Hacker Highschool

SECURITY AWARENESS FOR TEENS



УРОК **9**: ВЗЛОМ ЭЛЕКТРОННОЙ ПОЧТЫ

ВНИМАНИЕ

Проект Hacker Highschool является средством обучения и, как в любом обучающем средстве, существует опасность. Некоторые уроки, если ими злоупотреблять, могут привести к физической травме. Также дополнительные опасности могут быть там, где ещё недостаточно исследований о возможных последствиях излучений от специфической техники. Студенты, использующие эти уроки, находятся под контролем преподавателя и, в тоже время, должны быть мотивированы на изучение материалов и непрерывную практику. ISECOM не несёт ответственности за применение информации, полученной из данных материалов и за дальнейшие последствия.

Все представленные здесь материалы являются открытыми и общедоступными в соответствии с положениями и условиями организации ISECOM:

Все материалы проекта Hacker Highschool предназначены для некоммерческого использования в работе с учениками средних государственных или частных школ, техникумов, студентами высших учебных заведений, слушателями младших курсов Hacker Highschool и учащимися на дому. Эти материалы в любой форме не могут быть использованы для продажи. Обучение по этим материалом в обучающей организации, техникумах, университетах, профессионально-технических заведениях, летних или компьютерных лагерях и других организациях, в которых взимается плата за обучение, категорически запрещено без приобретения лицензии. Для более подробного ознакомления с условиями использования либо приобретения лицензии для коммерческого использования материалов, посетите раздел сайта предназначенный для Лицензирования http://www.hackerhighschool.org/licensing.html.

Проект HHS является результатом труда открытого сообщества и, если Вы находите наши труды ценными и полезными, мы просим Вас поддержать нас путём приобретения лицензии, пожертвований либо спонсорства.

Table of Contents

Сотрудники

Pete Herzog, ISECOM

Glenn Norman, ISECOM

Bob Monroe, ISECOM

Greg Playle, ISECOM

Marco Ivaldi, ISECOM

Simone Onofri, ISECOM

Peter Houppermans

Andrea Zwirner

Переводчики

Vadim Chakryan, Kharkiv National University of Radio Electronics

Olena Boiko, Kharkiv National University of Radio Electronics

Dmitriy Pichuev, Ukrainian Engineering Pedagogical Academy

Andrii Sezko, Kharkiv National University of Radio Electronics

ISECOM

Введение

Электронная почта известна уже давно; она появилась раньше Интернета. Это одна из первых форм обмена электронной информацией. До появления электронных писем были сигнальные ракеты, полуобнажённые ребята, выполнявшие роль посыльных, кирпичи с прикреплёнными записками, азбука Морзе, крупные камни, переброшенные через стены замка с написанными на них ругательствами и множество других подобных средств связи (к примеру, телефон или бумажная «улиточная почта» (на самом деле, она доставляется не улитками — это обычные письма, отправленные через почтовое отделение)). Для многих из этих оригинальных способов передачи сообщения нужны были специальные приспособления, особые навыки и много камней. К счастью, предприимчивые авторы придумали текст, который можно было написать на каменных табличках или в книгах и бросить людям или просто дать им его прочитать. Одной из первых была книга Сигнальные ракеты для чайников.

Работа электронной почты основывается на простых принципах передачи данных с промежуточным хранением (store and forward). Использование электронной почты оказывается достаточно простым (если только Вы не слишком спешите), очень надёжным и настолько дешёвым, что ею часто злоупотребляют в коммерческих и преступных целях. Асинхронная схема, лежащая в основе работы электронной почты, позволяет осуществлять общение без необходимости того, чтобы и отправитель, и получатель были одновременно в сети. Это можно сравнить с тем, как Ваша мама разговаривает с Вами, а Вы не обращаете никакого внимания до тех пор, пока она не задаст Вам вопрос. Во время передачи сообщения Вы «отсутствуете», но Вы должны быть хорошим игнорщиком. Эмм... приёмщиком. Да, хорошим приёмщиком.

В этом уроке мы рассмотрим работу современной электронной почты, а также вопросы хакинга и безопасности. Полученные знания Вы сможете использовать для развлечения или для своей выгоды.

В общем и целом: как работает электронная почта

Для начала представьте, что Вы — электронное письмо. Давайте проследим за тем, как Вы передаётесь и получаетесь, и определим различные составляющие компоненты, за счёт которых Вы перемещаетесь.

1. Email (Вы) создаётся (создаётесь) либо с помощью клиента email (например, Outlook, Mail, Eudora, Pegasus или Thunderbird), либо на веб-сервисе (к примеру, Yahoo Mail) через веб-интерфейс. Забавно, насколько сильно электронное письмо напоминает обычное письмо (которое передаётся «улиточной почтой») — оно тоже вкладывается в конверт, как на Рисунке 9.1.

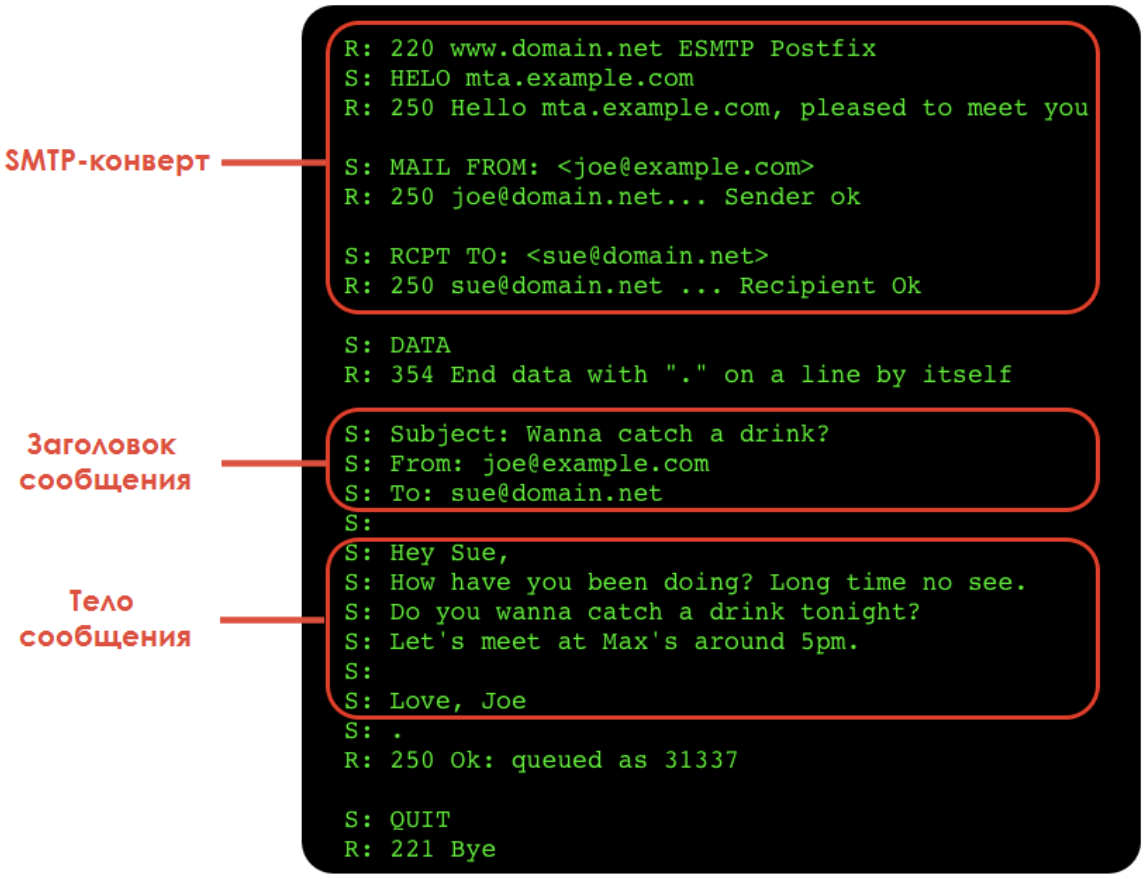

Рисунок **9.1:** Сообщение, заголовки и конверт электронного письма

2. Вы отправляетесь на почтовый сервер, который называется агентом пересылки сообщений **(Mail Transmission Agent, MTA)**; он ставит Вас в очередь для пересылки. Современные почтовые системы обычно используют для этого зашифрованный **SMTP (Simple Mail Transport Protocol**, простой протокол передачи почты**)**, поскольку они требуют аутентификацию для предотвращения нарушений использования, а шифрование защищает сведения о пользователях и содержимое письма от раскрытия. MTA, которые принимают электронное письмо (Вас) без какой-либо аутентификации, называются «открытыми серверами ретрансляции» (“open relays”); их, как правило, засоряют

отправители почтового мусора, также известного как UCE (Unsolicited Commercial Email, нежелательная коммерческая электронная почта) или спам.

3. Для каждого адреса («получателя») в сообщении MTA сначала проверяет, является ли получатель локальным (т. е. находится ли он на том же компьютере). Если нет, то MTA использует так называемую запись MX (которая рассматривается далее в уроке) для нахождения сервера для соответствующего домена. Если не найден соответствующий валидный хост, то отправитель получает сообщение об ошибке передачи на этот конкретный адрес.

4. MTA пробует доставить Вас по каждому из адресов. Если по каким-то причинам это не удалось, MTA вновь ставит сообщение в очередь для повторного отправления через некоторое время до тех пор, пока не истечёт время ожидания и не будет возвращено сообщение о сбое доставки (обычно в течение 48 часов). Так что Вам придётся ожидать около двух дней. Эта доставка изначально может быть преднамеренно отложенной принимающим MTA – так работает один из методов защиты от спама: спамерское программное обеспечение обычно не настолько умное и оно не будет выстраивать очередь и повторно доставлять сообщение (такой способ называется серыми списками **(greylisting)**). По умолчанию эта доставка осуществляется через незашифрованный SMTP. Зашифрованное соединение — это скорее исключение, а не правило.

5. Иногда ретрансляторы «подбирают» Вас и направляют к конечному пункту назначения. Такое происходит в системах с фильтрацией спама и вирусов и там, где безопасность требует использования многоуровневой модели (например, в сети предприятия или правительственного учреждения).

Вы обратили внимание на упоминание многоуровневой модели механизма защиты **(layered security model)**? Специалисты-безопасники, готовые работать в тяжёлом режиме, не могут создать конфеты M&Ms: твёрдые снаружи, но мягкие внутри. Они добавляют несколько слоёв защиты: регуляторы маршрутизаторов и брандмауэры, системы обнаружения вторжения (intrusion detection systems, IDS), системы защиты от вирусов, вредоносного ПО, спама и огромное множество других средств.

Похоже, что попытка взлома обречена на провал. Но никогда не забывайте о следующем: каждая установленная программа добавляет больше кода с возможными уязвимостями; то же касается и аппаратного обеспечения. Например, какое-нибудь крутое устройство для VPN может как обеспечить Вам «безопасную» сеть VPN, так и предоставить лазейки для злоумышленников. Всё зависит от того, принадлежите ли Вы к Красной команде («противникам») или к Синей.

6. Принимающий MTA восстанавливает адрес, если он представлен в виде алиаса или списка рассылки. Они не обязательно должны быть в одном домене: алиас может преобразоваться в совсем другой адрес на другом сервере. После получения полного адреса Вы вновь становитесь в очередь для последующего отправления.

7. Если адрес email относится к локальному почтовому ящику, то Вас направляют в этот почтовый ящик (если только объём хранящихся в нём писем не превысил допустимого предела). Вы можете оказаться слишком большим. Вы должны перестать есть столько низкокачественной пищи.

8. Далее по протоколу POP3 или IMAP Вас подбирает клиентская программа электронной почты. Обычно соединение защищено (с помощью SSL) для предотвращение утечки учётных данных пользователей; используются протоколы POP3S и SSL IMAP. POP3 осуществляет процесс «подбора»: он скачивает сообщения, а затем удаляет их с сервера (возможны настройки проведения этих действий на определённую дату/время). По протоколу IMAP осуществляется синхронизирующий процесс: почтовый ящик на стороне клиента должен быть идентичен ящику на учётной записи на сервере (для мобильных устройств эта процедура обычно проводится для определённого временнОго промежутка для сбережения памяти устройства); поэтому IMAP идеально подходит для использования электронной почты одновременно на нескольких устройствах.

9. Наконец, большинство клиентских программ электронной почты сейчас имеют встроенную систему определения спама; обычно эти системы основываются на Байесовских принципах классификации. Попробуйте отправить своему другу письмо, записав в поле «Тема» слово «Виагра», чтобы посмотреть эту систему в действии.

Три этапа фильтрации спама

a. Принимающие серверы сначала проверяют отправителя: SMTP-соединение не устанавливается с серверами из «чёрного списка» (существуют различные компании, которые предоставляют такие списки).
b. После принятия соединения сканируется содержимое письма. Некоторые организации обеспокоены тем, что письма могут быть ложно маркированы как спам; они могут потребовать, чтобы подозрительное письмо было маркировано как спам, но всё равно было доставлено.
c. Наконец, большинство клиентских программ электронной почты сейчас имеют встроенную систему определения спама; обычно они основываются на Байесовских принципах классификации.

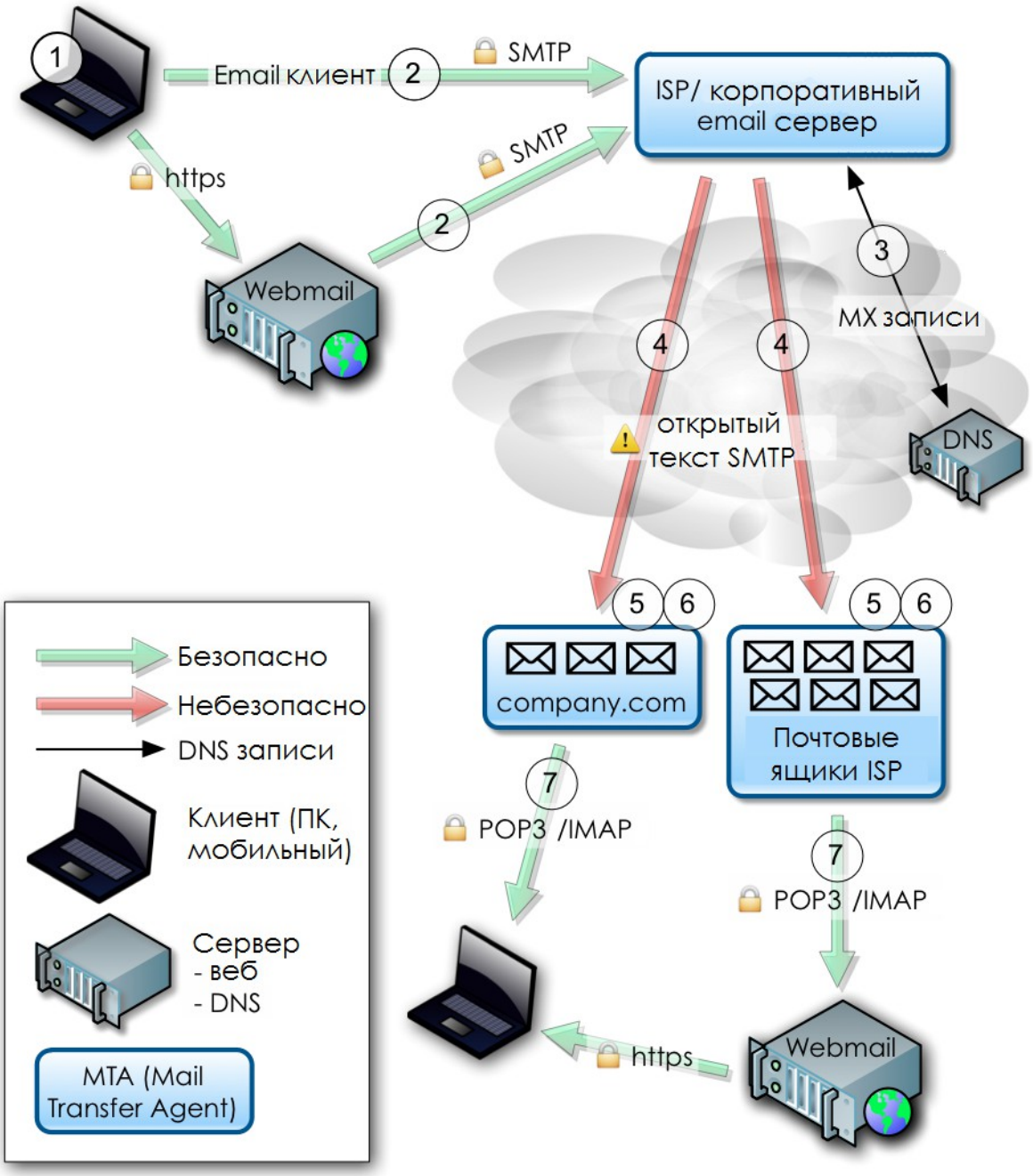

Рисунок **9.2:** Процесс обработки электронного письма

Вот и всё. Очень просто, не правда ли? Вы начинаете свой путь в одном месте, а затем можете оказаться (или не оказаться) в другом месте в зависимости от выполнения или невыполнения различных условий:

- У Вас есть правильный адрес
- Вы являетесь спамом
- Вы как письмо слишком большие
- Почтовый ящик получателя слишком маленький

- или Вы слишком старые.

Теперь Вы знаете, как электронные письма перемещаются по цифровому миру. Всё, что Вам нужно знать о жизни, можно получить из трафика электронной почты.

- Знайте, куда Вы направляетесь.
- Не потребляйте спам.
- Используйте большие почтовые ящики (много общайтесь).
- Не становитесь большим (Правильно питайтесь и занимайтесь спортом для поддержания здорового образа жизни).
- И, наконец, не старейте.

Видите, всё не так сложно!

Пища для ума: Заголовки **email**

Сообщение (с точки зрения SMTP) состоит из заголовков и тела. Заголовки — это данные, которые распознаются машиной; они содержат различную информацию. Среди наиболее простых — заголовок 'To:', в котором указывается получатель письма; заголовок 'Subject:' с темой письма. Казалось бы, заголовок адреса отправителя можно и не обсуждать, поскольку из названия понятно, что он означает, но вскоре мы увидим, что это более сложное понятие, чем кажется.

Тело сообщения содержит оставшуюся часть (т. е. всё, кроме заголовков); обычно MTA его не анализирует (хотя, как мы увидим далее, такой анализ возможен в целях фильтрации). Обычно тело сообщения содержит простой текст, но оно также может быть в формате HTML (что часто раздражает технических специалистов). В сообщениях, состоящих из нескольких частей (т. е. в сообщениях с вложениями) используется MIME. MIME расшифровывается как Multipurpose Internet Mail Extensions (многоцелевые расширения Интернет-почты). Это стандарт, который используется для отправки сообщений в кодировке, отличной от ASCII и двоичного содержимого. MIME при необходимости автоматически используется клиентом электронной почты.

Некоторые заголовки могут быть удалены, другие — модифицированы. Есть заголовки, которые будут добавлены различными компонентами в процессе передачи сообщения. Каждый MTA всегда должен добавлять заголовок "Received" («Получен») для прослеживания его роли во время передачи электронного письма. Теоретически, просматривая заголовки, Вы всегда должны иметь возможность определить исходного отправителя. Вскоре мы увидим, почему это не всегда так.

Существует набор заголовков, которые должно иметь каждое электронное письмо для того, чтобы быть проанализированным по стандарту SMTP; есть заголовки, которые большинство реализаций SMTP считают стандартными, но на самом деле это не так; и еще есть несколько обычных настраиваемых заголовков (X-*), которые могут содержать любую информацию. Это можно рассматривать как способ перемещения контента, определяемого пользователем, из тела в заголовки. Наиболее широко используются заголовки с информацией фильтрующих приложений (X-Spam) и MUA (X-Mailer) (MUA – Mail User Agent, это программа, с помощью которой пользователь осуществляет доступ). (Нередко в письмах можно заметить очень интересные пользовательские заголовки; в письмах от консультантов по безопасности можно увидеть и довольно

странные заголовки!)

Рассмотрим следующий пример.

[Пример сообщения]

```
From root@isecom.org Sat Sep 30 13:50:39 2006
Return-Path: <root@isecom.org>
Received: from isecom.org (localhost.localdomain [127.0.0.1])
      by isecom.org (8.13.8/8.13.7) with ESMTP id k8UBodHB001194
      for <test@isecom.org>; Sat, 30 Sep 2006 13:50:39 +0200
Received: (from root@localhost)
      by isecom.org (8.13.8/8.13.5/Submit) id k8UBoNcZ001193
      for root; Sat, 30 Sep 2006 13:50:23 +0200
Date: Sat, 30 Sep 2006 13:50:23 +0200
Message-Id: <200609301150.k8UBoNcZ001193@isecom.org>
From: root@isecom.org
To: test@isecom.org
Subject: foobar

test
```

Иногда в электронных письмах можно встретить дополнительный заголовок "From", за которым следует пробел и адрес отправителя без двоеточия как в обычном заголовке "From:". Это внутренний разделитель для сообщений, определённый форматом хранилища mbox, и он не является заголовком SMTP.

Агент доставки электронной почты **(Mail Delivery Agent (MDA))**, который является компонентом, ответственным за хранение сообщения на последнем этапе доставки, также защищает все строки, которые начинаются с "From" в теле сообщения; этот процесс часто неправильно интерпретируется.

Сообщение, показанное выше, было передано со следующей транзакцией SMTP:

```
CONNECT [127.0.0.1]
220 isecom.org ESMTP Sendmail 8.13.8/8.13.7; Sat, 30 Sep 2006
14:08:38 +0200
EHLO isecom.org
250-isecom.org Hello localhost.localdomain [127.0.0.1], pleased to
meet you
250-ENHANCEDSTATUSCODES
250-PIPELINING
```

```
250-8BITMIME
250-SIZE 5000000
250-DSN
250-ETRN
250-DELIVERBY
250 HELP
MAIL From:<root@isecom.org> SIZE=57
250 2.1.0 <root@isecom.org>... Sender ok
RCPT To:<test@isecom.org>
DATA
250 2.1.5 <test@isecom.org>... Recipient ok
Received: (from root@localhost)
      by isecom.org (8.13.8/8.13.5/Submit) id k8UC8EMj001346
      for root; Sat, 30 Sep 2006 14:08:14 +0200
Date: Sat, 30 Sep 2006 14:08:14 +0200
Message-Id: <200609301208.k8UC8EMj001346@isecom.org>
From: root@isecom.org
To: test@isecom.org
Subject: foobar

test
.
250 2.0.0 k8UC8c3M001347 Message accepted for delivery
QUIT
221 2.0.0 isecom.org closing connection
```

Путь сообщения можно проследить по заголовкам “Received”:

```
Delivered-To: <spoofer@isecom.org>
Return-Path: test@isecom.org
Received: from smtp.isecom.org (smtp.isecom.org [140.211.166.183])
        by azzurra.isecom.org (8.13.6/8.13.6) with ESMTP id
k4KL5UOq014773
        (version=TLSv1/SSLv3 cipher=DHE-RSA-AES256-SHA bits=256
verify=NO)
        for <spoofer@isecom.org>; Sat, 20 May 2006 21:05:30 GMT
Received: by smtp.isecom.org (Postfix)
```

```
        id D138A64413; Sat, 20 May 2006 21:05:29 +0000 (UTC)
Delivered-To: spoofer@isecom.org
Received: from localhost (localhost [127.0.0.1])
        by smtp.isecom.org (Postfix) with ESMTP id B87EF64409
        for <spoofer@isecom.org>; Sat, 20 May 2006 21:05:29 +0000
(UTC)
Received: from smtp.isecom.org ([127.0.0.1])
 by localhost (smtp.isecom.org [127.0.0.1]) (amavisd-new, port 10024)
 with ESMTP id 24780-13 for <spoofer@isecom.org>;
 Sat, 20 May 2006 21:05:23 +0000 (UTC)
Received: from mail2.isecom.org (bsiC.pl [83.18.69.210])
        (using TLSv1 with cipher DHE-RSA-AES256-SHA (256/256 bits))
        (No client certificate requested)
        by smtp.isecom.org (Postfix) with ESMTP id 6B37E64405
        for <spoofer@isecom.org>; Sat, 20 May 2006 21:05:23 +0000
(UTC)
Received: from localhost (localhost.isecom.org [127.0.0.1])
        by mail2.isecom.org (Postfix) with ESMTP id BDF11B02DE
        for <spoofer@isecom.org>; Sat, 20 May 2006 23:12:55 +0200
(CEST)
Received: from mail2.isecom.org ([127.0.0.1])
 by localhost ([127.0.0.1]) (amavisd-new, port 10024) with ESMTP
 id 11508-04 for <spoofer@isecom.org>; Sat, 20 May 2006 23:12:42
+0200 (CEST)
Received: from localhost (unknown [192.168.0.5])
        by mail2.isecom.org (Postfix) with ESMTP id 54666B02DC
        for <spoofer@isecom.org>; Sat, 20 May 2006 23:12:41 +0200
(CEST)
Date: Sat, 20 May 2006 23:05:04 +0200
From: John Doe <test@isecom.org>
To: spoofer@isecom.org
```

Утилита **dig**

Если Вы используете Linux или в общем UNIX, то **`dig`** – Ваш лучший товарищ для исследования настроек DNS. Записи MX очень важны для доставки электронной почты, поэтому давайте их кратко рассмотрим. Записи MX относятся к электронной почте и не имеют никакого отношения к веб-сайтам из того же домена. Веб-сервер "domain.com" может быть совсем другой системой, отличной от почтового сервера, и поэтому записи DNS определяются по-другому.

Получить записи MX можно с помощью команды `dig` в командной строке UNIX, Linux или OSX. `Dig` – это утилита для получения информации, связанной с DNS, и, как и любая другая UNIX-программа, она имеет несметное количество параметров. Мы будем использовать только один формат. С помощью команды

```
dig <имя домена> MX
```

можно вывести только записи обмена почтой от соответствующего домена. Ещё один простой пример представлен далее

```
dig <имя сервера> <тип>
```

В качестве примера можно протестировать публичный DNS-сервер 213.133.105.2 ns.second-ns.de. Посмотрите, от какого сервера клиент получит ответ.

```
dig sleepyowl.net
sleepyowl.net.          600     IN      A       78.31.70.238
;; SERVER: 192.168.51.254#53(192.168.51.254)
```

Ответил локальный маршрутизатор 192.168.51.254; ответом оказалась запись A. Можно запросить любую запись; DNS-сервер можно выбрать с помощью символа @:

```
dig MX google.com                   # Получить почтовые записи MX
dig @127.0.0.1 NS sun.com           # Тестирование локального сервера
dig @204.97.212.10 NS MX heise.de   # Запрос на внешний сервер
dig AXFR @ns1.xname.org cb.vu       # Получить всю зону (перенос зоны)
```

Команда `host` также предоставляет множество возможностей.

```
host -t MX cb.vu                    # Получить почтовые записи MX
host -t NS -T sun.com               # Получить запись NS
host -a sleepyowl.net               # Получить все данные
```

В качестве более объёмного примера рассмотрим записи MX для домена Google *gmail.com*:

```
;; ANSWER SECTION:
gmail.com.          893     IN      MX      10 alt1.gmail-smtp-in.l.google.com.
gmail.com.          893     IN      MX      40 alt4.gmail-smtp-in.l.google.com.
gmail.com.          893     IN      MX      30 alt3.gmail-smtp-in.l.google.com.
gmail.com.          893     IN      MX      20 alt2.gmail-smtp-in.l.google.com.
gmail.com.          893     IN      MX      5 gmail-smtp-in-v4v6.l.google.com.
```

В каждой строке есть три значения, которые представляют для нас интерес. “893” – это значение **time to live** (сколько секунд или сколько маршрутизаторов можно пройти), которое Вы найдёте в каждой записи DNS – оно определяет, насколько долго DNS разрешено хранить

запись в кэше до того, как информация будет считаться устаревшей и подлежащей обновлению.

Значение "10" в первой строке и значения "40", "30", "20" и "5" в последующих строках — это значение «предпочтения», за которым следует полностью определённое имя домена **(Fully Qualified Domain Name, FQDN)** системы, готовой обработать электронное письмо. Значения предпочтения используются MTA для того, чтобы определить, с какой машиной из списка записей MX работать первой, а с какими — далее по очереди в случае, если первая отбросит электронное письмо. Если не найден ни один сервер, который принял бы электронное письмо, то отправителю письма отправляется сообщение о сбое (используя информацию "reply-to" или "from"). Чем меньше значение, тем выше уровень предпочтения MTA. Таким образом, последняя запись в приведенном выше списке будет обработана первой, остальные будут запасными вариантами.

Сервис также может выдать записи с одинаковыми значениями предпочтения; ниже приведен ответ от yahoo.com, в котором значение предпочтения для всех записей равно «1»:

```
;; ANSWER SECTION:
yahoo.com.          48      IN      MX      1 mta6.am0.yahoodns.net.
yahoo.com.          48      IN      MX      1 mta5.am0.yahoodns.net.
yahoo.com.          48      IN      MX      1 mta7.am0.yahoodns.net.
```

Это означает, что загрузка электронного письма будет равномерно распределена на 3 системы. Очень маленькое значение TTL, равное «48», наводит на мысль, что запись DNS динамически управляемая, что свидетельствует об активной балансировке нагрузки. Функция устройств балансировки нагрузки соответствует их названию — с их помощью трафик (трафик входящих или исходящих сообщений, трафик с высоким или низким приоритетом) получает уровень внимания, который он заслуживает.

Последним, но не менее важным является то, что Вы также можете определить, использует ли домен получателя фильтрацию электронной почты. В известном домене no10.gsi.gov.uk (домен премьер-министра Великобритании) указано, что компания под названием MessageLabs на данный момент ответственна за фильтрацию почты:

```
;; ANSWER SECTION:
no10.gsi.gov.uk.    3600    IN      MX      20 cluster.gsi2.messagelabs.com.
no10.gsi.gov.uk.    3600    IN      MX      10 cluster.gsi.messagelabs.com.
```

Вам не нужно опасаться чёрных вертолётов, просматривая эти данные: эта информация общедоступна; иначе электронная почта не смогла бы работать. Кроме того, у вооружённых сил Великобритании есть только зелёные вертолёты!

Упражнения

9.1 Поддерживает ли Ваша платформа для электронных писем «Уведомление о доставке» ("Delivery Receipt") или любой другой флаг доставки, по которому можно определить (по крайней мере), что Ваше письмо дошло до определённого адресата? Если да, то обменяйтесь сообщениями с другом и просмотрите заголовки из этого трафика.

9.2 Выберите доменное имя. Определите, какая система обрабатывает электронные письма для этого домена, просмотрев записи MX.

Игра началась: Ловушка для жуков

Пол кафе был слегка влажный, почти как липкая лента для мух, и чувствовалось, что её обувь с резиновой подошвой прилипает к полу. Джейс смотрела на сияющий блеск грязного пола и удивлялась тому, как в месте, где подают еду, может быть такой ужасный запах и одновременно сияние, подобное зеркальному. Этот запах напомнил ей о том, как её дедушка раньше помещал ловушки для тараканов в квартире за диваном. Когда дедушка вытаскивал старую ловушку, Джейс могла посмотреть на покрывшиеся пылью остатки насекомых. Казалось, что ловушка внутри была полностью заполнена мёртвыми тараканами.

Она никогда не стеснялась задавать вопросы. «Почему тараканы просто не вылезут из коробки? Разве они не видят, что все их друзья внутри мертвы?» — неоднократно спрашивала она дедушку, чтобы убедиться, что каждый раз она получает правильный ответ. Джейс нравилось наблюдать за работой дедушки, часто при этом мешая ему, заглядывая ему через плечо. Он никогда не жаловался. Ему нравилось проводить как можно больше времени в компании своей внучки.

«Джейс, тараканов привлекает запах внутри коробки. Как только они попадают внутрь ловушки, они застревают в коробке, ведь дно очень липкое. Кажется, что они приклеены ко дну коробки. Похоже, что они не замечают внутри других мёртвых насекомых и они тоже погибают,» — когда Джейс спрашивала дедушку, он каждый раз отвечал её приблизительно одно и то же.

«Тараканы не очень умны,» — отвечала маленькая Джейс со слегка самодовольной улыбкой.

«Да, дорогая, ты намного умнее, чем эти тараканы.»

«Спасибо... наверное.»

Вернувшись мыслями в школьный кафетерий, Джейс продолжила смотреть на зеркальный пол; её волосы цвета шоколада спадали на её лицо; она должна была продолжить работу над домашним заданием.

Краем глаза Джейс увидела какую-то суету у двустворчатых дверей кафе. Они распахнулись, и в просторное помещение вошли несколько людей. Быстро перейдя в режим скрытности, она наклонилась вперёд, и её волосы длиной по плечи закрыли её лицо. Она услышала: «Там, она там, пытается спрятаться! Схватите Джейс. Не дайте ей убежать!» — несколько взрослых голосов пронзительно крикнули, как в былые времена восклицали охотники на ведьм.

Молодая хакерша сохраняла свою позицию за столом, крепко сжав свой рюкзак и притворяясь, что не знает о надвигающейся атаке. Ножи, вилы, паяльные лампы, разъярённая толпа и все картинки с монстрами из фильмов пронеслись перед её расчётливым умом. И всё-таки любопытство взяло верх — она подняла голову и увидела директора школы, его секретаря, мистера Три, троих первокурсников, которые играли в настольный теннис, и нескольких чудаков, которые приближались к ней. Грохот их голосов был оглушительным, он отражался от полированного пола в сторону Джейс.

«Постой-ка! Я сказал стоять,» — знакомый голос командовал где-то за сердитыми

чудаками. Люди замерли в ожидании. Первокурсники помогли начальнику полиции пройти сквозь толпу. «Хорошо, ребята, спасибо вам за помощь (даже чрезмерную) в поисках мисс Джейс. Теперь я хотел бы поговорить с ней наедине,» — сказал начальник полиции спокойным голосом. Таким же голосом он вёл переговоры с парнем, который хотел спрыгнуть с 14-этажного здания несколько лет назад. Тогда это сработало, и сейчас, похоже, тоже сработало. Толпа разредилась: люди пытались казаться занятыми, завязывали шнурки на ботинках и слишком явно пытались подслушать частный разговор Джейс с полицейским.

«Привет, Джейс,» — начальник полиции не придумал ничего другого, чтобы начать разговор.

«Здравствуйте. Чем я могу помочь Вам в МОЕЙ школе во время МОЕГО обеда. Когда МОИ друзья внимательно смотрят на МЕНЯ,» — она чуть было не сломала себе челюсть, стискивая зубы.

«Прошу прощения, я не хотел прерывать здесь твою встречу с друзьями, но сейчас мне нужна твоя помощь,» — сказал начальник полиции, пытаясь сдерживать себя, но в то же время давая Джейс понять, что сейчас не подходящее время усложнять дело. Джейс уже не так крепко сжимала свой рюкзак и посмотрела в лицо начальнику полиции. Он кивком головы указал на двустворчатые двери кафетерия, предлагая ей следовать за ним.

Джейс посмотрела на свой недоеденный бутерброд, борясь с внутренним сопротивлением. Начальник полиции не отводил от неё взгляда. Он поднял свою правую руку и щёлкнул пальцами. Джейс вздрогнула. Все, кто был в закусочной, вздрогнули. Директор Мэнтрал понял, что значит этот сигнал, и, спеша, принёс прозрачный полиэтиленовый пакет.

«Печенье, да?» — спросила Джейс.

«С шоколадной крошкой и орехами, испечённое женой офицера Хэнка,» — ответил начальник. — «Идёт?»

«Идёт,» — ответила она, уже дожёвывая одно печенье.

После того, как они вышли из школы, полицейский спросил Джейс, ездила ли она когда-нибудь раньше в фургоне спецназа. «Это было единственное транспортное средство, которое мне удалось достать в последний момент. Извини,» — сказал он. Они эффектно уехали из школы — в фургоне спецназа они были похожи на рок-звёзд. Джейс засмеялась, глядя в зеркало заднего вида на ошеломлённых студентов и учителей.

«Дело вот в чём. Кто-то просматривает мою электронную почту. Я не знаю, как, кто и почему, но я уверен, что мой ящик взломали. Мне нужно, чтобы ты помогла мне прекратить это. Из-за этого возникают серьёзные проблемы в деятельности правоохранительных органов,» — начальник не дал Джейс шанса прервать его. – «Когда ты прошлым летом настраивала нашу сеть, ты установила кучу дополнительных штук для обеспечения безопасности. Этого оказалось недостаточно. Я могу сказать тебе, что одно электронное письмо, написанное три недели назад, содержало информацию о кое-каком подозреваемом. Только я и окружной прокурор знали об этих подробностях.»

Начальник полиции протянул руку через салон фургона, чтобы взять печенье из открытой сумки. Джейс в шутку шлёпнула его руку. Он потянулся за полицейской дубинкой, которой у него не было при себе, поскольку он уже не был уличным полицейским. Джейс смягчилась и дала ему большое ореховое печенье, чтобы он не прерывал свой рассказ (а он его прервал); крошки с печенья сыпались с его формы.

«Два часа спустя после того, как мы с окружным прокурором обменялись письмами, мне

позвонил дежурный — подозреваемый только что внёс залог. Адвокат подозреваемого узнал о той подробности, а судья подписал документ об освобождении подозреваемого. О той информации знали только два человека и обмен ею был через мою почту,» — сказал начальник.

Он продолжил: «На прошлой неделе мне позвонили и сообщили о том, что на месте совершения преступления, возможно, отсутствовала некоторая улика. Это был просто анонимный звонок. В нём не было упоминания какой-то конкретной вещи. Я быстро написал электронное письмо нашему сотруднику, занимающемуся уликами, с запросом описания вещественных доказательств, фигурировавших в случаях, происшедших за всю неделю, особенно за тот день. Этот сотрудник отправил мне по электронной почте журнал улик, и я сравнил его с отчётом полиции с места преступления. Будучи доскональным следователем, я удалил из журнала всю информацию, не относящуюся к делу, и перенаправил его к нашей команде следователей, занимающихся служебной проверкой.»

Джейс пыталась понять, что он говорит по сути в промежутках между всем полицейским жаргоном. «И что?» — сказала она, почувствовав себя намного лучше после съеденного бутерброда и пяти печенек.

Начальник полиции выглядел немного раздражённым, но всё равно ответил: «И что? А то, что у нас нет никаких недостающих улик. Позже в тот же день окружной прокурор вновь позвонил мне; он спросил меня, где находится орудие убийства из того случая. Мне и в голову не пришло, что пистолета не было в ящичке для улик. И вновь спустя два часа другой подозреваемый был выпущен под залог из-за того, что полиция и суд не задокументировали или не предоставили пистолет, фигурировавший в преступлении».

Джейс с мыслью о том, что неплохо было бы сейчас запить печенье большим стаканом холодного молока, попыталась сделать вывод из всего услышанного: «То есть таинственный звонящий проверял, находится ли пистолет в полиции. Письмо, которое Вы отправили команде следователей, подтвердило, что это оружие никогда не числилось в качестве полицейского доказательства.»

На лице начальника полиции появилась довольная улыбка, когда она закончила свои умозаключения. «Знаешь, Джейс, ты могла бы стать отличным полицейским детективом, когда подрастёшь.»

Джейс ответила: «Да, возможно, но у меня слишком развито чувство собственного достоинства, чтобы становиться полицейским. Я лучше стану юристом или политиком или кем-то другим, относящимся к более низкоорганизованной форме жизни.» К счастью, она засмеялась, сказав последнее предложение, ведь полицейский после таких слов уже разозлился. «Я просто шучу.»

Игра продолжается...

Написание **e-mail –** дело рискованное

- Разглашение. Подумайте о том, кому, почему и как Вы отправляете электронные письма. Кроме того, что сама передача электронных писем по умолчанию небезопасна после отправки их с локального MTA, Вы также раскрываете некоторую информацию. Использование шифрования (такого, как PGP, GPG и S/MIME) требует, чтобы обе стороны были одинаково программно обеспечены, и обычно очень сложно в применении (другими словами — пользователи с удовольствием избегают этого). Альтернативным

способом защитить передачу писем является использования одинакового провайдера электронной почты: в этом случае письму не нужно «путешествовать» по Интернету в открытом виде. И здесь возникает важный вопрос: уверены ли Вы, что Ваш провайдер или провайдер получателя не прослушивается? Учитывайте это, отправляя какую-либо конфиденциальную информацию.

- Изменение маршрута. Электронное письмо не всегда обязательно остаётся в том домене, куда оно было отправлено; иногда оно может быть перенаправлено куда-то в другое место. Например, американская компания *pobox.com* продаёт только алиасы, но не почтовые ящики. Основным риском является то, что Ваше электронное письмо может таким образом перемещаться по регионам, подпадающим под другую правовую юрисдикцию, до того момента, как оно дойдёт в место своего назначения. В нашем примере алиас *pobox.com* всегда будет сперва проходить через MTA в США, и, таким образом, есть риск его перехвата согласно Закону US PATRIOT.
- Нарушение неприкосновенности частной жизни. Получатель, пользующийся такими сервисами, как Facebook или Google, раскрывает свою электронную почту автоматизированным сканерам содержимого, даже если отправитель не давал на это разрешение!
- Список адресатов. Если Вы используете список адресатов, то лучше используйте для этого поле BCC (blind carbon copy, «слепая» копия, скрытая копия). Адреса, указанные в поле TO: и CC:, видны каждому получателю письма; это может привести к попаданию содержимого списка адресатов к третьей стороне и повлечь за собой атаки спама на адреса получателей Вашего письма.
- Конфликт. Электронное письмо — это как обычное письмо, но оно пишется и отправляется гораздо быстрее, и, следовательно, у Вас меньше времени для того, чтобы продумать его содержание. Написание электронного письма — это как вождение автомобиля: в раздражённом состоянии этого лучше не делать. Если Вы эмоционально возбуждены, то сохраните написанное письмо в черновиках, а через час заново обдумайте, стОит ли Вам его отправлять. Это может сохранить Вам дружбу или карьеру.
- Неправильный адрес. Одной из основных причин того, что письмо не попадает к адресату, является указание неправильного адреса. Это часто происходит, когда почтовые клиенты пытаются автоматически дополнить адрес по первым символам, введённым пользователем. Всегда проверяйте, является ли адрес получателя именно тем адресом, который Вам нужен.
- Несколько получателей. Отправляя электронное письмо нескольким людям, убедитесь в том, что содержимое этого письма предназначено всем получателям. Также хорошо и этически правильно будет отправить копию человеку, если в письме речь идёт о нём или об информации, полученной от него.
- Юридические вопросы. Дисклеймер (отказ от ответственности) под Вашим электронным письмом может произвести впечатление, но он не имеет никакого юридического значения, не считая уведомления об авторском праве. Вы сами отправляете письмо, и Вы не можете снимать с себя ответственность за его содержимое (отчасти Вы, конечно, всегда можете заявить, что его отправитель был подменён), и Вы не можете указывать адресату, получившему письмо по ошибке, что делать с этим письмом, поскольку Вы, скорее всего, не имеете с ним договорных отношений. (См. «Полное освобождение от ответственности» в конце этого урока.)
- Топ-постинг. Когда Вы отвечаете на письмо, Ваш клиент автоматически размещает Ваш ответ над исходным сообщением? Часто по умолчанию настройки сконфигурированы именно так, но, к сожалению, это … не очень вежливо. Получатели, которые должны

сначала прочитать Ваш ответ и только в конце письма понять контекст сообщения, скорее всего, будут не особо Вам благодарны. С другой стороны, раз они начали это общение, то они должны быть в курсе, о чём идёт речь. Но подумайте, удобно ли Вам самим использовать топ-постинг.

- Почтовые автоответчики. «Вы отправили мне письмо, поэтому я отправляю Вам этот автоматически сгенерированный ответ, чтобы сообщить Вам, что я не прочту Ваше письмо, пока не вернусь; и да помогут нам небеса, если у Вас тоже есть автоответчик, ведь весь процесс пойдёт по кругу до конца существования Вселенной.» Такая штука не только надоедлива; она также помогает злоумышленнику — ведь, скорее всего, Вас нет дома. Так на какой улице, говорите, живёте?
- Подпись. Используете ли Вы подпись — автоматически сгенерированное сообщение «Искренне Ваш, Иван Клокотун, менеджер по автоматическим действиям», которое добавляется в конце каждого отправляемого Вами сообщения? Это не всегда плохо — до тех пор, пока они не становятся слишком длинными. И с десяток таких сообщений «складируются» в конце продолжительного диалога. И все они представлены в HTML (а не в виде обычного текста без форматирования), так что картинка с гориллой, взбирающейся на небоскрёб, будет появляться вновь и вновь несколько раз. Так что будьте внимательны, оформляя подпись, и не подвергайте Ваших адресатов опасностям электронных писем в формате HTML, если Вы не умеете с ними правильно обращаться.

Упражнения

9.3 Зайдите на сайт http://www.gaijin.at/en/olsmailheader.php и добавьте в специальное поле заголовок любого электронного письма. Эта программа — это анализатор, который определит для Вас информацию о заголовках электронного письма. Как Вы можете использовать полученную информацию?

Получение электронной почты

Почтовые клиенты соединяются с серверами, на которых хранятся почтовые ящики, и проверяют, не изменился ли счётчик сообщений. Некоторые клиенты делают это периодически (например, каждые 30 минут), для некоторых это нужно сделать «вручную» (обычно для снижения нагрузки на сеть), а некоторые поддерживают постоянное соединение с почтовым сервером, получая обновления, как только на почту приходит новое письмо (называемое уведомлением **(push notification)**).

При поступлении письма почтовый клиент забирает его через протокол POP3 или IMAP. Мобильные клиенты, как правило, скачивают лишь заголовок и небольшую часть сообщения для экономии трафика. Таким образом, пользователь может решить: загрузить письмо полностью, оставить на потом или удалить его.

В первые годы существования электронной почты коммуникация происходила по ненадёжному, медленному соединению, и обработка приложенных к письму файлов (документов, таблиц или изображений) все ещё проходит с тем же уровнем риска. Вложение всегда должно быть загружено полностью перед тем, как оно может быть отображено. Пользователи, использующие почтовый веб-интерфейс (веб-мейл) на сторонних компьютерах (например, в Интернет-кафе), должны быть осторожными: просмотр вложения означает, что Вы оставляете копию на жёстком диске системы. По умолчанию, после использования они не удаляются.

Использование веб-мейла на ненадёжном компьютере рискованно ещё и по другой причине: если Вы не используете одноразовые пароли, Вы можете оставить после себя в системе

учётные данные своей электронной почты, и нет никакой гарантии того, что сторонний компьютер не заражен или не прослушивается.

Системы с активной электронной почтой должны регулярно обновлять антивирусную защиту. Но при этом Вы должны понимать, что антивирус защищает лишь от известного вредоносного ПО. При целевых атаках может уйти несколько дней, прежде чем вредоносное ПО будет добавлено в вирусные сканеры; некоторые вредоносные программы вообще никогда туда не добавляются.

Входящая почта в заголовках содержит «путь» письма. Каждая пройденная письмом система добавляется строкой в скрытую часть заголовка, при этом последняя система будет указана самой первой. Однако знайте, что эти данные легко подделать: имейте в виду, что не все записи могут быть реальными.

Упражнения

9.4 Просмотрите «временные» файлы, которые оставляют пользователи в процессе использования почты. Вы можете увидеть множество из них, осмотрев временные папки temp (которых, как правило, больше, чем одна). Windows, к примеру, позволяет легко увидеть содержимое временных папок, даже не зная их расположение: переменная **%temp%** знает их все.

Откройте командную строку в Windows и вбейте

```
dir %temp%
```

Что Вы увидели?

Для более удобного просмотра, используйте Windows Explorer (он же Проводник), используя команду:

```
explorer %temp%
```

9.5 Откройте заголовок любого письма. Сможете ли Вы определить других получателей, кроме Вас? Они могут быть в секции копии письма (CC) в его заголовке.

- Выберите несколько писем. Проследите путь письма и определите его отправителя по заголовкам письма. Просмотрите заголовок на наличие прочей доступной информации (подсказка: почтовые клиенты и версии антивирусов, алгоритмы шифрования и др.).
- Сравните адрес отправителя и адрес для ответа.
- Просмотрите несколько писем из спама. Какие отличия Вы видите в их заголовках по сравнению с обычными письмами? Посмотрите, куда ведут ссылки (только по строке, не переходя по ним). Ведут ли ссылки туда, куда, согласно тексту письма, они ссылаются?

Ответ на письмо

Отвечая на письмо, нужно проявлять некоторую осторожность. Сколько раз Вы говорили или делали что-то, чего не хотели бы или о чём впоследствии жалели?

Прежде всего, НИКОГДА не отвечайте на то, что наверняка является спамом, даже если это отписка. Ответив на такое письмо, Вы подтвердите, что (a) этот почтовый аккаунт используется и (b) кто-то с этим адресом действительно читает спам. Результатом отписки в этом случае, по иронии судьбы, станет поступление большего количества спама.

Проверьте видимость адресов. Нужно ли всем получателям быть видимыми? Если Вы используете список адресатов, все ли получатели все ещё действительны? Всем ли получателям нужно видеть Ваш ответ?

Будьте лаконичны. Нужно ли при ответе цитировать полученное письмо целиком или Вы можете просто использовать его наиболее важные части? Если вы повторно используете части предыдущего письма, Вы можете их процитировать — таким образом Вы покажете, что повторяете часть письма. После этого ответьте на цитируемую часть.

Цитируя, будьте осторожны: всё ли в письме предназначено для получателей, которых Вы сейчас выбрали, или Вы включаете конфиденциальные сообщения (или их части), не предназначенные для новых получателей? Избегайте цитирования всего письма, включая подпись и большие дисклеймеры. Имейте в виду, что всё, что Вы отправляете, может быть перенаправлено кому-либо без вашего разрешения или ведома. Хорошей и вежливой привычкой является добавление человека в список получателей копии письма, если в этом письме речь идёт об этом человеке или о чём-то, что он сделал. А для Вас это будет своеобразным напоминанием: не следует утверждать то, о чём в будущем, возможно, будете жалеть. Флаги доставки полезны при отслеживании перемещения письма к пункту назначения, а при просмотре MX записей Вы можете выяснить, куда отправится письмо. Также Вы можете использовать геолокацию, чтобы узнать физическое месторасположение. Но флаги доставки увеличивают трафик. При установке флага доставки Ваш почтовый сервер должен отправить ответ. Такие пометки писем, как «срочное» или «важное», не всегда оказываются полезными. Такие флаги, как правило, являются признаком того, что отмеченное сообщение является спамом, если только оно не было отправлено сотрудником.

Упражнения

9.6 Перенаправьте письмо на другую почту и сравните заголовки.

- Каким образом заголовки могут быть использованы против Вас, и как Вы можете это предотвратить?
- Можете ли Вы перенаправить письмо, которое было Вам отправлено, как скрытую копию (BCC)?

9.7 Напишите и отправьте письмо самому себе. Во время отправления быстро отмените отправку этого письма. Если отправка письма была успешно отменена, взгляните на заголовок черновика. Скопируйте этот заголовок в текстовый редактор и посмотрите, можно ли определить, какой почтовый сервер остановил отправку письма. Правда круто?

Криптозащита содержимого

Простота электронной почты делает её уязвимой. Отправитель не может быть уверен в том, что письмо не изменено по пути к получателю, и нет возможности убедиться, что только получатель может прочесть письмо. В то же время и получатель не может быть уверен, что письмо было отправлено тем, кто указан в письме как отправитель.

Один из способов обеспечить конфиденциальность — зашифровать документ перед его вложением в письмо. Например, можно зашифровать текстовые документы и таблицы (например, те, которые создаются в OpenOffice), и PDF-файлы, которые также поддерживают шифрование. Однако применение криптографии к самому письму проще, при этом содержимое письма тоже защищено.

В то же время, заголовки писем нужно оставлять в виде открытого текста, чтобы почтовые серверы могли обработать и доставить почту.

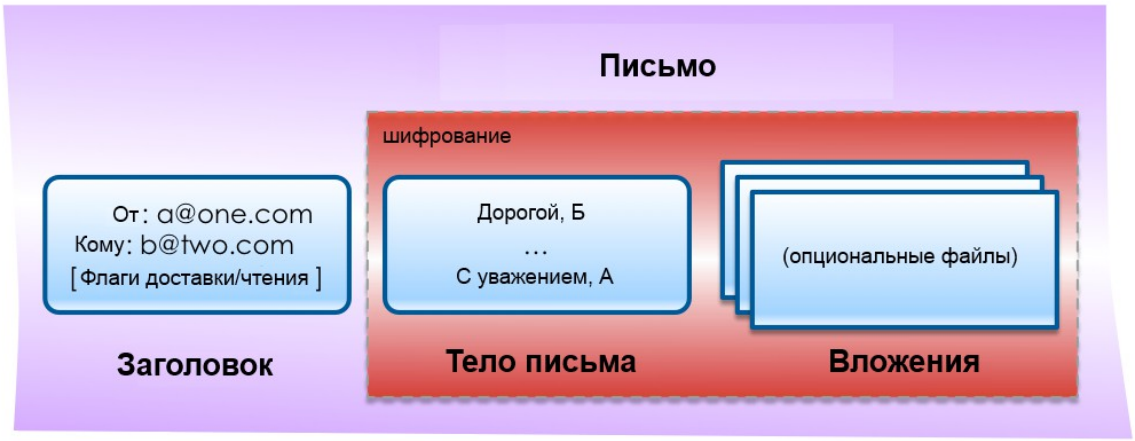

Рисунок **9.3:** Шифрование почты

Безопасность письма может быть достигнута двумя путями: с использованием PGP (или GPG) и S/MIME. В обоих случаях использование шифрования обеспечивает:

– Конфиденциальность (**C**onfidentiality): только ли предполагаемый получатель(ли) может читать это письмо?

– Целостность (**I**ntegrity): не изменилось ли содержимое электронного письма?

– Подлинность (**A**uthenticity): действительно ли электронное письмо пришло именно от этого отправителя?

(Легче всего запомнить этот список, используя первые три буквы каждого пункта: **CIA**.)

В общем подлинность и целостность объединены в цифровую подпись письма: рассчитывается контрольная сумма письма, а результат в зашифрованном виде встраивается в цифровую подпись, которая может быть создана только человеком, у которого есть нужный закрытый ключ (см. далее «PGP и GPG»).

Конфиденциальность обеспечивается путём использования чьего-то открытого ключа для шифрования тела письма, так что только обладатель правильного закрытого ключа может расшифровать и прочитать содержимое (см. далее «PGP и GPG»). Для большей уверенности такое сообщение также может быть подписано.

Вы должны иметь в виду, что шифрование электронной почты является довольно редким явлением, особенно в эпоху, когда люди добровольно разрешают сканировать свою почту таким компаниям, как Google и Facebook. Находясь в некоторых странах, Вы должны быть уверены, что у вас есть средства для доступа к Вашему почтовому ящику в случае, если власти потребуют этого от Вас, например, в США при пересечении границы (TSA, Transportation Security Administration, Управление транспортной безопасности) или в Великобритании на основании ордера в соответствии с законом «О следственных органах».

PGP и GPG

PGP означает Pretty Good Privacy (досл. «довольно хорошая секретность»). Она была разработана Филиппом Циммерманном (Phil Zimmermann). История PGP довольно интересна, и её стОит прочитать, но в данной главе мы сфокусируемся только на её использовании.

Самой распространённой является open source версия, которая называется GPG (GNU Privacy Guard). GPG бесплатна и доступна для большинства платформ. В ней используются только открытые публичные алгоритмы.

GPG работает по принципу управления открытым/закрытым ключами, который означает, что ключи имеют ОТКРЫТУЮ часть, которую Вы можете дать кому угодно, кто хочет отправить Вам зашифрованное письмо, и ЗАКРЫТУЮ часть, которую Вы должны держать в тайне, чтобы расшифровать входящее сообщение. Комбинация открытого и закрытого ключа называется парой ключей, и это первая вещь, которую Вы сгенерируете, когда установите GPG на машине. Пара ключей защищена паролем, поэтому изменить её может только её владелец. Изменения могут потребоваться в случае изменения почтового адреса, поддерживаемого ключом, или для использования других функций.

Вам понадобится чей-то открытый ключ для шифрования отправляемых сообщений. Для этих целей существуют серверы (например, pgp.mit.edu), где Вы можете скачать ключ или ключи, связанные с определённым почтовым адресом, или загрузить свой собственный. Вполне возможно, что срок действия ключа подошёл к концу или был утерян пароль, поэтому всегда используйте последний ключ или (что даже лучше) попросите получателя отправить свои ключи и подтвердить отпечаток ключа (короткая версия контрольной суммы).

MIME

MIME (Multipurpose Internet Mail Extensions, многоцелевые расширения Интернет-почты**)** — это почтовое расширение протокола Simple Mail Transfer Protocol (SMTP). MIME даёт Вам возможность передавать различные виды содержимого и данных, таких как аудио, видео, изображения, архивы и приложения как вложения к письму. Заголовок MIME вставляется в начало письма, и получивший это письмо клиент использует эту информацию, чтобы определить, какая программа связана со вложенным файлом. Сам по себе MIME не предоставляет защищённость ни письму, ни вложениям.

S/MIME (Secure/Multipurpose Internet Mail Extensions) — это протокол, который добавляет цифровые подписи и шифрование к письмам с MIME вложениями. Используя цифровые подписи, S/MIME обеспечивает аутентификацию, целостность сообщения и не-отказ отправителя («не-отказ» означает, что Вы не можете отрицать того, что Вы его отправили). S/MIME обеспечивает приватность и безопасность данных (используя шифрование) в письмах, которые используют данный протокол.

S/MIME — это одновременно и инструмент обеспечения безопасности, и одна из проблем обеспечения безопасности, поскольку пользователи могут отправлять уязвимые данные как вложения в исходящих письмах во избежание обнаружения. Поэтому использование S/MIME в компании должно происходить под наблюдением на почтовых серверах.

Доверие ключам

Можете ли Вы быть уверены, что ключ для получателя письма действительно принадлежит этому получателю, а не загружен кем-то другим? Решение этой проблемы заключается в том, что ключи могут быть подписаны другими. Представьте, что у Вас уже есть ключ кого-то, кому Вы доверяете, и кто-то другой знает того, кому Вы хотите отправить письмо. Этот второй может подписать открытый ключ, что означает, что Вы вкладываете в ключ немного больше доверия, зная эту личность. Такая ситуация называется унаследованным доверием **(inherited trust)**. Вы можете найти другой способ войти в контакт с человеком и либо полностью получить его открытый ключ, либо получить «отпечаток ключа» — контрольную сумму ключа, которую можно быстро проверить. На сервере ключей ключ также может иметь ID — еще одна контрольная сумма, которая играет ту же роль.

Отправка зашифрованного письма с использованием **GPG**

Большинство почтовых клиентов поддерживают плагины, которые упрощают работу с ключами и шифрованием. Самый лучший вариант действий — проверить заранее, есть ли у получателя открытый ключ и получить его с сервера ключей или лично от получателя.

После этого создайте обычное письмо (в очередной раз мы настоятельно рекомендуем создавать простое текстовое сообщение и не использовать HTML), добавьте вложения и с помощью почтового клиента зашифруйте и отправьте письмо. Если Вы решили подписать письмо, тогда почтовый клиент сначала использует Ваш закрытый ключ для подписи письма, затем использует открытый ключ Вашего получателя для шифрования письма и его вложений. Если Вы защищаете пару ключей кодовой фразой (мы рекомендуем делать именно так), то Ваш почтовый клиент у Вас её спросит.

Получение зашифрованного письма с использованием **GPG**

Письмо, зашифрованное с помощью GPG, содержит либо вложение, помеченное флагом GPG, либо блок текста с заголовком, в котором почтовому клиенту, поддерживающему GPG, сообщается о получении зашифрованного письма. Этот клиент теперь получит доступ к Вашему закрытому ключу (возможно, по паролю) и расшифрует сообщение и его вложения. Если сообщение не было зашифровано Вашим открытым ключом, расшифровка просто не удастся. Если письмо было подписано отправителем, GPG-плагин будет использовать соответствующий открытый ключ и для подтверждения подписи.

GPG-плагины будут уведомлять Вас о проблемах с подписями или вложениями, но в общем, едва установив плагин, Вы поймёте, что использовать GPG достаточно просто.

Последствия использования **GPG**

Имейте в виду, что большинство электронных писем не шифруются. И, вероятно, Ваши письма тоже входят в это большинство. Некоторые люди думают, что использование шифрования является подозрительным, и оно само по себе привлекает внимание. Но это Ваше право сохранять приватность при общении, так что мнения других не должны Вас волновать.

GPG непросто использовать в почте с веб-интерфейсом (и это не считая ответ на очевидный вопрос: а есть ли гарантия того, что третья сторона осуществит шифрование правильно и не прибегнет к использованию атаки «человек-посередине») и на мобильных клиентах. Будьте осторожны с мобильными приложениями, которые утверждают, что решают эту проблему: было обнаружено, что некоторые из них отправляли данные куда-то в другое место для обработки!

Существуют почтовые онлайн-сервисы, продающие зашифрованные почтовые учётные записи «с улучшенной безопасностью». Но будьте внимательны, читая текст, напечатанный в пользовательском соглашении мелким шрифтом. Он может выглядеть так:

«Я понимаю, что этот сервис не предназначен для ведения незаконной деятельности и что провайдеры этого сервиса будут сотрудничать с органами власти для получения доказательств согласно действующему законодательству.»

Конечно, «законодательство» включает в себя такие программы, как Echelon, Carnivore, PRISM, Патриотический акт (США) и XKeyscore. Просмотрите их и задайтесь вопросом,

насколько «улучшена» та «безопасность», за которую Вы будете платить.

По законам некоторых государств Вы обязаны суметь расшифровать любую информацию по решению суда. Например, в Великобритании Вы можете подпасть под действие закона «О следственных органах» 2000 года; его несоблюдение рассматривается как неуважение к суду, которое автоматически приводит к тюремному заключению. Это имеет неприятные последствия: если Вы экспериментировали с шифрованием и забыли ключи или пароли, Вы будете посажены в тюрьму за свою забывчивость (да, Вы будете обвиняемым, пока не сможете доказать свою невиновность). Таким образом, лучше удалять любой зашифрованный материал и электронные письма, к которым Вы больше не имеете доступа. В корпоративной среде необходимо тщательно контролировать и документировать изменения ключа и кодовой фразы и удаление зашифрованной информации.

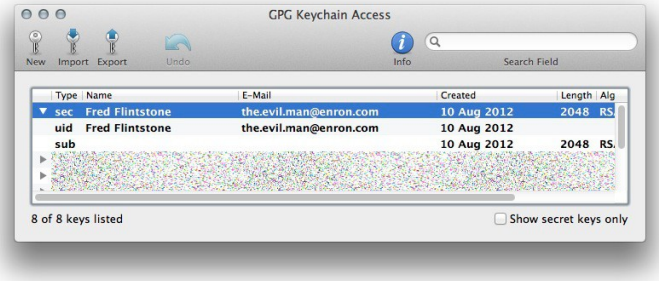

Рисунок **9.4:** Пара ключей GPG

Последним, но не менее важным является то, что использование адресов электронной почты для идентификации ключа является соглашением, а не установленным стандартом. Вполне возможно сгенерировать и использовать ключи для адресов электронной почты, которых не существует. Такие ключи все ещё принимаются на общедоступных серверах. Это называется «сокрытие у всех на виду» (hiding in plain sight): нет никакой связи между адресом электронной почты и ключом, используемым для шифрования/расшифрования трафика. Например, на изображении, представленном выше, и человек, и адрес электронной почты являются вымышленными.

Недостатком такого подхода является то, что он нарушает установленный способ работы, и плагины, такие как **Enigmail**, возможно, не сразу будут поддерживать такой творческий подход. Ещё одной областью для проведения исследований являются ключи с истёкшим сроком действия: окончание срока действия ключа не прекращает его функционирование.

Упражнения

9.8 Скачайте GPG-плагин для своего почтового клиента и установите его.

9.9 Узнайте, как сгенерировать собственный ключ. Сгенерированный ключ храните локально; отклоняйте любые предложения загрузить Ваш ключ на общедоступный сервер ключей.

9.10 Добавьте другие адреса к Вашему ключу, а затем измените кодовую фразу.

9.11 Теперь опубликуйте Ваш открытый ключ на сервере ключей.

9.12 Напишите кому-то письмо, используя GPG. Как бы Вы получили ключ адресата? Попробуйте его получить.

9.13 Что Вы можете сделать с сообщениями, когда у Вас есть только Ваш собственный ключ?

9.14 Создайте новый ключ для поддельного адреса электронной почты. Насколько легко это сделать на Вашем компьютере?

Уязвимости и угрозы электронной почты на стороне сервера

Все организации, от мала до велика, используют почтовые серверы для отправки и получения писем (только если они не передали эту задачу кому-то другому (outsource) или не используют облачные сервисы). Электронные письма предназначены для разных целей: некоторые из них хорошие, некоторые — нет. Почтовые серверы размещены на передовой линии атаки/защиты сетевого периметра.

Электронные письма используются для отправки фотографий с семейного отдыха, поздравительных открыток, домашних заданий, корпоративных сообщений, рассылки новостей и прочего контента. Электронная почта отлично подходит для ежедневного общения.

С другой стороны, электронная почта используется для отправки порно, пиратских MP3-записей, секретной информации, корпоративных секретов, угроз, вредоносного ПО, фишинга и спама. В 2012 году вложения в письма были отодвинуты на второй план по уровню угрозы; на первом месте оказались мошеннические веб-сайты — они стали основным инструментом для рассылки вредоносного ПО. Информация о жизненно важной части общественной жизни человека стала использоваться в преступных целях.

Потребление пропускной способности

Серверы электронной почты должны быть настроены так, чтобы блокировать плохие вещи, а хорошие — передавать Вам. Звучит достаточно просто, и нам будет легко Вам об этом рассказать. Но Вам предстоит много работы. Весь почтовый трафик, который проходит по сети, «съедает» часть пропускной способности. Вы никогда не услышите жалобу вроде «Мое соединение слишком быстрое». Чем раньше Вы сможете обнаружить и проинспектировать почтовый трафик (исходящий и особенно входящий) на сервере электронной почты, тем меньше пропускной способности Вы потратите. Кроме сохранения пропускной способности фильтрация нежелательных писем на ранней стадии облегчит работу ЦП сервера.

Некоторые исследования показывают, что 80% всей входящей почты является спамом. Вы действительно хотите ждать, пока этот хлам попадёт в Ваш почтовый ящик? Чем раньше спам будет перехвачен Вашими почтовыми серверами, тем лучше. Одна из техник, используемая при обнаружении спама, заключается в том, что сервер устраняет его после определенного количества времени. Это предотвращает удаление почтового трафика, который пользователь может ожидать. Отдел маркетинга Вашей организации, возможно, захочет получить письмо с темой «Как повысить производительность системы». Также отключите автоматические уведомления об электронной почте, чтобы сохранить пропускную способность. Поверьте нам, Ваши пользователи не будут возражать.

Поскольку Ваши почтовые серверы могут подвергнуться атакам из Интернета, Вы должны применить дополнительные меры предосторожности в отношении тех, у кого есть права администратора. Тот, кто имеет права администратора, никогда не должен отправлять или получать электронную почту тогда, когда он находится в системе с привилегиями администратора. На самом деле, права администратора следует использовать только для внутреннего обслуживания сети. На протяжении многих лет многие сети были взломаны

именно тогда, когда администратор вошёл в систему и просматривал веб-сайты, попутно отправляя электронную почту во время работы с повышенными привилегиями.

Уязвимости почтового сервера

Как видно из названия, почтовый сервер точно такой же сервер, как и многие другие. Сервер может иметь уязвимости, которые можно эксплуатировать. В базе данных Общих уязвимостей и перечислений (Common Vulnerabilities and Enumeration) по ссылке http://cve.mitre.org, перечислено в общей сложности 1043 уязвимости почтовых серверов по состоянию на 2012 год. Многие из них можно устранить, правильно настроив конфигурацию сервера и пользовательские привилегии. Другие проблемы решаются только устранением багов производителем ПО или бдительностью при покупке серверного программного обеспечения.

Полный список всех известных уязвимостей почтовых серверов можно просмотреть по ссылке http://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=email+server.

Угрозы почтовых серверов

Крупные почтовые веб-клиенты (к примеру, Gmail, Yahoo и Microsoft) мигрировали на новую криптографическую программу почтовой подписи, которая называется **DomainKeys Identified Mail (DKIM)**. DKIM «обёртывает» письмо криптографической подписью, которая подтверждает имя домена, через который было отправлено письмо. DKIM помогает фильтровать поддельные сообщения. Спецификацию DKIM можно найти на сайте http://www.dkim.org/.

Но существует проблема в использовании тестовых сообщений DKIM. В информационном сообщении, которое опубликовала **US-CERT (United States Computer Emergency Readiness Team,** Компьютерная команда экстренной готовности США**)** было указано, что злобный хакер при отправке письма может установить флаг, который означает, что он тестирует DKIM в сообщениях. Некоторые получатели будут «принимать сообщения DKIM в тестовом режиме, тогда сообщения должны рассматриваться, как если бы они не были подписаны DKIM».

Это не первая проблема DKIM, которая привлекла внимание CERN. Длина используемого для шифрования ключа подписи была уязвима ко взлому, когда размер ключа был слишком мал. Стандарты DKIM устанавливают минимальный размер ключа в 1024, при этом любая почта, которая использует меньший ключ, не принимается программой. Но на самом деле DKIM не отклоняла адреса с неподходящими ключами. Отправленные письма обрабатывались как обычные, при этом они были полностью уязвимы ко взлому. Как только ключ был взломан, хакер мог подменить электронную почту или отправить вредоносное ПО, используя ключ и адрес того пользователя.

DKIM предназначена для работы в качестве «доверительного» инструмента для проверки электронной почты. Система использует шифрование с открытым ключом, так же, как это делает PGP. При правильном использовании по электронному письму можно проследить его отправителя через процесс проверки домена. В принципе, Вы идентифицируете себя как отправитель по Вашему домену. Это должно существенно сократить количество поддельных писем и спама, а также упростить доказательство того, что конкретный пользователь отправил конкретное сообщение. Специалисты по безопасности называют это невозможностью отказа от авторства (non-repudiation).

При невозможности отказа от авторства данные об источнике информации не могут быть изменены. Информацию невозможно опровергнуть. Если Вы сказали: «Я хочу носить платье», то это заявление не может быть оспорено. Вы это сказали, это факт, и Вы не сможете отказаться от этого утверждения. Это важно, когда речь идёт о контрактах, о правовых вопросах и об оправданиях Вашему отцу, чтобы не выносить мусор.

Электронная почта для развлечений и выгоды

Благодаря выгодному рынку для корпоративного шпионажа, с помощью электронной почты можно легко найти списки контактов клиента, информацию о клиентах, протоколы встреч, информацию о новых разработках, ответы на следующий тест по математике и другие виды ценных данных. Мы даже не собираемся заниматься государственным шпионажем просто потому, что мы все знаем, что это имело место быть ещё на заре человечества. Есть несколько примитивных наскальных рисунков, изображающих то, как один пещерный человек следит за мамонтом другого пещерного человека. Можно только представить, как пещерный человек, возвращаясь к своему племени, описывает новейшую версию Мамонта 2.0.

Простым, но часто упускаемым из виду методом защиты электронной почты является проверка всех почтовых вложений. Сканирование должно быть применено ко всем пакетам данных, сжатым файлам, неизвестным типам файлов, мета-данным, файлам с URL и всему, что может быть результатом обработки файла. Это сканирование должно быть сосредоточено на входящем трафике, но также с подозрением относитесь к моментам, когда большие вложения отправляются из Вашей сети. Конфиденциальная информация компании должна быть зашифрована, особенно если она отправляется по электронной почте. И, кстати, действительно важная информация никогда не должна выходить за пределы сети. Если какой-то пользователь отправляет информацию за пределы сети, то Вам лучше проследить за его деятельностью.

Крупные организации (например, госпитали для ветеранов в США) для этих целей используют программное обеспечение для предотвращения потери данных **(data loss prevention, DLP)**. Никогда в шутку не отправляйте по электронной почте Ваши медицинские документы из таких госпиталей, иначе последствия будут серьёзными.

Ключ к успеху

Фильтрация по ключевым словам является одним из видов фильтрации на уровне приложений (7-й уровень OSI), который позволяет блокировать все сообщения, содержащие определённые ключевые слова или фразы (текстовые строки), которые обычно появляются в спаме. Другие формы фильтрации писем включают:

- Блокирование адреса: метод фильтрации, который блокирует письма, отправленные с определённых IP-адресов, адресов электронной почты или доменов известных спамеров.
- Байесовская фильтрация: «умное» программное обеспечение, которое может анализировать спам-сообщения и обучаться распознавать в других сообщениях спам, используя эвристики (модели поведения).
- Чёрные списки: списки адресов известных спамеров могут быть использованы совместно, так что нет необходимости, чтобы каждый пользователь составлял свой перечень с нуля. Такие списки можно получить у нескольких поставщиков. Они очень ценны для блокирования адресов.
- Белые списки: метод фильтрации, в котором вместо указания того, какие отправители должны быть заблокированы, определяются отправители, которые могут быть разрешены. Опять же, эти списки используются как часть блокирования адресов.
- Серые списки: в этом методе временно блокируются электронные письма из неизвестных источников. Приемлемое письмо будет повторно передано, а спам — нет.

- Фильтрация типа **«**Запрос/Ответ**»**: отвечает на электронные письма, полученные с тех адресов, которых нет в списке «надёжных отправителей», запросом, как правило, с задачей, которая проста в решении для человека, но сложная для автоматизированных ботов или скриптов.

Существует много приложений как бесплатных, так и платных, которые могут осуществлять эти виды фильтрации. Некоторые из них лучше, некоторые хуже. Но все они достаточно хорошо справляются со своими функциями.

Уязвимости и угрозы электронной почты на стороне клиента

Входящее письмо может содержать вредоносные программы, как правило, в виде вложения или веб-ссылки. Увидев подобное в Вашем сообщении, задумайтесь о возможных мошенниках.

- Непроверенный источник: кто отправил Вам это письмо и мог ли этот адресант отправить Вам письмо с подобным содержанием? Излюбленным приёмом спамеров является использование чужого действующего адреса электронной почты, таким образом спам не распознаётся фильтрами, и это увеличивает вероятность того, что пользователь откроет письмо.
- «Слишком хорошо, чтобы быть правдой»: неожиданное событие, например, выигрыш в лотерее, полученное наследство или банковская «ошибка» в Вашу пользу. Ещё бывают «нигерийские письма». Вы находили сходства во всех подобных сообщениях? Практически каждый из нас получал такие письма.
- Доменное несоответствие между адресом отправителя и адресом получателя ответа на отправленное сообщение.
- Странное, неправильное или слишком сложное использование языка.
- Необъяснимая или нелогичная неотложность. (Почему это письмо такое неотложное?)
- Встроенные веб-ссылки, которые ведут к доменам, отличным от читаемого имени домена (например, ссылка для перехода на веб-сайт www.bank.com в действительности ведёт на поддельный банковский веб-сайт www.l33thacker.org). Большинство почтовых клиентов теперь показывают реальный адрес веб-сайта при наведении курсора мыши на соответствующий текст.
- Вложения, содержащие активный контент (например, в формате .exe или .html). Это особенно рискованно на платформах, которые автоматически выполняют содержимое сообщения.

Упражнения

9.15 Перейдите по ссылке http://www.419eater.com/. Что такое приманки для жульничества (scam baiting)? Каким образом они работают? Какие существуют меры предосторожности? Это опасный материал. Знание о том, что такая техника существует, ещё не означает, что Вам следует это делать. Но, в любом случае, Вы не должны быть беззащитными.

Прольём свет

Содержимое электронной почты является прекрасным способом для распространения вредоносных ссылок. Одним из распространённых инструментов является **Blackhole Exploit**

Kit. Звучит страшно, не правда ли? Можете ли Вы произнести «Blackhole Exploit Kit» пять раз подряд очень быстро и без ошибок? Blackhole — это программа для эксплуатации веб-приложений, которая использует известные уязвимости в приложениях Java и Adobe. Она используется для отправки писем мошенников пользователю, чтобы последний перешёл по сомнительной веб-ссылке.

Фишинг является попыткой собрать важную информацию от жертвы с помощью социальной инженерии. Тысячам пользователей рассылаются убедительные письма. Типичные фишинговые письма приходят от хорошо известных и проверенных организаций. Мошенник использует логотип организации, похожий адрес электронной почты и профессиональную формулировку, таким образом обманывая большое количество людей. В письме содержится просьба к пользователю «проверить» или «обновить» данные кредитных карт, личную информацию о банковском счёте и другие вещи, которые Вы бы доверили только надёжному источнику.

Когда жертва нажимает на ссылку официального вида, ссылка отправляет её на фальшивую страницу, на которой происходит установка вредоносных программ на компьютер пользователя. Пользователь не знает, что его обманывают. К тому же не все антивирусные программы обнаруживают установку. После того, как программа установится на компьютере пользователя, мошенники смогут контролировать компьютер, а также любую информацию, которую они хотят извлечь из него.

Спам Blackhole «притворяется» письмом, отправленным из серьёзных компаний, таких как Amazon, Visa, Twitter, UPS и других организаций, которые не вызвали бы подозрений пользователя. Эта программа арендуется: плата осуществляется за серверное время на сервере Blackhole. Стоимость колеблется от $50 за день до $150 за месяц.

Вредоносные программы, трояны, руткиты

СМИ любят осветлять темы взлома электронной почты, потому что страх легко продаётся. (Помните, что тот, кто продаёт Вам что-то, пытается напугать Вас.) Но правда в том, что вредоносные программы существуют уже долгое время.

Доктор Фред Коэн написал кандидатскую диссертацию об идее компьютерного вируса в 1984 году, опубликовал её в 1985 году, и его работа была изъята из публичного доступа через несколько недель. 1985 год был давно, и средства массовой информации по-прежнему освещают события так, будто вредоносные программы — это новая огромная угроза для всего мира.

Мы не будем рассказывать Вам о всех существующих пересылаемых угрозах; Вы можете ознакомиться с ними самостоятельно в Уроке 6 «Вредоносные программы». Мы собираемся показать Вам, как работает защита электронной почты изнутри и снаружи.

Это сообщение выглядит как настоящее, давай откроем его

СТОП!!! Не открывайте это письмо пока что. Даже не просматривайте это сообщение. Существует несколько способов использования письма в качестве инструмента атаки. Социальная инженерия занимает первое место среди техник, применяющихся для того, чтобы заставить людей открыть электронное письмо, открыть вложения или нажать на вредоносные веб-ссылки в письме или сообщении. Социальная инженерия ориентирована на некоторые человеческие эмоции, включая любопытство, желание помочь, доверие к нашим друзьям, жадность и многие виды финансовых или медицинских опасений. В Уроке 20 Вы узнаете больше подробностей о социальной инженерии.

Наше любопытство к новой или неизвестной информации можно использовать, чтобы убедить нас совершить глупые поступки. Когда Вы получили электронное письмо, которое

содержит заголовок «Тема: Re: Re: Спасибо», Вы, как обычный пользователь, захотите узнать, почему кто-то поблагодарил Вас. В этом случае Вас заранее поблагодарили за возможность осуществления вредоносных действий на Вашем компьютере.

В таких типах электронных писем Вы можете встретить просьбу позвонить по телефонному номеру, нажать на ссылку в сообщении или сделать что-то, что может выдать все Ваши секреты.

Упражнения

Рассмотрим сообщение с таким заголовком:

От: Mr Norman Chan <naveen.kumar@iitg.ac.in>

Ответить: 2259575299@qq.com

Кому: (Ваш адрес электронной почты)

Дата: Mon, Nov 19, 2012 at 7:40 AM

Прислано: iitg.ac.in

9.16 Ответили бы Вы на электронное письмо, которое содержит в строке темы следующий текст: «Здравствуйте, я Норман Чан, у меня есть бизнес, который стоит 47.1 миллионов долларов, Вы будете со мной работать?» Адрес отправителя — «naveen.kumar@iitg.ac.in».

9.17 Исследуйте этот адрес электронной почты, чтобы убедиться в достоверности информации. Также проверьте адрес для ответа, «2259575299@qq.com». НЕ ПЕРЕХОДИТЕ НА QQ.COM.

9.18 Максимально усильте настройки безопасности вашего браузера перед выполнением этого задания. Сделайте небольшое исследование ресурса qq.com, но не переходите по этому адресу. НЕ ОТКРЫВАЙТЕ ЭТОТ URL. Основываясь на своём исследовании qq.com, сделайте выводы, является ли этот сайт для Вас вредоносным?

Захватывающие трюки с системами электронной почты (взлом почтальона)

Электронная почта, кажется, всегда играет определённую роль, когда дело доходит до нарушения безопасности или серьёзной атаки на сеть. Каждый вирус, каждый бит вредоносных программ, каждое фишинговое сообщение, кажется, использует электронные письма либо как основной транспортный механизм, либо как способ проникнуть в систему, чтобы начать атаку. Электронные сообщения могут быть не столь популярны, как другие формы связи (как, например, SMS или мгновенные сообщения), но это то, что наиболее обширно используется в корпоративном и правительственном мире. Сейчас мы внимательно рассмотрим саму идею электронной почты и то, как она может быть использована в качестве оружия или защиты.

Подключаясь к сети, мы должны знать несколько точек входа. Если мы полагаемся только на одну точку входа, то что мы будем делать, если используемая уязвимость будет исправлена? Несколько точек входа в сеть дают нам больше свободы для перемещения по этой сети и больше путей подхода. Пути подхода очень важны, поверьте нам на слово.

Знание схемы, по которой пользователям составляют имена, используемые организацией для электронной почты или доступа к сети, даёт нам большое преимущество. Зная имя

пользователя, мы можем сосредоточиться на получении пароля этого пользователя. Большинство организаций (но не все) используют схему «имя.фамилия@названиекомпании.com». Некоторые используют сочетание первого инициала и фамилия@названиекомпании.com. Другие используют сочетание фамилии и первого инициала с последующим @названиекомпании.com. Довольно опрометчиво, не правда ли? Также не стОит делать адрес электронной почты логином пользователя. Это очень распространённая ошибка.

У организаций в их сети есть каталог, который позволяет пользователям узнать, кто есть кто, где они работают и что они делают. Этот внутренний каталог является золотым прииском информации для злоумышленника. Вы можете просмотреть профили в Facebook или других социальных сетях, чтобы узнать больше о каждом пользователе. Вы можете узнать, когда они собираются в отпуск, чем они занимаются, какое у них хобби и другие зацепки к типам паролей, которые они могли бы использовать. Эта информация также окажется полезной, если Вы захотите использовать социальную инженерию против этих людей (для развлечения или выгоды).

Кто ищет, тот всегда найдёт

Давайте рассмотрим вопрос сбора адресов электронной почты и использование электронной почты в качестве инструмента взлома. Взлом электронной почты тесно связан с социальной инженерией (сообщаем ещё раз на всякий случай). **The Social Engineering Automation Kit (SEAK)** на http://www.seak.com.ar/ предназначен для того, чтобы использовать поисковые системы для нахождения адресов электронной почты в сети или на веб-сайте. SEAK представляет собой набор скриптов на языке Perl, которые позволяют поисковым системам проводить поиск в глубинах веб-страниц и сетей, а затем отобразить все адреса электронной почты, которые они находят. SEAK также может быть использован для поиска людей.

Также есть программа, аналогичная SEAK. Она называется **Esearchy**. Её можно скачать по ссылке https://github.com/FreedomCoder/ESearchy-ng. Esearchy делает то же, что SEAK, но делает это в среде Windows; эта программа также ищет документы. Esearchy ищет пароли, скрытые в метаданных, а также любую другую полезную информацию, например, адреса электронной почты, которые доступны для общественности.

Ещё одна утилита, **Maltego**, — это программа с открытым исходным кодом, которая может использоваться как анализатор в судебной экспертизе. Maltego предоставляет утилиты для обнаружения данных из открытых источников и показывает информацию в виде графа, что удобно для анализа ссылок и интеллектуального анализа данных. В целом с помощью Maltego можно анализировать реальные отношения между людьми и группами, веб-сайты, домены, сети и онлайн-сервисы (например, Ваши любимые социальные сети).

Ещё можно воспользоваться поиском в Google. Если Вы хотите увидеть всю информацию о профиле сотрудника, Вы можете использовать эту команду:

```
site:www.google.com intitle:"Google Profile" "Companies I've worked for"
"at company_name"
```

Если Вы хотите найти все адреса электронной почты в домене или URL, то Вы можете использовать Esearchy. Введите следующую команду одной строкой, заменив «company» на реальный домен.

```
esearchy -q"@company" -y
AwgiZ8rV34Ejo9hDAsmE925sNwU0iwXoFxBSEky8wu1viJqXjwyPP7No9DYdCaUW28y0.i8p
yTh4 -b 220E2E31383CA320FF7E022ABBB8B9959F3C0CFE --enable-bing --enable-
google --enable-yahoo --enable-pgp -m 500
```

Gpscan — это приложение, написанное на Ruby, которое может автоматизировать этот поиск и получить ещё больше результатов. В сочетании с командой, представленной выше, Gpscan становится мощным инструментом для разведки и социальной инженерии. Вы можете найти Gpscan по ссылке http://www.digininja.org/projects/gpscan.php.

Перед использованием любой из этих программ уделите время на то, чтобы разобраться, как они работают. Обратите особое внимание на синтаксис каждой утилиты и на то, что делает каждая из команд. Вы можете узнать довольно много о том, как поисковые системы могут быть использованы для охоты на адреса электронной почты, для их возврата и, возможно, нахождения некоторых паролей. Также выясните, какие поисковые механизмы используются для работы этих программ.

Упражнения

9.19 Теперь пришло время самостоятельно исследовать средства безопасности. Найдите **FOCA** (программа для работы с метаданными). Что она делает? Хотели бы Вы добавить её в свою коллекцию программ для этичного хакинга?

Спуфинг **vs.** вредоносные программы

В 2007 году генеральный директор компании Fortune 500 получил письмо от одного из старших сотрудников. В письме в поле **«От»:** было видно, что письмо отправлено по внутренней сети компании. В поле **«Тема»:** был текст «Как сократить расходы на электроэнергию». Когда генеральный директор открыл это электронное сообщение, он увидел в нём вложение и ссылку, которая также, казалось, была подлинной. Директор открыл вложение, но ничего не увидел на своём экране и закрыл письмо.

Несколько месяцев спустя ФБР сообщило генеральному директору, что из-за заражения вредоносными программами его персонального компьютера из его компании было украдено несколько терабайт данных. ФБР подтвердило, что именно то письмо с темой «Как сократить расходы на электроэнергию» содержало вредоносное вложение. Это сообщение было подделано.

Подобные ситуации происходят каждый день. Ваш дядя звонит Вам и спрашивает, почему Вы отправляете ему так много объявлений по электронной почте. В школе Ваш приятель получает от Вас бесполезную рекламу. Почему Вы отправляете все эти спам-сообщения?!

Но ведь Вы этого не делали.

Либо Ваш адрес электронной почты подделали, либо Ваш почтовый клиент взломали. Чтобы узнать, был ли подделан адрес электронной почты, Вам нужно будет посмотреть на заголовок отправленного сообщения. Мы узнали, как это сделать, ранее в этом уроке. Теперь используйте свои знания на практике.

Попросите любого, кто получил от Вас письмо, переслать его Вам обратно полностью (а не только текст сообщения). Заголовок покажет, был ли подменён Ваш адрес электронной почты. Посмотрите на поля Ответить и Отправлено в электронном письме. Как мы уже видели в предыдущих упражнениях, заголовок покажет, было ли это письмо отправлено Вами или кем-то другим.

Забавные трюки с электронной почтой

Когда дело доходит до личной жизни, веб-почта заботится о приватности в последнюю очередь. Веб-сервису может быть отправлен запрос на предоставление всех Ваших сообщений, контактов, записей в календаре и других данных на основании юридических документов, позволяющих получить эти данные. Один старый, но все ещё полезный трюк

заключается в создании учётной записи электронной почты под другим, не своим именем. Те, кому Вы хотите отправлять секретные сообщения, должны иметь доступ к Вашему почтовому аккаунту. Вы создаёте электронное письмо и сохраняете его как черновик. Вы никогда не отправляете сообщение, а просто создаете черновик с некоторым содержимым. Письмо остаётся на Вашем аккаунте, но его нельзя отследить, так как оно никогда не отправлялось. «Получатель» заходит на этот же аккаунт и читает черновик сообщения. После прочтения черновик может быть удалён или изменён — так создаётся новое сообщение для Вас. Это как пинг-понг без мяча. Кстати, так же можно работать и с общим Google-документом.

ПРИМЕЧАНИЕ: Вы не сможете стать директором Центрального разведывательного управления Соединенных Штатов Америки, не зная эту маленькую хитрость.

Метаданные электронной почты описаны в RFC 2822. Кто-то посчитал хорошей идеей включение метаданных в электронное сообщение! О чём они только думали? Метаданные электронной почты могут содержать следующую информацию:

- To (Кому)
- From (От кого)
- CC (копия)
- BCC (скрытая копия)
- Date (Дата)
- Subject (Тема)
- Sender (Отправитель)
- Received (Получено)
- Message-ID (ID сообщения)
- References (Ссылки)
- Recent (Недавнее)
- Return-Path (Путь возврата)
- Time/Date (Время/дата)
- Encrypted (Зашифрованный)
- In-Reply-To (В ответ на)

Не слишком беспокойтесь по поводу метаданных электронной почты, описанных в RFC 2822. Дело в том, что этот RFC охватывает только электронный текстовый трафик. Ваши SMS-сообщения, все Ваши мгновенные сообщения и фотографии, которыми Вы хотели поделиться, предполагают вторжение в Вашу личную жизнь. Тем не менее, эта скрытая информация рассматривается в рамках другого RFC.

Как перехитрить почтовых ботов (обфускация электронной почты)

Это так просто, что Вы будете смеяться над собой, что не знали об этом раньше.

Если Вам нужно отправить кому-либо свой адрес электронной почты, Вы отправите его в виде обычного текста? В таком случае Вы раскрываете свой адрес для спам-ботов. Эти спам-боты — порочные создания, которые перемещаются по Интернету и ищут адреса электронной почты.

Это как подключение нового компьютера к Интернету без включения каких-либо функций безопасности: электронный адрес, отправленный в виде простого текста, просто напрашивается на неприятности. В общем, это очень плохая идея.

Чтобы перехитрить спам-ботов, Вы можете попробовать изменить свой адрес электронной почты при его отправлении. Нужно найти компромисс между простотой использования и безопасностью. Есть несколько методов, просто используйте своё воображение.

`somebodyatsome.whereelse`

`Somebody@somedotwhereelse`

`somebody2some.whereelse`

Такие комбинации успешно используются для передачи адресов электронной почты, минуя спам-ботов. Но, возможно, вскоре они смогут распознавать такие хитрости.

Упражнения

9.20 Перейдите по ссылке для просмотра программы Etherios EasyDescribe: http://appexchange.salesforce.com/listingDetail?listingId=a0N300000018leZEAQ

Это бесплатная программа для просмотра и извлечения метаданных. Проанализируйте несколько электронных писем с помощью Etherios. Какие метаданные есть в этих письмах, но при этом отсутствуют в заголовке?

9.21 Если некоторые данные находятся не в заголовке, то в какой части электронного письма они могут быть скрыты?

9.22 Требует ли RFC 2822, чтобы метаданные были встроены в электронное сообщение или это просто стандартизированный метод для трафика электронной почты?

9.23 Пользуясь любыми средствами, попытайтесь найти правильный рабочий адрес электронной почты руководителей трёх компаний, перечисленных ниже. Подсказка: сначала выясните, кто они такие.

Coca Cola

Kia

British Aerospace Engineering (BAE)

Выводы

Теперь, когда Вы вполне разобрались (или совсем запутались) в вопросах, относящихся к работе с электронной почтой, Вы можете согласиться с тем, что этот простой инструмент коммуникации не так уж прост. Работа электронной почты в различных системах может быть достаточно сложной и требует соответствия определённым критериям. Вспомните, как в начале урока Вы почувствовали себя в роли электронного письма, как Вас отправляли, какой путь Вы проделали и как, в конце концов, оказались в месте назначения. Кстати, Вы хорошо справились с этой задачей.

Помните о важности соблюдения этикета при использовании электронной почты, поскольку отправка письма, написанного в плохом настроении, может в дальнейшем создать для Вас нежелательные проблемы. При ответе на письмо, не отправляйте всем подряд адреса,

указанные в поле «Копия». Если Вы собираетесь отвечать большому количеству людей, используйте BCC для сохранения конфиденциальности почтовых адресов других пользователей.

Продолжая тему неприкосновенности частной жизни, мы обсудили использование таких программ для шифрования, как PGP и GPG, предназначенных для безопасной отправки и получения электронных писем. Самая интересная часть этого раздела была посвящена созданию и использованию ключа. Это было не очень сложно, не правда ли? Если Вам так не показалось, жаль. Мы уверены, что в местном ресторане быстрого питания по-прежнему есть вакансии, так как безопасность — это не Ваше призвание. Мы надеемся, что Вы справились с тем заданием, потому что нам нужно как можно больше специалистов по безопасности.

В следующем разделе мы приступили к более сложным вопросам безопасности. Хорошо, возможно, они не такие уж и сложные, но мы думаем, что Вам пригодятся эти знания. Признайтесь, что разбираться с уязвимостями и угрозами на стороне почтового сервера и на стороне клиента было очень занимательно. Нам было весело писать о них. Вы должны следить за спамом. Большое количество спама съедает ценную пропускную способность, так что Вы должны фильтровать его на ранних этапах. Только не путайте почтовый спам с торговой маркой Spam.

Dig является важной утилитой для работы с электронной почтой для пользователей Linux и Unix; с её помощью можно отслеживать нужную информацию. Если Вы видите, что из Вашей сети по электронной почте во вложениях передаются большие объёмы данных, то проверьте, не содержатся ли в этих письмах секреты компании. Мы обсуждали один интересный момент, касающийся использования сервера Blackhole для эксплуатации уязвимости в сетях. Эта техника широко применялась для отправки вредоносного ПО по электронной почте, если было известно, что кто-то, скорее всего, откроет это сообщение или кликнет по зараженной ссылке в этом электронном документе. Этот вид угрозы может быть предотвращён путём фильтрации почтового трафика и обучения пользователей по этому вопросу. Обучение пользователей является ключевым элементом в обеспечении безопасности.

В заключение мы дадим Вам несколько советов, которые, возможно, Вас заинтересуют. Просто знайте, что безопасность электронной почты является вызовом для кибербезопасности. Ваш взгляд на этот факт зависит от того, на какой стороне Вы находитесь.

Полное освобождение от ответственности

Питер Хоперман, автор *The Evil Guide to Privacy*, пишет:

Вы когда-нибудь хотели подчеркнуть глупость отказа от ответственности, который используется в электронных письмах? Это сделал Питер Хоперман, собрав подборку очень старых сообщений USENET с некоторыми собственными дополнениями. Важной частью становления успешного хакера является чувство юмора: оно не только делает Вас непредсказуемым, но также помогает не унывать после неудачных экспериментов. Смейтесь над своими неудачами, переведите дыхание и продолжайте борьбу. Компьютеры не могут выиграть, Вы можете просто выключить их.

Точка зрения, выраженная здесь, является мнением автора, она может не совпадать с точкой зрения его работодателя или кого-то ещё.

Информация и любые вложения, содержащиеся в этом электронном сообщении, являются бессмысленными и вряд ли политкорректными. Я искренне верю, что совершенно бессмысленно объяснять Вам, что делать с этим сообщением, если я отправил его не туда. Это сообщение не содержит изображений обнажённого тела (пока), и никакие милые животные или киты не пострадали во время его написания, поскольку их не было в наличии. Это письмо, выполненное в истинном консалтинговом стиле, составлено из шаблонов и копипаста из многих других электронных сообщений, ориентированных на другие группы пользователей. Это письмо может навредить пищеварительной системе при проглатывании (особенно при печати на картоне). Автор может подать в суд, содержание можно урегулировать. Не подходит для людей в возрасте до 18 и тем, у кого отсутствует чувство юмора. Не держите вверх ногами, откройте с другого конца. Если Вы получили это письмо по ошибке, Вы молодцы.

Не следует доверять или надеяться на любые вложения, но они могут оказаться очень интересными.

Этот отказ от ответственности предназначен исключительно для образовательных целей. Не отправляйте сейчас деньги. Проконсультируйтесь с Вашим врачом или фармацевтом. Для предотвращения поражения электрическим током не открывайте заднюю панель. Внутри нет частей, обслуживаемых пользователем. Вы можете иметь или можете не иметь дополнительные права, которые могут различаться в зависимости от страны. Не рекомендуется для детей до двенадцати лет. Батарейки в комплект не входят. Ограничение: один экземпляр в одни руки. Любое сходство с реальными лицами, живыми или мёртвыми, является чисто случайным. Хранить вдали от открытого пламени или искры. Недействительно там, где запрещено. Требует сборки. Все права защищены. Храните чеки отдельно по номеру банка. Содержимое может осесть во время транспортировки. Используйте только по назначению. Рекомендуется родительский присмотр. Не предоставляются никакие другие гарантии, явно выраженные или подразумеваемые. Несанкционированное копирование этой подписи строго запрещено. Не читайте во время управления транспортным средством или перевозки тяжёлого оборудования. Посылка будет оплачена за счёт получателя. В случае попадания в глаза промойте водой. Должно быть заверено. Это не является предложением о продаже ценных бумаг. Наносить только на поражённый участок. Может быть слишком впечатляющим для некоторых зрителей. Не сгибать, не скручивать, не ломать. Использовать только для оздоровления. Требуется дополнительная погрузка и разгрузка. Ни одно животное не пострадало в производстве этой подписи. Не беспокоить. Все модели старше 18 лет. Если состояние не улучшается, обратитесь к врачу. Самая свежая, если пить до даты истечения срока на упаковке. Цены могут быть

изменены без предварительного уведомления. Приблизительное время. Доставка не обязательна, если посылка из Сингапура. При проглатывании не вызывайте рвоту. Разрыв печати подразумевает принятие соглашения. Только для использования в условиях бездорожья. Как можно увидеть на ТВ. Мы оставляем за собой право ограничивать количество. Один размер подходит всем. Не оставляйте средства без присмотра. Многие чемоданы выглядят так же. Содержит значительное количество неактивных ингредиентов. Цвета могут со временем выгорать. Мы отправили товар, подходящий именно Вам. Скользкий во влажном состоянии. Гарантия предоставляется только первоначальному розничному покупателю или получателю подарка. Только для использования в офисе. Вес нетто перед приготовлением. Не связаны с Красным Крестом. Поверхность должна быть очищена от краски, жира, грязи и т. п. Опустить в любой почтовый ящик. Редактировано для телевидения. Хранить в прохладном месте; обрабатывать быстро. Посылка не будет доставлена без оплаты. Репродукция. Список действителен на момент печати. Только для личного использования. Вернуть отправителю, нет пункта назначения, невозможно отправить. Не подвергать воздействию прямых солнечных лучей. Не несёт ответственности за прямые, непрямые, побочные или косвенные убытки, связанные с любым дефектом, ошибкой или неисполнением. Не принимаем канадские монеты. Не прокалывать и не сжигать пустой контейнер. Смотрите инструкцию на этикетке. Цены могут быть изменены без предварительного уведомления. Не пишите ниже этой линии. Сейф с замком с часовым механизмом, работник не может открыть. Только в задействованных участках. Серийные номера должны быть видны. Аккуратно сложите части, затем свяжите. Зона обвала. Хранить в недоступном для детей месте. Чек является Вашей квитанцией. Проверьте подачу бумаги. Поставьте штамп здесь. Избегать контакта с кожей. Проведена санитарная обработка. Подписать без признания вины. Не входить агентам по распространению заказов. Чуть выше на запад от Миссисипи. Температура хранения: от *-30°C (-22 F)* до *40°C (104 F)*. Сотрудники и члены их семей не могут участвовать. Остерегайтесь собаки. Конкурсанты были проинструктированы перед шоу. Нет необходимости в покупке. Ограниченное предложение, звоните сейчас, чтобы обеспечить быструю доставку. Вы должны присутствовать, чтобы выиграть. Погасить все сигнальные огни. Обработано в месте, указанном на штампе на коробке. Используйте только в хорошо проветриваемых помещениях. Заменить аналогичным экземпляром. Аксессуары продаются отдельно. Палатки для двоих или более. Хранить вдали от открытого пламени. Некоторое показанное оснащение не является обязательным Цена не включает налоги. Зона повышенной опасности. Предзапись выпуска шоу для этой временной зоны. Копирование строго запрещено. Только лицам, достигшим *18* лет. Открепить и сохранить для справки. Запрещён вход с алкоголем, собаками или лошадьми. Это демо-версия, не для продажи. Выберите по крайней мере две альтернативные даты. Позвоните по бесплатному телефону, прежде чем решить. Водитель не носит с собой наличные. Некоторые из товарных знаков, указанных в данном продукте, появляются только в целях идентификации. Удаление тега наказуемо законом.

Если Вы всё это прочитали, то Вы чрезвычайно любопытный человек. Или юрист.

open to them and they don't have the knowledge to defend themselves against the fraud, identity theft, privacy leaks and other attacks made against them just for using the Internet. This is the reason for Hacker Highschool.

The Hacker Highschool project is the development of security and privacy awareness learning materials for junior high and high school students.

Hacker Highschool is a set of lessons and a practical means of making hackers. Beyond just providing cybersecurity awareness and critical Internet skills, we need to teach the young people of today how to be resourceful, creative, and logical, traits synonymous with hackers. The program contains free security and privacy awareness teaching materials and back-end support for teachers of accredited junior high, high schools, and home schooling. There are multiple workbooks available in multiple languages. These are lessons that challenge teens to be as resourceful as hackers, including safe Internet use, web privacy, researching on the internet, avoiding viruses and Trojans, legalities and ethics, and more.

The HHS program is developed by ISECOM, a non-profit, open-source research group focused on security awareness and professional security development and accreditation.