для получения преобразований подключается к серверам Maltego. Если Maltego успешно инициализируется, на экране появится следующее диалоговое окно (рис. 4.2).

Если вы увидели на экране компьютера это диалоговое окно, значит, инициализация клиентского приложения Maltego прошла успешно. Теперь вы можете приступать к его использованию.

Прежде чем использовать клиент Maltego, ознакомимся с его интерфейсом (рис. 4.3).

В верхней части интерфейса находятся вкладки групп команд. Чтобы выбрать нужную вкладку, достаточно щелкнуть на ее ярлыке. Вкладка Investigate (Исследо-

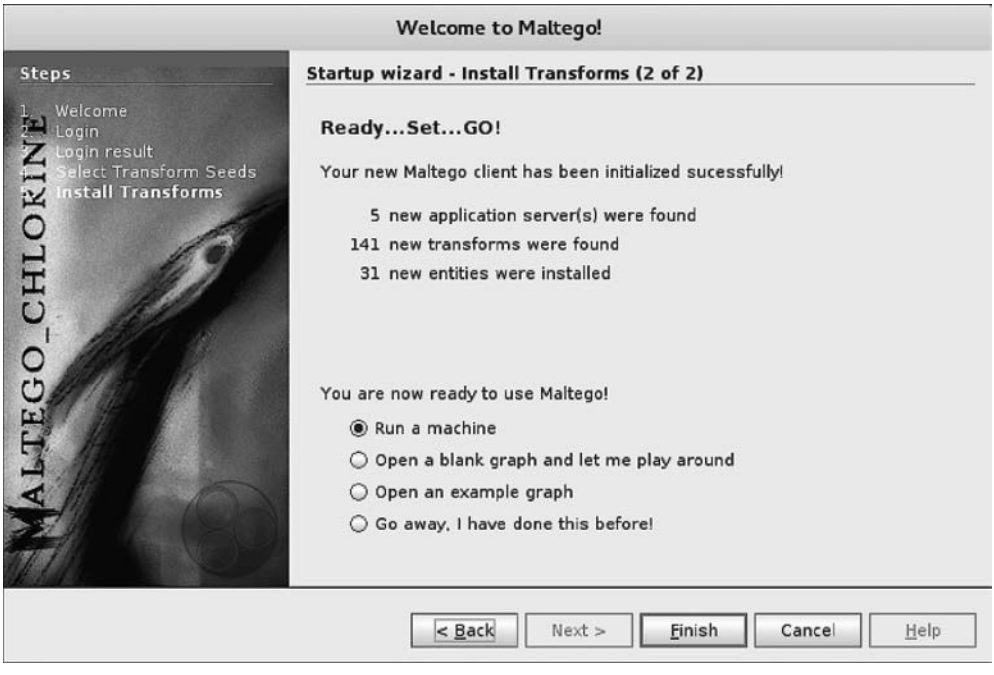

Рис. 4.2. Диалоговое окно мастера установки Maltego

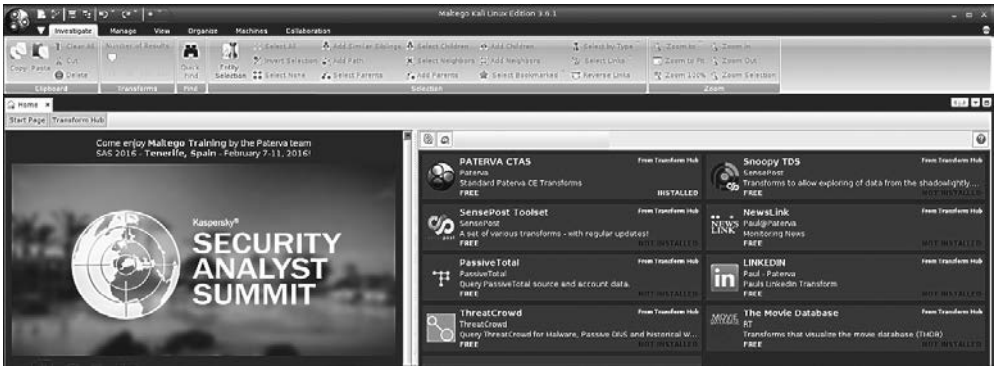

Рис. 4.3. Интерфейс клиентского приложения Maltego

вать) содержит команды, позволяющие выбрать тип объекта исследования. Maltego делит объекты на шесть групп.

- *Устройства:* телефон или камера.
- *Инфраструктуры:* DNS-имя домена, IP-адрес IPv4, MX-запись, NS-запись, блок сети, URL-адрес и сайт.

- *Расположение*.
- *Тест на проникновение*.
- *Личные данные:* псевдоним, документ, адрес электронной почты, фотография человека и фраза.
- *Социальные сети*, такие как Facebook, Twitter, причастность к Facebook или Twitter.

Правее вы увидите ярлык вкладки View (Вид). Используя ее команды, вы сможете выбрать режим отображения.

- Main View (Общий вид).
- Bubble View (Вид «Пузырьки»).
- Entity List (Список объектов).

Смена режима отображения используется для извлечения информации, которую тяжело заметить на больших графиках, где аналитик с помощью ручного контроля данных не может увидеть четких связей. Main View (Общий вид) — режим, в котором вы работаете большую часть времени. При выборе вида Bubble View (Вид «Пузырьки») все узлы будут отображаться в виде пузырьков. Если выбрать вид Entity List (Список объектов), все узлы будут отображены в виде списка.

Далее находится вкладка, где можно выбрать различные алгоритмы компоновки. Maltego поддерживает четыре алгоритма компоновки.

- Block layout (Макет блока) — выбран по умолчанию и используется во время интеллектуального анализа данных.
- Hierarchical layout (Иерархическая компоновка) — показывает формирование дерева узлов сети от корня до конечных ветвей. С помощью этого режима можно понять структуру ветвей и увидеть родительские/дочерние связи.
- Centrality layout (Центральное расположение) — показывает центральный узел, а затем подключенные к нему узлы. Эта функция может быть полезной при проверке нескольких узлов, связанных с одним центральным узлом.
- Organic layout (Органическая компоновка) — органическая компоновка так отображает узлы сети, когда расстояние между ними минимизируется, позволяя аналитику лучше понять общую картину узлов и их взаимосвязей.

После краткого ознакомления с интерфейсом клиента Maltego приступим к практическим действиям.

Предположим, у вас появилась необходимость собрать информацию о домене. Для эксперимента мы воспользуемся доменом example.com. Описание эксперимента вы найдете в следующих разделах.

1. Создайте новый график (Ctrl+T) и перейдите на вкладку Palette (Палитра).
2. Выберите Infrastructure (Инфраструктура) и щелкните кнопкой мыши на Domain (Домен).

3. Перетащите домен в главное окно. Если вы все сделаете правильно, то в главном окне увидите домен с именем paterva.com.
4. Дважды щелкните на имени и дайте ему имя целевого домена, например example.com (рис. 4.4).

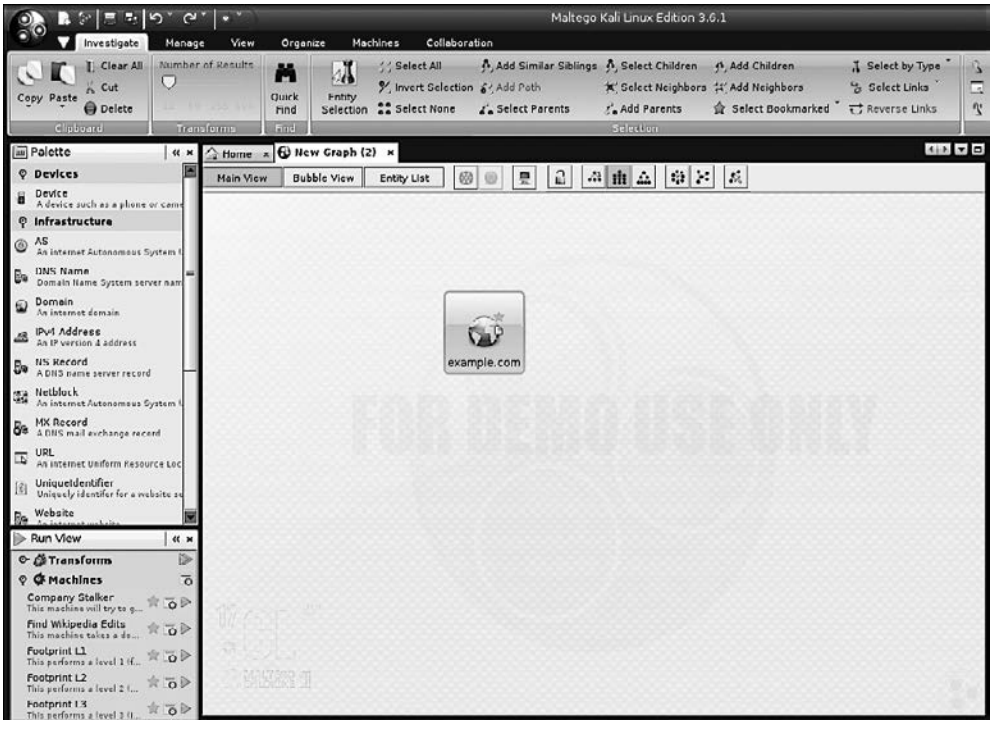

Рис. 4.4. Указание имени целевого домена

5. Если вы щелкнете правой кнопкой мыши на имени домена, то увидите список всех преобразований, которые можно с ним выполнить:
   - получить DNS домена;
   - получить сведения о владельце домена;
   - получить адреса электронной почты из домена;
   - получить файлы и документы из домена;
   - выполнить другие преобразования, такие как To Person (К человеку), To Phone numbers (К телефонному номеру) и To Website (К сайту).
6. Выберем DomainToDNSNameSchema из преобразований domain (для этого выполните Run Transform ▸ Other Transforms ▸ DomainToDNSNameSchema (Выполнить преобразование ▸ Другие преобразования ▸ DomainToDNSNameSchema)). Результат показан на рис. 4.5.

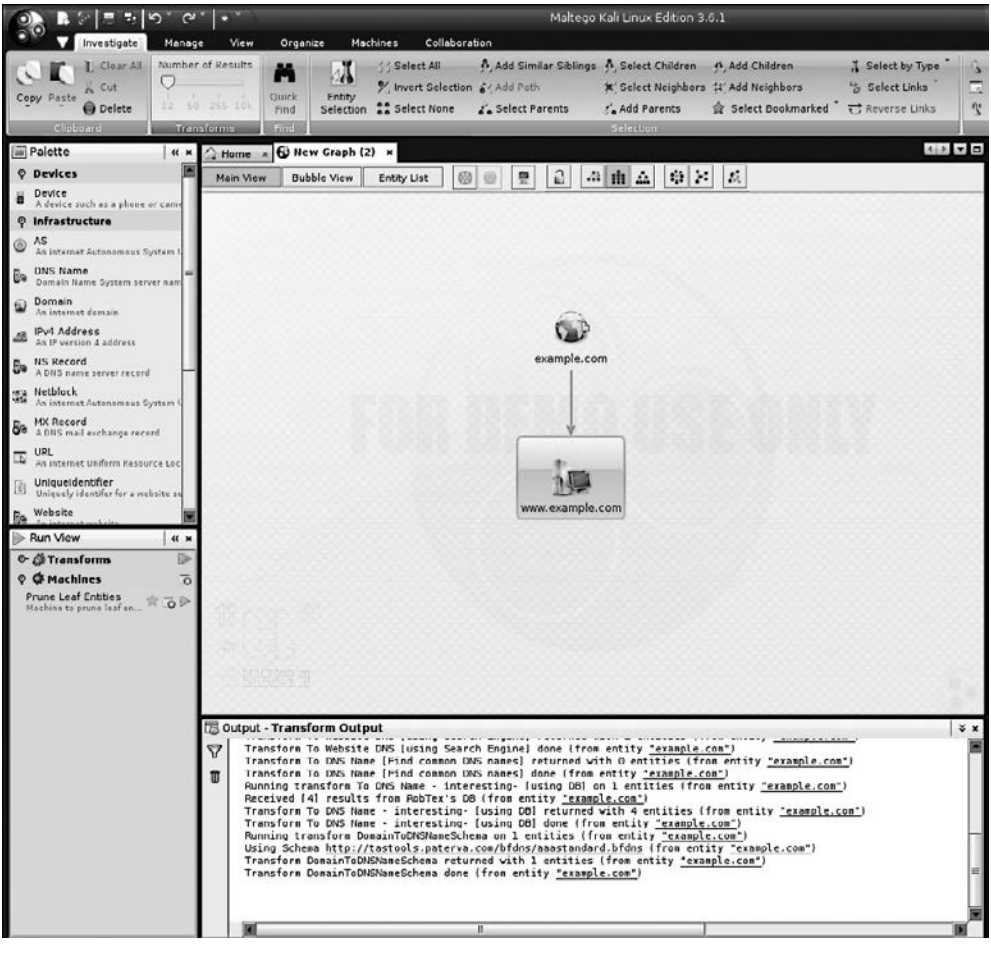

Рис. 4.5. Результат преобразований

После преобразования DNS из домена мы получили информацию об адресе сайта (www.example.com), связанного с доменом example.com.

В целевом домене можно выполнить и другие преобразования.

Если вы хотите изменить домен, сначала необходимо сохранить текущий график. Для этого сделайте следующее.

1. Щелкните на значке Maltego и выберите команду Save (Сохранить).
2. График будет сохранен в формате Maltego graph (.mtgx). Чтобы изменить домен, просто дважды щелкните на нем и измените его имя.

Далее мы опишем несколько инструментов, которые можно использовать для получения информации о маршрутизации.