Hacker Highschool

SECURITY AWARENESS FOR TEENS



УРОК 9:
ЗЛОМ ЕЛЕКТРОННОЇ ПОШТИ

Hacker Highschool
SECURITY AWARENESS FOR TEENS

ISECOM

WWW.ISECOM.ORG - WWW.OSSTMM.ORG - WWW.HACKERHIGHSCHOOL.ORG - WWW.BADPEOPLEPROJECT.ORG - WWW.OSSTMMTRAINING.ORG

УВАГА

Проект Hacker Highschool є засобом навчання і, як в будь-якому навчальному засобі, існує небезпека. Деякі уроки, якщо ними зловживати, можуть призвести до фізичної травми. Також додаткові небезпеки можуть бути там, де ще недостатньо досліджень про можливі наслідки випромінювань від специфічної техніки. Студенти, які використовують ці уроки, повинні перебувати під контролем викладача і, в той же час, заохочуватися на вивчення, практику і заняття. ISECOM не несе відповідальності за застосування інформації, отриманої з даних матеріалів, і за подальші наслідки.

Наступні уроки та книги є відкритими і загальнодоступними на наступних умовах ISECOM:

Всі роботи проекту Hacker Highschool призначені для некомерційного використання з учнями початкової школи, слухачами юнацьких курсів Highschool і студентами вищих навчальних закладів, приватних організацій або частково для домашнього навчання. Ці матеріали в будь-якій формі не можуть бути використані для продажу. Надання цих матеріалів будь-якому класу, навчальній організації або табору, в яких стягується плата, категорично заборонено без ліцензії, в тому числі на уроки в коледжі, університеті, професійно-технічних заняттях, літніх або комп'ютерних таборах тощо. Для придбання ліцензії відвідайте розділ сайту призначений для Ліцензування: http://www.hackerhighschool.org/licensing.html.

Проект HHS є результатом праці відкритого співтовариства і, якщо Ви знаходите наші труди цінними і корисними, ми просимо Вас підтримати нас шляхом придбання ліцензії, пожертвувань або спонсорства.

Table of Contents

Співробітники журналу

Pete Herzog, ISECOM

Glenn Norman, ISECOM

Bob Monroe, ISECOM

Greg Playle, ISECOM

Marco Ivaldi, ISECOM

Simone Onofri, ISECOM

Peter Houppermans

Andrea Zwirner

Перекладачі

Vadim Chakryan, Kharkiv National University of Radio Electronics

Olena Boiko, Kharkiv National University of Radio Electronics

ISECOM

Вступ

Електронна пошта відома вже давно; вона з'явилася раніше ніж Інтернет. Це одна з перших форм обміну електронною інформацією. До появи електронних листів були сигнальні ракети, напівоголені хлопці, які виконували роль посланців, цеглини з прикріпленими повідомленнями, азбука Морзе, велике каміння, перекинуте через стіни замку з написаними на них лайками та безліч інших подібних засобів зв'язку (наприклад, телефон або паперова «равликова пошта» (насправді, її доставляють не равлики — це звичайні листи, відправлені через поштове відділення)). Для багатьох з цих оригінальних способів передачі повідомлення потрібні були спеціальні пристосування, особливі навички та багато каміння. На щастя, заповзятливі автори придумали текст, який можна було написати на кам'яних табличках або в книгах та кинути людям або просто дати їм його прочитати. Однією з перших була книга *Сигнальні ракети для чайників*.

Робота електронної пошти ґрунтується на простих принципах передачі даних з проміжним зберіганням (store and forward). Використання електронної пошти виявляється досить простим (якщо тільки Ви не дуже поспішаєте), дуже надійним і настільки дешевим, що нею часто зловживають у комерційних та злочинних цілях. Асинхронна схема, що лежить в основі роботи електронної пошти, дозволяє здійснювати спілкування без необхідності того, щоб і відправник, і отримувач були одночасно в мережі. Це можна порівняти з тим, як Ваша мама розмовляє з Вами, а Ви не звертаєте уваги до тих пір, доки вона на задасть Вам питання. Під час передачі повідомлення Ви «відсутні», але Ви повинні бути хорошим ігнорувальником. Емм... приймальником. Так, хорошим приймальником.

У цьому уроці ми розглянемо роботу сучасної електронної пошти, а також питання хакінгу та безпеки. Отримані знання Ви зможете використовувати для розваги або для власної вигоди.

Взагалі та в цілому: як працює електронна пошта

Для початку уявіть, що Ви — електронний лист. Давайте простежимо за тим, як Ви передаєтесь і отримуєтесь, та визначимо різні складові компоненти, за рахунок яких Ви переміщуєтесь.

1. Email (Ви) створюється (створюєтеся) або за допомогою **клієнта** email (наприклад, Outlook, Mail, Eudora, Pegasus або Thunderbird), або на веб-сервісі (наприклад, Yahoo Mail) через веб-інтерфейс. Кумедно, наскільки сильно електронний лист нагадує звичайний лист (який передається «равликовою поштою») — він також вкладається у конверт, як на Рисунку 9.1.

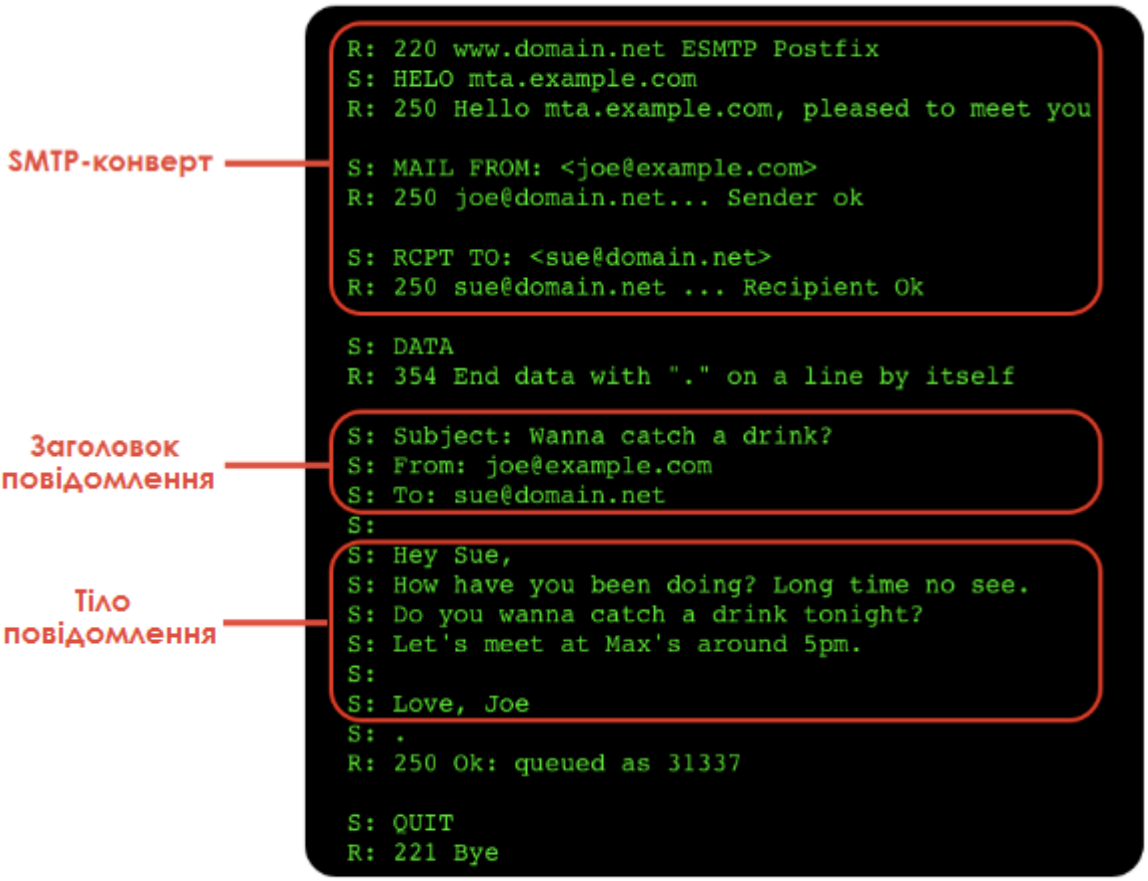

Рисунок 9.1: Повідомлення, заголовки і конверт електронного листа

2. Ви відправляєтеся на поштовий сервер, який називається **агентом пересилання повідомлень (Mail Transmission Agent, MTA)**; він ставить Вас у чергу для пересилання. Сучасні поштові системи зазвичай використовують для цього зашифрований **SMTP (Simple Mail Transport Protocol, простий протокол передачі пошти)**, оскільки вони ставлять вимогу автентифікуватися для запобігання порушень використання, а шифрування захищає відомості про користувачів та вміст листа від розкриття. MTA, які приймають електронний лист (Вас) без будь-якої аутентифікації, називаються «відкритими серверами ретрансляції» (“open relays”); їх, як правило, засмічують відправники поштового сміття, також відомого як UCE

(Unsolicited Commercial Email, небажана комерційна електронна пошта) або **спам**.

3. Для кожної адреси («отримувача») у повідомленні MTA спочатку перевіряє, чи є отримувач локальним (тобто чи знаходиться він на тому ж комп'ютері). Якщо ні, то MTA використає так званий запис MX (який розглядається далі в уроці) для знаходження сервера для відповідного домену. Якщо відповідний валідний хост не був знайдений, то відправник отримує повідомлення про помилку передачі на цю конкретну адресу.

4. MTA пробує доставити Вас за кожною з адрес. Якщо з якихось причин це не вдалося, MTA знову ставить повідомлення у чергу для повторного відправлення через деякий час до тих пір, доки не сплине час очікування і не буде відправлене повідомлення про перебої доставки (зазвичай протягом 48 годин). Так що Вам доведеться чекати близько двох днів. Ця доставка від початку може бути навмисно відкладеною приймаючим MTA — так працює один з методів захисту від спаму: спамерське програмне забезпечення зазвичай не настільки розумне і воно не буде вишиковувати чергу та повторно доставляти повідомлення (такий спосіб називається **сірими списками (greylisting)**). Стандартно ця доставка здійснюється через **незашифрований** SMTP. Зашифроване з'єднання — це скоріше виключення, а не правило.

5. Іноді ретранслятори «підбирають» Вас і направляють до кінцевого пункту призначення. Таке трапляється в системах з фільтрацією спаму та вірусів і там, де безпека потребує використання багаторівневої моделі (наприклад, в мережі підприємства або урядового закладу).

Ви звернули увагу на згадування **багаторівневої моделі механізму захисту (layered security model)**? Спеціалісти в області безпеки, які готові працювати у тяжкому режимі, не можуть створити цукерки M&Ms: тверді зовні, але м'які усередині. Вони додають декілька шарів захисту: регулятори маршрутизаторів і брандмауери, системи виявлення вторгнень (intrusion detection systems, IDS), системи захисту від вірусів, шкідливого ПЗ, спаму та велику кількість інших засобів.

Схоже, що спроба зламування приречена на провал. Але ніколи не забувайте про наступне: кожна встановлена програма додає більше коду з можливими уразливостями; те ж стосується і апаратного забезпечення. Наприклад, якийсь крутий прилад для VPN може як забезпечити Вам «безпечну» мережу VPN, так і надати лазівки для зловмисників. Все залежить від того, чи належите Ви до Червоної команди («супротивникам») або до Синьої.

6. Приймаючий MTA відновлює адресу, якщо вона представлена у вигляді аліасу або списку розсилки. Вони не обов'язково повинні бути в одному домені: аліас може перетворюватися у зовсім іншу адресу на іншому сервері. Після отримання повної адреси Ви знову стаєте в чергу для подальшого відправлення.

7. Якщо адреса email відноситься до локальної поштової скриньки, то Вас направляють до цієї поштової скриньки (якщо тільки об'єм листів, які в ньому

зберігаються, не перевищив допустимої межі). Ви можете виявитися занадто великим. Ви повинні перестати їсти стільки низькоякісної їжі.

8. Далі за протоколом POP3 або IMAP Вас підбирає клієнтська програма електронної пошти. Зазвичай з'єднання захищене (за допомогою SSL) для запобігання витоку облікових даних користувачів; використовуються протоколи POP3S та SSL IMAP. POP3 здійснює процес «підбору»: він скачує повідомлення, а потім видаляє їх з сервера (можливі налаштування проведення цих дій на певну дату/час). За протоколом IMAP здійснюється синхронізувальний процес: поштова скринька на стороні клієнта повинна бути ідентичною скриньці на обліковому запису на сервері (для мобільного пристрою ця процедура зазвичай проводиться для певного проміжку часу для збереження пам'яті пристрою); тому IMAP ідеально підходить для використання електронної пошти одночасно на декількох пристроях.

9. Нарешті, більшість клієнтських програм електронної пошти зараз мають вбудовану систему визначення спаму; зазвичай ці системи ґрунтуються на Байєсівських принципах класифікації. Спробуйте відправити своєму другу листа, записавши в полі «Тема» слово «Віагра», щоб подивитися цю систему у дії.

Три етапи фільтрації спаму

a. Приймаючі сервери спочатку перевіряють відправника: SMTP-з'єднання не встановлюється з серверами з «чорного списку» (існують різні компанії, які надають такі списки).
b. Після прийняття з'єднання сканується вміст листа. Деякі організації занепокоєні тим, що листи можуть бути хибно марковані як спам; вони можуть поставити вимогу, щоб підозрілий лист був маркований як спам, але все одно був доставлений.
c. Нарешті, більшість клієнтських програм електронної пошти зараз мають вбудовану систему визначення спаму; зазвичай вони ґрунтуються на Байєсівських принципах класифікації.

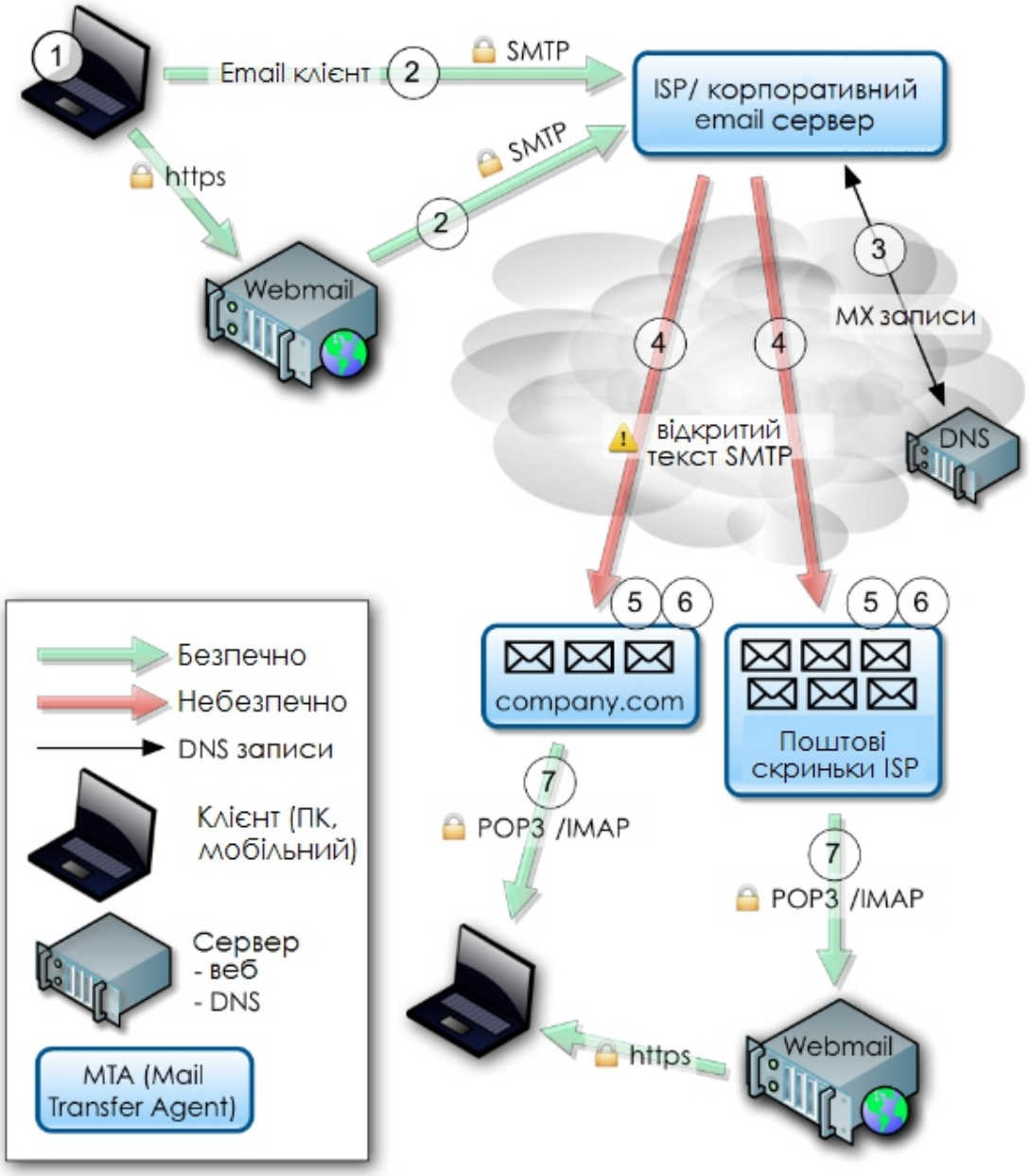

Рисунок 9.2: Процес обробки електронного листа

Ось і все. Дуже просто, чи не правда? Ви починаєте свій шлях в одному місці, а потім можете опинитися (або не опинитися) в іншому місці в залежності від виконання або невиконання різних умов:

- У Вас є правильна адреса
- Ви — спам
- Ви як лист занадто великі
- Поштова скринька отримувача занадто маленька
- або Ви занадто старі.

Тепер Ви знаєте, як електронні листи переміщуються по цифровому світу. Все, що Вам потрібно знати про життя, можна отримати з трафіку електронної пошти.

- Знайте, куди Ви направляєтеся.
- Не споживайте спам.
- Використовуйте великі поштові скриньки (багато спілкуйтеся).
- Не ставайте великим (правильно харчуйтеся та займайтеся спортом для підтримки здорового способу життя).
- І, нарешті, на старійте.

Бачите, все на так складно!

Пожива для розуму: Заголовки email

Повідомлення (з точки зору SMTP) складається із **заголовків** і **тіла**. Заголовки — це дані, які розпізнаються машиною; вони містять різну інформацію. Серед найбільш простих — заголовок 'To:', в якому вказується отримувач листа; заголовок 'Subject:' з темою листа. Здавалося б, заголовок адреси відправника можна і не обговорювати, оскільки з назви зрозуміло, що він значить, але скоро ми побачимо, що це більш складне поняття, ніж здається.

Тіло повідомлення містить частину, що залишилася (тобто все, окрім заголовків); зазвичай MTA його не аналізує (хоча, як ми побачимо далі, такий аналіз можливий з метою фільтрації). Зазвичай тіло повідомлення містить простий текст, але воно також може бути у форматі HTML (що часто дратує технічних спеціалістів). У повідомленнях, які складаються з декількох частин (тобто у повідомленнях з файлами-додатками), використовується MIME. MIME розшифровується як Multipurpose Internet Mail Extensions (багатоцільові розширення Інтернет-пошти). Це стандарт, який використовується для відправлення повідомлень в кодуванні, що відрізняється від ASCII та двійкового вмісту. MIME за необхідністю автоматично використовується клієнтом електронної пошти.

Деякі заголовки можуть бути видалені, інші — модифіковані. Є заголовки, які будуть додані різними компонентами в процесі передачі повідомлення. Кожний MTA завжди повинен додавати заголовок "Received" («Отриманий») для простежування його ролі під час передачі електронного листа. Теоретично, переглядаючи заголовки, Ви завжди повинні мати можливість визначити початкового відправника. Скоро ми побачимо, що це не завжди так.

Існує набір заголовків, які повинен мати кожний електронний лист для того, щоб бути проаналізованим за стандартом SMTP; є заголовки, які більшість реалізацій SMTP вважають стандартними, але насправді це не так; і є ще декілька звичайних заголовків (X-*), які можна налаштувати і які можуть містити будь-яку інформацію. Це можна розглядати як спосіб переміщення контенту, який визначається користувачем, з тіла до заголовків. Найбільш широко використовуються заголовки з інформацією прикладних програм, що фільтрують (X-Spam), та MUA (X-Mailer) (MUA – Mail User Agent, це програма, за допомогою якої користувач здійснює доступ). (Нерідко у листах можна помітити дуже цікаві користувацькі заголовки; у листах від консультантів з безпеки можна побачити і достатньо дивні заголовки!)

Розглянемо наступний приклад.

```
[Приклад повідомлення]

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
```

Іноді в електронних листах можна зустріти додатковий заголовок "From", за яким йде пробіл і адреса відправника без двокрапки як у звичайному заголовку "From:". Це внутрішній роздільник для повідомлень, визначений форматом сховища mbox, і він не є заголовком SMTP.

Агент доставки електронної пошти (Mail Delivery Agent (MDA)), який є компонентом, що відповідає за зберігання повідомлень на останньому етапі доставки, також захищає всі рядки, які починаються з "From" в тілі повідомлення; цей процес часто неправильно інтерпретується.

Повідомлення, що показане вище, було передане з наступною транзакцією 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
```

Шлях повідомлення можна прослідкувати за заголовками “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
```

Утиліта dig

Якщо Ви використовуєте Linux або взагалі UNIX, то **dig** — Ваш найкращий товариш для дослідження налаштувань DNS. Записи MX дуже важливі для доставки електронної пошти, тому давайте їх стисло розглянемо. Записи MX відносяться до електронної пошти і не мають ніякого відношення до веб-сайтів з того ж домену. Веб-сервер "domain.com" може бути зовсім іншою системою, що відрізняється від поштового сервера, і тому записи DNS визначаються по-іншому.

Отримати записи MX можна за допомогою команди `dig` у командному рядку UNIX, Linux або OSX. `Dig` — це утиліта для отримання інформації, що пов'язана з DNS, і, як і будь-яка інша UNIX-програма, вона має незчисленну кількість параметрів. Ми будемо використовувати тільки один формат. За допомогою команди

```
dig <ім'я домену> MX
```

можна вивести тільки записи обміну поштою від відповідного домену. Ще один приклад наведений далі

```
dig <ім'я сервера> <тип>
```

Як приклад можна протестувати публічний DNS-сервер 213.133.105.2 ns.second-ns.de. Погляньте, від якого сервера клієнт отримає відповідь.

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

Відповів локальний маршрутизатор 192.168.51.254; відповіддю виявився запис A. Можна запитати будь-який запис; DNS-сервер можна вибрати за допомогою символу @:

```
dig MX google.com                   # Отримати поштові записи MX
dig @127.0.0.1 NS sun.com           # Тестування локального сервера
dig @204.97.212.10 NS MX heise.de   # Запит на зовнішній сервер
dig AXFR @ns1.xname.org cb.vu       # Отримати всю зону (перенесення зони)
```

Команда `host` також надає багато можливостей.

```
host -t MX cb.vu                    # Отримати поштові записи MX
host -t NS -T sun.com               # Отримати запис NS
host -a sleepyowl.net               # Отримати всі дані
```

У якості більш об'ємного прикладу розглянемо записи MX для домену 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.
```

У кожному рядку є три значення, які є для нас цікавими. "893" — це значення **time to live** (скільки секунд або скільки маршрутизаторів можна пройти), яке Ви знайдете у

кожному запису DNS — воно визначає, наскільки довго DNS дозволено зберігати запис у кеші до того, як інформація буде вважатися застарілою і такою, що повинна бути оновленою.

Значення "10" у першому рядку і значення "40", "30", "20" та "5" в наступних рядках — це значення «переваги», за яким наведене **повністю визначене ім'я домену (Fully Qualified Domain Name, FQDN)** системи, яка готова обробити електронний лист. Значення переваги використовується MTA для того, щоб визначити, з якою машиною зі списку записів MX працювати першою, а з якими — далі за чергою, якщо перша відкине електронний лист. Якщо не знайдений жоден сервер, який прийняв би електронний лист, то відправнику листа відправляється повідомлення про перебій (використовуючи інформацію "reply-to" або "from"). Чим менше значення, тим вище рівень переваги MTA. Таким чином, останній запис у списку, що наведений вище, буде оброблений першим, решта будуть запасними варіантами.

Сервіс також може видати записи з однаковими значеннями переваги; нижче наведена відповідь від yahoo.com, в якій значення переваги для всіх записів дорівнює «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.
```

Це означає, що завантаження електронного листа буде рівномірно розподілене на 3 системи. Дуже маленьке значення TTL, що дорівнює «48», наводить на думку, що запис DNS налаштовується динамічно, що свідчить про активне балансування навантаження. Функція приладів балансування відповідає їхній назві — за їхньою допомогою трафік (трафік вхідних або вихідних повідомлень, трафік з високим або низьким пріоритетом) отримує рівень уваги, якого він заслуговує.

Останнім, але не менш важливим є те, що Ви також можете визначити, чи використовує домен отримувача фільтрацію електронної пошти. У відомому домені no10.gsi.gov.uk (домен прем'єр-міністра Великої Британії) вказано, що компанія з назвою MessageLabs на даний момент відповідальна за фільтрацію пошти:

```
;; 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 потрібно побоюватися чорних гелікоптерів, переглядаючи ці дані: ця інформація є загальнодоступною; інакше електронна пошта не змогла би працювати. Крім того, у збройних сил Великої Британії є тільки *зелені* гелікоптери!

Вправи

9.1 Чи підтримує Ваша платформа для електронних листів «Сповіщення про доставку» ("Delivery Receipt") або будь-який інший прапор доставки, за яким можна визначити (принаймні), що Ваш лист дійшов до певного адресата? Якщо так, то обміняйтеся повідомленнями з другом і перегляньте заголовки з цього трафіку.

9.2 Оберіть доменне ім'я. Визначте, яка система обробляє електронні листи для цього домену, переглянувши записи MX.

Гра почалася: Пастка для жуків

Підлога кафе була трохи вологою, майже як липка стрічка для мух, і вона відчувала, що її взуття з гумовою підошвою прилипає до підлоги. Джейс дивилася на сяючий блиск брудної підлоги і дивувалася тому, як у місці, де подають їжу, може бути такий жахливий запах і водночас таке дзеркальне сяйво. Цей запах нагадав їй про те, як її дідусь раніше розміщував пастки для тарганів у квартирі за диваном. Коли дідусь витягав стару пастку, Джейс могла подивитися на решткі комах, що укрилися пилом. Здавалося, що пастка всередині була повністю заповнена мертвими тарганами.

Вона ніколи не соромилася ставити питання. «Чому таргани просто не вилізуть з коробки? Хіба вони не бачать, що всі їхні друзі всередині мертві?» — неодноразово питала вона дідуся, щоб упевнитися, що кожного разу вона отримує правильну відповідь. Джейс подобалося спостерігати за роботою дідуся, часто при цьому заважаючи йому, заглядаючи йому через плече. Він ніколи не скаржився. Йому подобалося проводити якомога більше часу у компанії своєї онуки.

«Джейс, тарганів приваблює запах всередині коробки. Як тільки вони потрапляють всередину пастки, вони застрягають у коробці, адже дно дуже липке. Здається, що вони приклеєні до дна коробки. Схоже, що вони не помічають всередині інших мертвих комах і вони також гинуть,» — коли Джейс запитувала у дідуся, він кожного разу відповідав їй приблизно одне й те ж.

«Таргани не дуже розумні,» — відповідала маленька Джейс з трохи самовдоволеною посмішкою.

«Так, люба, ти набагато розумніша, ніж ці таргани.»

«Дякую... мабуть.»

Повернувшись думками до шкільного кафетерію, Джейс продовжила дивитися на дзеркальну підлогу; її волосся кольору шоколаду спадало на її обличчя; вона повинна була продовжити роботу над домашнім завданням.

Краєм ока Джейс побачила якусь метушню біля двійчастих дверей кафе. Вони відчинилися, і в просторе приміщення ввійшли декілька людей. Швидко перейшовши у режим таємності, вона нахилилася вперед, і її волосся довжиною до плечей закрило її обличчя. Вона почула: «Там, вона там, намагається сховатися! Схопіть Джейс. Не дайте їй втекти!» — декілька дорослих голосів пронизливо гримнули, як у минулі часи вигукували мисливці на відьом.

Молода хакерша зберігала свою позицію за столом, міцно стиснувши рюкзак і удаючи, що не знає про атаку, що насувається. Ножі, вили, паяльні лампи, розлючений натовп і всі картинки з монстрами з фільмів пронеслися перед її розважливим розумом. І все-таки цікавість перемогла — вона підняла голову і побачила директора школи, його секретаря, містера Трі, трьох першокурсників, які грали у настільний теніс, та декількох диваків, які наближалися до неї. Гуркіт їхніх голосів був оглушливим, він відбивався від полірованої підлоги у сторону Джейс.

«Стривай-но! Я сказав стояти,» — знайомий голос командував десь за сердитими

диваками. Люди завмерли в очікуванні. Першокурсники допомогли начальнику поліції пройти скрізь натовп. «Добре, хлопці, дякую вам за допомогу (навіть надмірну) у пошуках міс Джейс. Тепер я хотів би поговорити з нею наодинці,» — сказав начальник поліції спокійним голосом. Таким самим голосом він вів перемовини з хлопцем, який хотів зістрибнути з 14-поверхової будівлі декілька років тому. Тоді це спрацювало, і зараз, здається, теж спрацювало. Натовп розрідився: люди намагалися здаватися зайнятими, зав'язували шнурки на черевиках і занадто неприховано намагалися підслухати приватну розмову Джейс з поліцейським.

«Привіт, Джейс,» — начальник поліції не придумав нічого іншого, щоб почати розмову.

«Вітаю. Чим я можу допомогти Вам в МОЇЙ школі під час МОГО обіду? Коли МОЇ друзі уважно дивляться на МЕНЕ,» — вона ледь не зламала собі щелепу, стискуючи зуби.

«Вибач, я не хотів переривати тут твою зустріч з друзями, але зараз мені потрібна твоя допомога,» — сказав начальник поліції, намагаючись стримувати себе, але в той самий час даючи Джейс зрозуміти, що зараз не час ускладнювати справу. Джейс вже не так міцно стискала свій рюкзак і подивилася в обличчя начальнику поліції. Він кивком голови показав на двійчасті двері кафетерію, пропонуючи їй прямувати за ним.

Джейс подивилася на свій недоїдений бутерброд, борючись з внутрішнім спротивом. Начальник поліції не відводив від неї погляду. Він підняв свою праву руку і ляснув пальцями. Джейс здригнулася. Усі, хто був у кафетерії, здригнулися. Директор Ментрал зрозумів, що означає цей сигнал, і, поспішаючи, приніс прозорий поліетиленовий пакет.

«Печиво, так?» — спитала Джейс.

«З шоколадною крихтою і горіхами, спечене дружиною офіцера Хенка,» — відповів начальник. — «Домовилися?»

«Домовилися,» — відповіла вона, вже дожовуючи одне печиво.

Після того, як вони вийшли зі школи, поліцейський спитав Джейс, чи їздила вона коли-небудь раніше у фургоні військ спеціального призначення. «Це був єдиний транспортний засіб, який мені вдалося дістати в останню мить. Вибач,» — сказав він. Вони ефектно виїхали зі школи — у фургоні військ спеціального призначення вони були схожі на рок-зірок. Джейс засміялася, дивлячись у дзеркало заднього огляду на ошелешених студентів і вчителів.

«Справа ось у чому. Хтось переглядає мою електронну пошту. Я не знаю, як, хто і чому, але я впевнений, що мою скриньку зламали. Мені потрібно, щоб ти допомогла мені припинити це. Через це виникають серйозні проблеми в діяльності правоохоронних органів,» — начальник не дав Джейс шансу перервати його. — «Коли ти минулого літа налаштовувала нашу мережу, ти встановила купу додаткових штук для забезпечення безпеки. Цього виявилося недостатньо. Я можу сказати тобі, що один електронний лист, написаний три тижні тому, містив інформацію про деякого підозрюваного. Тільки я і окружний прокурор знали про ці подробиці.»

Начальник поліції простягнув руку через салон фургона, щоб взяти печиво з відкритої сумки. Джейс жартома ляснула його руку. Він потягнувся за поліцейським кийком, якого у нього не було при собі, оскільки він вже не був

вуличним поліцейським. Джейс полагіднішала і дала йому велике горіхове печиво, щоб він не переривав свою розповідь (а він її перервав); крихти з печива сипалися з його форми.

«Через дві години після того, як ми з окружним прокурором обмінялися листами, мені подзвонив черговий — підозрюваний тільки що вніс заставу. Адвокат підозрюваного дізнався про ті подробиці, а суддя підписав документ про звільнення підозрюваного. Про ту інформацію знали тільки дві людини, і обмін нею був через мою пошту,» — сказав начальник.

Він продовжив: «Минулого тижня мені подзвонили і повідомили про те, що на місці скоєння злочину, можливо, був відсутній деякий доказ. Це був просто анонімний дзвінок. У ньому не було згадки про якусь конкретну річ. Я швидко написав електронний лист нашому співробітнику, який займається доказами, з запитом опису речових доказів, які фігурували у випадках, які трапилися за весь тиждень, особливо за той день. Цей співробітник відправив мені електронною поштою журнал доказів, і я порівняв його з звітом поліції з місця злочину. Будучи доскональним слідчим, я видалив з журналу всю інформацію, яка не відносилася до справи, і перенаправив його до нашої команди слідчих, які займаються службовою перевіркою.»

Джейс намагалася зрозуміти, що він каже по суті в проміжках між всім поліцейським жаргоном. «І що?» — сказала вона, почуваючи себе набагато краще після з'їденого бутерброда та печива.

Начальник поліції виглядав трохи роздратованим, але все одно відповів: «І що? А те, що у нас нема ніяких відсутніх доказів. Пізніше в той самий день окружний прокурор знову подзвонив мені; він спитав мене, де знаходиться речовий доказ з того випадку. Мені і на думку не прийшло, що пістолета не було в шухлядці для доказів. І знову через дві години іншого підозрюваного випустили під заставу через те, що поліція і суд не задокументували або не надали пістолет, який фігурував у злочині.»

Джейс з думкою про те, що непогано було б зараз запити печиво великою склянкою холодного молока, спробувала зробити висновок із всього почутого: «Тобто той, хто дзвонив, перевіряв, чи знаходиться пістолет в поліції. Лист, який Ви відправили команді слідчих, підтвердив, що ця зброя ніколи не була поліцейським доказом.»

На обличчі начальника поліції з'явилася задоволена посмішка, коли вона закінчила свої висновки. «Знаєш, Джейс, ти могла б стати зразковим поліцейським детективом, коли підростеш.»

Джейс відповіла: «Так, можливо, але в мене надто розвинене почуття власної гідності, щоб ставати поліцейським. Я краще стану юристом або політиком або кимось іншим, хто відноситься до більш низькоорганізованої форми життя.» На щастя, вона засміялася, сказавши останнє речення, адже поліцейський після таких слів вже розізлився. «Я просто жартую.»

Гра продовжується...

Написання e-mail – справа ризикована

- **Розголошення.** Подумайте про те, кому, чому і як Ви відправляєте електронні листи. Крім того, що сама передача електронних листів є небезпечною після відправлення їх з локального MTA, Ви також розкриваєте певну інформацію. Використання шифрування (такого, як PGP, GPG і S/MIME) потребує, щоб обидві сторони були однаково програмно забезпечені, і зазвичай воно дуже складне у застосуванні (іншими словами — користувачі з задоволенням уникають цього). Альтернативним способом захистити передачу листів є використання *однакового* провайдера електронної пошти: у цьому випадку листу не треба «подорожувати» Інтернетом у відкритому вигляді. І тут постає важливе питання: чи впевнені Ви, що Ваш провайдер або провайдер отримувача не прослуховується? Враховуйте це, відправляючи будь-яку конфіденційну інформацію.
- **Зміна маршруту.** Електронний лист не завжди обов'язково залишається в тому домені, куди він був відправлений; іноді він може бути перенаправлений кудись в інше місце. Наприклад, американська компанія *pobox.com* продає тільки аліаси, але не поштові скриньки. Основним ризиком є те, що Ваш електронний лист може таким чином переміщуватися регіонами, які підпадають під іншу правову юрисдикцію, до того моменту, як він дійде до місця свого призначення. У нашому прикладі аліас *pobox.com* завжди буде спершу проходити через MTA у США, і, таким чином, є ризик його перехвату згідно з Законом US PATRIOT.
- **Порушення недоторканності приватного життя.** Отримувач, який користується такими сервісами, як Facebook або Google, розкриває свою електронну пошту автоматизованим сканерам вмісту, навіть якщо *відправник* не давав на це дозволу!
- **Список адресатів.** Якщо Ви використовуєте список адресатів, то краще використовуйте для цього поле BCC (blind carbon copy, «сліпа» копія, прихована копія). Адреси, які вказані в полі TO: і CC:, може побачити кожен отримувач листа; це може призвести до потрапляння вмісту списку адресатів до третьої сторони і спричинити атаки спаму на адреси отримувачів Вашого листа.
- **Конфлікт.** Електронний лист — це як звичайний лист, але він пишеться і відправляється набагато швидше, отже у Вас менше часу для того, щоб продумати його вміст. Написання електронного листа — це як водіння автомобіля: у роздратованому стані цього краще не робити. Якщо Ви емоційно збуджені, то збережіть написаний лист у чернетках, а через годину обдумайте, чи варто Вам його відправляти. Це може зберегти Вам дружбу або кар'єру.
- **Неправильна адреса.** Однією з основних причин того, що лист не потрапляє до адресата, є зазначення неправильної адреси. Це часто трапляється, коли поштові клієнти намагаються автоматично доповнити адресу за першими символами, які вводить користувач. Завжди перевіряйте, чи є адреса отримувача саме тією адресою, яка Вам потрібна.
- **Декілька отримувачів.** Відправляючи електронний лист декільком людям, переконайтесь у тому, що вміст цього листа призначений всім отримувачам. Також добре і етично правильно буде відправити копію людині, якщо у листі мова йде про нього або про інформацію, яка отримана від нього.
- **Юридичні питання.** Дисклеймер (відмова від відповідальності) під Вашим електронним листом може справити враження, але він не має ніякого юридичного значення, не враховуючи повідомлення про авторське право. Ви самі відправляєте лист, і Ви не можете знімати з себе відповідальність за його вміст

(почасти Ви, звісно, завжди можете заявити, що відправник був підмінений), і Ви не можете вказувати адресату, який отримав лист помилково, що робити з цим листом, оскільки Ви, скоріш за все, не маєте з ним договірних відношень. (Див. «Повне звільнення від відповідальності» наприкінці цього уроку.)

- **Топ-постинг.** Коли Ви відповідаєте на лист, Ваш клієнт автоматично розміщує Вашу відповідь над початковим повідомленням? Часто стандартне налаштування сконфігуровано саме так, але, на жаль, це … не дуже чемно. Отримувачі, які повинні спочатку прочитати Вашу відповідь і тільки в кінці листа зрозуміти контекст повідомлення, скоріш за все, будуть не дуже Вам вдячні. З іншого боку, оскільки вони почали це спілкування, то вони повинні розуміти, про що йде мова. Але подумайте, чи зручно Вам самим використовувати топ-постинг.
- **Поштові автовідповідачі.** «Ви відправили мені лист, тому я відправляю Вам цю автоматично згенеровану відповідь, щоб повідомити Вас, що я не прочитаю Ваш лист, доки не повернусь; і хай допоможе нам небо, якщо у Вас теж є автовідповідач, адже весь процес піде по колу до кінця існування Всесвіту.» Така штука не тільки надокучлива; вона також допомагає зловмиснику — адже, скоріш за все, Вас немає вдома. Так на якій вулиці, кажете, живете?
- **Підпис.** Чи використовуєте Ви підпис — автоматично згенероване повідомлення «Щиро Ваш, Іван Клокотун, менеджер з автоматичних дій», яке додається у кінці кожного повідомлення, яке Ви відправляєте? Це не завжди погано — доки вони на стають занадто довгими. І з десяток таких повідомлень «складаються» у кінці довготривалого діалогу. І всі вони представлені в HTML (а не у вигляді звичайного тексту без форматування), отже картинка з горилою, яка піднімається на хмарочос, буде з'являтися знову і знову декілька разів. Так що будьте уважними, оформлюючи підпис, і не наражайте Ваших адресатів на небезпеки електронних листів у форматі HTML, якщо Ви не вмієте з ними правильно обходитися.

Вправи

9.3 Зайдіть на сайт http://www.gaijin.at/en/olsmailheader.php і додайте у спеціальне поле заголовок будь-якого електронного листа. Ця програма — це аналізатор, який визначить для Вас інформацію про заголовки електронного листа. Як Ви можете використати отриману інформацію?

Отримання електронної пошти

Поштові клієнти з'єднуються з серверами, на яких зберігаються поштові скриньки, і перевіряють, чи не змінився лічильник повідомлень. Деякі клієнти роблять це періодично (наприклад, кожні 30 хвилин), для деяких це потрібно зробити «руками» (зазвичай для зниження навантаження на мережу), а деякі підтримують постійне з'єднання з поштовим сервером, отримуючи оновлення, як тільки на пошту надходить новий лист (який називається **оповіщенням (push notification)**).

При надходженні листа поштовий клієнт забирає його за протоколом POP3 або IMAP. Мобільні клієнти, як правило, завантажують лише заголовок і невелику частину повідомлення для економії трафіку. Таким чином, користувач може вирішити: завантажити лист повністю, залишити на потім або видалити його.

У перші роки існування електронної пошти комунікація проходила через ненадійне повільне з'єднання, і обробка файлів, доданих до листа (документів, таблиць та зображень) все ще проходить з тим самим рівнем ризику. Додаток завжди повинен

бути завантажений повністю перед тим, як він може бути показаний. Користувачі, які використовують поштовий веб-інтерфейс (веб-мейл) на сторонніх комп'ютерах (наприклад, в Інтернет-кафе), повинні бути обережними: **перегляд додатку означає, що Ви залишаєте копію на твердому диску системи**. За стандартними налаштуваннями після використання вони **не** видаляються.

Використовувати веб-мейл на ненадійному комп'ютері ризиковано ще й з іншої причини: якщо Ви не використовуєте одноразові паролі, Ви можете залишити після себе у системі облікові дані своєї електронної пошти, і немає ніякої гарантії того, що сторонній комп'ютер не заражений або не прослуховується.

Системи з активною електронною поштою повинні регулярно оновлювати антивірусний захист. Але при цьому Ви повинні розуміти, що антивірус захищає тільки від **відомого** шкідливого ПЗ. При цільових атаках може пройти декілька днів, перш ніж шкідливе ПЗ буде додано до вірусних сканерів; деякі шкідливі програми взагалі ніколи туди не додаються.

Вхідна пошта в заголовках містить «шлях» листа. Кожна система, яку пройшов лист, додається рядком до прихованої частини заголовка, при цьому остання система буде вказана найпершою. Однак знайте, що ці дані легко підробити: майте на увазі, що не всі записи можуть бути реальними.

Вправи

9.4 Перегляньте «тимчасові» файли, які залишають користувачі в процесі використання пошти. Ви можете побачити багато з них, оглянувши тимчасові теки temp (яких, як правило, більше, ніж одна). Windows, наприклад, дозволяє легко побачити вміст тимчасових тек, навіть не знаючи їх розташування: змінна **%temp%** знає їх всі.

Відкрийте командний рядок в Windows і введіть

```
dir %temp%
```

Що Ви побачили?
Для більш зручного перегляду використовуйте Windows Explorer (він же Провідник), використовуючи команду:

```
explorer %temp%
```

9.5 Відкрийте заголовок будь-якого листа. Чи зможете Ви визначити інших отримувачів, окрім Вас? Вони можуть бути у секції копії листа (CC) в його заголовку.

- Оберіть декілька листів. Прослідкуйте шлях листа і визначте його відправника за заголовками листа. Перегляньте заголовок на наявність іншої доступної інформації (підказка: поштові клієнти і версії антивірусів, алгоритми шифрування та інше).
- Порівняйте адресу відправника і адресу для відповіді.
- Перегляньте декілька листів зі спаму. Які відмінності Ви бачите в їхніх заголовках у порівнянні із звичайними листами? Подивіться, куди ведуть посилання (тільки за рядком, не переходячи по них). Чи ведуть посилання туди, куди, згідно з текстом листа, вони посилаються?

Відповідь на лист

Відповідаючи на лист, треба проявляти певну обережність. Скільки разів Ви казали або робили щось, чого не хотіли би або про що потім жалкували?

Перш за все, НІКОЛИ не відповідайте на те, що напевне є спамом, навіть якщо це відписка. Відповівши на такий лист, Ви підтвердите, що (a) цей поштовий акаунт використовується і (b) хтось з цією адресою дійсно читає спам. Результатом відписки в цьому випадку, за іронією долі, стане надходження *більшої* кількості спаму.

Перевірте видимість адрес. Чи потрібно всім отримувачам бути видимими? Якщо Ви використовуєте список адресатів, чи всі отримувачі все ще дійсні? Чи всім отримувачам потрібно бачити Вашу відповідь?

Будьте лаконічними. Чи потрібно при відповіді цитувати отриманий лист повністю або Ви можете просто використати його найбільш важливі частини? Якщо Ви повторно використовуєте частини попереднього листа, Ви можете їх процитувати — таким чином Ви покажете, що повторюєте частину листа. Після цього відповідайте на частину, що цитується.

Цитуючи, будьте обережними: чи все в листі призначено для отримувачів, яких Ви зараз обрали, або Ви включаєте конфіденційні повідомлення (або їх частини), які не призначені для нових отримувачів? Уникайте цитування всього листа, включаючи підпис і великі дисклеймери. Майте на увазі, що все, що Ви відправляєте, може бути перенаправленим будь-кому без Вашого дозволу або відома. Гарною і ввічливою звичкою є додавання людини до списку отримувачів копії листа, якщо в цьому листі йде мова про цю людину або про щось, що вона зробила. А для Вас це буде своєрідним нагадуванням: не слід стверджувати те, про що в майбутньому, можливо, будете шкодувати. Прапори доставки корисні при відстежуванні переміщення листа до пункту призначення, а при перегляді MX-записів Ви можете з'ясувати, куди відправиться лист. Також Ви можете використати геолокацію, щоб дізнатися фізичне місцерозташування. Але прапори доставки збільшують трафік. При встановленні прапора доставки Ваш поштовий сервер повинен відправити відповідь. Такі помітки листів, як «термінове» або «важливе», не завжди виявляються корисними. Такі прапори, як правило, є ознакою того, що відмічене повідомлення є спамом, якщо тільки воно не було відправлене співробітником.

Вправи

9.6 Перенаправте лист на іншу пошту і порівняйте заголовки.
- Яким чином заголовки можуть бути використані проти Вас, і як Ви можете цьому запобігти?
- Чи можете Ви перенаправити лист, який був Вам відправлений, як приховану копію (BCC)?

9.7 Напишіть і відправте лист самому собі. Під час відправлення швидко відмініть відправлення цього листа. Якщо відправлення листа було успішно відмінено, погляньте за заголовок чернетки. Скопіюйте цей заголовок у текстовий редактор і подивіться, чи можна визначити, який поштовий сервер зупинив відправлення листа. Чи не правда круто?

Криптозахист вмісту

Простота електронної пошти робить її уразливою. Відправник не може бути впевненим, що лист не змінений на шляху до отримувача, і немає можливості впевнитися, що тільки отримувач може прочитати лист. У той самий час і отримувач не може бути впевненим, що лист був відправлений тим, хто вказаний у листі як відправник.

Один зі способів забезпечити конфіденційність — зашифрувати документ перед його додаванням до листа. Наприклад, можна зашифрувати текстові документи і таблиці (наприклад, ті, які створюються в OpenOffice), та PDF-файли, які також підтримують шифрування. Однак застосування криптографії до власне листа простіше, при цьому вміст листа також захищений.

У той самий час, заголовки листів треба залишати у вигляді відкритого тексту, щоб поштові сервери могли обробити і доставити пошту.

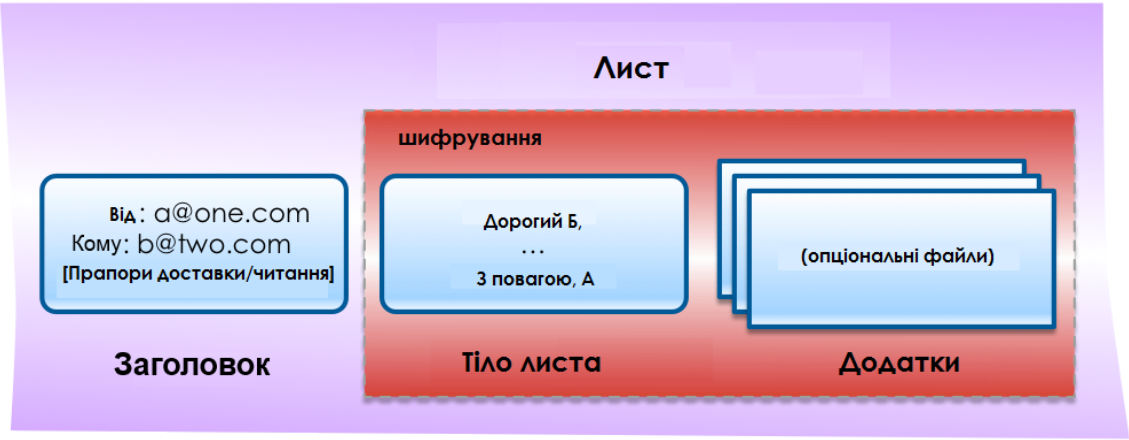

Рисунок 9.3: Шифрування пошти

Безпека листа може бути досягнута двома шляхами: з використанням PGP (або GPG) і S/MIME. В обох випадках використання шифрування забезпечує:

– Конфіденційність (**C**onfidentiality): тільки передбачуваний отримувач(і) може читати цей лист?

– Цілісність (**I**ntegrity): чи не змінився вміст електронного листа?

– Автентичність (**A**uthenticity): чи дійсно електронний лист прийшов саме від цього відправника?

(Найлегше запам'ятати цей список, використовуючи перші три літери кожного пункту: **CIA**.)

Загалом автентичність і цілісність об'єднані в цифровий **підпис** листа: розраховується контрольна сума листа, а результат у зашифрованому вигляді вбудовується в цифровий підпис, який може бути створений тільки людиною, у якої є потрібний закритий ключ (див. далі «PGP і GPG»).

Конфіденційність забезпечується шляхом використання чийогось відкритого ключа для шифрування тіла листа, так що тільки власник правильного закритого ключа може розшифрувати і прочитати вміст (див. далі «PGP і GPG»). Для більшої впевненості таке повідомлення може бути підписане.

Ви повинні мати на увазі, що шифрування електронної пошти є доволі рідким явищем, особливо в епоху, коли люди добровільно дозволяють сканувати свою пошту таким компаніям, як Google і Facebook. Знаходячись в деяких країнах, Ви повинні бути впевненими, що у Вас є засоби для доступу до Вашої поштової скриньки у випадку, якщо влада буде вимагати це від Вас, наприклад, в США при перетинанні кордону (TSA, Transportation Security Administration, Управління транспортною безпекою) або у Великій Британії на підставі ордера відповідно до закону «Про слідчі органи».

PGP і GPG

PGP означає Pretty Good Privacy (досл. «досить хороша секретність»). Вона була розроблена Філіпом Циммерманном (Phil Zimmermann). Історія PGP досить цікава, і її варто прочитати, але у цьому розділі ми сфокусуємося тільки на її використанні.

Найпоширенішою є open source версія, яка називається GPG (GNU Privacy Guard). GPG безкоштовна і доступна для більшості платформ. У ній використовуються тільки відкриті публічні алгоритми.

GPG працює за принципом **управління відкритим/закритим ключами**, який означає, що ключі мають ВІДКРИТУ частину, яку Ви можете дати будь-кому, хто хоче відправити Вам лист, і ЗАКРИТУ частину, яку Ви повинні тримати в таємниці, щоб розшифрувати вхідне повідомлення. Комбінація відкритого і закритого ключа називається **парою ключів**, і це перша річ, яку Ви згенеруєте, коли встановите GPG на машині. Пара ключів захищена паролем, тому змінити її може тільки її власник. Змінення можуть знадобитися у випадку змінення поштової адреси, який підтримується ключем, або для використання інших функцій.

Вам знадобиться чийсь відкритий ключ для шифрування повідомлень, які відправляються. Для цих цілей існують сервери (наприклад, pgp.mit.edu), де Ви можете завантажити ключ або ключі, які пов'язані з певною поштовою адресою, або завантажити свій власний. Цілком можливо, що термін дії ключа закінчився або був загублений пароль, тому завжди використовуйте останній ключ або (що навіть краще) попросіть отримувача відправити свої ключі і підтвердити відбиток ключа (коротка версія контрольної суми).

MIME

MIME (Multipurpose Internet Mail Extensions, багатоцільові розширення Інтернет-пошти) — це поштове розширення протоколу Simple Mail Transfer Protocol (SMTP). MIME дає Вам можливість передавати різні види вмісту і даних, таких як аудіо, відео, зображення, архіви і програмні застосунки як додатки до листів. Заголовок MIME вставляється на початок листа, і клієнт, який отримав цей лист, використовує цю інформацію, щоб визначити, яка програма пов'язана з доданим файлом. Сам по собі MIME не надає захищеності ні листу, ні додаткам.

S/MIME (Secure/Multipurpose Internet Mail Extensions) — це протокол, який додає цифрові підписи і шифрування до листів з MIME додатками. Використовуючи цифрові підписи, S/MIME забезпечує автентифікацію, цілісність повідомлення і **не-відмову** відправника («не-відмова» означає, що Ви не можете заперечувати того, що Ви його відправили). S/MIME забезпечує приватність і безпеку даних (використовуючи шифрування) в листах, які використовують даний протокол.

S/MIME — це одночасно і інструмент забезпечення безпеки, і одна з проблем забезпечення безпеки, оскільки користувачі можуть відправляти уразливі дані як додатки в вихідних листах заради запобігання виявлення. Тому використання S/MIME в компанії повинно проходити під наглядом на поштових серверах.

Довіра ключам

Чи можете Ви бути впевненими, що ключ для отримувача листа дійсно належить цьому отримувачу, а не завантажений кимось іншим? Рішення цієї проблеми полягає в тому, що ключі можуть бути підписані іншими. Уявіть, що у Вас вже є ключ когось, кому Ви довіряєте, і хтось інший знає того, кому Ви хочете відправити лист. Цей

інший може **підписати** відкритий ключ, що означає, що Ви вкладаєте в ключ більше довіри, знаючи цю особу. Така ситуація називається **успадкованою довірою (inherited trust)**. Ви можете знайти інший спосіб увійти в контакт з людиною і або повністю отримати його відкритий ключ, або отримати «відбиток ключа» — контрольну суму ключа, яку можна швидко перевірити. На сервері ключів ключ також може мати ID — ще одна контрольна сума, яка грає ту ж роль.

Відправлення зашифрованого листа з використанням GPG

Більшість поштових клієнтів підтримують плагіни, які спрощують роботу з ключами і шифруванням. Найкращий варіант дій — перевірити заздалегідь, чи є в отримувача відкритий ключ і отримати його з сервера ключів або особисто від отримувача.

Після цього створіть звичайний лист (знову ми настійно рекомендуємо створювати просте текстове повідомлення і не використовувати HTML), додайте додатки і за допомогою поштового клієнта зашифруйте і відправте лист. Якщо Ви вирішили підписати лист, тоді поштовий клієнт спочатку використає Ваш закритий ключ для підпису листа, потім використає відкритий ключ Вашого отримувача для шифрування листа і його додатків. Якщо Ви захищаєте пару ключів кодовою фразою (ми рекомендуємо робити саме так), то Ваш поштовий клієнт у Вас її запитає.

Отримання зашифрованого листа з використанням GPG

Лист, зашифрований за допомогою GPG, містить або додаток, позначений прапором GPG, або блок тексту з заголовком, в якому поштовому клієнту, який підтримує GPG, повідомляється про отримання зашифрованого листа. Цей клієнт тепер отримає доступ до Вашого закритого ключа (можливо, за паролем) і розшифрує повідомлення та його додатки. Якщо повідомлення не було зашифроване Вашим відкритим ключем, розшифрування просто не вдасться. Якщо лист був підписаний відправником, GPG-плагін буде використовувати відповідний відкритий ключ і для підтвердження підпису.

GPG-плагіни будуть повідомляти Вам про проблеми з підписами або додатками, але загалом, щойно встановивши плагін, Ви зрозумієте, що користуватися GPG достатньо просто.

Наслідки використання GPG

Майте на увазі, що більшість електронних листів не шифруються. І, ймовірно, Ваші листи також належать до цієї більшості. Деякі люди думають, що використання шифрування є підозрілим, і воно саме по собі привертає увагу. Але це Ваше право зберігати приватність при спілкуванні, так що думки інших не повинні Вас хвилювати.

GPG непросто використовувати у пошті з веб-інтерфейсом (і це не враховуючи відповідь на очевидне питання: а чи є гарантія того, що третя сторона здійснить шифрування правильно і не буде використовувати атаку «людина-посередині») та на мобільних клієнтах. Будьте обережними з мобільними застосунками, які стверджують, що вирішують цю проблему: було виявлено, що деякі з них відправляли дані кудись в інше місце для обробки!

Існують поштові онлайн-сервіси, які продають зашифровані поштові облікові записи «з покращеною безпекою». Але будьте уважними, читаючи текст,

надрукований в користувацькій угоді дрібним шрифтом. Він може виглядати так:

«Я розумію, що цей сервіс не призначений для ведення незаконної діяльності і що провайдери цього сервісу будуть співпрацювати з органами влади для отримання доказів відповідно до чинного законодавства.»

Звісно, до «законодавства» відносяться такі програми, як Echelon, Carnivore, PRISM, Патріотичний акт (США) і XKeyscore. Перегляньте їх і подумайте, наскільки «покращена» та «безпека», за яку Ви будете платити.

За законами деяких країн Ви зобов'язані зуміти розшифрувати будь-яку інформацію за рішенням суду. Наприклад, у Великій Британії Ви можете підпасти під дію закону «Про слідчі органи» 2000 року; його недотримання розглядається як неповага до суду, яка автоматично приводить до тюремного ув'язнення. Це має неприємні наслідки: якщо Ви експериментували зі шифруванням і забули ключі або паролі, Вас посадять до тюрми за Вашу забудькуватість (так, Ви будете звинуваченим, доки не зможете довести свою невинуватість). Таким чином, краще видаляти будь-який зашифрований матеріал і електронні листи, до яких Ви більше не маєте доступу. У корпоративному середовищі необхідно ретельно контролювати і документувати змінення ключа і кодової фрази та видалення зашифрованої інформації.

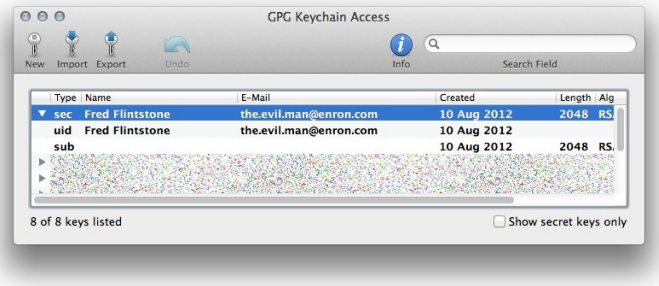

Рисунок 9.4: Пара ключів GPG

Останнім, але не менш важливим є те, що використання адрес електронної пошти для ідентифікації ключа є **згодою**, а не встановленим стандартом. Цілком можливо згенерувати і використовувати ключі для адрес електронної пошти, яких не існує. Такі ключі все ще приймаються на загальнодоступних серверах. Це називається «приховування у всіх на видноті» (hiding in plain sight): немає ніякого зв'язку між адресою електронної пошти і ключем, який використовується для шифрування/розшифрування трафіку. Наприклад, на зображенні, яке представлене вище, і людина, і адреса електронної пошти є вигаданими.

Недоліком такого підходу є те, що він порушує встановлений спосіб роботи, і плагіни, такі як **Enigmail**, можливо, не одразу будуть підтримувати такий творчий підхід. Ще однією галуззю для проведення досліджень є ключі з терміном дії, що витік: закінчення терміну дії ключа не припиняє його функціонування.

Вправи

9.8 Завантажте GPG-плагін для свого поштового клієнта і встановіть його.

9.9 Дізнайтеся, як згенерувати власний ключ. Згенерований ключ зберігайте локально; відхиляйте будь-які пропозиції завантажити Ваш ключ на загальнодоступний сервер ключів.
9.10 Додайте інші адреси до Вашого ключа, а потім змініть кодову фразу.
9.11 Тепер опублікуйте Ваш відкритий ключ на сервері ключів.
9.12 Напишіть комусь лист, використовуючи GPG. Як би Ви отримали ключ адресата? Спробуйте його отримати.
9.13 Що Ви можете зробити з повідомленнями, коли у Вас є тільки Ваш власний ключ?
9.14 Створіть новий ключ для підробленої адреси електронної пошти. Наскільки легко це зробити на Вашому комп'ютері?

Уразливості і загрози електронної пошти на стороні сервера

Всі організації — і маленькі, і великі — використовують поштові сервери для відправлення і отримання листів (тільки якщо вони не передали цю задачу комусь іншому (outsource) або не використовують хмарні сервіси). Електронні листи призначені для різних цілей: деякі з них хороші, деякі — ні. Поштові сервери розташовані на передовій лінії атаки/захисту мережевого периметра.

Електронні листи використовуються для відправлення фотографій з сімейного відпочинку, вітальних листівок, домашніх завдань, корпоративних повідомлень, розсилки новин та іншого контенту. Електронна пошта чудово підходить для повсякденного спілкування.

З іншого боку, електронна пошта використовується для відправлення порно, піратських MP3-записів, секретної інформації, корпоративних таємниць, погроз, фішингу і спаму. У 2012 році додатки до листів відійшли на другий план за рівнем загрози; на першому місці опинилися шахрайські веб-сайти — вони стали основним інструментом для розсилки шкідливого ПЗ. Інформація про життєво важливі частини суспільного життя людини стала використовуватися із злочинними цілями.

Споживання пропускної здатності

Сервери електронної пошти повинні бути налаштовані так, щоб блокувати погані речі, а хороші — передавати Вам. Звучить достатньо просто, і нам буде легко Вам про це розповісти. Але на Вас чекає багато роботи. Весь поштовий трафік, який проходить по мережі, «з'їдає» частину пропускної здатності. Ви ніколи не почуєте скаргу на зразок «Моє з'єднання занадто швидке». Чим раніше Ви зможете виявити і проінспектувати поштовий трафік (вихідний та особливо вхідний) на сервері електронної пошти, тим менше пропускної здатності Ви витратите. Крім збереження пропускної здатності фільтрація небажаних листів на ранній стадії полегшить роботу ЦП сервера.

Деякі дослідження показують, що 80% всієї вхідної пошти є спамом. Ви дійсно хочете чекати, доки цей мотлох потрапить до Вашої поштової скриньки? Чим раніше спам буде перехоплений Вашими поштовими серверами, тим краще. Одна з технік, яка використовується при виявленні спаму, полягає в тому, що сервер усуває його після певної кількості часу. Це запобігає видаленню поштового трафіку, який користувач може очікувати. Відділ маркетингу Вашої організації, можливо, захоче отримати лист з темою «Як підвищити продуктивність системи». Також вимкніть автоматичні повідомлення про електронну пошту, щоб зберегти пропускну здатність. Повірте нам, Ваші користувачі не будуть заперечувати.

Оскільки Ваші поштові сервери можуть наразитися на атаки з Інтернету, Ви повинні провести додаткові запобіжні заходи у відношенні тих, у кого є права адміністратора. Той, хто має права адміністратора, ніколи не повинен відправляти або отримувати електронну пошту тоді, коли він знаходиться в системі з привілеями адміністратора. Насправді, права адміністратора треба використовувати тільки для внутрішнього обслуговування мережі. Протягом багатьох років багато мереж були зламані саме тоді, коли адміністратор ввійшов в систему і переглядав веб-сайти, одночасно відправляючи електронну пошту під час роботи з підвищеними привілеями.

Уразливості поштового сервера

Як видно з назви, поштовий сервер є точно таким сервером, як і багато інших. Сервер може мати уразливості, які можна експлуатувати. У базі даних Загальних уразливостей і перерахувань (Common Vulnerabilities and Enumeration) за посиланням http://cve.mitre.org, перераховано загалом 1043 уразливості поштових серверів станом на 2012 рік. Багато з них можна усунути, правильно налаштувавши конфігурацію сервера і користувацькі привілеї. Інші проблеми вирішуються тільки усуванням багів виробником ПЗ або пильністю при купівлі серверного програмного забезпечення.

Повний список всіх відомих уразливостей поштових серверів можна переглянути за посиланням http://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=email+server.

Загрози поштових серверів

Великі поштові веб-клієнти (наприклад, Gmail, Yahoo і Microsoft) мігрували на нову криптографічну програму поштового підпису, яка називається **DomainKeys Identified Mail (DKIM)**. DKIM «обгортає» лист криптографічним підписом, який підтверджує ім'я домену, через який був відправлений лист. DKIM допомагає фільтрувати підроблені повідомлення. Специфікацію DKIM можна знайти на сайті http://www.dkim.org/.

Але існує проблема у використанні тестових повідомлень DKIM. В інформаційному повідомленні, яке опублікувала **US-CERT (United States Computer Emergency Readiness Team, Комп'ютерна команда екстреної готовності США)** було зазначено, що злісний хакер при відправленні листа може встановити прапор, який означає, що він тестує DKIM в повідомленнях. Деякі отримувачі будуть «приймати повідомлення DKIM в тестовому режимі, тоді повідомлення повинні розглядатися так, як якщо б вони не були підписані DKIM».

Це не перша проблема DKIM, яка привернула увагу CERN. Довжина ключа підпису, який використовується для шифрування, була уразлива до злому, коли розмір ключа був занадто малим. Стандарти DKIM встановлюють мінімальний розмір ключа в 1024, при цьому будь-яка пошта, яка використовує менший ключ, не приймається програмою. Але насправді DKIM не відхиляла адреси з невідповідними ключами. Відправлені листи оброблялися як звичайні, при цьому вони були повністю уразливі до злому. Як тільки ключ був зламаний, хакер міг підмінити електронну пошту або відправити шкідливе ПЗ, використовуючи ключ і адресу того користувача.

DKIM призначена для роботи в якості інструмента, «що виражає довіру», для перевірки електронної пошти. Система використовує шифрування з відкритим ключем, так само, як це робить PGP. При правильному використанні за електронним листом можна прослідкувати його відправника через процес перевірки домену. В принципі, Ви ідентифікуєте себе як відправник за Вашим доменом. Це повинно суттєво скоротити кількість підроблених листів і спаму, а також спростити доказ того,

що конкретний користувач відправив конкретне повідомлення. Спеціалісти з безпеки називають це неможливістю відмови від авторства (non-repudiation).

При неможливості відмови від авторства дані про джерело інформації не можуть бути змінені. Інформацію неможливо спростувати. Якщо Ви сказали: «Я хочу носити плаття», то ця заява не може бути заперечена. Ви це сказали, це факт, і Ви не зможете відмовитися від цього твердження. Це важливо, коли мова йде про контракти, про правові питання і про виправдання Вашому батьку, щоб не виносити сміття.

Електронна пошта для розваг і вигоди

Завдяки вигідному ринку для корпоративного шпіонажу, за допомогою електронної пошти можна легко знайти списки контактів клієнта, інформацію про клієнтів, протоколи зустрічей, інформацію про нові розробки, відповіді на наступний тест з математики та інші види цінних даних. Ми навіть не збираємося займатися державним шпіонажем просто тому, що ми всі знаємо, що це було ще на зорі розвитку людства. Існує декілька примітивних наскельних малюнків, на яких зображено те, як одна печерна людина слідкує за мамонтом іншої печерної людини. Можна тільки уявити, як печерна людина, повертаючись до свого племені, описує найновішу версію Мамонта 2.0.

Простим (але часто таким, що випускається з уваги) методом захисту електронної пошти є перевірка всіх поштових додатків. Сканування повинно бути застосоване до всіх пакетів даних, стиснутих файлів, невідомих типів файлів, мета-даних, файлів з URL і всього, що може бути результатом обробки файлу. Це сканування повинно бути зосереджене на вхідному трафіку, але також з підозрою віднесіться до моментів, коли великі додатки відправляються з Вашої мережі. Конфіденційна інформація компанії повинна бути зашифрована, особливо якщо вона відправляється електронною поштою. І, до речі, дійсно важлива інформація ніколи не повинна виходити за межі мережі. Якщо якийсь користувач відправляє інформацію за межі мережі, то Вам краще прослідкувати за його діяльністю.

Великі організації (наприклад, шпиталі для ветеранів в США) з цією метою використовують програмне забезпечення для **запобігання витоку даних (data loss prevention, DLP)**. Ніколи жартома не відправляйте електронною поштою Ваші медичні документи з таких шпиталів, інакше наслідки будуть серйозними.

Ключ до успіху

Фільтрація за ключовими словами є одним з видів фільтрації на прикладному рівні (7-й рівень OSI), який дозволяє блокувати всі повідомлення, які містять певні ключові слова або фрази (текстові рядки), які зазвичай з'являються в спамі. Інші форми фільтрації листів включають:

- **Блокування адреси**: метод фільтрації, який блокує листи, які відправлені з певних IP-адрес, адрес електронної пошти або доменів відомих спамерів.
- **Байєсівська фільтрація**: «розумне» програмне забезпечення, яке може аналізувати спам-повідомлення і навчатися розпізнавати в інших повідомленнях спам, використовуючи **евристики** (моделі поведінки).
- **Чорні списки**: списки адрес відомих спамерів можуть бути використані спільно, так що немає необхідності, щоб кожний користувач складав свій перелік з нуля. Такі списки можна отримати у декількох постачальників. Вони є дуже цінними для блокування адрес.

- **Білі списки**: метод фільтрації, в якому замість вказання того, які відправники повинні бути заблоковані, визначаються відправники, які можуть бути дозволені. Знову-таки, ці списки використовуються як частина блокування адрес.
- **Сірі списки**: в цьому методі тимчасово блокуються електронні листи з невідомих джерел. Прийнятний лист буде повторно переданий, а спам — ні.
- **Фільтрація типу «Запит/Відповідь»**: відповідає на електронні листи, отримані з тих адрес, яких немає в списку «надійних відправників», запитом, як правило, з задачею, яка є простою у рішенні для людини, але складною для автоматизованих ботів або скриптів.

Існує багато програмних застосунків як безкоштовних, так і платних, які можуть виконувати ці види фільтрації. Деякі з них кращі, деякі гірші. Але всі вони достатньо добре справляються зі своїми функціями.

Уразливості і загрози електронної пошти на стороні клієнта

Вхідний лист може містити шкідливі програми, як правило, у вигляді додатків або веб-посилання. Побачивши подібне у Вашому повідомленні, задумайтесь про можливих шахраїв.

- Неперевірене джерело: хто відправив Вам цей лист і чи міг цей адресант відправити Вам лист з подібним вмістом? Улюбленим прийомом спамерів є використання чужої діючої адреси електронної пошти, таким чином спам не розпізнається фільтрами, і це збільшує імовірність того, що користувач відкриє лист.
- «Занадто добре, щоб бути правдою»: неочікувана подія, наприклад, виграш в лотереї, отриманий спадок або банківська «помилка» на Вашу користь. Ще бувають «нігерійські листи». Ви знаходили подібності у всіх таких повідомленнях? Практично кожен з нас отримував такі листи.
- Доменна невідповідність між адресою відправника і адресою отримувача відповіді на відправлене повідомлення.
- Дивне, неправильне або занадто складне використання мови.
- Непояснена або нелогічна невідкладність. (Чому цей лист такий невідкладний?)
- Вбудовані веб-посилання, які ведуть до доменів, які відрізняються від імені домену, який можна прочитати (наприклад, посилання для переходу на веб-сайт www.bank.com в дійсності веде до підробленого банківського веб-сайту www.l33thacker.org). Більшість поштових клієнтів тепер показують реальну адресу веб-сайту при наведенні курсора миші на відповідний текст.
- Додатки, які містять активний контент (наприклад, у форматі .exe або .html). Це особливо ризиковано на платформах, які автоматично виконують вміст повідомлення.

Вправи

9.15 Перейдіть за посиланням http://www.419eater.com/. Що таке примани для шахрайства (scam baiting)? Яким чином вони працюють? Які існують *запобіжні заходи*? Це небезпечний матеріал. Знання про те, що така техніка існує, ще не

означає, що Вам варто це робити. Але, у будь-якому випадку, Ви не повинні бути беззахисними.

Проллємо світло

Вміст електронної пошти є прекрасним способом для розповсюдження шкідливих посилань. Одним з поширених інструментів є **Blackhole Exploit Kit**. Звучить страшно, чи не так? Чи можете Ви вимовити «Blackhole Exploit Kit» п'ять разів підряд дуже швидко і без помилок? Blackhole — це програма для експлуатації веб-застосунків, яка використовує відомі уразливості в застосунках Java і Adobe. Вона використовується для відправлення листів шахраїв користувачу, щоб останній перейшов за сумнівним веб-посиланням.

Фішинг є спробою зібрати важливу інформацію від жертви за допомогою **соціальної інженерії**. Тисячі користувачів отримують переконливі листи. Типові фішінгові листи приходять від добре відомих і перевірених організацій. Шахрай використовує логотип організації, схожу адресу електронної пошти і професійне формулювання, таким чином обманюючи велику кількість людей. У листі міститься прохання до користувача «перевірити» або «оновити» дані кредитних карт, особисту інформацію про банківський рахунок та інші речі, які Ви б довірили тільки надійному джерелу.

Коли жертва натискає на посилання офіційного вигляду, посилання відправляє її на фальшиву сторінку, на якій відбувається встановлення шкідливих програм на комп'ютер користувача. Користувач не знає, що його обманюють. До того ж не всі антивірусні програми виявляють установлення. Після того, як програма встановиться на комп'ютері користувача, шахраї зможуть контролювати комп'ютер, а також будь-яку інформацію, яку вони хочуть вилучити з нього.

Спам Blackhole «прикидається» листом, відправленим від серйозних компаній, таких як Amazon, Visa, Twitter, UPS та інших організацій, які не викликали б підозр користувача. Ця програма орендується: плата відбувається за серверний час на сервері Blackhole. Вартість коливається від $50 за день до $150 за місяць.

Шкідливі програми, трояни, руткіти

ЗМІ люблять висвітлювати теми злому електронної пошти, тому що страх легко продається. (Пам'ятайте, що той, хто продає Вам щось, намагається налякати Вас.) Але правда в тому, що шкідливі програми існують вже довгий час.

Доктор Фред Коен написав кандидатську дисертацію про ідею комп'ютерного вірусу у 1984 році, опублікував її у 1985 році, і його робота була вилучена з публічного доступу через декілька тижнів. 1985 рік був давно, і засоби масової інформації досі висвітлюють події так, немов шкідливі програми — це нова величезна загроза для всього світу.

Ми не будемо розповідати Вам про всі існуючі загрози, які можна переслати; Ви можете ознайомитися з ними самостійно в Уроці 6 «Шкідливі програми». Ми збираємося показати Вам, як працює захист електронної пошти зсередини і зовні.

Це повідомлення виглядає як справжнє, давай відкриємо його

СТОП!!! Не відкривайте цей лист поки що. Навіть не переглядайте це повідомлення. Існує декілька способів використання листа у якості інструмента атаки. Соціальна інженерія займає перше місце серед технік, які застосовуються для того, щоб змусити людей відкрити електронний лист, відкрити додатки або натиснути на шкідливі веб-посилання в листі або повідомленні. Соціальна інженерія орієнтована на

деякі людські емоції, включаючи цікавість, бажання допомогти, довіру до наших друзів, жадібність і багато видів фінансових та медичних побоювань. В Уроці 20 Ви дізнаєтеся більше подробиць про соціальну інженерію.

Нашу цікавість до нової або невідомої інформації можна використовувати, щоб переконати нас здійснювати нерозумні вчинки. Коли Ви отримали електронний лист, який містить заголовок «Тема: Re: Re: Дякую», Ви, як звичайний користувач, захочете дізнатися, чому хтось подякував Вам. У цьому випадку Вам наперед подякували за можливість здійснення шкідливий дій на Вашому комп'ютері.

У таких типах електронних листів Ви можете зустріти прохання подзвонити за телефонним номером, натиснути на посилання у повідомленні або зробити щось, що може видати всі Ваші таємниці.

Вправи

Розглянемо повідомлення з таким заголовком:

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

Відповісти: 2259575299@qq.com

Кому: (Ваша адреса електронної пошти)

Дата: Mon, Nov 19, 2012 at 7:40 AM

Прислано: iitg.ac.in

9.16 Чи відповіли б Ви на електронний лист, який містить у рядку теми наступний текст: «Вітаю, я Норман Чан, у мене є бізнес, вартість якого складає 47.1 мільйонів доларів, Ви будете зі мною працювати?» Адреса відправника — «naveen.kumar@iitg.ac.in».

9.17 Дослідіть цю адресу електронної пошти, щоб впевнитися в достовірності інформації. Також перевірте адресу для відповіді, «2259575299@qq.com». НЕ ПЕРЕХОДЬТЕ НА QQ.COM.

9.18 Максимально посильте налаштування безпеки Вашого браузера перед виконанням цього завдання. Зробіть невелике дослідження ресурсу qq.com, але не переходьте за цією адресою. НЕ ВІДКРИВАЙТЕ ЦЕЙ URL. На основі свого дослідження qq.com зробіть висновки, чи є цей сайт для Вас шкідливим?

Захоплюючі трюки із системами електронної пошти (злом листоноші)

Електронна пошта, здається, завжди грає певну роль, коли справа доходить до порушення безпеки або серйозної атаки на мережу. Кожний вірус, кожний біт шкідливих програм, кожне фішингове повідомлення, здається, використовує електронні листи або як основний транспортний механізм, або як спосіб проникнути в систему, щоб розпочати атаку. Електронні повідомлення можуть бути не настільки популярними, як інші форми зв'язку (як, наприклад, SMS або миттєві повідомлення), але це те, що найбільш широко використовується в корпоративному і урядовому світі. Зараз ми уважно розглянемо саму ідею електронної пошти і те, як вона може бути використана в якості зброї або захисту.

Підключаючись до мережі, ми повинні знати декілька точок входу. Якщо ми розраховуємо тільки на одну точку входу, то що ми будемо робити, якщо уразливість, що використовується, буде виправлена? Декілька точок входу в мережу дають нам

більше свободи для переміщення цією мережею і більше шляхів підходу. Шляхи підходу дуже важливі, повірте нам на слово.

Знання схеми, за якою користувачам складають імена, які використовуються організацією для електронної пошти або доступу до мережі, дає нам велику перевагу. Знаючи ім'я користувача, ми можемо зосередитися на отриманні пароля цього користувача. Більшість організацій (але не всі) використовують схему «ім'я.прізвище@назвакомпанії.com». Деякі використовують поєднання першого ініціала і прізвище@назвакомпанії.com. Інші використовують поєднання прізвища і першого ініціала з @назвакомпанії.com. Досить нерозважливо, чи не так? Також не варто робити адресу електронної пошти логіном користувача. Це дуже розповсюджена помилка.

У організацій в їхній мережі є каталог, який дозволяє користувачам дізнатися, хто є хто, де вони працюють і що вони роблять. Цей внутрішній каталог є золотою копальнею інформації для зловмисника. Ви можете переглянути профілі в Facebook або інших соціальних мережах, щоб дізнатися більше про кожного користувача. Ви можете дізнатися, коли вони збираються у відпустку, чим вони займаються, яке у них хобі та інші зачіпки до типів паролів, які вони могли б використати. Ця інформація також виявиться корисною, якщо Ви захочете використати соціальну інженерію проти цих людей (для розваги або вигоди).

Хто шукає, той завжди знайде

Давайте розглянемо питання збору адрес електронної пошти і використання електронної пошти в якості інструмента злому. Злом електронної пошти тісно пов'язаний із соціальною інженерією (повідомляємо ще раз про всяк випадок). **The Social Engineering Automation Kit (SEAK)** на http://www.seak.com.ar/ призначений для того, щоб використовувати пошукові системи для знаходження адрес електронної пошти в мережі або на веб-сайті. SEAK представляє собою набір скриптів на мові Perl, які дозволяють пошуковим системам проводити пошук у глибинах веб-сторінок і мереж, а потім вивести всі адреси електронної пошти, які вони знаходять. SEAK також може бути використаний для пошуку людей.

Також є програма, аналогічна SEAK. Вона називається **Esearchy**. Її можна завантажити за посиланням https://github.com/FreedomCoder/ESearchy-ng. Esearchy робить те саме, що SEAK, але робить це в Windows; ця програма також шукає документи. Esearchy шукає паролі, приховані в метаданих, а також будь-яку іншу корисну інформацію, наприклад, адреси електронної пошти, які доступні для громадськості.

Ще одна утиліта, **Maltego**, — це програма з відкритим програмним кодом, яка може використовуватися як аналізатор у судовій експертизі. Maltego надає утиліти для виявлення даних з відкритих джерел і показує інформацію у вигляді графа, що зручно для аналізу посилань та інтелектуального аналізу даних. У цілому за допомогою Maltego можна аналізувати реальні відношення між людьми і групами, веб-сайти, домени, мережі та онлайн-сервіси (наприклад, Ваші улюблені соціальні мережі).

Ще можна скористатися пошуком в Google. Якщо Ви хочете побачити всю інформацію про профіль співробітника, Ви можете використати цю команду:

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

Якщо Ви хочете знайти всі адреси електронної пошти в домені або URL, то Ви можете використовувати Esearchy. Введіть наступну команду одним рядком, замінивши «company» на реальний домен.

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

Gpscan — це програма, написана на Ruby, яка може автоматизувати цей пошук і отримати ще більше результатів. У поєднанні з командою, представленою вище, Gpscan стає потужним інструментом для розвідки і соціальної інженерії. Ви можете знайти Gpscan за посиланням http://www.digininja.org/projects/gpscan.php.

Перед використанням будь-якої з цих програм виділіть час на те, щоб розібратися, як вони працюють. Зверніть особливу увагу на синтаксис кожної утиліти і на те, що робить кожна з команд. Ви можете взнати досить багато про те, як пошукові системи можуть бути використані для полювання на адреси електронної пошти, для їх повернення і, можливо, знаходження нових паролів. Також з'ясуйте, які пошукові механізми використовуються для роботи цих програм.

Вправи

9.19 Тепер настав час самостійно дослідити засоби безпеки. Знайдіть **FOCA** (програма для роботи з метаданими). Що вона робить? Чи хотіли б Ви додати її до своєї колекції програм для етичного хакінга?

Спуфінг vs. шкідливі програми

У 2007 році генеральний директор компанії Fortune 500 отримав лист від одного зі старших співробітників. У листі в полі **«Від»:** було видно, що лист відправлений внутрішньою мережею компанії. У полі **«Тема»:** був текст «Як скоротити витрати на електроенергію». Коли генеральний директор відкрив це електронне повідомлення, він побачив у ньому додаток і посилання, яке також, здавалося, було справжнім. Директор відкрив додаток, але нічого не побачив на своєму екрані і закрив лист.

Через декілька місяців ФБР повідомило генеральному директору, що через зараження шкідливими програмами його персонального комп'ютера з його компанії було вкрадено декілька терабайтів даних. ФБР підтвердило, що саме той лист з темою «Як скоротити витрати на електроенергію» містило шкідливий додаток. Це повідомлення було підроблене.

Подібні ситуації трапляються кожного дня. Ваш дядечко дзвонить Вам і питає, чому Ви відправляєте йому так багато оголошень електронною поштою. У школі Ваш приятель отримує від Вас непотрібну рекламу. Чому Ви відправляєте всі ці спам-повідомлення?!

Але ж Ви цього не робили.

Або Вашу адресу електронної пошти підробили, або Ваш поштовий клієнт зламали. Щоб дізнатися, чи була підроблена адреса електронної пошти, Вам потрібно буде подивитися на заголовок відправленого повідомлення. Ми дізналися, як це зробити, раніше у цьому уроці. Тепер використайте свої знання на практиці.

Попросіть будь-кого, хто отримав від Вас лист, переслати його Вам назад повністю (а не тільки текст повідомлення). Заголовок покаже, чи була підмінена Ваша адреса електронної пошти. Подивіться на поля **Відповісти** і **Відправлено** в електронному листі. Як ми вже бачили в попередніх вправах, заголовок покаже, чи був цей лист відправлений Вами або кимось іншим.

Кумедні трюки з електронною поштою

Коли справа доходить до приватного життя, веб-пошта турбується про приватність в останню чергу. Веб-сервісу може бути відправлений запит на надання всіх Ваших повідомлень, контактів, записів у календарі та інших даних на підставі юридичних документів, які дозволяють отримати ці дані. Один старий, але все ще корисний трюк полягає у створенні облікового запису електронної пошти під іншим, не своїм іменем. Ті, кому Ви відправляєте секретні повідомлення, повинні мати доступ до Вашого поштового акаунту. Ви створюєте електронний лист і зберігаєте його як чернетку. Ви ніколи не відправляєте повідомлення, а просто створюєте чернетку з деяким вмістом. Лист залишається на Вашому акаунті, але його не можна відслідкувати, оскільки він ніколи не відправлявся. «Отримувач» заходить на той самий акаунт і читає чернетку повідомлення. Після прочитання чернетка може бути видалена або змінена — так створюється нове повідомлення для Вас. Це як пінг-понг без м'яча. До речі, так само можна працювати і зі спільним Google-документом.

ПРИМІТКА: Ви не зможете стати директором Центрального розвідувального управління Сполучених Штатів Америки, не знаючи цю маленьку хитрість.

Метадані електронної пошти описані у RFC 2822. Хтось вважав хорошою ідеєю включення метаданих в електронне повідомлення! Про що вони тільки думали? Метадані електронної пошти можуть містити наступну інформацію:

- To (Кому)
- From (Від кого)
- CC (копія)
- BCC (прихована копія)
- Date (Дата)
- Subject (Тема)
- Sender (Відправник)
- Received (Отримано)
- Message-ID (ID повідомлення)
- References (Посилання)
- Recent (Нещодавнє)
- Return-Path (Шлях повернення)
- Time/Date (Час/дата)
- Encrypted (Зашифрований)
- In-Reply-To (У відповідь на)

Не дуже хвилюйтеся про метадані електронної пошти, які описані у RFC 2822. Річ у тому, що цей RFC охоплює тільки електронний текстовий трафік. Ваші SMS-повідомлення, всі Ваші миттєві повідомлення і фотографії, якими Ви хотіли поділитися, припускають вторгнення у Ваше приватне життя. Тим не менш, ця прихована інформація розглядається у рамках іншого RFC.

Як перехитрити поштових ботів (обфускація електронної пошти)

Це так просто, що Ви будете сміятися з себе, що не знали про це раніше.

Якщо Вам потрібно відправити комусь свою адресу електронної пошти, Ви відправите її у вигляді звичайного тексту? У такому випадку Ви розкриваєте свою адресу для спам-ботів. Ці спам-боти — шкідливі створіння, які переміщуються Інтернетом і шукають адреси електронної пошти.

Це як підключення нового комп'ютера до Інтернету без включення будь-яких функцій безпеки: електронна адреса, відправлена у вигляді простого тексту, просто напрошується на неприємності. Загалом, це дуже погана ідея.

Щоб перехитрити спам-ботів, Ви можете спробувати змінити свою адресу електронної пошти при її відправленні. Треба знайти компроміс між простотою використання і безпекою. Є декілька методів, просто використайте свою уяву.

`somebodyatsome.whereelse`

`Somebody@somedotwhereelse`

`somebody2some.whereelse`

Такі комбінації успішно використовуються для передачі адрес електронної пошти, оминаючи спам-ботів. Але, можливо, скоро вони зможуть розпізнавати такі хитрощі.

Вправи

9.20 Перейдіть за посиланням для перегляду програми Etherios EasyDescribe: http://appexchange.salesforce.com/listingDetail?listingId=a0N300000018leZEAQ

Це безкоштовна програма для перегляду і добування метаданих. Проаналізуйте декілька електронних листів за допомогою Etherios. Які метадані є в цих листах, але при цьому відсутні в заголовку?

9.21 Якщо деякі дані знаходяться не в заголовку, то в якій частині електронного листа вони можуть бути приховані?

9.22 Чи ставить вимогу RFC 2822, щоб метадані були вбудовані в електронне повідомлення, або це просто стандартизований метод для трафіку електронної пошти?

9.23 Користуючись будь-якими засобами, спробуйте знайти правильну робочу адресу електронної пошти керівників трьох компаній, перерахованих нижче. Підказка: спочатку з'ясуйте, хто вони такі.

Coca Cola
Kia
British Aerospace Engineering (BAE)

Висновки

Тепер, коли Ви сповна розібралися (або зовсім заплуталися) у питаннях, які відносяться до роботи з електронною поштою, Ви можете погодитися з тим, що цей простий інструмент комунікації не такий вже простий. Робота електронної пошти в різних системах може бути достатньо складною і потребує відповідності певним критеріям. Згадайте, як на початку уроку Ви уявили себе у ролі електронного листа, як Вас відправляли, який шлях Ви пройшли і як, нарешті, опинилися у місці призначення. До речі, Ви добре справилися з цією задачею.

Пам'ятайте про важливість дотримання етикету при використанні електронної пошти, оскільки відправлення листа, написаного у поганому настрої, може в подальшому створити для Вас небажані проблеми. При відповіді на лист, не відправляйте всім підряд адреси, вказані в полі «Копія». Якщо Ви збираєтеся відповідати великій кількості людей, використовуйте BCC для збереження конфіденційності поштових адрес інших користувачів.

Продовжуючи тему недоторканності приватного життя, ми обговорили використання таких програм для шифрування, як PGP і GPG, призначених для безпечного відправлення та отримання електронних листів. Найцікавіша частина цього розділу була присвячена створенню і використанню ключа. Це було не дуже складно, чи не так? Якщо Вам так не здалося, шкода. Ми впевнені, що в місцевому ресторані швидкого харчування ще є вакансії, оскільки безпека — це не Ваше покликання. Ми сподіваємося, що Ви справилися з тим завданням, тому що нам потрібно якомога більше спеціалістів з безпеки.

У наступному розділі ми перейшли до більш складних питань безпеки. Гаразд, можливо, вони не такі вже й складні, але ми думаємо, що Вам стануть у нагоді ці знання. Зізнайтеся, що розбиратися з уразливостями і загрозами на стороні поштового сервера і на стороні клієнта було дуже захопливо. Нам було весело писати про них. Ви повинні слідкувати за спамом. Велика кількість спаму споживає цінну пропускну здатність, тому Ви повинні фільтрувати його на ранніх етапах. Тільки не плутайте поштовий спам з торговою маркою Spam.

Dig є важливою утилітою для роботи з електронною поштою для користувачів Linux і Unix; з її допомогою можна відслідковувати потрібну інформацію. Якщо Ви бачите, що з Вашої мережі електронною поштою у додатках передаються великі об'єми даних, то перевірте, чи не містяться в цих листах секрети компанії. Ми обговорювали один цікавий момент щодо використання сервера Blackhole для експлуатації уразливості в мережах. Ця техніка широко використовувалась для відправлення шкідливого ПЗ електронною поштою, якщо було відомо, що хтось, скоріше за все, відкриє це повідомлення або натисне на заражене посилання у цьому електронному документі. Цього виду загрози можна уникнути шляхом фільтрації поштового трафіку і навчання користувачів по цьому питанню. Навчання користувачів є ключовим елементом у забезпеченні безпеки.

Наостанок ми дамо Вам декілька порад, які, можливо, Вас зацікавлять. Просто знайте, що безпека електронної пошти є викликом для кібербезпеки. Ваш погляд на цей факт залежить від того, на якій стороні Ви знаходитесь.

Повне звільнення від відповідальності

Пітер Хоперман, автор *The Evil Guide to Privacy*, пише:

Ви коли-небудь хотіли підкреслити нерозумність відмови від відповідальності, яке використовується в електронних листах? Це зробив Пітер Хоперман, зібравши добірку дуже старих повідомлень USENET з деякими власними доповненнями. Важливою частиною становлення успішного хакера є почуття гумору: воно не тільки робить Вас непередбачуваним, але також допомагає не сумувати після невдалих експериментів. Посмійтеся зі своїх невдач, переведіть подих і продовжуйте боротьбу. Комп'ютери не можуть виграти, Ви можете просто вимкнути їх.

Точка зору, представлена тут, є думкою автора, вона може не збігатися з точкою зору його роботодавця або когось ще.

Інформація і будь-які додатки, що містяться в цьому електронному повідомленні, є безглуздими і навряд чи політкоректними. Я щиро вірю, що зовсім не має сенсу пояснювати Вам, що робити з цим повідомленням, якщо я відправив його не туди. Це повідомлення не містить зображень оголеного тіла (поки), і ніякі милі тварини або кити не постраждали під час його написання, оскільки їх не було в наявності. Цей лист, виконаний в істинно консалтинговому стилі, складений зі шаблонів і копіпасту з багатьох інших електронних повідомлень, орієнтованих на інші групи користувачів. Цей лист може нашкодити травній системі при проковтуванні (особливо при друку на картоні). Автор може подати в суд, зміст можна врегулювати. Не підходить для людей у віці до 18 і тим, у кого відсутнє почуття гумору. Не тримайте догори ногами, відкрийте з іншого боку. Якщо Ви отримали цей лист помилково, Ви молодці.

Не варто довіряти або сподіватися на будь-які додатки, але вони можуть виявитися дуже цікавими.

Ця відмова від відповідальності призначена виключно для освітніх цілей. Не відправляйте зараз гроші. Проконсультуйтеся з Вашим лікарем або фармацевтом. Для запобігання ураження електричним струмом не відкривайте задню панель. Всередині немає частин, які обслуговуються користувачем. Ви можете мати або не мати додаткові права, які можуть відрізнятися в залежності від країни. Не рекомендується для дітей до дванадцяти років. Батарейки у комплект не входять. Обмеження: один екземпляр в одні руки. Будь-яка схожість із реальними особами, живими або мертвими, є суто випадковою. Зберігати подалі від відкритого вогню або іскри. Недійсне там, де заборонене. Потребує збирання. Усі права захищені. Зберігайте чеки окремо за номером банку. Вміст може осісти під час транспортування. Використовуйте тільки за призначенням. Рекомендується батьківський нагляд. Не надаються ніякі інші гарантії, явно виражені або ті, які можна припустити. Несанкційоване копіювання цього підпису суворо заборонене. Не читайте під час управління транспортним засобом або перевезення тяжкого обладнання. Посилка буде оплачена за рахунок отримувача. У випадку потрапляння в очі промийте водою. Повинно бути завірено. Це не є пропозицією про продаж цінних паперів. Наносити тільки на вражену ділянку. Може бути занадто вражаючим для деяких глядачів. Не згинати, не скручувати, не ламати. Використовувати тільки для оздоровлення. Потребується додаткове завантаження і розвантаження. Жодна тварина не постраждала у виробництві цього підпису. Не турбувати. Усі моделі старші

18 років. Якщо стан не покращується, зверніться до лікаря. Найсвіжіша, якщо пити до дати закінчення терміну на упаковці. Ціни можуть бути змінені без попереднього сповіщення. Приблизний час. Доставка не обов'язкова, якщо посилка зі Сингапуру. При проковтуванні не викликає блювоти. Розрив печатки означає прийняття угоди. Тільки для використання в умовах бездоріжжя. Як можна побачити на ТБ. Ми залишаємо за собою право обмежувати кількість. Один розмір підходить всім. Не залишайте засоби без нагляду. Багато валіз виглядають так само. Містить значну кількість неактивних інгредієнтів. Кольори можуть з часом вигорати. Ми відправили товар, який підходить саме Вам. Слизький у вологому стані. Гарантія надається тільки первісному роздрібному покупцю або отримувачу подарунка. Тільки для використання в офісі. Вага нетто перед приготуванням. Не пов'язані з Червоним Хрестом. Поверхня повинна бути очищена від фарби, жиру, бруду і т. п. Опустити в будь-яку поштову скриньку. Пройшло редакцію для телебачення. Зберігати в прохолодному місці; обробляти швидко. Посилка не буде доставлена без оплати. Репродукція. Список дійсний на момент друку. Тільки для особистого використання. Повернути відправнику, немає пункту призначення, неможливо відправити. Не піддавати впливу прямих сонячних променів. Не несе відповідальності за прямі, непрямі, побічні збитки, пов'язані з будь-яким дефектом, помилкою або невиконанням. Не приймаємо канадські монети. Не проколювати і не спалювати пустий контейнер. Дивіться інструкцію на етикетці. Ціни можуть бути змінені без попереднього сповіщення. Не пишіть нижче цієї лінії. Сейф із замком з часовим механізмом, робітник не може відкрити. Тільки в задіяних ділянках. Серійні номери повинні бути видними. Акуратно складіть частини, потім зв'яжіть. Зона обвалу. Зберігайте в недосяжному для дітей місці. Чек є Вашою квитанцією. Перевірте подачу паперу. Поставте штамп тут. Уникати контакту зі шкірою. Проведена санітарна обробка. Підписати без признання провини. Не входити агентам з розповсюдження замовлень. Трохи вище на захід від Міссісіпі. Температура зберігання: від -30°C (-22 F) до 40°C (104 F). Співробітники і члени їхніх родин не можуть брати участь. Остерігайтеся собаки. Конкурсанти були проінструктовані перед шоу. Немає необхідності у покупці. Обмежена пропозиція, дзвоніть зараз, щоб забезпечити швидку доставку. Ви повинні бути присутнім, щоб виграти. Загасити всі сигнальні вогні. Оброблено в місці, вказаному на штампі на коробці. Використовуйте тільки в добре провітрюваних приміщеннях. Замінити аналогічним екземпляром. Аксесуари продаються окремо. Намети для двох або більше. Зберігати подалі від відкритого полум'я. Деяке показане оснащення не є обов'язковим. Ціна не включає податки. Зона підвищеної небезпеки. Попередній запис випуску шоу для цієї часової зони. Копіювання суворо заборонено. Тільки особам віком більше 18 років. Відкріпити і зберегти для довідки. Заборонений вхід з алкоголем, собаками або конями. Це демо-версія, не для продажу. Оберіть принаймні дві альтернативні дати. Подзвоніть за безкоштовним телефоном перед тим, як вирішити. Водій не носить із собою готівку. Деякі з товарних знаків, вказаних в цьому продукті, з'являються тільки з метою ідентифікації. Видалення тегу карається законом.

Якщо Ви все це прочитали, то Ви надзвичайно цікава людина. Або 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.

Hacker Highschool
SECURITY AWARENESS FOR TEENS

ISECOM